

de Gruyter Expositions in Mathematics 47

Editors

V. P. Maslov, Academy of Sciences, Moscow
W. D. Neumann, Columbia University, New York
R. O. Wells, Jr., International University, Bremen

Groups of Prime Power Order

Volume 2

by

Yakov Berkovich and Zvonimir Janko



Walter de Gruyter · Berlin · New York

Authors

Yakov Berkovich
Jerusalem str. 53, apt. 15
Afula 18251
Israel
E-Mail: berkov@math.haifa.ac.il

Zvonimir Janko
Mathematisches Institut
Ruprecht-Karls-Universität Heidelberg
Im Neuenheimer Feld 288
69120 Heidelberg
E-Mail: janko@mathi.uni-heidelberg.de

Mathematics Subject Classification 2000: 20-02, 20D15, 20E07

Key words: Finite p -group theory, minimal nonabelian subgroups, metacyclic subgroups, extraspecial subgroups, equally partitioned groups, p -groups with given maximal subgroups, 2-groups with few cyclic subgroups of given order, Ward's theorem on quaternion-free groups, 2-groups with small centralizers of an involution, Blackburn's theorem on minimal nonmetacyclic groups.

- ⊗ Printed on acid-free paper which falls within the guidelines of the ANSI to ensure permanence and durability.

ISSN 0938-6572
ISBN 978-3-11-020419-3

Bibliographic information published by the Deutsche Nationalbibliothek

The Deutsche Nationalbibliothek lists this publication in the Deutsche Nationalbibliografie;
detailed bibliographic data are available in the Internet at <http://dnb.d-nb.de>.

© Copyright 2008 by Walter de Gruyter GmbH & Co. KG, 10785 Berlin, Germany.
All rights reserved, including those of translation into foreign languages. No part of this book may
be reproduced or transmitted in any form or by any means, electronic or mechanical, including
photocopy, recording, or any information storage or retrieval system, without permission in writing
from the publisher.

Typeset using the authors' TeX files: Kay Dimler, Müncheberg.
Printing and binding: Hubert & Co. GmbH & Co. KG, Göttingen.
Cover design: Thomas Bonnie, Hamburg.

Contents

List of definitions and notations	viii
Preface	xiv
§46 Degrees of irreducible characters of Suzuki p -groups	1
§47 On the number of metacyclic epimorphic images of finite p -groups	14
§48 On 2-groups with small centralizer of an involution, I	19
§49 On 2-groups with small centralizer of an involution, II	28
§50 Janko's theorem on 2-groups without normal elementary abelian subgroups of order 8	43
§51 2-groups with self centralizing subgroup isomorphic to E_8	52
§52 2-groups with Ω_2 -subgroup of small order	75
§53 2-groups G with $c_2(G) = 4$	96
§54 2-groups G with $c_n(G) = 4, n > 2$	109
§55 2-groups G with small subgroup $\langle x \in G \mid o(x) = 2^n \rangle$	122
§56 Theorem of Ward on quaternion-free 2-groups	134
§57 Nonabelian 2-groups all of whose minimal nonabelian subgroups are isomorphic and have exponent 4	140
§58 Non-Dedekindian p -groups all of whose nonnormal subgroups of the same order are conjugate	147
§59 p -groups with few nonnormal subgroups	150
§60 The structure of the Burnside group of order 2^{12}	151
§61 Groups of exponent 4 generated by three involutions	163
§62 Groups with large normal closures of nonnormal cyclic subgroups	169
§63 Groups all of whose cyclic subgroups of composite orders are normal	172

§64	p -groups generated by elements of given order	179
§65	\mathcal{A}_2 -groups	188
§66	A new proof of Blackburn's theorem on minimal nonmetacyclic 2-groups	197
§67	Determination of U_2 -groups	202
§68	Characterization of groups of prime exponent	206
§69	Elementary proofs of some Blackburn's theorems	209
§70	Non-2-generator p -groups all of whose maximal subgroups are 2-generator	214
§71	Determination of \mathcal{A}_2 -groups	233
§72	\mathcal{A}_n -groups, $n > 2$	248
§73	Classification of modular p -groups	257
§74	p -groups with a cyclic subgroup of index p^2	274
§75	Elements of order ≤ 4 in p -groups	277
§76	p -groups with few \mathcal{A}_1 -subgroups	282
§77	2-groups with a self-centralizing abelian subgroup of type $(4, 2)$	316
§78	Minimal nonmodular p -groups	323
§79	Nonmodular quaternion-free 2-groups	334
§80	Minimal non-quaternion-free 2-groups	356
§81	Maximal abelian subgroups in 2-groups	361
§82	A classification of 2-groups with exactly three involutions	368
§83	p -groups G with $\Omega_2(G)$ or $\Omega_2^*(G)$ extraspecial	396
§84	2-groups whose nonmetacyclic subgroups are generated by involutions .	399
§85	2-groups with a nonabelian Frattini subgroup of order 16	402
§86	p -groups G with metacyclic $\Omega_2^*(G)$	406
§87	2-groups with exactly one nonmetacyclic maximal subgroup	412
§88	Hall chains in normal subgroups of p -groups	437
§89	2-groups with exactly six cyclic subgroups of order 4	454

§90	Nonabelian 2-groups all of whose minimal nonabelian subgroups are of order 8	463
§91	Maximal abelian subgroups of p -groups	467
§92	On minimal nonabelian subgroups of p -groups	474

Appendix

A.16	Some central products	485
A.17	Alternate proofs of characterization theorems of Miller and Janko on 2-groups, and some related results	492
A.18	Replacement theorems	501
A.19	New proof of Ward's theorem on quaternion-free 2-groups	506
A.20	Some remarks on automorphisms	509
A.21	Isaacs' examples	512
A.22	Minimal nonnilpotent groups	516
A.23	Groups all of whose noncentral conjugacy classes have the same size	519
A.24	On modular 2-groups	522
A.25	Schreier's inequality for p -groups	526
A.26	p -groups all of whose nonabelian maximal subgroups are either absolutely regular or of maximal class	529
	Research problems and themes II	531
	Author index	593
	Subject index	594

List of definitions and notations

Set theory

$|M|$ is the cardinality of a set M (if G is a finite group, then $|G|$ is called its order).

$x \in M$ ($x \notin M$) means that x is (is not) an element of a set M . $N \subseteq M$ ($N \not\subseteq M$) means that N is (is not) a subset of the set M ; moreover, if $M \neq N \subseteq M$ we write $N \subset M$.

\emptyset is the empty set.

N is called a nontrivial subset of M , if $N \neq \emptyset$ and $N \subset M$. If $N \subset M$ we say that N is a proper subset of M .

$M \cap N$ is the intersection and $M \cup N$ is the union of sets M and N . If M, N are sets, then $N - M = \{x \in N \mid x \notin M\}$ is the difference of N and M .

\mathbb{Z} is the set (ring) of integers: $\mathbb{Z} = \{0, \pm 1, \pm 2, \dots\}$.

\mathbb{N} is the set of all natural numbers.

\mathbb{Q} is the set (field) of all rational numbers.

\mathbb{R} is the set (field) of all real numbers.

\mathbb{C} is the set (field) of all complex numbers.

Number theory and general algebra

p is always a prime number.

π is a set of primes; π' is the set of all primes not contained in π .

m, n, k, r, s are, as a rule, natural numbers.

$\pi(m)$ is the set of prime divisors of m ; then m is a π -number.

n_p is the p -part of n , n_π is the π -part of n .

(m, n) is the greatest common divisor of m and n .

$m \mid n$ should be read as: m divides n .

$m \nmid n$ should be read as: m does not divide n .

$\text{GF}(p^m)$ is the finite field containing p^m elements.

\mathbb{F}^* is the multiplicative group of a field \mathbb{F} .

$\mathcal{L}(G)$ is the lattice of all subgroups of a group G .

If $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ is the standard prime decomposition of n , then $\lambda(n) = \sum_{i=1}^k \alpha_i$.

Groups

We consider only finite groups which are denoted, with a pair exceptions, by upper case Latin letters.

If G is a group, then $\pi(G) = \pi(|G|)$.

G is a p -group if $|G|$ is a power of p ; G is a π -group if $\pi(G) \subseteq \pi$.

G is, as a rule, a finite p -group.

$H \leq G$ means that H is a subgroup of G .

$H < G$ means that $H \leq G$ and $H \neq G$ (in that case H is called a *proper* subgroup of G). $\{1\}$ denotes the group containing only one element.

H is a nontrivial subgroup of G if $\{1\} < H < G$.

H is a maximal subgroup of G if $H < G$ and it follows from $H \leq M < G$ that $H = M$.

$H \trianglelefteq G$ means that H is a normal subgroup of G ; moreover, if, in addition, $H \neq G$ we write $H \triangleleft G$ and say that H is a proper normal subgroup of G . Expressions ‘normal subgroup of G ’ and ‘ G -invariant subgroup’ are synonyms.

$H \triangleleft G$ is called a nontrivial normal subgroup of G provided $H > \{1\}$.

H is a minimal normal subgroup of G if (a) $H \trianglelefteq G$; (b) $H > \{1\}$; (c) $N \triangleleft G$ and $N < H$ implies $N = \{1\}$. Thus, the group $\{1\}$ has no minimal normal subgroup.

G is simple if it is a minimal normal subgroup of G (so $|G| > 1$).

H is a maximal normal subgroup of G if $H < G$ and G/H is simple.

The subgroup generated by all minimal normal subgroups of G is called the *socle* of G and denoted by $\text{Sc}(G)$. We put, by definition, $\text{Sc}(\{1\}) = \{1\}$.

$\text{N}_G(M) = \{x \in G \mid x^{-1}Mx = M\}$ is the normalizer of a subset M in G .

$\text{C}_G(x)$ is the centralizer of an element x in G : $\text{C}_G(x) = \{z \in G \mid zx = xz\}$.

$\text{C}_G(M) = \bigcap_{x \in M} \text{C}_G(x)$ is the centralizer of a subset M in G .

If $A \leq B$ and $A, B \trianglelefteq G$, then $\text{C}_G(B/A) = H$, where $H/A = \text{C}_{G/A}(B/A)$.

$A \text{ wr } B$ is the wreath product of the ‘passive’ group A and the transitive permutation group B (in what follows we assume that B is regular); B is called the active factor of the wreath product). Then the order of that group is $|A|^{|B|}|B|$.

$\text{Aut}(G)$ is the group of automorphisms of G (the automorphism group of G).

$\text{Inn}(G)$ is the group of all inner automorphisms of G .

$\text{Out}(G) = \text{Aut}(G)/\text{Inn}(G)$, the outer automorphism group of G .

If $a, b \in G$, then $a^b = b^{-1}ab$.

An element $x \in G$ inverts a subgroup $H \leq G$ if $h^x = h^{-1}$ for all $h \in H$.

If $M \subseteq G$, then $\langle M \rangle = \langle x \mid x \in M \rangle$ is the subgroup of G generated by M .

$M^x = x^{-1}Mx = \{y^x \mid y \in M\}$ for $x \in G$ and $M \subseteq G$.

$[x, y] = x^{-1}y^{-1}xy = x^{-1}x^y$ is the *commutator* of elements x, y of G . If $M, N \subseteq G$ then $[M, N] = \langle [x, y] \mid x \in M, y \in N \rangle$ is a subgroup of G .

$o(x)$ is the order of an element x of G .

An element $x \in G$ is a π -element if $\pi(o(x)) \subseteq \pi$.

G is a π -group, if $\pi(G) \subseteq \pi$. Obviously, G is a π -group if and only if all of its elements are π -elements.

G' is the subgroup generated by all commutators $[x, y]$, $x, y \in G$ (i.e., $G' = [G, G]$), $G^{(2)} = [G', G'] = G'' = (G')'$, $G^{(3)} = [G'', G''] = (G'')'$ and so on. G' is called the *commutator* (or *derived*) subgroup of G .

$Z(G) = \bigcap_{x \in G} C_G(x)$ is the center of G .

$Z_i(G)$ is the i -th member of the upper central series of G ; in particular, $Z_0(G) = \{1\}$, $Z_1(G) = Z(G)$.

$K_i(G)$ is the i -th member of the lower central series of G ; in particular, $K_2(G) = G'$. We have $K_i(G) = [G, \dots, G]$ ($i \geq 1$ times). We set $K_1(G) = G$.

If G is nonabelian, then $\eta(G)/K_3(G) = Z(G/K_3(G))$.

$\mathcal{M}(G) = \langle x \in G \mid C_G(x) = C_G(x^p) \rangle$ is the Mann subgroup of a p -group G .

$\text{Syl}_p(G)$ is the set of p -Sylow subgroups of an arbitrary finite group G .

S_n is the *symmetric* group of degree n .

A_n is the *alternating* group of degree n

Σ_{p^n} is a Sylow p -subgroup of S_{p^n} .

$\text{GL}(n, F)$ is the set of all nonsingular $n \times n$ matrices with entries in a field F , the n -dimensional *general linear* group over F , $\text{SL}(n, F) = \{A \in \text{GL}(n, F) \mid \det(A) = 1 \in F\}$, the n -dimensional *special linear* group over F .

If $H \leq G$, then $H_G = \bigcap_{x \in G} x^{-1}Hx$ is the *core* of the subgroup H in G and $H^G = \bigcap_{H \leq N \trianglelefteq G} N$ is the *normal closure* or *normal hull* of H in G . Obviously, $H_G \trianglelefteq G$.

If G is a p -group, then $p^{b(x)} = |G : C_G(x)|$; $b(x)$ is said to be the *breadth* of $x \in G$, where G is a p -group; $b(G) = \max \{b(x) \mid x \in G\}$ is the *breadth* of G .

$\Phi(G)$ is the Frattini subgroup of G (= the intersection of all maximal subgroups of G), $\Phi(\{1\}) = \{1\}$, $p^{d(G)} = |G : \Phi(G)|$.

$\Gamma_i = \{H < G \mid \Phi(G) \leq H, |G : H| = p^i\}$, $i = 1, \dots, d(G)$, where $G > \{1\}$.

If $H < G$, then $\Gamma_1(H)$ is the set of all maximal subgroups of H .

$\exp(G)$ is the exponent of G (the least common multiple of the orders of elements of G). If G is a p -group, then $\exp(G) = \max \{o(x) \mid x \in G\}$.

$k(G)$ is the number of conjugacy classes of G (= G -classes), the class number of G .

K_x is the G -class containing an element x (sometimes we also write $ccl_G(x)$).

C_m is the cyclic group of order m .

G^m is the direct product of m copies of a group G .

$A \times B$ is the direct product of groups A and B .

$A * B$ is a central product of groups A and B , i.e., $A * B = AB$ with $[A, B] = \{1\}$.

$E_{p^m} = C_p^m$ is the elementary abelian group of order p^m . G is an elementary abelian p -group if and only if it is a p -group $> \{1\}$ and G coincides with its socle. Next, $\{1\}$ is elementary abelian for each prime p .

A group G is said to be *homocyclic* if it is a direct product of isomorphic cyclic subgroups (obviously, elementary abelian p -groups are homocyclic).

$ES(m, p)$ is an *extraspecial* group of order p^{1+2m} (a p -group G is said to be extraspecial if $G' = \Phi(G) = Z(G)$ is of order p). Note that for each $m \in \mathbb{N}$, there are exactly two nonisomorphic extraspecial groups of order p^{2m+1} .

$S(p^3)$ is a nonabelian group of order p^3 and exponent $p > 2$.

A *special* p -group is a nonabelian p -group G such that $G' = \Phi(G) = Z(G)$ is elementary abelian. Direct products of extraspecial p -groups are special.

D_{2m} is the *dihedral* group of order $2m$, $m > 2$. Some authors consider E_{2^2} as the dihedral group D_4 .

Q_{2^m} is the *generalized quaternion* group of order $2^m \geq 2^3$.

SD_{2^m} is the *semidihedral* group of order $2^m \geq 2^4$.

M_{p^m} is a nonabelian p -group containing exactly p cyclic subgroups of index p .

$\text{cl}(G)$ is the *nilpotence class* of a p -group G .

$\text{dl}(G)$ is the *derived length* of a p -group G .

$\text{CL}(G)$ is the set of all G -classes.

A p -group of *maximal class* is a nonabelian group G of order p^m with $\text{cl}(G) = m - 1$.

$\Omega_m(G) = \langle x \in G \mid o(x) \leq p^m \rangle$, $\Omega_m^*(G) = \langle x \in G \mid o(x) = p^m \rangle$ and $\mathfrak{O}_m(G) = \langle x^{p^m} \mid x \in G \rangle$.

A p -group is *absolutely regular* if $|G/\mathfrak{O}_1(G)| < p^p$.

A p -group is *thin* if it is either absolutely regular or of maximal class.

$G = A \cdot B$ is a *semidirect product* with *kernel* B and *complement* A .

A group G is an extension of $N \trianglelefteq G$ by a group H if $G/N \cong H$. A group G splits over N if $G = H \cdot N$ with $H \leq G$ and $H \cap N = \{1\}$ (in that case, G is a semidirect product of H and N with kernel N).

$H^\# = H - \{e_H\}$, where e_H is the identity element of the group H . If $M \subseteq G$, then $M^\# = M - \{e_G\}$.

An automorphism α of G is *regular* ($=$ fixed-point-free) if it induces a regular permutation on $G^\#$ (a permutation is said to be *regular* if it has no fixed points).

An *involution* is an element of order 2 in a group.

A *section* of a group G is an epimorphic image of some subgroup of G .

If $F = \text{GF}(p^n)$, then we write $\text{GL}(m, p^n), \text{SL}(m, p^n), \dots$ instead of $\text{GL}(m, F), \text{SL}(m, F), \dots$

$c_n(G)$ is the number of cyclic subgroups of order p^n in a p -group G .

$s_n(G)$ is the number of subgroups of order p^n in a p -group G .

$e_n(G)$ is the number of subgroups of order p^n and exponent p in G .

\mathcal{A}_n -group is a p -group G all of whose subgroups of index p^n are abelian but G contains a nonabelian subgroup of index p^{n-1} . In particular, \mathcal{A}_1 -group is a minimal nonabelian p -group for some p .

$\alpha_n(G)$ is the number of \mathcal{A}_n -subgroups in a p -group G .

Characters and representations

$\text{Irr}(G)$ is the set of all *irreducible* characters of G over \mathbb{C} .

A character of degree 1 is said to be *linear*.

$\text{Lin}(G)$ is the set of all *linear* characters of G (obviously, $\text{Lin}(G) \subseteq \text{Irr}(G)$).

$\text{Irr}_1(G) = \text{Irr}(G) - \text{Lin}(G)$ is the set of all *nonlinear* irreducible characters of G ;
 $n(G) = |\text{Irr}_1(G)|$.

$\chi(1)$ is the *degree* of a character χ of G ,

χ_H is the *restriction* of a character χ of G to $H \leq G$.

χ^G is the character of G induced from the character χ of some subgroup of G .

$\bar{\chi}$ is a character of G defined as follows: $\bar{\chi}(x) = \overline{\chi(\bar{w})}$ (here \bar{w} is the complex conjugate of $w \in \mathbb{C}$).

$\text{Irr}(\chi)$ is the set of irreducible constituents of a character χ of G .

If χ is a character of G , then $\ker(\chi) = \{x \in G \mid \chi(x) = \chi(1)\}$ is the *kernel* of a character χ .

$Z(\chi) = \{x \in G \mid |\chi(x)| = \chi(1)\}$ is the *quasikernel* of χ .

If $N \trianglelefteq G$, then $\text{Irr}(G \mid N) = \{\chi \in \text{Irr}(G) \mid N \not\leq \ker(\chi)\}$.

$\langle \chi, \tau \rangle = |G|^{-1} \sum_{x \in G} \chi(x) \tau(x^{-1})$ is the *inner product* of characters χ and τ of G .

$I_G(\phi) = \langle x \in G \mid \phi^x = \phi \rangle$ is the *inertia subgroup* of $\phi \in \text{Irr}(H)$ in G , where $H \triangleleft G$.

1_G is the *principal character* of G ($1_G(x) = 1$ for all $x \in G$).

$M(G)$ is the *Schur multiplier* of G .

$\text{cd}(G) = \{\chi(1) \mid \chi \in \text{Irr}(G)\}$.

$\text{mc}(G) = k(G)/|G|$ is the *measure of commutativity* of G .

$T(G) = \sum_{\chi \in \text{Irr}(G)} \chi(1)$, $f(G) = T(G)/|G|$.

Preface

This is the second part of the book. Sections 48–57, 60, 61, 66, 67, 70, 71, 73–75, 77–87, 89–92 and Appendix 19 are written by the second author, all other sections – by the first author. This volume contains a number of very strong results on 2-groups due to the second author. All exercises and about all problems are due to the first author. All material of this part is appeared in the book form at the first time.

Some outstanding problems of p -group theory are solved in this volume:

- (i) classification of 2-groups with exactly three involutions,
- (ii) classification of 2-groups containing exactly one nonmetacyclic maximal subgroup,
- (iii) classification of 2-groups G containing an involution t such that $C_G(t) = \langle t \rangle \times Q$, where Q contains only one involution,
- (iv) classification of 2-groups all of whose minimal nonabelian subgroups have the same order 8,
- (v) classification of 2-groups of rank 3 all of whose maximal subgroups are of rank 2,
- (vi) classification of 2-groups containing selfcentralizing noncyclic abelian subgroups of order 8, and so on.

There are, in this part, a number of new proofs of known important results:

- (a) Blackburn's classification of minimal nonmetacyclic groups (we presented, in Sec. 66 and 69, two different proofs),
- (b) classification of p -groups all of whose subgroups of index p^2 are abelian,
- (c) Ward's theorem on quaternion-free 2-groups (we presented two different proofs),
- (d) classification of p -groups with cyclic subgroup of index p^2 ,
- (e) Kazarin's classification of p -groups all of whose cyclic subgroups of order $> p$ are normal,
- (f) Iwasawa's classification of modular p -groups, and so on.

Some results proved in this part have no analogs in existing literature:

- (a) classification of 2-groups all of whose minimal nonabelian subgroups are isomorphic and have order 16,
- (b) study the 2-groups with at most $1 + p + p^2$ minimal nonabelian subgroups,

- (c) classification of 2-groups all of whose nonabelian two-generator subgroups are of maximal class,
- (d) classification of 2-groups G with $|\Omega_2(G)| \leq 2^4$ and $|\Omega_2^*(G)| = 2^4$,
- (e) classification of p -groups G with $\Omega_2(G)$ or $\Omega_2^*(G)$ is metacyclic (extraspecial),
- (f) classification of 2-groups all of whose nonabelian subgroups are generated by involutions, and so on.

As the previous part, this one contains a great number of open problems posed, as a rule, by the first author; some of these problems are solved and solutions are presented below.

The first author is indebted to Avinoam Mann for numerous useful discussions and help. The correspondence with Martin Isaacs allowed us to acquaint the reader with a number of his old and new important results. Moreover, Mann and Isaacs familiarized us with a number of their papers prior of publication. Noboru Ito read a number of sections and all appendices and made numerous useful remarks and suggestions. The help of Lev Kazarin was very important and allowed us to improve a number of places of the book, especially, in §§46 and 63; he also acquainted the first author with a fragment of his PhD thesis (see §§65, 71). The first author also indebted to Gregory Freiman, Marcel Herzog (both at Tel-Aviv University), Moshe Roitman and Izu Vaisman (both at University of Haifa) for help and support.

The publication of the book gives us great pleasure. We are grateful to the publishing house of Walter de Gruyter and all who promoted the publication, among of them Prof. M. Hazewinkel, Dr. R. Plato and K. Dimler, for their support and competent handling of the project.

§46

Degrees of irreducible characters of Suzuki p -groups

The results of this section are due to I. A. Sagirov [Sag1, Sag2]. Throughout this section we use the following notation: $\mathbb{F} = \text{GF}(p^m)$, $m > 1$; θ is an automorphism of \mathbb{F} of order k for some divisor $k > 1$ of m (recall that the group of automorphisms of \mathbb{F} is cyclic of order m whose generator is $a \mapsto a^p$ for all $a \in \mathbb{F}$); $n = \frac{m}{k} (< m)$. Let, for example, $\theta : a \mapsto a^{p^n}$ ($a \in \mathbb{F}$). The set of fixed points of θ is a subfield \mathbb{F}_θ of \mathbb{F} satisfying $a^{p^n} = 1$ so containing p^n elements (for example, if $k = m$, then $\mathbb{F}_\theta = \mathbb{F}_0$, the prime subfield of \mathbb{F}). Let \mathbb{F}^* be the (cyclic) multiplicative group of \mathbb{F} . Next, let $\text{Irr}_1(G)$ denote the set of all nonlinear irreducible characters of G . Put $\text{cd}(G) = \{\chi(1) \mid \chi \in \text{Irr}(G)\}$. Next, $\text{Irr}_{(t)}(G)$ denotes the number of characters of degree t in $\text{Irr}(G)$.

Definition. The Suzuki p -group $A_p(m, \theta)$ is the set $\mathbb{F} \times \mathbb{F}$ with multiplication defined as follows: $(a, b)(c, d) = (a + c, b + d + a\theta(c))$.

Let $G = A_p(m, \theta)$; then $|G| = |\mathbb{F}|^2 = p^{2m}$. It follows from the definition that elements (a, b) and (c, d) commute if and only if $c\theta(a) = a\theta(c)$, i.e., either $a = 0$ or $\theta(c/a) = c/a$ so $c = au$ for some $u \in \mathbb{F}_\theta$. The identity element of G is $(0, 0)$ and $(a, b)^{-1} = (-a, -b + a\theta(a))$. Since so defined multiplication is associative, G indeed is a group. If $(c, d) \in Z(G)$ and $(a, b) \in G$, then $c = au$ for $u \in \mathbb{F}_\theta$ and all $a \in \mathbb{F}$ which implies $c = 0$ since $k > 1$. Thus, $Z(G) = \{(0, d) \mid d \in \mathbb{F}\}$. We have $Z(G) \cong E_{p^m}$. It is easy to prove, by induction that $(a, b)^n = (na, nb + \binom{n}{2} \cdot a\theta(a))$. Taking $n = p$, we get $(a, b)^p \in Z(G)$; moreover, if $p > 2$, then $\exp(G) = p$.

1^o. Throughout this subsection $p = 2$ and $G = A(m, \theta) = A_2(m, \theta)$. Our aim is to find $\text{cd}(G)$ and the number of irreducible characters of every degree $s \in \text{cd}(G)$.

Theorem 46.1 ([Sag1]). *Suppose that $p = 2$, $G = A(m, \theta)$, where $m > 1$ and θ is an automorphism of the field $\mathbb{F} = \text{GF}(2^m)$ of order $k > 1$ and $n = \frac{m}{k}$. Then one of the following holds:*

- (a) *If k is odd, then $\text{cd}(G) = \{1, 2^{\frac{1}{2}(m-n)}\}$.*
- (b) *If $k = 2$, then $\text{cd}(G) = \{1, 2^{m/2}\} = \{1, 2^n\}$.*
- (c) *If $k > 2$ is even, then $\text{cd}(G) = \{1, 2^{m/2}, 2^{(m/2)-n}\}$, $|\text{Irr}_{(2^{m/2})}(G)| = \frac{(2^m-1)2^n}{2^n+1}$ and $|\text{Irr}_{(2^{(m/2)-n})}(G)| = \frac{(2^m-1)2^{2n}}{2^n+1}$.*

If $x \in \mathbb{F}$ then, since θ is an automorphism of \mathbb{F} of order $k > 1$, then $\theta(x) = x^{2^s}$ for some nonnegative s independent of x and $\theta^k(x) = x$, $x \in \mathbb{F}$. On the other hand, $\theta^k(x) = x^{2^{sk}}$ so $x^{2^{sk}} = x$, and this is true for each $x \in \mathbb{F}$. If x is a primitive element of \mathbb{F} , it follows that $2^m - 1$ divides $2^{sk} - 1$ so $m (= nk)$ divides sk (see Lemma 46.5 below) hence n divides s , and we conclude that $s = nt$, where $(t, k) = 1$ since $o(\theta) = k$. Thus, $\theta(x) = x^{2^{nt}}$. Therefore, the number of automorphisms of \mathbb{F} of order k equals $\varphi(k)$, where $\varphi(*)$ is the Euler's totient function. Then $\{a \in \mathbb{F} \mid \theta(a) = a\} = \mathbb{F}_\theta$ is the set of elements $a \in \mathbb{F}$ such that $a^{2^{nt}} = a$ and the cardinality of that set is 2^n . As we have shown, if $a \neq 0$, then $C_G((a, b)) = \{(az, u) \mid z \in \mathbb{F}_\theta, u \in \mathbb{F}\}$ so $|C_G((a, b))| = 2^{m+n}$. In particular, the size of every noncentral G -class equals $\frac{2^{2m}}{2^{m+n}} = 2^{m-n}$. If $a \in \mathbb{F} - \{0\}$, then $(a, b)^2 = (0, a\theta(a)) \neq (0, 0)$ so $Z(G) = \Omega_1(G)$. Therefore, since $\exp(G) = 4$, we get $\Omega_1(G) = \mathcal{V}_1(G) = \Phi(G)$.

Lemma 46.2. $|G'| \geq 2^{m-n}$.

Indeed, $|G'|$ is at least the size of a noncentral G -class. However, all noncentral G -classes have the same size 2^{m-n} . From the last assertion follows

Lemma 46.3. $k(G) = |Z(G)| + \frac{|G| - |Z(G)|}{2^{m-n}} = 2^{m+n} + 2^m - 2^n$.

An element $\lambda \in \mathbb{F}$ is said to be *primitive* if the (cyclic) multiplicative group $\mathbb{F}^* = \langle \lambda \rangle$.

Lemma 46.4. A mapping $\varphi_\lambda((a, b)) = (\lambda a, \lambda\theta(\lambda)b)$ is an automorphism of G of order $o(\lambda)$ for every element $\lambda \in (\mathbb{F}^*)^\#$.

Proof. Set $\lambda\theta(\lambda) = \mu$. Then $\varphi_\lambda((a, b)) = (\lambda a, \mu b)$, $\varphi_\lambda((c, d)) = (\lambda c, \mu d)$,

$$\varphi_\lambda((a, b)(c, d)) = \varphi_\lambda((a+c, b+d+a\theta(c))) = (\lambda(a+c), \mu(b+d+a\theta(c))).$$

On the other hand,

$$\begin{aligned} \varphi_\lambda((a, b))\varphi_\lambda((c, d)) &= (\lambda a, \mu b)(\lambda c, \mu d) = (\lambda(a+c), \mu b + \mu d + \lambda a\theta(\lambda)c) \\ &= (\lambda(a+c), \mu(b+d+a\theta(c))). \end{aligned}$$

It follows that φ_λ is an endomorphism of G . Next, $(\lambda a, \mu b) = \varphi_\lambda((a, b)) = (0, 0)$ if and only if $(a, b) = (0, 0)$ so φ_λ is an automorphism of G since G is finite.

Set $o(\lambda) = d$. Then $\varphi_\lambda^d((a, b)) = (\lambda^d a, (\lambda\theta(\lambda))^d b) = (a, b)$ and, if $a \neq 0$, then $\varphi_\lambda^r((a, b)) \neq (a, b)$ for $r \in \{1, 2, \dots, d-1\}$. It follows that $o(\varphi_\lambda) = d = o(\lambda)$. \square

Lemma 46.5. Given $a > 1$, m, n , we have $(a^m - 1, a^n - 1) = a^{(m,n)} - 1$.

Proof. Set $(m, n) = \delta$ and $d = (a^m - 1, a^n - 1)$. Then there exist $u, v \in \mathbb{N}$ such that $\delta = mu - nv$. Clearly, $a^\delta - 1$ divides d . On the other hand, d divides $a^{mu} - 1$ and $a^{nv} - 1$. Hence d divides the number $a^{mu} - 1 - (a^{nv} - 1) = a^{nv}(a^{mu-nv} - 1) = a^{nv}(a^\delta - 1)$ so d divides $a^\delta - 1$ since $(d, a) = 1$, and we conclude that $d = a^\delta - 1$. \square

Lemma 46.6. Let $m = nk$, where $n, k \in \mathbb{N}$, and let $t \in \mathbb{N}$ be coprime with k ; then $(m, nt) = n$.

- (a) Set $d = (2^m - 1, 2^{nt} + 1)$. Then $d = 1$ if k is odd and $d = 2^n + 1$ if k is even.
- (b) Suppose that $2^n + 1$ divides $2^m - 1$. Then $2n$ divides m .

Proof. (a) The number $d_0 = (2^m - 1, 2^{2nt} - 1)$ equals $2^{(nk, 2nt)} - 1 = 2^n - 1$ if k is odd and $d_0 = 2^{2n} - 1$ if k is even (Lemma 46.5). Since $2^{nt} + 1$ divides $2^{2nt} - 1$, the number d divides d_0 .

We claim that $(2^{nt} + 1, 2^n - 1) = 1$. Indeed, if a prime p divides that number, then $2^n \equiv 1 \pmod{p}$ so $2^{nt} \equiv 1^t \equiv 1 \pmod{p}$, a contradiction since p (if it exists) must be odd and $2^{nt} \equiv -1 \pmod{p}$.

Suppose that k is odd. By definition, d divides $2^{nt} + 1$ and, by the first paragraph, d divides $d_0 = 2^n - 1$ so d divides $(2^{nt} + 1, 2^n - 1) = 1$ (see the previous paragraph), and we get $d = 1$. This proves the first assertion in (a).

Now suppose that k is even; then t is odd. In that case, by the first paragraph, d divides $d_0 = 2^{2n} - 1 = (2^n - 1)(2^n + 1)$ and, by definition, d divides $2^{nt} + 1$. Therefore, by the second paragraph, d divides $(2^n + 1, 2^{nt} + 1) = 2^n + 1$ since t is odd. Since $2^n + 1$ divides d , we get $d = 2^n + 1$. The proof of (a) is complete.

(b) Since $(2^n - 1, 2^n + 1) = 1$ and $2^n - 1$ divides $2^m - 1 = 2^{nk} - 1$, it follows that $2^{2n} - 1 = (2^n - 1)(2^n + 1)$ divides $2^m - 1$ and so $2n$ divides m (Lemma 46.5). \square

Write $\Phi_\lambda = \langle \varphi_\lambda \rangle$ ($\lambda \in \mathbb{F}^\#$); then $|\Phi_\lambda| = o(\lambda)$. If λ is primitive, we write $\Phi = \Phi_\lambda$.

Lemma 46.7. Let $\lambda \in \mathbb{F}$ be primitive; then $|\Phi| = o(\lambda) = 2^m - 1$ and:

- (a) The size of every Φ -orbit on the set $G - Z(G)$ equals $2^m - 1$.
- (b) For odd k , there is only one Φ -orbit on the set $Z(G)^\#$. (In that case, $\Phi \cdot G$ is a Frobenius group with minimal normal subgroup $Z(G)$, its kernel.)
- (c) For even k , the size of every Φ -orbit on the set $Z(G)^\#$ equals $\frac{2^m - 1}{2^n + 1}$ (in that case, the number of Φ -orbits on $Z(G)^\#$ equals $2^n + 1$).

Proof. (a) For $(a, b) \in G$ and $i \in \mathbb{N}$, we have $\varphi_\lambda^i((a, b)) = (\lambda^i a, (\lambda\theta(\lambda))^i b)$. Let $(a, b) \in G - Z(G)$. In that case, $a \neq 0$ so $\varphi_\lambda^i((a, b)) = (a, b)$ if and only if $\lambda^i = 1$, i.e., i is divisible by $2^m - 1$ since λ is primitive. This proves (a).

(b) Now let k be odd and $b \neq 0$. Then $\varphi_\lambda^i((0, b)) = (0, (\lambda\theta(\lambda))^i b) = (0, b)$ if and only if $(\lambda\theta(\lambda))^i = 1$. Since $\theta(\lambda) = \lambda^{2^{nt}}$ with $(t, k) = 1$, we get $1 = (\lambda\theta(\lambda))^i = \lambda^{(2^{nt}+1)i}$. Therefore, $o(\lambda) = 2^m - 1$ divides $(2^{nt} + 1)i$. By Lemma 46.6(a), if k is odd, $2^m - 1$ divides i since $(2^m - 1, 2^{nt} + 1) = 1$, so the Φ -orbit of $(0, b)$ contains $2^m - 1$ elements. Then all elements of $Z(G)^\#$ are Φ -conjugate, and (b) is proven.

(c) Let k be even. The minimal positive integer i such that $\lambda^{(2^{nt}+1)i} = 1$ equals $\frac{2^m - 1}{2^n + 1}$, by Lemma 46.6(a), and this number is the size of the Φ -orbit of the element $(0, b) \in Z(G)^\#$. It follows that the number of Φ -orbits on $Z(G)^\#$ equals $2^n + 1$, completing the proof of (c). \square

For $\lambda \in \mathbb{F}^* - \{1_{\mathbb{F}}\}$, φ_λ has no fixed points on $(G/\text{Z}(G))^\#$ (check!) so $\langle \varphi_\lambda, G/\text{Z}(G) \rangle$ is a Frobenius group.

Corollary 46.8. *If k is odd, then $G' = \text{Z}(G)$.*

Proof. Indeed, $\text{Z}(G)$ is a minimal normal subgroup of $\langle \varphi_\lambda, \text{Z}(G) \rangle$, where λ is a primitive element of \mathbb{F} , by Lemma 46.7(b), and $G' \leq \text{Z}(G)$ so $G' = \text{Z}(G)$. \square

Remark. Suppose that $\chi \in \text{Irr}_1(G)$, $\chi(1) = 2^a$ and $Z_0 = \text{Z}(G) \cap \ker(\chi)$, where $G = A(m, \theta)$. Then $|\text{Z}(G) : Z_0| = 2$ since the center of $G/\ker(\chi)$ is cyclic. It follows that $G'Z_0 = \text{Z}(G)$, $\text{cd}(G/Z_0) = \{1, 2^a\}$ [Isa1, Theorem 2.31] and so $|\text{Irr}_1(G/Z_0)| = \frac{2^{m+1}-2^m}{2^{2a}} = 2^{m-2a}$. A character $\chi \in \text{Irr}_1(G)$ determines Z_0 uniquely.

Theorem 46.9 ([Han]). *If $G = A(m, \theta)$ is a Suzuki 2-group, where θ is an automorphism of \mathbb{F} of odd order $k > 1$, then $\text{cd}(G) = \{1, 2^{(m-n)/2}\}$ (here $n = \frac{m}{k}$).*

Proof. Let $\lambda \in \mathbb{F}$ be primitive. Consider the action of the automorphism φ_λ on subgroups of index 2 in $\text{Z}(G)$. By Lemma 46.7(b), $\langle \varphi_\lambda, \text{Z}(G) \rangle$ is a Frobenius group and $\text{Z}(G)^\#$ is the unique φ_λ -orbit. By Maschke's theorem, if $\varphi_\lambda^s \neq \text{id}$, then that automorphism has no invariant subgroups of index 2 in $\text{Z}(G)$, i.e., $\langle \varphi_\lambda \rangle$ acts on the set of such subgroups in a fixed-point-free manner. Since the order of φ_λ equals $2^m - 1$, all $2^m - 1$ subgroups of index 2 in $\text{Z}(G)$ are $(\Phi =) \langle \varphi_\lambda \rangle$ -conjugate.

Let $\chi \in \text{Irr}_1(G)$, $Z_0 = \text{Z}(G) \cap \ker(\chi)$. Then the isomorphism type of G/Z_0 independent of χ , since all subgroups of index 2 in $\text{Z}(G)$ are Φ -conjugate. It follows that $\text{cd}(G) = \{1, d\}$ for some $d > 1$, by the Remark. By Lemma 46.3 and Corollary 46.8, we get $2^m + (2^{m+n} - 2^n)d^2 = 2^{2m}$ so $d = 2^{\frac{1}{2}(m-n)}$. \square

Thus, Theorem 46.1(a) is proven. In what follows, k is even.

Lemma 46.10. *Let $\lambda \in \mathbb{F}$ be primitive and k even. Then:*

- (a) *If $k > 2$, i.e., $m = kn > 2n$, then $G' = \text{Z}(G)$ and the number of Φ -orbits on $(G')^\#$ equals $2^n + 1$, and all these orbits have the same size $\frac{2^m-1}{2^n+1}$.*
- (b) *If $k = 2$, i.e., $m = 2n$, then either $G' = \text{Z}(G)$ and $(G')^\#$ has $2^n + 1$ distinct Φ -orbits of size $\frac{2^m-1}{2^n+1} = 2^n - 1$ or else $|G'| = 2^n (= 2^{\frac{m}{2}})$ and all elements of $(G')^\#$ are Φ -conjugate.*

Proof. The assertion on the sizes of Φ -orbits follows from Lemma 46.7(c). Suppose that the number of Φ -orbits on $(G')^\#$ equals t and $|G'| = 2^f$. Then $2^f - 1 = t \cdot \frac{2^m-1}{2^n+1}$ (see Lemma 46.7(c)). It follows that $t - 1 = t \cdot 2^m + 2^n - 2^{f+n} - 2^f$. By Lemma 46.2, $f \geq m - n \geq n$ so 2^n divides $t - 1$. It follows that either $t = 1$ or $t \geq 2^n + 1$.

On the other hand, $f \leq m$ since $G' \leq \text{Z}(G)$ and, by the previous paragraph, $t \cdot \frac{2^m-1}{2^n+1} = 2^f - 1 \leq 2^m - 1$. It follows that $t \leq 2^n + 1$ so $t \in \{1, 2^n + 1\}$.

Suppose that $t = 1$. Then, by the previous paragraph, $2^f - 1 = \frac{2^m-1}{2^n+1}$ so $2^n(2^{m-n} + 1) = 2^f(2^n + 1)$. It follows that then $f = n$ and $m - n = n$, i.e., $m = 2n$, $k = 2$. In that case, $f = n = \frac{1}{2}m$, and we have the second possibility in (b).

Suppose that $t = 2^n + 1$. Then $2^f - 1 = (2^n + 1)\frac{2^m-1}{2^n+1} = 2^m - 1$ so $f = m$. \square

In what follows we first assume that $G' = \text{Z}(G)$. Then the number of Φ -orbits on $(G')^\#$ equals $2^n + 1$ and all these orbits have the same size $\frac{2^m - 1}{2^n + 1}$ (Lemma 46.10).

Lemma 46.11. *Suppose that $G' = \text{Z}(G)$, $\lambda \in \mathbb{F}$ is primitive and k is even.*

- (a) *Under Φ , the set of subgroups of index 2 in $\text{Z}(G)$ is partitioned in $2^n + 1$ orbits of size $\frac{2^m - 1}{2^n + 1}$.*
- (b) *Under Φ , the set $\text{Irr}(G) - \{1_G\}$ is partitioned in 2^n orbits of size $2^m - 1$ and $2^n + 1$ orbits of size $\frac{2^m - 1}{2^n + 1}$.*

Proof. $\text{Z}(G)$ has $2^m - 1$ subgroups of index 2 and $|\text{Irr}(G)| = 2^{m+n} + 2^m - 2^n$.

(a) By Lemma 46.7, the restriction of φ_λ to $\text{Z}(G)^\#$ is a product of $2^n + 1$ independent cycles of size $\frac{2^m - 1}{2^n + 1}$. This proves (a) (see the first paragraph in the proof of Lemma 46.9).

(b) Define the action of φ_λ on the set $\text{Irr}(G)$ as follows. Let R be a representation affording the character $\chi \in \text{Irr}(G)$. Set $T = R \circ \varphi_\lambda^{-1}$, i.e., $T(g) = R(g\varphi_\lambda^{-1})$ for $g \in G$. If $h \in G$, then since $\varphi_\lambda \in \text{Aut}(G)$, we get

$$T(gh) = R((gh)\varphi_\lambda^{-1}) = R(g\varphi_\lambda^{-1} \cdot h\varphi_\lambda^{-1}) = R(g\varphi_\lambda^{-1})R(h\varphi_\lambda^{-1}) = T(g)T(h),$$

i.e., T is a representation of G . Clearly, the value of the character $\chi^{\varphi_\lambda}(g)$ of T equals $\chi(g\varphi_\lambda^{-1})$ for every $g \in G$, and this character is also irreducible.

Let $\text{CL}(G) = \{K_1, \dots, K_r\}$ be the set of G -classes, $x_i \in K_i$, all i , and let $X = X(G) = (\chi_i(x_j))$ be the character table of G . Then φ_λ acts on columns and rows of X by permutations π_1 and π_2 , respectively, in such a way that if one considers these permutations as elements of $\text{GL}(r, \mathbb{C})$, then $\pi_2 X = (\chi_i^{\varphi_\lambda}(x_j)) = (\chi_i(x_j^{\varphi_\lambda^{-1}})) = X\pi_1$. Since the matrix X is nonsingular, we get $\pi_1 = X^{-1}\pi_2 X$ in $\text{GL}(r, \mathbb{C})$. Then, by Vishnevetsky's lemma [BZ, Lemma 10.4(a)], π_1 and π_2 are conjugate in the symmetric group S_r and so they have the same cycle structure. Now the result follows from Lemma 46.7. Indeed, under Φ , there are exactly $2^n + 1$ orbits of size $\frac{2^m - 1}{2^n + 1}$ on nonidentity central G -classes and $\frac{2^{m+n} - 2^n}{2^m - 1} = 2^n$ orbits of size $2^m - 1$ on noncentral G -classes. It follows that Φ has $2^n + 1$ orbits of size $\frac{2^m - 1}{2^n + 1}$ and 2^n orbits of size $2^m - 1$ on the set $\text{Irr}(G) - \{1_G\}$. \square

Lemma 46.12. *If $\chi \in \text{Irr}_1(G)$, k is even and $\chi(1) = 2^a$, then $\frac{1}{2}m - n \leq a \leq \frac{1}{2}m$.*

Proof. By the Remark, we have $\chi \in \text{Irr}_1(G/Z_0)$, where $Z_0 < \text{Z}(G)$ is of index 2, and $\text{cd}(G/Z_0) = \{1, 2^a\}$ so $|\text{Irr}_1(G/Z_0)| = 2^{m-2a}$. It follows that $m - 2a \geq 0$ so $a \leq \frac{1}{2}m$.

Let Z_1, \dots, Z_{2^n+1} be a transversal of the set of Φ -orbits on the set \mathfrak{M} of subgroups of index 2 in $\text{Z}(G)$. By the Remark, $\text{cd}(G/Z_i) = \{1, 2^{a_i}\}$, $|\text{Irr}_1(G/Z_i)| = 2^{m-2a_i}$, all i . Next, if Z_i and $Z_{i,1}$ belong to the same Φ -orbit, then, obviously, $G/Z_i \cong G/Z_{i,1}$. Since $|\text{Irr}_1(G)| = 2^{m+n} - 2^n$, we get $2^{m+n} - 2^n = \frac{2^m - 1}{2^n + 1} \sum_{i=1}^{2^n+1} 2^{m-2a_i}$ (here $\frac{2^m - 1}{2^n + 1}$ is the common size of Φ -orbit) which implies that $\sum_{i=1}^{2^n+1} 2^{m-2a_i} = 2^n(2^n + 1)$.

Assume that $m - 2a_i > 2n$ for some i . Then $2^{m-2a_i} \geq 2^{2n+1} > 2^n(2^n + 1)$, contrary to the result of the previous paragraph. It follows that $m - 2a_i \leq 2n$ so $a_i \geq \frac{1}{2}m - n$ for all i . \square

Theorem 46.13. *If k is even and $G' = Z(G)$, then $\text{cd}(G) = \{1, 2^{(m/2)-n}, 2^{m/2}\}$. Next, $|\text{Irr}_{(2^{(m/2)-n})}(G)| = (2^m - 1)2^{2n}/(2^n + 1)$, $|\text{Irr}_{(2^{m/2})}(G)| = (2^m - 1)2^n/(2^n + 1)$.*

Proof. Set $s = \frac{2^m - 1}{2^n + 1}$.

By Lemma 46.11(b), the set $\text{Irr}(G) - \{1_G\}$ is partitioned under the action of Φ in 2^n orbits of size $2^m - 1$ and $2^n + 1$ orbits of size s . Since $\langle \Phi, G \rangle / G'$ is a Frobenius group (see the paragraph following Lemma 46.7), all $|G : G'| - 1 = 2^m - 1$ nonprincipal linear characters of G are Φ -conjugate. Therefore, under Φ , there are exactly $2^n - 1$ orbits of size $2^m - 1$ on $\text{Irr}_1(G)$.

By Lemma 46.11(a), the set \mathfrak{M} of subgroups of index 2 in $Z(G)$ is partitioned in exactly $2^n + 1$ orbits of size s under Φ . Then, if $Z_0 \in \mathfrak{M}$, then $\varphi_\lambda^s(Z_0) = Z_0$ since the order of the restriction of φ_λ to \mathfrak{M} is s .

Suppose that the size of the Φ -orbit of $\chi \in \text{Irr}_1(G)$ equals $2^m - 1$ and $\chi \in \text{Irr}_1(G/Z_0)$ for some $Z_0 \in \mathfrak{M}$. Then $\chi \neq \chi^{\varphi_\lambda^i} \in \text{Irr}_1(G/Z_0)$ for $0 < i < 2^n + 1$ so the number of Φ -conjugates of χ equals $2^n + 1$.

Suppose that for some $Z_0 \in \mathfrak{M}$, $\text{Irr}_1(G/Z_0)$ has no characters belonging to a Φ -orbit of size s . Let $\text{cd}(G/Z_0) = \{1, 2^a\}$. Then all of the 2^{m-2a} characters of the set $\text{Irr}_1(G/Z_0)$ are partitioned in $\langle \Phi \rangle$ -orbits of the same odd size > 1 , which is not the case. It follows that, for each $Z_0 \in \mathfrak{M}$, there exists in $\text{Irr}_1(G/Z_0)$ a character such that its Φ -orbit has size s . Since the number of such Φ -orbits is $2^n + 1$ and, under Φ , the set \mathfrak{M} has exactly $2^n + 1$ orbits of size s (Lemma 46.11(a)), it follows that each set $\text{Irr}_1(G/Z_0)$ (where $Z_0 \in \mathfrak{M}$) has exactly one character belonging to a Φ -orbit of size s since $s(2^n + 1) = 2^m - 1$ is the total number of nonprincipal irreducible characters in Φ -orbits of size s , by Lemma 46.11(b).

Now suppose that the size of the Φ -orbit of a character $\chi \in \text{Irr}_1(G)$ is $2^m - 1$ (such χ exists since $|\text{Irr}_1(G)| = 2^n(2^m - 1) > s(2^n + 1)$), $\chi(1) = 2^a$ and $\chi \in \text{Irr}_1(G/Z_0)$, where $Z_0 \in \mathfrak{M}$. By the previous paragraph, $|\text{Irr}_1(G/Z_0)| = 2^{m-2a} = 1 + t(2^n + 1)$, where t is the number of orbits of characters in $\text{Irr}_1(G/Z_0)$ belonging to Φ -orbits of size $\neq s$ (there are in $\text{Irr}_1(G/Z_0)$ exactly $2^n + 1$ characters conjugate with χ under Φ). It follows that $2^n + 1$ divides $2^{m-2a} - 1$, and so n divides $m - 2a$ (Lemma 46.5) and $\frac{m-2a}{n}$ is even (Lemma 46.6(b)). By Lemma 46.12, $m - 2a \leq 2n \leq m$ so $\frac{m-2a}{n} \leq 2$, i.e., $\frac{m-2a}{n} \in \{0, 2\}$. Since G/Z_0 has at least two nonlinear irreducible characters, by the previous paragraph, $m - 2a > 0$. Hence, $m - 2a = 2n$ so $a = \frac{1}{2}m - n$ and $\text{Irr}_1(G/Z_0)$ has exactly $2^{m-2a} = 2^{2n}$ characters that lie in $t = \frac{2^{m-2a}-1}{2^n+1} = \frac{2^{2n}-1}{2^n+1} = 2^n - 1$ distinct Φ -orbits of size $2^m - 1$ and one Φ -orbit of size s .

We see that there are $2^{2n}s = 2^{2n} \cdot \frac{2^m - 1}{2^n + 1}$ nonlinear irreducible characters of G of degree $2^{(m/2)-n}$. The sum of squares of their degrees is $2^{m-2n}2^{2n} \cdot \frac{2^m - 1}{2^n + 1} = 2^m \cdot \frac{2^m - 1}{2^n + 1}$. The sum of squares of degrees of remaining $t_1 = 2^n(2^m - 1) - 2^{2n} \frac{2^m - 1}{2^n + 1} =$

$2^n \frac{2^m - 1}{2^n + 1}$ nonlinear irreducible characters of G is $\Sigma = 2^m(2^m - 1) - 2^m \cdot \frac{2^m - 1}{2^n + 1} = 2^m \cdot \frac{2^n(2^m - 1)}{2^n + 1}$. If $\chi \in \text{Irr}_1(G)$, then $\chi(1)^2 \leq |G : Z(G)| = 2^m$. Since $\Sigma = t_1 \cdot 2^m$, it follows that all latter characters have the same degree $2^{m/2}$. This means that $\text{cd}(G) = \{1, 2^{(m/2)-n}, 2^{m/2}\}$, and G has exactly 2^{2n} irreducible characters of degree $2^{(m/2)-n}$ and $t_1 = 2^n$ irreducible characters of degree $2^{m/2}$. \square

Corollary 46.14. *If $k = 2$, i.e., $m = 2n$, then $|G'| = 2^{m/2}$.*

Proof. In that case, by Lemma 46.10, either $|G'| = 2^{m/2}$ or else $|G'| = 2^m$. In the second case, however, by Theorem 46.13, $\text{cd}(G) = \{1, 2^{(m/2)-n}, 2^{m/2}\}$, which is not the case since $m - 2n = 0$. \square

Theorem 46.15. *If $k = 2$, then $\text{cd}(G) = \{1, 2^{m/2}\}$.*

Proof. By Corollary 46.14, $|G'| = 2^{m/2}$, $|G : G'| = 2^{m+(m/2)} = 2^{m+n} = |\text{Lin}(G)|$. Since $\text{k}(G) = 2^{m+n} + 2^m - 2^n$, we get $|\text{Irr}_1(G)| = |\text{Irr}(G)| - 2^{m+n} = 2^m - 2^n = 2^{m/2}(2^{m/2} - 1)$. By the remark following Corollary 46.8, if $\chi \in \text{Irr}_1(G)$, then $\chi \in \text{Irr}_1(G/Z_0)$, where $Z_0 \in \mathfrak{M}$, $G' \not\leq Z_0$. The number of such subgroups Z_0 equals $2^m - 1 - (2^{m/2} - 1) = 2^{m/2}(2^{m/2} - 1) = |\text{Irr}_1(G)|$. (Here $2^m - 1 = |\mathfrak{M}|$ and $2^{m/2} - 1$ is the number of subgroups of index 2 in $Z(G)/G'$; this explains our formula.) Thus, to every subgroup Z_0 corresponds the unique nonlinear irreducible character of G/Z_0 . Since $|G/Z_0| = 2^{m+1}$ and $|(G/Z_0)'| = 2$ so G/Z_0 is extraspecial, we get $\text{cd}(G/Z_0) = \{1, 2^{m/2}\}$. \square

Theorem 46.1 is proven.

Corollary 46.16. *If $k = 2$ and $\chi \in \text{Irr}_1(G)$, then G/Z_0 is extraspecial for every subgroup Z_0 of index 2 in $Z(G)$ such that $G' \not\leq Z_0$.*

Proof. Suppose that $\chi \in \text{Irr}_1(G/Z_0)$; then $\chi(1) = 2^{\frac{1}{2}m}$, by Theorem 46.15. It follows that $|Z(G/Z_0)| = 2$, so G/Z_0 is extraspecial since its center and derived subgroup have order 2. \square

2^o . In this subsection, $p > 2$. Thus, $\mathbb{F} = \text{GF}(p^m)$, $m \in \mathbb{N}$ with $m > 1$, $q = p^m$, θ is an automorphism of \mathbb{F} of order k for some divisor $k > 1$ of m , $\frac{m}{k} = n$ and $G = \text{A}_p(m, \theta)$ is the generalized Suzuki p -group of order q^2 . Our aim in this subsection is to prove the following

Theorem 46.17 ([Sag2]). *If $G = \text{A}_p(m, \theta)$ is a p -group of order q^2 , where $p > 2$, $m > 1$ is an integer, $q = p^m$, θ is an automorphism of the field $\mathbb{F} = \text{GF}(q)$ of order $k > 1$ and $\frac{m}{k} = n$, then one of the following holds:*

(a) *If k is odd, then $\text{cd}(G) = \{1, p^{(m-n)/2}\}$.*

(b) *If $k = 2$, then $\text{cd}(G) = \{1, p^{m/2}\}$.*

(c) If $k > 2$ is even, then $\text{cd}(G) = \{1, p^{m/2}, p^{(m/2)-n}\}$, $|\text{Irr}_{(p^{m/2})}(G)| = \frac{p^m-1}{p^n+1} \cdot p^n$ and $|\text{Irr}_{(p^{(m/2)-n})}(G)| = \frac{p^m-1}{p^n+1} \cdot p^{2n}$.

By the text preceding 1^o, $\exp(G) = p$, $(a, b)^{-1} = (-a, -b + a\theta(a))$, $Z(G) = \{(0, b) \mid b \in \mathbb{F}\}$ is of order q and the centralizer of every element from $G - Z(G)$ has order p^{m+n} . It follows that $\text{k}(G) = p^{m+n} + p^m - p^n$ so the number of noncentral G -classes is $p^{m+n} - p^n$. Next, $|G'| \geq p^{m-n}$. We see that Lemmas 46.2, 46.3 and 46.4 are also true for odd p . Argument following Lemma 46.4, is also true for odd p . Therefore, for every $x \in \mathbb{F}$, $\theta(x) = x^{p^{nt}}$ for some t coprime with k .

Lemma 46.18. (a) Suppose that $m = nk$, $(t, k) = 1$ and $(p^m - 1, p^{nt} + 1) = d$. If k is odd, then $d = 2$. If k is even, then $d = p^n + 1$.

(b) Suppose that $k, n \in \mathbb{N}$, k even and $(p^m - 1, p^n + 1) = d$. Then $d = 2$ if $\frac{n}{(m/2, n)}$ is even and $d = p^{(m/2, n)} + 1$ if $\frac{n}{(m/2, n)}$ is odd.

Proof. (a) Since $(k, t) = 1$, then d divides $(p^m - 1, p^{2nt} - 1) = (p^m - 1, p^{2n} - 1) = p^{(m, 2n)} - 1$ (Lemma 46.5). If k is odd then $(m, 2n) = (nk, 2n) = n$ so d divides $p^n - 1$. If k is even, then $(m, 2n) = 2n$ so d divides $p^{2n} - 1$. Let us find $d_0 = (p^{nt} + 1, p^n - 1)$.

Let k be odd; then d divides $p^n - 1$ so d divides d_0 . If $r > 2$ is a prime divisor of d_0 , then $p^n \equiv 1 \pmod{r}$ so $p^{nt} + 1 \equiv 2 \pmod{r}$, a contradiction. The same argument also works in the case $r = 4$. It follows that $d_0 = 2$ since d_0 is even. Since the even number d divides $d_0 = 2$, we get $d = 2$.

Suppose that k is even; then t is odd and so $p^n + 1$ divides $(p^m - 1, p^{nt} + 1) = d$. Next, $p^{nt} + 1 = (p^n + 1)A$ and $p^m - 1 = (p^n + 1)B$, where $A = p^{n(t-1)} - p^{n(t-2)} + \dots + p^{2n} - p^n + 1$ and $B = p^{n(k-1)} - p^{n(k-2)} + \dots + p^n - 1$. The number A is odd since t is odd, and B is even since k is even. In that case, $d = (p^n + 1)(A, B)$ so $\frac{d}{p^n+1} = (A, B) = u$ is odd. Since $d = (p^n + 1)u$ with odd u divides $p^{2n} - 1 = (p^n - 1)(p^n + 1)$ and $(p^{nt} + 1, p^n - 1) = 2$ (see the previous paragraph!), we get $d = p^n + 1$.

(b) Set $d = (p^m - 1, p^n + 1)$, $m = 2m_1$, $d_0 = (p^{(m_1, n)} + 1, p^n + 1)$. Then d divides the number

$$(p^m - 1, p^{2n} - 1) = p^{(m, 2n)} - 1 = p^{2(m_1, n)} - 1 = (p^{(m_1, n)} - 1)(p^{(m_1, n)} + 1).$$

As in the proof of (a), $(p^{(m_1, n)} - 1, p^n + 1) = 2$ and $d_0 = 2$ if $\frac{n}{(m_1, n)}$ is even and $d_0 = p^{(m_1, n)} + 1$ if $\frac{n}{(m_1, n)}$ is odd.

Suppose that $\frac{n}{(m_1, n)}$ is even. Then $d \in \{2, 4\}$ since d divides

$$(p^n + 1, p^{(m_1, n)} - 1)(p^n + 1, p^{(m_1, n)} + 1) = 2.$$

Indeed, since n is even, we get $p^n + 1 \equiv 2 \pmod{4}$ so $d = 2$.

Suppose that $s = \frac{n}{(m_1, n)}$ is odd and set $t = (m_1, n)$. Then

$$p^n + 1 = p^{ts} + 1 = (p^t + 1)(p^{t(s-1)} - p^{t(s-2)} + \cdots + p^{2t} - p^t + 1)$$

so $\frac{p^n+1}{p^t+1}$ is odd. \square

Let ϕ_λ be as in Lemma 46.4 and set $\Phi = \langle \phi_\lambda \rangle$ provided λ is a primitive element of the field \mathbb{F} .

Lemma 46.19. *If λ is a primitive element of the field \mathbb{F} , then:*

- (a) *The size of Φ -orbits on $G - Z(G)$ is $p^m - 1$.*
- (b) *The size of Φ -orbits on $Z(G)^\#$ is $\frac{1}{2}(p^m - 1)$ for odd k and $\frac{p^m - 1}{p^n + 1}$ for even k .*

Proof. By definition, $\phi_\lambda^i((a, b)) = (\lambda^i a, (\lambda\theta(\lambda))^i b)$. If $a \neq 0$, the assertion follows since λ is primitive. Let $a = 0$. Then $\phi_\lambda^i(0, b) = (0, (\lambda\theta(\lambda))^i b) = (0, b)$ if and only if $(\lambda\theta(\lambda))^i = 1$. Since $\theta(\lambda) = \lambda^{p^n}$, we obtain $\lambda^{(p^n+1)i} = 1$. It follows that $\phi(\lambda) = p^m - 1$ divides $(p^n + 1)i$, and the assertion follows from Lemma 46.18(a). \square

Lemma 46.20. *Suppose that $\chi \in \text{Irr}_1(G)$, $\chi(1) = p^a$, $Z_0 = Z(G) \cap \ker(\chi)$. Then $|Z(G) : Z_0| = p$, $G' \not\leq Z_0$, $\text{cd}(G/Z_0) = \{1, p^a\}$, and $|\text{Irr}_1(G/Z_0)| = (p-1)p^{m-2a}$. Next, every nonlinear irreducible character of G is a character of exactly one group G/Z , where Z is a subgroup of index p in $Z(G)$ not containing G' .*

Proof. Since $Z(G/\ker(\chi))$ is cyclic and $Z(G)$ is elementary abelian, we get $|Z(G) : Z_0| = p$. Let us consider the quotient group G/Z_0 . Since χ is nonlinear and $G' \not\leq Z_0$ but $G' \leq Z(G)$, we get $G'Z_0 = Z(G)$. Next, $|(G/Z_0)'| = p$ and $\exp(G/Z_0) = p$. It follows that $G/Z_0 = (G_1/Z_0) \times (Z_1/Z_0)$, where $Z_1/Z_0 < Z(G/Z_0)$ and G_1/Z_0 is extraspecial. Now all assertions of the lemma are obvious. \square

Theorem 46.21. *If $G = A_p(m, \theta)$, where θ an automorphism of \mathbb{F} of odd order $k > 1$, then $\text{cd}(G) = \{1, p^{\frac{m-n}{2}}\}$, where $n = \frac{m}{k}$.*

Proof. Let λ be a primitive element of \mathbb{F} . In that case, there are two Φ -orbits of size $\frac{1}{2}(p^m - 1)$ on $Z(G)$, where Φ is a cyclic subgroup generated by ϕ_λ , by Lemma 46.19(b). If $g \in G'$, then the Φ -orbit of g lies in G' since G' is characteristic in G . It follows that $|G'| - 1 \geq \frac{1}{2}(p^m - 1)$ so $|G'| = p^m$ since $|G'|$ divides p^m . It follows that $G' = Z(G)$. By Lemma 46.19(b), there are at most two Φ -orbits on the set of all subgroups of order p in $Z(G)$. It follows that there are at most two Φ -orbits on the set of maximal subgroups of $Z(G)$. Since $G/Z_0 \cong G/Z_0^{\phi_\lambda}$ for every subgroup Z_0 of index p in $Z(G)$ and $|\text{cd}(G/Z_0)| = 2$, by Lemma 46.20, then G has at most two distinct degrees of nonlinear irreducible characters.

Assume that $\text{cd}(G) = \{1, p^a, p^b\}$. Then there are two Φ -orbits on the set of subgroups of index p in $Z(G)$ and the sizes of these orbits are $\frac{p^m - 1}{2(p-1)}$. In that case, there are $\frac{p^m - 1}{2(p-1)}(p-1)p^{m-2a} = \frac{1}{2}(p^m - 1)p^{m-2a}$ characters of degree p^a in $\text{Irr}_1(G)$

and, similarly, $\frac{p^m-1}{2(p-1)}(p-1)p^{m-2b} = \frac{1}{2}(p^m-1)p^{m-2b}$ characters of degree p^b in $\text{Irr}_1(G)$. It follows that

$$p^{m+n} - p^n = |\text{Irr}_1(G)| = \frac{1}{2}(p^m-1)p^{m-2a} + \frac{1}{2}(p^m-1)p^{m-2b}$$

so that $p^n = \frac{1}{2}(p^{m-2a} + p^{m-2b})$ or, what is the same, $p^{n+2a+2b} = \frac{1}{2}p^m(p^{2a} + p^{2b})$. Let, for definiteness, $a \geq b$. Then $p^{n+2a+2b} = \frac{1}{2}p^{m+2b}(p^{2a-2b}-1)$. The last equality is possible if and only if $p^{2a-2b}-1=0$. Thus $a=b$ so $\text{cd}(G) = \{1, p^a\}$. It follows that $|G| = p^{2m} = p^m + (p^{m+n} - p^n)p^{2a}$ so $a = \frac{1}{2}(m-n)$. \square

Hence, the Theorem 46.17 is proven for odd k .

Lemma 46.22. *Suppose that $\lambda \in \mathbb{F}$ is primitive and k is even. Then:*

- (a) *If $k > 2$, i.e., $m > 2n$, then $G' = Z(G)$ and the number of Φ -orbits on $(G')^\#$ equals $p^n + 1$; all these orbits have size $\frac{p^m-1}{p^n+1}$.*
- (b) *If $k = 2$, i.e., $m = 2n$, then either $G' = Z(G)$ and the number of Φ -orbits on $(G')^\#$ equals $p^n + 1$ and all these orbits are of size $\frac{p^m-1}{p^n+1} = p^n - 1$, or $|G'| = p^{\frac{m}{2}} = p^n$ and all elements of $(G')^\#$ are conjugate under Φ .*

Proof. Repeat, word for word, the proof of Lemma 46.10. \square

Lemma 46.23. *Let $\lambda \in \mathbb{F}$ be primitive, k even and $G' = Z(G)$. Then $\text{Irr}(G) - \{1_G\}$ is partitioned, under action of Φ , in p^n orbits of size $p^m - 1$ and $p^n + 1$ orbits of size $\frac{p^m-1}{p^n+1}$.*

Proof. See the proof of Lemma 46.11(b). \square

Lemma 46.24. *Let $\lambda \in \mathbb{F}$ be primitive, k even and $G' = Z(G)$. Then the set of all subgroups of $Z(G)$ of index p is partitioned, under action of Φ , either in $p^n + 1$ orbits of size $\frac{p^m-1}{(p^n+1)(p-1)}$ or in $\frac{1}{2}(p^n + 1)$ orbits of size $\frac{2(p^m-1)}{(p^n+1)(p-1)}$.*

Proof. Consider a subgroup $P = \langle(0, x)\rangle$ of $Z(G)$ of order p . Let $s \in \mathbb{N}$ be minimal such that $\phi_\lambda^s((0, x)) \in P$. Since $o((\phi_\lambda)_{Z(G)}) = \frac{p^m-1}{p^n+1}$ and $P^\#$ is partitioned in $\frac{p-1}{t}$ orbits of size t under action of $\langle\phi_\lambda^s\rangle$, $st = \frac{p^m-1}{p^n+1}$. Then the size of Φ -orbit containing P equals s . Let $P_1 = \langle(0, y)\rangle$ be another subgroup of order p in $Z(G)$. Since $Z(G) = \{(0, b) \mid b \in \mathbb{F}\}$ and $\lambda \in F$ is primitive, we get $(0, y) = (0, \lambda^f x)$ for some $f \in \mathbb{N}$. Next, since $\phi_\lambda^s((0, x)) \in P$, we get $\phi_\lambda^s((0, x)) = (0, (\lambda\theta(\lambda))^s x) = (0, x)^r = (0, rx)$ for some $r \in \mathbb{N}$. Then

$$\begin{aligned} \phi_\lambda^s((0, y)) &= (0, (\lambda\theta(\lambda))^s y) = (0, (\lambda\theta(\lambda))^s \lambda^f x) \\ &= (0, r\lambda^f x) = (0, ry) = (0, y)^r. \end{aligned}$$

This means that the size of the Φ -orbit containing P_1 , is also equal to s . Thus, the sizes of all Φ -orbits on the set of all subgroups of order p in $Z(G)$ are equal. It follows

from $c_1(Z(G)) = \frac{p^m-1}{p-1}$, that the number of Φ -orbits on the set of such subgroups equals $\frac{p^m-1}{s(p-1)} = \frac{t(p^n+1)}{p-1}$. Since $(p^n+1, p-1) = 2$, we get $t \in \{p-1, \frac{1}{2}(p-1)\}$. Hence, the set of all subgroups of order p in $Z(G)$ is partitioned, under action of Φ , either in p^n+1 orbits of size $\frac{p^m-1}{(p^n+1)(p-1)}$ or in $\frac{1}{2}(p^n+1)$ orbits of size $\frac{2(p^m-1)}{(p^n+1)(p-1)}$.

Now let $Q < G$ be of index p . Since $Q = P_1 \times \cdots \times P_{m-1}$ with $|P_i| = p$ for all i , then $\phi_\lambda^s(Q) = Q$. If for some natural $s_1 < s$ we have $\phi_\lambda^{s_1}(Q) = Q$, then by Maschke's theorem, $Z(G) = Q \times P$, where P is a subgroup of order p and $\phi_\lambda^{s_1}(P) = P$, contrary to the minimal choice of s . Now the conclusion of the lemma follows from the previous paragraph. \square

Lemma 46.25. Suppose that $\chi \in \text{Irr}_1(G)$, $\chi(1) = p^a$. Then $a \leq \frac{1}{2}m$. Next, $a \geq \frac{1}{2}m - n$ if the number of Φ -orbits on the set of subgroups of index p in $Z(G)$ equals p^n+1 and $a > \frac{1}{2}m - n$, if the number of Φ -orbits on the same set equals $\frac{1}{2}(p^n+1)$.

Proof. By Lemma 46.20, $\chi \in \text{Irr}_1(G/Z_0)$, where Z_0 is a subgroup of index p in $Z(G)$ and $|\text{Irr}_1(G/Z_0)| = (p-1)p^{m-2a}$. It follows that $a \leq \frac{1}{2}m$.

Let Z_1, \dots, Z_t be the set of representatives of Φ -orbits on the set of maximal subgroups of $Z(G)$. Then $\text{cd}(G/Z_i) = \{1, p^{a_i}\}$, $|\text{Irr}_1(G/Z_i)| = (p-1)p^{m-2a_i}$. Next, any two subgroups of index p in $Z(G)$ belonging to the same Φ -orbit, lead to isomorphic quotient groups. Since $|\text{Irr}_1(G)| = p^{m+n} - p^n$, we get $p^{m+n} - p^n = \frac{p^m-1}{t(p-1)} \sum_{i=1}^t (p-1)p^{m-2a_i}$ so $tp^n = \sum_{i=1}^t p^{m-2a_i}$.

Suppose that $t = p^n + 1$. If $m - 2a_i > 2n$ for some i , then $p^{m-2a_i} \geq p^{2n+1} > p^n(p^n+1) = tp^n$, a contradiction. Thus, $m - 2a_i \leq 2n$ so $a_i \geq \frac{1}{2}m - n$ for all i .

Suppose that $t = \frac{1}{2}(p^n+1)$. If $m - 2a_i \geq 2n$ for some i , then $p^{m-2a_i} \geq p^{2n} > \frac{1}{2}p^n(p^n+1) = tp^n$, a contradiction. Thus, $a_i > \frac{1}{2}m - n$ for all i . \square

Theorem 46.26. If $G' = Z(G)$ and k is even, then $\text{cd}(G) = \{1, p^{\frac{1}{2}m-n}, p^{\frac{1}{2}m}\}$. In that case, $|\text{Irr}_{(p^{\frac{1}{2}m-n})}(G)| = \frac{p^m-1}{p^n+1} \cdot p^{2n}$, $|\text{Irr}_{(p^{\frac{1}{2}m})}(G)| = \frac{p^m-1}{p^n+1} \cdot p^n$.

Proof. By Lemma 46.23, the set $\text{Irr}(G) - \{1_G\}$, under action of Φ , is partitioned in p^n orbits of size $p^m - 1$ and $p^n + 1$ orbits of size $\frac{p^m-1}{p^n+1}$. Since $|\text{Lin}(G)| = |G/G'|$ and $\Phi \cdot (G/G')$ is a Frobenius group, nonprincipal linear characters lie in the same Φ -orbit of length $p^m - 1$. Therefore, under Φ , there are on $\text{Irr}_1(G)$ exactly $p^n - 1$ orbits of size $p^m - 1$. By Lemma 46.21, each character from $\text{Irr}_1(G)$ is contained in $\text{Irr}_1(G/Z_0)$, where Z_0 is a subgroup of index p in $Z(G)$. By Lemma 46.24, the set \mathfrak{M} of all $\frac{p^m-1}{p-1}$ subgroups of index p in $Z(G)$, under action of Φ , is partitioned either in $p^n + 1$ orbits of size $\frac{p^m-1}{(p^n+1)(p-1)}$ or in $\frac{1}{2}(p^n + 1)$ orbits of size $\frac{2(p^m-1)}{(p^n+1)(p-1)}$.

First suppose that the set \mathfrak{M} is partitioned in $p^n + 1$ orbits under action of Φ . Consider $\chi \in \text{Irr}_1(G/Z_0)$, $Z_0 \in \mathfrak{M}$. If the size of the Φ -orbit of χ equals $p^m - 1$, then $\text{Irr}_1(G/Z_0)$ contains exactly $(p-1)(p^n+1)$ characters from that orbit. If the size of Φ -orbit of χ equals $\frac{p^m-1}{p^n+1}$, then $\text{Irr}_1(G/Z_0)$ contains exactly $p-1$ characters from

that orbit. Note that if, for some $Z_0 \in \mathfrak{M}$, $\text{Irr}_1(G/Z_0)$ has no orbits of size $\frac{p^m-1}{p^n+1}$, then $\text{Irr}_1(G/Z_0)$ is partitioned in orbits of sizes $(p-1)(p^n+1)$. Since $|\text{Irr}_1(G/Z_0)| = p^{m-2a}$, where $p^a \in \text{cd}(G/Z_0)$, then p^n+1 divides p^{m-2a} , which is a contradiction. It follows that for every $Z_0 \in \mathfrak{M}$, there are in $\text{Irr}_1(G/Z_0)$ at least $p-1$ characters whose Φ -orbits have size $\frac{p^m-1}{p^n+1}$. Since the number of such characters is p^m-1 and $|\mathfrak{M}| = \frac{p^m-1}{p-1}$, every group G/Z_0 has exactly $p-1$ characters belonging to orbits of size $\frac{p^m-1}{p^n+1}$.

Let $\text{cd}(G/Z_0) = \{1, p^a\}$ and let $\text{Irr}_1(G/Z_0)$ contain exactly $t(p-1)(p^n+1)$ characters belonging to Φ -orbits of size p^m-1 . Then $(p-1)p^{m-2a} = |\text{Irr}_1(G/Z_0)| = (p-1) + t(p-1)(p^n+1)$. It follows that $p^{m-2a}-1 = t(p^n+1)$ so p^n+1 divides $p^{m-2a}-1$. It follows that n divides $m-2a$ and $\frac{m-2a}{n}$ is even. By Lemma 46.25, $\frac{1}{2}m-n \leq a \leq \frac{1}{2}m$ so that $0 \leq \frac{m-2a}{n} \leq 2$. Suppose that $t > 0$. Then $|\text{Irr}_1(G/Z_0)| > p-1$ or $m-2a > 0$. It follows that $\frac{m-2a}{n} = 2$ and so $a = \frac{1}{2}m-n$, $|\text{Irr}_1(G/Z_0)| = (p-1)p^{2n}$, $t = p^n-1$. Since $t = p^n-1$, $\text{Irr}_1(G/Z_0)$ contains representatives of all Φ -orbits of size p^m-1 on $\text{Irr}_1(G)$. Therefore, all characters from a Φ -orbit of size p^m-1 belong to members of \mathfrak{M} contained in the same Φ -orbit. Then $|\text{Irr}_{(p^{\frac{1}{2}m-n})}(G)| = \frac{p^m-1}{p^n+1} \cdot p^{2n}$. The number of remaining irreducible nonlinear characters equals $t_1 = p^n(p^m-1) - \frac{p^m-1}{p^n+1} \cdot p^{2n} = \frac{p^m-1}{p^n+1} \cdot p^n$ and the sum of squares of their degrees is $\Sigma = p^m(p^m-1) - \frac{p^m-1}{p^n+1} \cdot p^m = \frac{p^m-1}{p^n+1} \cdot p^{m+n}$. If $\chi \in \text{Irr}_1(G)$, then $\chi(1)^2 \leq |G : Z(G)| = p^m$. Since $\Sigma = t_1 p^m$, all other nonlinear irreducible characters are of degree $p^{\frac{1}{2}m}$.

Now suppose that the number of Φ -orbits on \mathfrak{M} equals $\frac{1}{2}(p^n+1)$. Recall that all these orbits are of size $\frac{2(p^m-1)}{(p-1)(p^n+1)}$. If $\chi \in \text{Irr}_1(G/Z_0)$ ($Z_0 \in \mathfrak{M}$) belongs to the Φ -orbit of size p^m-1 , then that set of characters contains also exactly $(p-1)\frac{1}{2}(p^n+1)$ Φ -conjugates with χ . Similarly, as before, we can show that then $\text{Irr}_1(G/Z_0)$ ($Z_0 \in \mathfrak{M}$) contains a character representing a Φ -orbit of size $\frac{p^m-1}{p^n+1}$.

Suppose that, for some $Z_0 \in \mathfrak{M}$, the set $\text{Irr}_1(G/Z_0)$ has exactly $\frac{1}{2}(p-1)$ characters every of which is contained in a Φ -orbit of size $\frac{p^m-1}{p^n+1}$. Then $|\text{Irr}_1(G/Z_0)| = (p-1)p^{m-2a} = \frac{1}{2}(p-1) + t(p-1) \cdot \frac{1}{2}(p^n+1)$, $t \geq 0$. It follows that $2p^{m-2a} = 1 + t(p^n+1)$, which is impossible since p^n+1 is even. Therefore, every group G/Z_0 ($Z_0 \in \mathfrak{M}$) has at least $p-1$ characters every of which belongs to a Φ -orbit of size $\frac{p^m-1}{p^n+1}$. Since $|\mathfrak{M}| = \frac{p^m-1}{p-1}$ and the number of the above characters is p^m-1 , every group G/Z_0 ($Z_0 \in \mathfrak{M}$) has exactly $p-1$ characters belonging to Φ -orbits of size $\frac{p^m-1}{p^n+1}$ (these characters belong to two different Φ -orbits).

Now let G/Z_0 ($Z_0 \in \mathfrak{M}$) have a character belonging to a Φ -orbit of size p^m-1 . Then, by the above, $|\text{Irr}_1(G/Z_0)| = (p-1)p^{m-2a} = (p-1) + t(p-1) \cdot \frac{p^n+1}{2}$ so $2(p^{m-2a}-1) = t(p^n+1)$. Since m is even then $m-2a$ is also even; therefore, using Lemma 46.18, we can show that either n divides $\frac{1}{2}(m-2a)$, p^n+1 divides $p^{m-2a}-1$ and $t = \frac{2(p^{m-2a}-1)}{p^n+1}$ or $p=3$, $n=1$ and $t = \frac{1}{2}(3^{2m-2a}-1)$. However,

by hypothesis, $n > 1$. In the first case we get either $2n \leq m - 2a$, $a \leq \frac{1}{2}m - n$, contrary to Lemma 46.25, or else $m - 2a = 0$, $a = \frac{1}{2}m$, $t = 0$, a contradiction again.

Thus, the case where \mathfrak{M} is partitioned in $\frac{1}{2}(p^n + 1)$ orbits under Φ is impossible. \square

Corollary 46.27. *If $m = 2n$, then $|G'| = p^{\frac{1}{2}m}$.*

Proof. Assume that $G' = Z(G)$ holds. Then, by Theorem 46.26, we have $cd(G) = \{1, p^{\frac{1}{2}m-n}, p^{\frac{1}{2}m}\}$, which is impossible since $\frac{1}{2}m - n = 0$. \square

Theorem 46.28. *If $m = 2n$, then $cd(G) = \{1, p^{\frac{1}{2}m}\}$.*

Proof. By Lemma 46.22 and Corollary 46.27, $|G'| = p^{\frac{1}{2}m}$, $|G : G'| = p^{m+\frac{1}{2}m} = p^{m+n} = |\text{Lin}(G)|$ so $|\text{Irr}_1(G)| = p^m - p^n = p^{\frac{1}{2}m}(p^{\frac{1}{2}m} - 1)$. Every nonlinear character of G is a character of G/Z_0 , where $Z_0 \in \mathfrak{M}$ and $G' \not\leq Z_0$. The number of such subgroups is $\frac{p^m - 1}{p-1} - \frac{p^{\frac{1}{2}m} - 1}{p-1} = \frac{p^{\frac{1}{2}m} - 1}{p-1} \cdot p^{\frac{1}{2}m}$, and every group G/Z_0 has at least $p - 1$ nonlinear irreducible characters. Comparing the number $|\text{Irr}_1(G)|$ with the number of subgroups of index p in $Z(G)$ not containing G' , we see that every group G/Z_0 has exactly $p - 1$ nonlinear irreducible characters. Let $cd(G) = \{1, p^a\}$. Then $p - 1 = |\text{Irr}_1(G/Z_0)| = (p - 1)p^{m-2a}$ so $a = \frac{1}{2}m$, completing the proof. \square

Theorem 46.17 is proven.

On the number of metacyclic epimorphic images of finite p -groups

In this section we prove the following

Theorem 47.1 ([Ber33]). *Let G be a nonmetacyclic p -group of order p^m and let $n < m$.*

- (a) *If $p = 2$ and $n > 3$, then the number of normal subgroups D of G such that G/D is metacyclic of order 2^n , is even.*
- (b) *If $p > 2$ and $n > 2$, then the number of normal subgroups D of G such that G/D is metacyclic of order p^n , is a multiple of p .*

Remarks. 1. Let G be a two-generator nonmetacyclic 2-group. Then all epimorphic images of G of order 8 are metacyclic. Since the number of normal subgroups of given index in a 2-group G is odd, it follows that Theorem 47.1(a) is not true for $n = 3$.

2. Let $r \geq s \geq t > 0$, $r + s + t > 3$ and $G = \langle a \rangle \times \langle b \rangle \times \langle c \rangle$, where $o(a) = p^r$, $o(b) = p^s$, $o(c) = p^t$, be an abelian p -group of rank three. Let us check Theorem 47.1 for $n = r + s + t - 1$. Let μ be the number of subgroups D of G of order p such that G/D is metacyclic. If $t > 1$, then $\Omega_1(G) \leq \Phi(G)$; then $\mu = 0$. Suppose that $s > t = 1$. If $D < \langle a \rangle \times \langle b \rangle$, then G/D is nonmetacyclic. If $D \not\leq \langle a \rangle \times \langle b \rangle$, then G/D is abelian of type (p^r, p^s) so metacyclic, and in that case, $\mu = p^2$. Now suppose that $r > s = 1$. Then $D = \mathfrak{U}_{r-1}(G)$ is the unique normal subgroup of order p in G such that G/D is not metacyclic so $\mu = p^2 + p$. Thus, p divides μ in all cases.

3. Suppose that $G = \langle a, b \mid a^4 = b^4 = c^2 = 1, c = [a, b], [a, c] = [b, c] = 1 \rangle$ is a nonmetacyclic minimal nonabelian group of order 2⁵. Let us check Theorem 47.1(a) for $n = 4$. The group G has exactly seven central subgroups of order 2:

$$\begin{aligned} X_1 &= \langle a^2 \rangle, & X_2 &= \langle b^2 \rangle, & X_3 &= \langle a^2 b^2 \rangle, & X_4 &= \langle c \rangle, \\ X_5 &= \langle a^2 c \rangle, & X_6 &= \langle b^2 c \rangle, & X_7 &= \langle a^2 b^2 c \rangle. \end{aligned}$$

Then G/X_i is metacyclic for $i = 3, 4, 5, 6$ and nonmetacyclic for $i = 1, 2, 7$.

4. Suppose that $G = \langle a, b \mid a^{2^m} = b^2 = c^2 = 1, m > 2, c = [a, b], [a, c] = [b, c] = 1 \rangle$ is a nonmetacyclic minimal nonabelian group of order 2 ^{$m+2$} . Set $\alpha =$

$a^{2^{m-1}}$; then $\Delta_1 = \{\langle c\alpha \rangle, \langle \alpha \rangle, \langle c \rangle\}$ is the set of central subgroups of order 2 in G . Then $G/\langle c \rangle$ and $G/\langle c\alpha \rangle$ are metacyclic and $G/\langle \alpha \rangle$ is not metacyclic.

Let $\text{Sc}(G) = \Omega_1(\text{Z}(G))$ be the socle of G . Let Δ_i denote, for all i such that $p^i \leq |\text{Sc}(G)|$, the set of subgroups of order p^i in $\text{Sc}(G)$. Let \mathfrak{M} be a set of nonidentity normal subgroups of G . Given $H \in \Delta_1 \cup \Delta_2 \cup \dots \cup \{\text{Sc}(G)\}$, let $\alpha(H)$ be the number of members of the set \mathfrak{M} containing H . Set $|\text{Sc}(G)| = p^t$ so that $\Delta_t = \{\text{Sc}(G)\}$. We claim that the following identity holds (see §10):

$$(1) \quad \alpha(G) = |\mathfrak{M}| = \sum_{i=1}^t (-1)^{i-1} p^{\binom{i}{2}} \sum_{H \in \Delta_i} \alpha(H).$$

Indeed, let $D \in \mathfrak{M}$ and $|D \cap \text{Sc}(G)| = p^k$; then $k \geq 1$ since $D > \{1\}$. For natural numbers $u \geq v$, let $\varphi_{u,v}$ denote the number of subgroups of order p^v in E_{p^u} . Then the contribution of D in the right-hand side of (1) is equal to $\sum_{i=1}^k (-1)^{i-1} p^{\binom{i}{2}} \varphi_{k,i}$, and that number equals 1, by Hall's identity (Theorem 5.2). Since the contribution of D in the left-hand side of (1) is also equal 1, identity $(*)$ is true. In particular,

$$(2) \quad \alpha(G) = |\mathfrak{M}| \equiv \sum_{H \in \Delta_1} \alpha(H) \pmod{p}.$$

Remark 5. Suppose that G is a noncyclic group of order p^m , $m > 2$ and $1 < n < m$. We claim that the number $c(G)$ of normal subgroups N of G such that G/N is cyclic of order p^n , is a multiple of p . One may assume that $c(G) > 0$. Let $n = m - 1$. There is $N \leq \text{Z}(G)$ of order p such that G/N is cyclic. Then G is abelian of type (p^{m-1}, p) so $G = Z \times N$, where Z is cyclic of order $p^{m-1} = p^n$ hence $c(G) = p$. Now let $n < m - 1$. Take $H \in \Delta_1$. Suppose that G/H is cyclic; then G is abelian of type (p^{m-1}, p) . The group G contains exactly $p + 1$ subgroups of index p^n . If N is one of such subgroups, then G/N is cyclic if and only if $N \not\leq \Phi(G)$ so, since $\Phi(G)$ is cyclic, we get $c(G) = p$. Next we assume that G is not abelian of type (p^{m-1}, p) ; then G/H is not cyclic for all $H \in \Delta_1$, therefore, by induction on m , we get $\alpha(H) \equiv 0 \pmod{p}$ so $c(G) \equiv 0 \pmod{p}$, by (2).

Suppose that G is a group of order p^m and $p^n \leq |G : G'|$. We claim that then the number $v(G)$ of $N \triangleleft G$ such that G/N is nonabelian of order p^n is a multiple of p . One may assume that $v(G) > 0$; then $n > 2$. The number of normal subgroups of given index in G is $\equiv 1 \pmod{p}$ (Sylow). If $N \triangleleft G$ has index p^n , then G/N is nonabelian if and only if $G' \not\leq N$. Therefore, $v(G) \equiv 0 \pmod{p}$ (Sylow again).

If a 2-group G of order $2^m > 2^3$ is not of maximal class, then the number of $N \triangleleft G$ such that G/N is nonabelian of order 2^3 is even since $|G : G'| \geq 2^3$.

Proof of Theorem 47.1. Suppose that \mathcal{M} is the set of normal subgroups D of G such that G/D is metacyclic of order p^n . One may assume that $\mathcal{M} \neq \emptyset$. As above, $\alpha(H)$ is the number of members of the set \mathcal{M} containing $H \in \Delta_1$.

A. First we consider the most difficult case $n = m - 1$; then $\mathcal{M} \subseteq \Delta_1$. One may assume that G is nonabelian (Remark 2). We have to prove that p divides $|\mathcal{M}| (= \alpha(G))$, i.e., $|\Delta_1 - \mathcal{M}| \equiv 1 \pmod{p}$. By (2), we have to prove that

$$(3) \quad \alpha(G) \equiv \sum_{H \in \Delta_1} \alpha(H) \equiv 0 \pmod{p}.$$

Let $U \in \mathcal{M}$ and suppose that $U \not\leq \Phi(G)$. Then $G = U \times M$, where $M \in \Gamma_1$ is metacyclic. If $V \in \Delta_1$ and $V \not\leq M$, then $G = V \times M$ so $V \in \mathcal{M}$. If $W \leq Z(M)$ is a member of the set \mathcal{M} , then M/W is cyclic and G is abelian of rank 3 so p divides $|\mathcal{M}|$ (Remark 2). We see that $|\mathcal{M}| = |\Delta_1| - c_1(Z(M)) \equiv 0 \pmod{p}$. Next we assume that all members of the set \mathcal{M} are contained in $\Phi(G)$.

(i) Let $p > 2$. Then $|G/\mathfrak{U}_1(G)| \geq p^3$ since G is nonmetacyclic (Theorem 9.11). Take $D \in \mathcal{M}$; then G/D is metacyclic. Assuming that $|G/\mathfrak{U}_1(G)| \geq p^4$, we conclude that $G/D\mathfrak{U}_1(G)$ is of order $\geq p^3$ and exponent p so nonmetacyclic, a contradiction. Thus, $|G/\mathfrak{U}_1(G)| = p^3$. Take $U \in \Delta_1 - \mathcal{M}$; then G/U is not metacyclic so $|(G/U)/\mathfrak{U}_1(G/U)| \geq p^3$ (Theorem 9.11 again) and so $U \leq \mathfrak{U}_1(G)$. Thus, all members of the set $\Delta_1 - \mathcal{M}$ are contained in $\mathfrak{U}_1(G)$. Conversely, if $V \in \Delta_1$ is contained in $\mathfrak{U}_1(G)$, then G/V is not metacyclic. Thus, $|\Delta_1 - \mathcal{M}|$ equals the number of those members of the set Δ_1 that are contained in $\mathfrak{U}_1(G)$. By Sylow, the last number is $\equiv 1 \pmod{p}$ so $|\mathcal{M}| \equiv |\Delta_1| - 1 = \varphi_{t,1} - 1 \equiv 0 \pmod{p}$.

(ii) Suppose that $p = 2$. Here we have to consider the nonmetacyclic quotient group $G/\mathfrak{U}_2(G)$ (see Lemma 42.2(b)) of order $\geq 2^4$.

(ii1) Assume that $|G/\mathfrak{U}_2(G)| = 2^4$. Then $\mathfrak{U}_2(G) > \{1\}$ since $m > 4$. The number of members of the set Δ_1 contained in $\mathfrak{U}_2(G)$, is odd (Sylow). Therefore, if all members of the set $\Delta_1 - \mathcal{M}$ are contained in $\mathfrak{U}_2(G)$, then $\alpha(G) = |\mathcal{M}|$ is even since $|\Delta_1|$ is odd, so we assume that there is $U \in \Delta_1 - \mathcal{M}$ such that $U \not\leq \mathfrak{U}_2(G)$; then $\bar{G} = G/U$ is nonmetacyclic. It follows from Theorem 44.2 that $\bar{G}/\mathfrak{U}_2(\bar{G})$ is nonmetacyclic so its order is $\geq 2^4$. Write $\bar{H} = \mathfrak{U}_2(\bar{G})$; then $G/H (\cong \bar{G}/\bar{H})$ is not metacyclic of order $\geq 2^4$ and exponent 4. It follows that $H = \mathfrak{U}_2(G)$ since $|G/\mathfrak{U}_2(G)| = 2^4$, contrary to the choice of U : $U \not\leq \mathfrak{U}_2(G)$.

(ii2) Let $|G/\mathfrak{U}_2(G)| > 2^4$. Take $D \in \mathcal{M}$; then, by Theorem 44.2, $D \not\leq \mathfrak{U}_2(G)$. Write $\bar{G} = G/D$. We claim that $|G/\mathfrak{U}_2(G)| \leq 2^5$. Indeed, $G/D\mathfrak{U}_2(G)$, as an epimorphic image of groups $\bar{G} = G/D$ and $G/\mathfrak{U}_2(G)$, is metacyclic of exponent 4 so its order is $\leq 2^4$, and our claim on order follows since $D\mathfrak{U}_2(G) = D \times \mathfrak{U}_2(G)$ and $|D| = 2$. Thus, $|G/\mathfrak{U}_2(G)| = 2^5$, by (ii1). Since G/D is metacyclic, we have $|Sc(G/D)| \leq 2^2$ so $|Sc(G)| \leq |D||Sc(G/D)| = 2^3$, and we conclude that $|\Delta_1| \in \{1, 3, 7\}$. Since $|\Delta_1|$ is odd, to complete this case, it suffices to show that the number $|\Delta_1 - \mathcal{M}|$ is also odd. But G/D is metacyclic so $D \not\leq G'$ (Theorem 36.1) and hence $G' \cong (G/D)'$ is cyclic. Since all members of the set \mathcal{M} are contained in $\Phi(G)$, we get $d(G) = 2$.

Let $\bar{H} = \mathfrak{U}_2(\bar{G})$ (\bar{G} is defined in (ii1)). Since $G/D\mathfrak{U}_2(G)$ is metacyclic, its order is $\leq 2^4$ so $H = D\mathfrak{U}_2(G) = D \times \mathfrak{U}_2(G)$ and $|\bar{G}/\mathfrak{U}_2(\bar{G})| = 2^4$ since $|G/\mathfrak{U}_2(G)| = 2^5$.

Set $\mathcal{N}_0 = \{V \in \Delta_1 \mid V \leq \mathfrak{U}_2(G)\}$; then $|\mathcal{N}_0|$ is odd (Sylow) and $\mathcal{N}_0 \subseteq \Delta_1 - \mathcal{M}$. One may assume that $\mathcal{N}_0 \subset \Delta_1 - \mathcal{M}$ (otherwise, $|\mathcal{M}| = |\Delta_1| - |\mathcal{N}_0|$ is even). In that case, there is $U_1 \in \Delta_1 - (\mathcal{M} \cup \mathcal{N}_0)$; then $\bar{G} = G/U_1$ is not metacyclic. Write $\bar{H} = \mathfrak{U}_2(\bar{G})$; then \bar{G}/\bar{H} is not metacyclic (Theorem 44.2) and, since $U_1 \mathfrak{U}_2(G) \leq H$ and $U_1 \not\leq \mathfrak{U}_2(G)$, we get $H_1 = U_1 \times \mathfrak{U}_2(G)$ and $|G/H_1| = \frac{1}{2}|G/\mathfrak{U}_2(G)| = \frac{1}{2} \cdot 2^5 = 2^4$. If $V < H_1$ is a member of the set Δ_1 , then G/V is nonmetacyclic. Let $\mathcal{N}_1 = \{U_0 \in \Delta_1 - \mathcal{N}_0 \mid U_0 < H_1\}$. Then $|\mathcal{N}_0 \cup \mathcal{N}_1| = |\mathcal{N}_0| + |\mathcal{N}_1|$, the number of members of the set Δ_1 contained in H_1 , is odd (Sylow). It follows that the number $|\mathcal{N}_1|$ is even since the number $|\mathcal{N}_0|$ is odd. Since $U_1 \in \mathcal{N}_1$, we obtain $|\mathcal{N}_1| \geq 2$ so $|\mathcal{N}_0 \cup \mathcal{N}_1| \geq 1 + 2 = 3$. Assuming that $\mathcal{N}_0 \cup \mathcal{N}_1 \subset \Delta_1 - \mathcal{M}$, we add to the set $\mathcal{N}_0 \cup \mathcal{N}_1$ the set \mathcal{N}_2 (of even cardinality > 0) of new members of the set $\Delta_1 - \mathcal{M}$. Indeed, if $U_2 \in \Delta_1 - (\mathcal{N}_0 \cup \mathcal{N}_1 \cup \mathcal{M})$, then, writing $H_2 = U_2 \mathfrak{U}_2(G)$, we conclude, as above with U_1 and H_1 , that G/H_2 is nonmetacyclic of order 2^4 . We have $H_1 \cap H_2 = \mathfrak{U}_2(G)$ since $\mathfrak{U}_2(G) \leq H_1 \cap H_2$ has index 2^5 in G and H_1, H_2 are distinct of index 2^4 in G , so \mathcal{N}_2 is the set of members of the set $\Delta_1 - (\mathcal{N}_0 \cup \mathcal{N}_1)$ contained in H_2 but not in H_1 and $|\mathcal{N}_2| > 0$ is even (if $V_i \in \mathcal{N}_i$, then $V_i \mathfrak{U}_2(G) = H_i$, $i = 0, 1, 2$). Thus, we get $|\mathcal{N}_0 \cup \mathcal{N}_1 \cup \mathcal{N}_2| \geq 1 + 2 + 2 = 5$. We claim that then the set $\mathcal{N}_0 \cup \mathcal{N}_1 \cup \mathcal{N}_2$, which contains exactly five members, coincides with the set $\Delta_1 - \mathcal{M}$. Indeed, otherwise, we can, acting as above, add to that sum-set at least two new members of the set $\Delta_1 - \mathcal{M}$, which is impossible since $|\Delta_1 - \mathcal{M}| \leq 6$: the set $\mathcal{M} \neq \emptyset$ and $|\Delta_1| = 7$. Thus, in any case, the number $|\Delta_1 - \mathcal{M}|$ is odd so that the number $|\mathcal{M}|$ is even.

B. Now let $n < m - 1$. Here we consider cases $p = 2$ and $p > 2$ together. We proceed by induction on $|G|$. Take $H \in \Delta_1$.

If G/H is metacyclic, then $\alpha(H) \equiv 1 \pmod{p}$ (Sylow). However, the number of such H , by part A of the proof, is a multiple of p . Therefore, the contribution of such H in the sum on the right-hand side of formula (2), is a multiple of p . Now suppose that G/H is not metacyclic. Then, by induction, $\alpha(H) \equiv 0 \pmod{p}$. Therefore, the contribution of such H in the sum on the right-hand side of formula (2), is a multiple of p again. Thus, congruence (3) is proven. \square

Supplement to Theorem 47.1. Let $1 \leq k \leq p - 1$, $k < n < m$ and a p -group G of order p^m satisfies $|G/\mathfrak{U}_1(G)| > p^k$. Then the number of normal subgroups D of G such that $|(G/D)/\mathfrak{U}_1(G/D)| \leq p^k$ and $|G/D| = p^n$, is a multiple of p .

2^o. Here we prove the following

Theorem 47.2. If G be a nonabelian metacyclic p -group, then all representation groups of G are also metacyclic so that $M(G)$, the Schur multiplier of G , is cyclic.

Proof. Let Γ be a representation group of G . By definition, there is in $Z(\Gamma) \cap \Gamma'$ a subgroup $M \cong M(G)$ such that $\Gamma/M \cong G$. Since G is nonabelian, we get $M < \Gamma'$. Since $\Gamma/M \cong G$ is metacyclic, Γ is also metacyclic, by Theorem 36.1. \square

The cyclicity of Schur multipliers of metacyclic p -groups is known, their orders are also computed in [Kar, Theorem 10.1.25].

Isaacs has reported (in letter at Jan 10, 2006) that he also proved Theorem 47.3. His proof is based on the following

Lemma 47.3 (Isaacs). *Let G be a p -group and let $Z \leq Z(G) \cap G'$ be of order p . If G/Z is metacyclic, then G is metacyclic.*

Proof. Let $U/Z \triangleleft G/Z$ be with cyclic U/Z and G/U . Note that $|U/Z| > p$ since G/Z is not abelian. We want to show that U is cyclic.

Now let $\langle xU \rangle = G/U$. Since U is abelian and normal in U and G/U is cyclic, we see that $G' = [U, x] = \langle [u, x] \mid u \in U \rangle$ is isomorphic to $U/C_U(x)$ [Isa2, Lemma 12.12]. But Z is contained in $C_U(x)$ and U/Z is cyclic, and hence G' is cyclic as an epimorphic image of U/Z . Since $G' > Z$ is cyclic, we have $Z \leq \Phi(G') \leq \Phi(U)$ so $d(U) = d(U/Z) = 1$ and U is cyclic. (In fact, Theorem 36.1 and Lemma 47.4 are equivalent.) \square

§48

On 2-groups with small centralizer of an involution, I

All results of this section are due to the second author. The main part of this section coincides with [Jan1].

In this section we give the classification of 2-groups containing an involution t such that $C_G(t) = \langle t \rangle \times C_{2^m}$, $m \geq 1$. We may assume from the start that $m > 1$ since, if $m = 1$, G is a 2-group of maximal class, by Proposition 1.8. Note that case $m = 2$ was considered in [GLS, Proposition 10.27].

Exercise 1. Let G be a nonabelian 2-group and t an involution in $G - Z(G)$.

- (a) Prove that $|N_G(C_G(t)) : C_G(t)| < c_1(C_G(t))$, where $c_1(G)$ is the number of subgroups of order 2 (or, what is the same, involutions) in G .
- (b) Let $C_G(t) = \langle t \rangle \times Q$, where Q is either cyclic of order 2^m , $m > 1$, or $Q \cong Q_{2^m}$, $m \geq 3$. Then $|N_G(C_G(t)) : C_G(t)| = 2$, by (a), and
 - (b1) $\Omega_1(Z(G)) = Z(Q)$.
 - (b2) If u is an involution in Q , then t and tu are conjugate in $N_G(C_G(t))$.
 - (b3) If $t \in \Phi(G)$, then $|\Phi(G)| > 4$.

Solution. (a) One may assume that $C_G(t) \trianglelefteq G$. Then G acts transitively on the conjugacy class K_t containing t . Since $|G : C_G(t)| > 1$ is a power of 2 and $c_1(C_G(t)) > 1$ is odd (Sylow), the inequality follows.

(b1, b2) Let $u \in Z(G)$ be an involution. Then u is a square and t is not, so t and u are not conjugate in G . The result follows since $C_G(t)(> Z(G))$ has exactly 3 involutions.

(b3) Assume that $|\Phi(G)| = 4$. Then $\Phi(G) \leq Z(G)$, by [BZ, Lemma 31.8], a contradiction since $t \notin Z(G)$.

Theorem 48.1 ([Jan1]). *Let G be a nonabelian 2-group containing an involution t such that the centralizer $C_G(t) = \langle t \rangle \times C$, where C is a cyclic group of order 2^m , $m \geq 1$ (clearly, $t \notin Z(G)$). Then G has no elementary abelian subgroups of order 16 and G is generated by at most three elements. Next, G has no t -invariant elementary abelian subgroups of order 8.*

(A1) If G has no elementary abelian subgroups of order 8, then one of the following holds:

- (a) $G \in \{D_{2^n}, SD_{2^n}\}$. Here we have $m = 1$.
- (b) $G \cong M_{2^n}$. Here we have $m = n - 2$.
- (c) $|G : C_G(t)| = 2$, $t \in \Phi(G)$, $Z(G)$ is a cyclic subgroup of order ≥ 4 not contained in $\Phi(C_G(t))$, $G/Z(G)$ is dihedral with cyclic subgroup $L/Z(G)$ of index 2, L is abelian of type $(2, 2^m)$, $m \geq 2$, $t \in L$. If x is an element of maximal order in $G - L$, then $\langle x^2 \rangle = Z(G)$. (In that case $C_G(t) = L$.)
- (d) G has a subgroup S of index ≤ 2 , where $S = AL$, the subgroup L is normal in G , $L = \langle b, t \mid b^{2^{n-1}} = t^2 = 1, b^t = b^{-1}, n \geq 3 \rangle \cong D_{2^n}$. $A = \langle a \rangle$ is cyclic of order 2^m , $m \geq 2$, $A \cap L = Z(L)$, $[a, t] = 1$, $\Omega_1(G) = \Omega_1(S) = \Omega_2(A) * L$. If $|G : S| = 2$, then there is an element $x \in G - S$ so that $t^x = tb$ and $C_G(t) = \langle t \rangle \times \langle a \rangle$. Next, $G = \langle a, b, t \rangle$ if $G = S$ and $G = \langle a, t, x \rangle$ if $S < G$.

(A2) If G has an elementary abelian subgroup of order 8, then $Z(G)$ is of order 2, $C_G(t) = \langle t \rangle \times \langle a \rangle$, where $A = \langle a \rangle$ has order 2^m ($m \geq 2$), G has a normal subgroup L such as in (A1)(d), $A \cap L = Z(L) = \langle z \rangle$, $S = AL$ is a normal subgroup of index ≤ 2 in G and G is isomorphic to one of the following groups:

- (e) $G = \langle a, b, t \mid a^{2^m} = b^{2^{n-1}} = t^2 = [a, t] = 1, m \geq 3, n \geq 4, b^t = b^{-1}, a^{2^{m-1}} = b^{2^{n-2}} = z, b^a = b^{1+2^i}, i = n - m \geq 2 \rangle$. We have $G = AL = S$ and the cyclic group $\langle a \rangle / \langle z \rangle$ acts faithfully on L .
- (f) $G = \langle a, b, t, s \mid a^{2^m} = b^{2^{n-1}} = t^2 = s^2 = [a, t] = 1, m \geq 4, n \geq 5, b^t = b^s = b^{-1}, a^{2^{m-1}} = b^{2^{n-2}} = z, b^a = b^{1+2^i}, i = n - m + 1 \geq 2, t^s = tb, s^a = a^{2^{m-2}} b^{-2^{i-1}} s \rangle$. Here $S = AL$ is a subgroup of index 2 in G and $\Omega_1(S) = \Omega_2(A) * L$. Also $G = \langle s \rangle \cdot S$, $M = \langle s \rangle L \cong D_{2^{n+1}}$, $N_G(M) = \langle a^2 \rangle M$ and s inverts $\Omega_2(A)$. The order of G is 2^{m+n} and $G = \langle a, t, s \rangle$.
- (g) Groups $G = F(m, n)$ (see Appendix 14). Here we have $G = \langle a, b, t, s \mid a^{2^m} = b^{2^{n-1}} = t^2 = s^2 = [a, t] = [a, b] = 1, m \geq 2, n \geq 3, b^t = b^s = b^{-1}, a^{2^{m-1}} = b^{2^{n-2}} = z, t^s = tb, a^s = a^{-1}z^v, v = 0, 1$, and if $v = 1$, then $m \geq 3 \rangle$. Here $S = A * L$ and $G = \langle s \rangle \cdot S$, where $|G : S| = 2$. We have $M = \langle s \rangle L \cong D_{2^{n+1}}$ and $G = \langle a, t, s \rangle$.
- (h) $G = \langle a, b, t, s \mid a^{2^m} = b^{2^{n-1}} = t^2 = s^2 = [a, t] = 1, m, n \geq 4, b^t = b^s = b^{-1}, a^{2^{m-1}} = b^{2^{n-2}} = z, t^s = tb, b^a = bz, a^s = a^{-1+2^{m-2}} b^{2^{n-3}} \rangle$. Here we have again $G = \langle s \rangle \cdot S$ so that $|G : S| = 2$. Finally, $M = \langle s \rangle \cdot L \cong D_{2^{n+1}}$ and $G = \langle a, t, s \rangle$.

Proof. Let G be a 2-group containing a noncentral involution t such that $C_G(t) = \langle t \rangle \times C$, where C is cyclic of order 2^m , $m \geq 1$. By Proposition 1.8, if $m = 1$, then $G \in \{D_{2^n}, n \geq 3, SD_{2^n}, n \geq 4\}$. In what follows we assume that $m > 1$. Then G is not of maximal class so it contains a normal abelian subgroup U of type $(2, 2)$ (Lemma 1.4). It follows from the structure of $C_G(t)$ that $Z(G)$ is cyclic of order 2^m

at most (see Exercise 1(b1)) so $T = C_G(U)$ has index 2 in G . Let u be the involution in C ; then $u \in Z(G)$ (Exercise 1(b1)). If an element $x \in N_G(C_G(t)) - C_G(t)$, then $t^x = tu$, by Exercise 1(b2).

Assume that E is a t -invariant elementary abelian subgroup of G of order 8. Set $H = \langle t, E \rangle$. Since H is not of maximal class, $|C_E(t)| > 2$, by Suzuki's theorem. Then the elementary abelian subgroup $\langle t \rangle \times C_E(t)$ of order ≥ 8 is contained in (the metacyclic subgroup) $C_G(t)$, which is a contradiction. Hence E does not exist. It follows that every t -invariant abelian subgroup of G is metacyclic.

(*) We examine now the case where $t \in T = C_G(U)$. Then $\langle t, U \rangle \leq C_G(t)$ so $t \in U$ since $C_G(t)$ has no elementary abelian subgroups of order 8. Also we see that $T = C_G(U) = \langle t \rangle \times C$ has index 2 in G since $U \not\leq Z(G)$, and $T = C_G(t)$.

(1*) Suppose that U is the only normal abelian subgroup of type $(2, 2)$ in G . Set $\Omega_1(C) = \langle u \rangle = \mathfrak{V}_{m-1}(T)$ so that $U = \langle t, u \rangle = \Omega_1(T)$ and $u \in Z(G)$. Since $Z(G)$ is cyclic, $\langle u \rangle = \Omega_1(Z(G))$. Next, $\mathfrak{V}_1(C) \leq \mathfrak{V}_1(G) \leq \Phi(G)$.

(1.1*) Suppose, in addition, that $t \notin \Phi(G)$. Then there exists a maximal subgroup M of G such that $t \notin M$; in that case, $G = \langle t \rangle \cdot M$, a semidirect product with kernel M . Setting $M_0 = T \cap M$, we get, by the modular law, $T = \langle t \rangle \times M_0$. It follows from the structure of T that $M_0 \cong C_{2^m}$. If M is cyclic, then, clearly, $G \cong M_{2^{m+2}}$, and this is the case (b) of the theorem. So assume that M is not cyclic. Since $U \not\leq M$ since $t \in U$ and $t \notin M$, the subgroup M has no G -invariant subgroups of type $(2, 2)$ (by assumption in (1*), U is the unique G -invariant four-subgroup) so M is of maximal class, by Lemma 1.4. Then $Z(M) = \langle u \rangle$, where $\langle t, u \rangle = U$. Let $\langle v \rangle$ be the cyclic subgroup of order 4 contained in M_0 (recall that, by assumption, $m \geq 2$; obviously, $v^2 = u$) and let $y \in M - M_0$; then $v^y = v^{-1} = vv^2 = vu$ and $t^y = tu$ (see Exercise 1(b2)). Hence we have $(tv)^y = t^yv^y = tu \cdot vu = tv$ so $K = \langle tv \rangle$ is a cyclic subgroup of order 4 contained in T but not contained in M_0 , and $(tv)^2 = t^2v^2 = v^2 = u$ since, by the choice, $v \in C_G(t)$. We have $C_G(tv) \geq \langle T, y \rangle = G$. It follows that $G = M * K$, the central product, $M \cap K = Z(M)$. This group is then a group in part (d) of the theorem (with $S = G$ and A is of order 4 centralizing L). In the case under consideration, $\Phi(G) = \mathfrak{V}_1(C)$ so C is normal in G .

(1.2*) It remains to consider the case $t \in \Phi(G)$. In this case $\langle t \rangle \times \mathfrak{V}_1(C) \leq \Phi(G)$ has index 4 in G so there we have equality and hence G is generated by two elements. If $m = 2$, then $\Phi(G) = U$, being a four-group, is contained in $Z(G)$, by Exercise 1(b3), which is a contradiction. Hence, we must have $m \geq 3$. There is an element $x \in G - T$ such that $x^2 \in \Phi(G) - (\mathfrak{V}_1(C) \cup U)$. This is due to the fact that $Z(G)$ is cyclic. Indeed, there exists an element $x \in G - T$ such that $x^2 \notin C$ (otherwise, $\Phi(G) = \mathfrak{V}_1(G) = \mathfrak{V}_1(C)$, which is a contradiction). Next, if $x^2 \in U$, then $C_G(x^2) \geq \langle x, T \rangle = G$ so $Z(G)$ is not cyclic since it contains a noncyclic subgroup $\langle u, x^2 \rangle$, a contradiction. Our claim about the existence of x is justified. Then $o(x^2) \geq 4$ since $x^2 \notin U = \Omega_1(\Phi(G))$. Set $C = \langle a \rangle$ so that $a^{2^{m-1}} = u$, $T = C_G(t) = \langle t \rangle \times \langle a \rangle$. Also, $\mathfrak{V}_1(T) = \mathfrak{V}_1(C) = \langle a^2 \rangle$ is normal

in G since T is, and $\Phi(G) = \langle t \rangle \times \langle a^2 \rangle$, where $o(a^2) = 2^{m-1} \geq 4$. It follows from the choice of x that $\Phi(G) = \langle a^2, x^2 \rangle$ (however, generators x^2 and a^2 are not independent). By Exercise 1(b2), we have $t^x = tu$. If x would centralize a^2 , then x centralizes $\langle a^2, x^2 \rangle = \Phi(G)$ and $\Phi(G)$ contains t so $x \in C_G(t) = T$, contrary to the choice of x . If $y \in G - T$, then $y^2 \in Z(G)$ since T is abelian and generates G together with y . Therefore, $x^2 \in Z(G)$. Since $x \notin C_G(a^2)$, we get $a^2 \notin Z(G)$. It follows that all elements in $(G/Z(G)) - (T/Z(G))$ are involutions. Since $Z(G) \not\leq \Phi(T)$, it follows that $T/Z(G)$ is cyclic. In that case, $G/Z(G)$ is dihedral. Indeed, since $d(G) = 2$ and $Z(G) \not\leq \Phi(G)$, we conclude that $G/Z(G)$ is not abelian of type $(2, 2)$. If z is an element of maximal order in $G - T$, then z^2 is a generator of $Z(G)$ since $zZ(G)$ is a noncentral involution in the dihedral group $G/Z(G)$. As we saw, $|Z(G)| \geq 4$. We obtain a group in part (c) of the theorem.

(**) In the rest of the proof we assume that G has a normal abelian subgroup U of type $(2, 2)$ which does not contain our involution t (if G has two normal abelian subgroups of type $(2, 2)$, then one of them does not contain t : otherwise $t \in Z(G)$, which is not the case since G is nonabelian). Therefore, this case includes the one where G has at least two distinct normal four-subgroups. Set again $T = C_G(U)$ so that $G = \langle t \rangle \cdot T$ since $t \notin T$. By the modular law, $G_0 = C_G(t) = \langle t \rangle \times A$, where $A = C_G(t) \cap T = C_T(t)$ is cyclic of order 2^m , $m \geq 2$, and so $Z = \Omega_1(A) = C_U(t) = \Omega_1(Z(G))$ is of order 2. We have $Z(G) \leq C_G(U) \cap C_G(t) = T \cap C_G(t) = C_T(t) = A$. Set $G_1 = N_G(G_0)$, where $G_0 = C_G(t)$; then $G_1 > G_0$ since $G > G_0$ is nonabelian. Since t and the generator z of $\Omega_1(A)$ are not conjugate in view of $m > 1$, t has only two conjugates t and tz in G_1 , and we have $\Omega_1(G_0) = \langle t, z \rangle$. It follows that $2 = |G_1 : C_{G_1}(t)| = |G_1 : G_0|$ (see also Exercise 1(a)) and so $G_1 = G_0U$ because $G_0U \leq G_1$ and $|G_0U : G_0| = 2$ since $G_0 \cap U = \Omega_1(A)$. Set $D_0 = \langle t \rangle \cdot U$; then $D_0 \cong D_8$ since it is nonabelian of order 8 and generated by involutions, and G_1 is the central product $G_1 = A * D_0$ with $A \cap D_0 = \langle z \rangle$ (indeed, A centralizes t and U so $\langle t, U \rangle = D_0$; before we used the product formula). We also have $U = \langle u, z \rangle < D_0$ for some involution u . Let v be an element of order 4 in D_0 and y an element of order 4 in A ; then $y^2 = v^2 = z$, and since $x^2 = y^2v^2 = y^4 = 1$, $x = yv$ is an involution in $G_1 - D_0$. Since $x^t = y^tv^t = yv^{-1} = yv \cdot v^2 = xz$, we see that $D_1 = \langle x, t \rangle \cong D_8$. Because $A = Z(G_1)$, we also have $G_1 = A * D_1$, $t \in D_1$ and $D_1 \cap U = Z(D_1) = \langle z \rangle$.

In the rest of the proof we consider a subgroup S of G which is maximal subject to the following four conditions:

- (i) S contains $G_1 = A * D_1$.
- (ii) $S = AL$, where L is a normal subgroup of S and $L \cong D_{2^n}$, $n \geq 3$,
- (iii) $A \cap L = \langle z \rangle = Z(L)$, and
- (iv) $L \cap G_1 = D_1 \cong D_8$.

We recall that $A = \langle a \rangle$ is of order 2^m , $m \geq 2$, and $Z(G) \leq A = Z(G_1)$ so $Z(G)$

is cyclic of order $\leq 2^m$, and $\Omega_1(A) = \langle z \rangle = Z(D_1) = Z(L) = \Omega_1(Z(G))$, $t \in D_1$, $C_G(t) = \langle t \rangle \times A$. Also G_1 contains $U = \langle z, u \rangle$ which is a normal abelian subgroup of G of type $(2, 2)$ and $u^t = uz$. Now we act with A on the dihedral group L , where we set $L = \langle b, t \mid b^{2^{n-1}} = t^2 = 1, b^t = b^{-1} \rangle$. Here $\langle b \rangle$ is the unique cyclic subgroup of index 2 in L so $\langle b \rangle$ is A -admissible (recall that L is normal in $S = AL$). We have $|\langle b \rangle \cap D_1| = 4$ (since $D_1 \leq L$, by (iv)), A centralizes D_1 (by (i)) and $C_L(a) = \langle t \rangle(C_L(a) \cap \langle b \rangle)$, by the modular law, and so $C_L(a)$ is a dihedral subgroup of L of order ≥ 8 containing D_1 (recall that $t \in D_1$). Looking at $\text{Aut}(L)$ (see Proposition 34.8, where $\text{Aut}(D_{2^n})$ is described) we see that A induces on L a cyclic group of automorphisms of order at most 2^{n-3} and so $|A : C_A(L)| \leq 2^{n-3}$. Since $S/L > \{1\}$ is cyclic, $U \not\leq L$ and L is generated by involutions, we have $\Omega_1(S) = UL$. It follows that $\Omega_1(S) \cap A = \langle y \rangle$, where $o(y) = 4$ (by the product formula) with $y^2 = z$, and we have $\langle y \rangle = \Omega_2(A)$.

Let us consider at first the case where y induces on L a nonidentity automorphism so that $C_A(L) = \langle z \rangle$ and the group $\langle a \rangle/\langle z \rangle$ acts faithfully on L . Then y induces an automorphism of order 2 on L and since $L > C_L(A) \geq D_1 \cong D_8$ we must have $n \geq 4$, $[y, t] = 1$ (recall that the element $y \in A$ centralizes t) and $b^y = bz$, $(b^2)^y = (bz)^2 = b^2$ so that $C_L(y) = \langle t, b^2 \rangle \cong D_{2^{n-1}}$ and $C_L(y)$ is a maximal subgroup of L . Let v be an element of order 4 in D_1 ; then $v \in \langle b \rangle$. Since $U = \langle z, u \rangle \leq AD_1$, we may set $u = yv$. We have $y^b = y (= y \cdot y^2 = y^{-1})$, and so $u^{tb} = (uz)^b = (yvz)^b = y^{-1}vz = y^{-1}vy^2 = yv = u$ so that $\langle z, u, tb \rangle$ is an elementary abelian subgroup of order 8 since tb is an involution not contained in U . Obviously, $C_{\Omega_1(S)}(u) = C_S(u) \cap \Omega_1(S) = \langle u \rangle \times \langle tb, b^2 \rangle$, where $\langle tb, b^2 \rangle \cong D_{2^{n-1}}$, and since $C_G(t) = \langle t \rangle \times A$ does not contain an elementary abelian subgroup of order 8, t cannot be fused in G to any involution contained in $C_S(u) \cap \Omega_1(S)$ since the centralizer of any involution from $C_S(u) \cap \Omega_1(S)$ contains a subgroup isomorphic to E_8 . On the other hand, it is easy to compute that any involution in S lies in $L \cup (C_G(u) \cap \Omega_1(S))$ since $\Omega_1(S) = UL$. Naturally, t cannot be fused in G to any involution in $U \triangleleft G$ since $t \notin U$. It follows that the G -class of t contains at most 2^{n-2} elements so $|G : C_G(t)| = 2^{n-2} = |S : C_S(t)|$. Since $C_G(t) = C_S(t)$, this forces that $S = G$. If $m = 2$, we have $G = F(2, n)$, stated in part (g) since $\langle t, b^2 \rangle \cong D_{2^{n-1}}$ centralizes A and the involution tb inverts A . So assume that $m \geq 3$. Then we may set (see Proposition 34.8) $b^a = b^{1+2^i}$, where $i \geq 2$ because $C_L(a) \geq D_1$. Since $C_L(a) \cong D_{2^{i+1}}$ and $C_L(a^{2^{m-1}}) \cong D_{2^{i+m}}$ and $a^{2^{m-1}} = z \in Z(L)$, we get $C_L(a^{2^{m-1}}) = L$. It follows that $i = n - m$. We have obtained exactly the groups stated in part (e).

In what follows we shall assume always, that $\langle y \rangle = \Omega_2(A)$ centralizes L so that $\Omega_1(S) = L * \Omega_2(A)$, the central product (of order 2^{n+1}). In this case each involution in S is contained in $L \cup U$ (see Appendix 16, where we have proved that $D_{2^n} * C_4 \cong Q_{2^n} * C_4$); it follows that U as the unique normal abelian subgroup of type $(2, 2)$ in S , is characteristic in S and so the subgroup L being generated by its own involutions is characteristic in $\Omega_1(S)$ and so in S (see also Appendix 16). If $S = G$, we get some groups stated in part (d) of the theorem.

From now on we shall assume, in addition, that $S < G$. Let $W = N_G(\Omega_1(S))$; obviously, $S < W$. Let K_x denotes the G -class containing an element $x \in G$. Since W fuses $K_t \cap \Omega_1(S)$ with $K_{tb} \cap \Omega_1(S)$ and $C_G(t), C_G(tb) < S$, where both classes are of size 2^{n-2} and are contained in L , we get $|W : S| = 2$, S is normal in W so L is normal in W since L is characteristic in S , by the above. Suppose that $W < G$ and let $g \in N_G(W) - W$ be such that $g^2 \in W$. We have $\langle K_t \cap W \rangle \geq \langle t, tb \rangle = L$ (indeed, involutions t and tb are not conjugate in L so they generate L), U is normal in G and all involutions in S lie in $L \cup U$ (see Appendix 16). Therefore (replacing g with gw , $w \in W$, if necessary) one may assume that $s = t^g \in W - S$; indeed, by assumption $W < G$ and the subgroup $\Omega_1(S)$ is not normal in G). Since s normalizes L and $C_G(t) \cap (\langle s \rangle \cdot L) = \langle t, z \rangle$, we have $\langle s \rangle \cdot L \cong D_{2^{n+1}}$: indeed, by Proposition 1.8 (Suzuki's theorem), $\langle s \rangle \cdot L$ is of maximal class and $s \notin L$. Now L and L^g are normal in W (since L is characteristic in $S \triangleleft W$), $L^g \cap S = L^g \cap L$, $L^g S = W$, $|L^g S : S| = |L^g : (L^g \cap S)| = |L^g : (L \cap L^g)| = 2$ and $|LL^g| = 2^{n+1}$, and so $LL^g = \langle s \rangle \cdot L$. Hence, $(LL^g)^g = L^g L^{g^2} = L^g L = LL^g$ since $g^2 \in W$ and L is normal in W , and so $\langle s \rangle \cdot L$ is the dihedral group of order 2^{n+1} which is normal in W . We have $W = A(\langle s \rangle \cdot L)$ and this contradicts the maximality of $S = AL$ (see (i–iv)). Hence we must have $W = G$ in any case. If $\Omega_1(S) = \Omega_1(G)$, we get the groups stated in part (d) of the theorem.

In view of the result of the previous paragraph, in what follows we assume, in addition, that $\Omega_1(S) \neq \Omega_1(G)$. Then for each involution $s \in G - S$, s normalizes L since L is characteristic in $\Omega_1(G) \triangleleft G$, and so $M = \langle s \rangle \cdot L \cong D_{2^{n+1}}$, by Suzuki's theorem (see Proposition 1.8) since $C_G(t) \cap M = \langle t, z \rangle$ is abelian of type $(2, 2)$. Because of the maximality of S (see (i–iv)), M is not normal in G (otherwise, A would normalize the dihedral subgroup M containing L properly, $A \cap M = \Omega_1(A)$ and $M \cap G_1 = D_1$, against the choice of S and L); moreover, the above argument shows also that M is not A -invariant. But L is normal in G so since $t \in L$, we get $A_0 = C_G(L) = C_A(L)$ (containing $\Omega_2(A)$, by assumption) is also normal in G and we have $A_0 = Z(S)$ which is of order ≥ 4 . We look at the structure of $\bar{G} = G/L$ which is a group with cyclic subgroup $\bar{S} = \bar{A} = (AL)/L \cong A/\langle z \rangle$ (bar convention!) of order 2^{m-1} and index 2 and with a subgroup $\bar{M} = M/L$ of order 2 which intersects \bar{A} trivially. Since M is not normal in G , we see that $\bar{G} = \bar{M} \cdot \bar{A}$, a semidirect product, is nonabelian. We conclude that $|\bar{A}| \geq 4$ so $m \geq 3$ since $\bar{A} = |A/\Omega_1(A)| < |A|$. Now $|A_0| \geq 4$ and so $|\bar{A}_0| \geq 2$ and \bar{A}_0 is normal in \bar{G} (recall that $A_0 = Z(S)$ is characteristic in S so normal in G) and $\bar{A}_0 \leq \bar{A}$. Since \bar{G}/\bar{A}_0 is a subgroup of the outer automorphism group of the dihedral group L , it follows that \bar{G}/\bar{A}_0 is abelian (see Proposition 34.8).

Suppose at first that \bar{G} is not of maximal class; in that case, $\bar{G} \cong M_{2^m}$, where $2^m = |A|$ (see Theorem 1.2), so that $\Omega_1(\bar{G}) = (UM)/L$ and $UM = \Omega_1(G)$ since U and M are generated by involutions. Since M is not normal in G , it follows that s must invert $Z(\Omega_1(S)) = \Omega_2(A)$ and so $\langle z, u, s \rangle \cong E_8$. Namely, if s centralizes $\Omega_2(A)$, then $\Omega_1(G) = \Omega_2(A) * M$, the central product, and each involution in G

lies in $M \cup U$ and so M would be characteristic in $\Omega_1(G)$ so normal in G , which contradicts the maximal choice of S since $S < AM$ (see (i–iv)). If we set $A = \langle a \rangle$, then $N_G(M) = M\langle a^2 \rangle$ which follows from the structure of $\bar{G} \cong M_{2^m}$ (see Theorem 1.2). Since $\Omega_2(A)$ centralizes L but $\Omega_2(A)/\langle z \rangle$ acts faithfully on M , it follows that $\langle a^2 \rangle/\langle z \rangle$ acts faithfully on M and so $\langle a^2 \rangle/\Omega_2(A)$ acts faithfully on L and $C_G(L) = \Omega_2(A) = A_0$. It follows that $Z(G) < A_0 = \Omega_2(G)$ is of order 2 and $A/\Omega_2(A)$ acts faithfully on L (since the cyclic group $\mathfrak{V}_1(A)/\Omega_2(A)$, as we saw, acts faithfully on L). We have $m \geq 4$ since $\bar{G} \cong M_{2^m}$ in view of the fact that \bar{G} is not of maximal class, by the assumption of this paragraph; we conclude that $|\bar{A}| \geq 8$. One may assume that the involution s acts on $L = \langle b, t \rangle$ as follows: $b^s = b^{-1}$ and $t^s = tb$ and we set $b^{2^{n-2}} = z$, where z generates $Z(G)$. Replacing a with a^r (r is odd), one may assume that $b^a = b^{1+2^i}$, $i \geq 2$, because $C_L(a) \geq D_1 \cong D_8$. Hence we have $C_L(a) \cong D_{2^{i+1}}$ and so $C_L(a^{2^{m-2}}) \cong D_{2^{i+m-1}} \cong L \cong D_{2^n}$, where we have taken into account that $A/\langle a^{2^{m-2}} \rangle = A/\Omega_2(A)$ acts faithfully on L and $\Omega_2(A)$ centralizes L . Thus, $i+m-1 = n$ and so $i = n-m+1$. Since $i \geq 2$, we must have $n \geq m+1$. Because $m \geq 4$, we have here $n \geq 5$. It remains to determine the commutator $[a, s]$. We know that $A = \langle a \rangle$ does not normalize M (indeed, $G = AM$ and M is not normal in G) and so $\langle [\bar{a}, \bar{s}] \rangle = \bar{A}_0$ which yields $[a, s] = a_0l$, where a_0 , a generator of A_0 , has order 4, $a_0^2 = z$ and $l \in L$. We can also write $[a, s] = (a_0z)(zl) = (a_0a_0^2)(zl) = a_0^{-1}(zl)$, and so replacing l with zl , if necessary, one may assume that $a_0 = a^{2^{m-2}}$ and s inverts $\langle a_0 \rangle$. Hence we get $[a, s] = a^{-1}sas = a_0l$ and so $s^a = a_0ls$. Since, by the previous equality, a_0ls is an involution, we must have $l = b^j$ for a suitable integer j . Therefore, $t^{a^{-1}sa} = t^{a_0b^js}$ which yields $b^a = b^{1-2j}$. On the other hand, $b^a = b^{1+2^i}$ and so $j \equiv -2^{i-1} \pmod{2^{n-2}}$. This yields

- (1) $s^a = a^{2^{m-2}}b^{-2^{i-1}}s$ or
- (2) $s^a = a^{2^{m-2}}b^{-2^{i-1}}sz$.

However, replacing b with $b' = b^{1-2^{n-i-1}}$ and t with $t' = tb^{2^{n-i-2}}$, we see that all so far obtained relations in this case go into the same relations with b' instead of b but the relation (1) goes into relation (2). (Note that $L = \langle b, t \rangle = \langle b', t' \rangle$). Therefore we may choose relation (1). We have determined in this case the structure of G uniquely and this the group given in part (f) of the theorem.

Suppose now that $\bar{G} = G/L$ is of maximal class. Since \bar{G}/\bar{G}' is of order 4 and \bar{G}/\bar{A}_0 is abelian, we have $|\bar{A} : \bar{A}_0| \leq 2$.

We consider at first the case $\bar{A} = \bar{A}_0$ which means that $A = C_G(L)$ and so $S = A * L$ (a central product) with $A \cap L = \langle z \rangle = Z(L)$. Hence $A = Z(S)$ and so A is normal in G . Since $A\langle s \rangle/\langle z \rangle$ is of maximal class and the case $[A, s] \leq \langle z \rangle$ is not possible because $M = \langle s \rangle \cdot L$ is not normal in G , we have either $a^s = a^{-1}$ or $a^s = a^{-1}z$, which is possible only when $m \geq 3$. Our group is isomorphic to a group $F(m, n)$ as stated in part (g). Also we have here $\langle z, u, s \rangle \cong E_8$.

It remains to consider the case where $|\bar{A} : \bar{A}_0| = 2$ so that $C_G(L) = A_0$ is of index 2 in A . We have $A_0 = \langle a^2 \rangle = Z(S)$ and so a induces an automorphism of

order 2 on L with $C_L(a) \geq D_1$. This yields at once that $b^a = bz$ and so $n \geq 4$. Hence we also have $a^b = az$. Since $[A, L] = \langle z \rangle$ and $L/\langle z \rangle$ is a dihedral group of order $2^{n-1} \geq 8$, it follows that $C_S(L/\langle z \rangle) \cong A * \langle b' \rangle$, where $\langle b' \rangle$ is a cyclic subgroup of order 4 in L . Hence $A * \langle b' \rangle$ is normal in G since $L/\langle z \rangle$ is G -invariant. If s normalizes A , then $a^s = a^{-1}z^\nu$, $\nu = 0, 1$, since $A\langle s \rangle/\langle z \rangle$ is of maximal class. But from $sts = tb$ we get acting on a : $a^{sts} = a^{tb}$ which yields $az = a$. Indeed, $a^{sts} = (a^{-1}z^\nu)^{ts} = (a^{-1}z^\nu)^s = az^\nu z^\nu = a$, and this is a contradiction. Hence s does not normalize A . Since $A^s \leq A^*\langle b' \rangle$ and $(A\langle b' \rangle/\langle b' \rangle)\langle s \rangle$ is of maximal class, one may set

$$(3) \quad a^s = a^{-1}b' \text{ or}$$

$$(4) \quad a^s = a^{-1+2^{m-2}}b'.$$

We must have $a^{s^2} = a^1 = a$. But in case (3) this yields $(a^{-1}b')^s = a$ and so $az = a$, which is a contradiction. Hence we must have relation (4). Replacing a with a^{-1} in (4), we get $(a^{-1})^s = (a^{-1})^{-1+2^{m-2}}(b')^{-1}$ and other relations in this case are not changed. Thus one may put $b' = b^{2^{m-3}}$ in (4). This determines the group G as stated in part (h) of the theorem. Here we have also $\langle z, u, s \rangle \cong E_8$.

An inspection of obtained groups shows that in any case G has no elementary abelian subgroups of order 16. Indeed, S has no elementary abelian subgroups of order 8 since S/L is cyclic and L is dihedral. It follows from $|G : S| \leq 2$ that G has no elementary abelian subgroups of order 16, as desired. It follows from defining relations of G that it is generated by 3 elements. Also in case where G has an elementary abelian group of order 8, we see that $Z(G)$ has order 2. The proof is complete. \square

Since G of Theorem 48.1 has no normal subgroups isomorphic to E_8 , each subgroup of G is generated by 4 elements, by MacWilliams' theorem [MacW]. (See the proof of this theorem of MacWilliams in §50.)

Let $G = U \wr V$, where $U \cong C_{2^m}$ and $V = \langle t \rangle \cong C_2$. Then $C_G(t) = \langle t \rangle \times C$, where C , the diagonal of $U \times U^t$, is cyclic of order 2^m , $Z(G) = C$.

Exercise 2. Let L be a subgroup of maximal class in a 2-group G . Suppose that, whenever an involution $s \in G - L$, then $\langle s, L \rangle$ is of maximal class. Is G of maximal class?

Solution. Yes. If $G - L$ has no involutions, G is of maximal class, by Theorem 1.17(a). So suppose that $G - L$ has an involution. Assume that G is a counterexample of minimal order. Then $|G : L| > 2$ and all maximal subgroups of G containing L are of maximal class. The number of maximal subgroups of G containing L which are of maximal class is even (see §13). Since the number of maximal subgroups of G containing L is odd, we get a contradiction.

Exercise 3. Let t be an involution of a 2-group G such that $C_G(t) = \langle t \rangle \times Q$, where $Q \cong Q_{2^m}$. Prove that (i) G has no normal elementary abelian subgroups of order 8, (ii) $|N_G(C_G(t)) : C_G(t)| \leq 2$.

Exercise 4. Let G be a nonabelian p -group, p is odd. Suppose that G has an element t of order p such that $C_G(t) = \langle t \rangle \times C$, where C is cyclic of order p^m , $m > 1$. Prove that G has no $\langle t \rangle$ -invariant subgroups of order p^{p+1} and exponent p . (*Hint.* Use Theorem 9.6.)

Problems

Problem 1. Classify the 2-groups G containing an abelian subgroup A of type $(4, 2)$ such that $C_G(A) = A$.

Problem 2. Classify the 2-groups containing a cyclic subgroup Z of order 4 such that $C_G(Z) = Z \times C_2$. (For a solution, see §77.)

Problem 3. Let a 2-group G admit an automorphism α of order 2 and set $C_G(\alpha) = Q$, where Q is either cyclic or of maximal class. Describe the structure of G . (See §51.)

Problem 4. Classify the 2-groups G containing an involution t such that $C_G(t) = \langle t \rangle \times M_{2^m}$.

Problem 5 (Janko). Classify the 2-groups G such that $C_G(E) = E$ for some elementary abelian subgroup E of order 8. (For solution, see §51.)

Problem 6 (Blackburn). Classify the nonabelian p -groups G , $p > 2$, containing an element t of order p such that $C_G(t) = \langle t \rangle \times C$, where $C \cong C_{p^m}$, $m > 1$.

Problem 7. Classify the 2-groups G containing a nonabelian subgroup D of order 8 such that $|C_G(D)| = 4$.

Problem 8. Study the 2-groups G containing an extraspecial subgroup E of order $> 2^3$ such that $C_G(E) = Z(E)$.

Problem 9. Study the 2-groups G containing a subgroup $M \cong M_{2^n}$ such that we have $C_G(M) = Z(M)$.

§49

On 2-groups with small centralizer of an involution, II

In the previous section finite 2-groups G have been classified with the property that G has an involution t such that $C_G(t) = \langle t \rangle \times C$, where $C \cong C_{2^m}$ is a cyclic group of order 2^m , $m \geq 1$.

There is one more case of the centralizer of an involution in 2-groups which is very important. This is seen from the following “conditionless” Theorem 10.26:

For a finite p -group G , one of the following holds:

- (a) G has no maximal elementary abelian subgroups of order p^2 .
- (b) $|\Omega_1(G)| \leq p^2$.
- (c) There exists in G an element x of order p such that $C_G(x) = \langle x \rangle \times Q$, where Q is cyclic or generalized quaternion.

In this section we classify the finite 2-groups G which possess an involution t such that $C_G(t) = \langle t \rangle \times Q$, where $Q \cong Q_{2^m}$ is generalized quaternion of order 2^m , $m \geq 3$. Of course, the situation becomes more complicated; however, in spite of that, the exposition remains elementary.

From the start, it is clear, that such a group G cannot be of maximal class. Then, by the known results, G must contain a normal four-subgroup U . We have two essentially different possibilities according to $t \in U$ or $t \notin U$.

In the first case, where $t \in U$, we have either $C_G(t) = G$ or the order of G is equal to 2^{m+2} and then we get four classes of 2-groups which will be given in terms of generators and relations (see Theorem 49.1).

In the second case, where $t \notin U$ (Theorem 49.2), the situation is more complicated since the order of G is not bounded with the parameter m . In fact, in some cases with given $m \geq 3$, we get infinitely many 2-groups with the same centralizer of our involution t . The idea of the proof in the second case is to construct certain large subgroup S of the known structure with $UC_G(t) \leq S$ and then to show that S is normal in G and that $|G/S| \leq 4$. This last “closure” argument is the main trick in the proof. The corresponding argument in the previous “cyclic” case, which was treated in the previous subsection, was considerably simpler. As a result, we obtain three different types of 2-groups G , since we have exactly three possibilities for the structure of S . In two of these types, the groups G could possess elementary abelian

subgroups of order 16 and in that case the corresponding series of 2-groups will be given in terms of generators and relations (Theorem 49.3). The first member of one of these series is a 2-group of order 2^7 which is isomorphic to a Sylow 2-subgroup of the simple group J_2 of order 604800. Finally, it turns out that the case $m = 3$ of an ordinary quaternion group $Q \cong Q_8$ is more difficult than the general case $m \geq 4$.

As a direct application of these results and the results in the previous subsection, we obtain a classification of 2-groups which have more than 3 involutions but which do not have an elementary abelian subgroup of order 8 (Theorem 49.4). Such groups have been considered by D. J. Rusin [Rus] by using a heavy cohomological machinery. Our methods are completely elementary.

Let $G = Q \text{ wr } C$, where $Q \cong Q_{2m}$ and $C = \langle t \rangle \cong C_2$. Then $C_G(t) = \langle t \rangle \times D$, where D is the diagonal of the base $Q \times Q^t$ so $D \cong Q_{2m}$.

Let G be a 2-group possessing an involution t such that $C_G(t) = \langle t \rangle \times Q$, where $Q \cong Q_{2m}$. We claim that then G has no normal elementary subgroups of order 8. Assume that this is false, and let $E \cong E_8$ be normal in G . Clearly, $t \notin E$. Set $H = \langle t \rangle \cdot E$. Then $C_H(t)$ contains an elementary abelian subgroup of order 8, by Proposition 1.8 (Suzuki's theorem), which is not the case. We see that the group G is one of the groups of §50. It follows from Theorem 50.3 that every subgroup of G is generated by four elements.

1^o. *The case $t \in U$.* In this subsection we prove the following

Theorem 49.1. *Let G be a 2-group containing an involution t such that $C_G(t) = \langle t \rangle \times Q$, where Q is a generalized quaternion group of order 2^m , $m \geq 3$. We assume, in addition, that t is contained in each normal four-subgroup U of G and that $G \neq C_G(t)$. Then we have the following possibilities:*

(A1) *If $t \notin \Phi(G)$, then G has a maximal subgroup M so that $G = M\langle t \rangle$, where $M \cong Q_{2m+1}$ or $M \cong SD_{2m+1}$ and $C_M(t) \cong Q_{2m}$.*

(A2) *If $t \in \Phi(G)$, then one of the following assertions holds:*

- (a) *$m = 3$ and $G = \langle t, u, v, w, y \mid y^2 = tv, w^2 = v^2 = u, u^2 = t^2 = [t, v] = [t, w] = 1, [v, w] = u, t^y = tu, v^y = v^{-1}, w^y = wt \rangle$. We have $|G| = 2^5$, $Z(G) = \langle u \rangle$ has order 2, $\Phi(G) = \langle t \rangle \times \langle v \rangle$ is abelian of type $(4, 2)$, $G' = \langle u, t \rangle$ is a four-group and $C_G(t) = \langle t \rangle \times \langle v, w \rangle$, where $\langle v, w \rangle \cong Q_8$. Also $G = \langle y, w \rangle$ and G has exactly three involutions.*
- (b) *$m \geq 4$ and $G = \langle a, b, t, u, x \rangle$, where $a^{2^{m-1}} = t^2 = [t, a] = [t, b] = [a, x] = 1, b^2 = a^{2^{m-2}} = u, a^b = a^{-1}, x^2 = a^{2^{m-3}}, b^x = bt, t^x = tu$. The order of G is 2^{m+2} , $Z(G) = \langle u \rangle$ is of order 2, $\Phi(G) = G' = \langle t \rangle \times \langle a^2 \rangle$ is abelian of type $(2^{m-2}, 2)$ and G is not an Ω -group since there exist involutions in $G - \langle a, b, t \rangle$ but G has no subgroups isomorphic to E_8 . Also, $G/\Phi(G)$ has order 8 and $C_G(t) = \langle t \rangle \times \langle a, b \rangle$, where $\langle a, b \rangle \cong Q_{2m}$ and $G = \langle a, b, x \rangle$.*

- (c) $m \geq 4$ and $G = \langle a, b, t, u, x \rangle$, where $a^{2^{m-1}} = t^2 = [t, a] = [t, b] = [a, x] = 1$, $b^2 = a^{2^{m-2}} = u$, $a^b = a^{-1}$, $x^2 = a^{1+2^{m-3}}$, $b^x = bat$, $t^x = tu$. The order of G is 2^{m+2} , $Z(G) = \langle u \rangle$ is of order 2, $\Phi(G) = \langle t \rangle \times \langle a \rangle$ is abelian of type $(2^{m-1}, 2)$ and $G' = \langle at \rangle$ is cyclic of order 2^{m-1} . Also, G has exactly 3 involutions, $G/\Phi(G)$ has order 4, $C_G(t) = \langle t \rangle \times \langle a, b \rangle$, where $\langle a, b \rangle \cong Q_{2^m}$ and $G = \langle b, x \rangle$.
- (d) $m \geq 5$ and $G = \langle a, b, t, u, x \rangle$, where $a^{2^{m-1}} = t^2 = [t, a] = [t, b] = x^2 = 1$, $b^2 = a^{2^{m-2}} = u$, $a^b = a^{-1}$, $t^x = tu$, $a^x = a^{1+2^{m-3}}t$, $b^x = b$. The order of G is 2^{m+2} , $Z(G) = \langle u \rangle$ is of order 2, $\Phi(G) = G' = \langle t \rangle \times \langle a^2 \rangle$. Also, G is not an Ω -group but G has no subgroups isomorphic to E_8 . We have $C_G(t) = \langle t \rangle \times \langle a, b \rangle$, where $\langle a, b \rangle \cong Q_{2^m}$ and $G = \langle a, b, x \rangle$, Here we have $C_G(x) \cong C_2 \times Q_{2^{m-2}}$.

Proof. Suppose that G satisfies the assumptions of the theorem and let U be a normal four-subgroup of G . By assumption, we have $t \in U$. Let $T = C_G(U)$, so that $|G : T| = 2$. We have $T = \langle t \rangle \times Q$, where $Q \cong Q_{2^m}$, $m \geq 3$. Set $\Omega_1(Q) = \langle u \rangle$ and then we have $U = \langle t, u \rangle = \Omega_1(T)$ and obviously $Z(G) = \langle u \rangle$.

We consider at first the easy case $t \notin \Phi(G)$. Let M be a maximal subgroup of G such that $t \notin M$. Then $G = \langle t \rangle \cdot M$ and, by the modular law, $C_G(t) = \langle t \rangle \times M_0$, where $M_0 = T \cap M \cong Q_{2^m}$. If M is not of maximal class, then by Lemma 1.4, M contains a G -invariant four-subgroup U_0 . But then $t \notin U_0$, which contradicts the assumption of our theorem. Thus, M is of maximal class and therefore $M \cong Q_{2^{m+1}}$ or $M \cong SD_{2^{m+1}}$ (see Theorem 1.2). There is an element $y \in M - M_0$ such that $y^2 \in \langle u \rangle = Z(M)$. We have $y^{-1}ty = ut$ so that $tyt = yu$ and this determines the action of t on M since all such y 's together with M_0 generate M . We have obtained the group G stated in part (A1) of the theorem.

We examine now the difficult case $t \in \Phi(G)$ and suppose at first that $Q \cong Q_8$ so that $\langle u \rangle = Z(Q) = Z(G) = \Phi(T)$ and $U = \langle t, u \rangle$. It follows from $u \in \Phi(Q) \leq \Phi(G)$ and $U \not\leq Z(G)$ that $U < \Phi(G)$, by Exercise 1(b3). Since $\Phi(G) < T$, we get, by the modular law, $\Phi(G) = \langle t \rangle \times \langle v \rangle$, where $\langle v \rangle$ is a cyclic subgroup of order 4 in Q and $v^2 = u$; then $\Phi(G)$ is abelian of type $(4, 2)$ and G is generated by two elements. Because in case of 2-groups $\Phi(G) = \mathfrak{U}_1(G)$ and here we have $\Phi(G) > U$, it follows that there are elements $y, z \in G - T$ so that $y^2 = tv$ and $z^2 = v$ since t and tu are not squares. Next, $\langle y \rangle \not\trianglelefteq G$ (otherwise, G is metacyclic since $G/\langle y \rangle$ is cyclic in view of $\Phi(G) \not\leq \langle y \rangle$). Similarly, $\langle z \rangle \not\trianglelefteq G$. If z normalizes Q , then $\langle Q, z \rangle$ is of maximal class and order 16, by Theorem 1.2, a contradiction since $\Phi(G)$ is not isomorphic to subgroup of a 2-group of maximal class. Thus, y does not normalize Q so Q is not normal in G . It follows that the core $\langle z \rangle_G = \langle v \rangle$ (let us consider the representation of G by permutations of left cosets of $\langle z \rangle$). Since $c_2(\Phi(G)) = 2$, $\langle vt \rangle$ is also normal in G . We have $t^y = tu = t^z$, by Exercise 1(b2). It follows from $tv = (tv)^y = t^yv^y = tuv^y$ that $v^y = vu = v^3 = v^{-1}$. Take an element $w \in Q - \langle v \rangle$ so that $Q = \langle v, w \rangle$. Since $G/\Phi(G)$ is abelian and $Q \not\trianglelefteq G$, $\langle v \rangle \triangleleft G$, we

have $w^y = wv^r t$ for some integer r . If r is odd, then $[w, y] = v^r t = (vt)^r$. Thus, modulo $\langle vt \rangle$, elements w , y and v are pairwise permutable. Since $G = \langle Q, y \rangle = \langle v, w, y \rangle$ and $v^2 = w^2 = u$ and $y^2 = vt$ are contained in $\langle vt \rangle$, we see that $G/\langle vt \rangle$ is elementary abelian, contrary to the fact that $\Phi(G)$ is noncyclic. Thus, r is even, and we get $w^y = wt$ or $w^y = wut = w^{-1}t$. However, if $w^y = w^{-1}t$, then replacing y with yv , we get $w^{yv} = (w^{-1}t)^v = wt$ and other relations remain unchanged: $t^{yv} = tu$, $v^{yv} = v^{-1}$, $(yv)^2 = yvyv = y^2v^yv = tvv^{-1}v = tv$. Hence we may assume from the start that $w^y = wt$. The structure of the group G of order 2^5 is uniquely determined and this is the group stated in part (A2)(a) of our theorem.

We turn now to the general case $Q \cong \mathrm{Q}_{2^m}$, $m \geq 4$. Let a be an element of order 2^{m-1} in Q so that $\langle a \rangle$ is the unique cyclic subgroup of index 2 in Q . Here $C_G(t) = \langle t \rangle \times Q = T = C_G(U)$, where $U = \langle t, u \rangle$ is the G -invariant four-subgroup in T , $\langle u \rangle = Z(Q) = Z(G)$ and $\langle u \rangle < \langle a \rangle$. Now, $T/U \cong Q/\langle u \rangle \cong \mathrm{D}_{2^{m-1}}$ so that $\langle a, U \rangle/U$ is the unique cyclic subgroup of T/U of order $2^{m-2} \geq 4$ and so $L = \langle a, U \rangle = \langle t \rangle \times \langle a \rangle$ is normal in G . If $b \in Q - \langle a \rangle$, then $b^2 = u$ and $a^b = a^{-1}$. Taking any $x \in G - T$, we have $t^x = tu$ and $a^x \in L$. If x does not normalize $\langle a \rangle$, then $\langle a \rangle \cap \langle a^x \rangle$ is an x -invariant subgroup of index 2 in $\langle a \rangle$ since $|L : \langle a \rangle| = 2$ (here we use the product formula). Hence, in any case, $\langle a^2 \rangle$ is a cyclic normal subgroup of order $2^{m-2} \geq 4$ of G . In particular, the cyclic subgroup $\langle v \rangle$ of order 4 contained in $\langle a^2 \rangle$ is normal in G . Thus, $A = \langle t \rangle \times \langle v \rangle$ is a normal abelian subgroup of type $(4, 2)$ in G . We have $C_G(A) = L$ so that G/L acts as an automorphism group of order 4 on A . Since $\langle v \rangle$ is normal in G and $v^b = v^{-1}$, so there is an element x in $G - T$ with $v^x = v$ and also $t^x = tu = tv^2$. Indeed, $C_G(v)$ is a maximal subgroup of G different of T so as x we can take every element in $C_G(v) - T$. Since $t^b = t$, we see that b and x induce two distinct involutory automorphisms on A and therefore G/L is an elementary abelian group of order 4 (recall that $b \notin L$ and $t, v \in L$). In particular, we get that $\Phi(G) \leq L$. On the other hand, $\Phi(G) \geq \langle t, a^2 \rangle$. Hence we have either $\Phi(G) = L = \langle t, a \rangle$ or $\Phi(G) = \langle t, a^2 \rangle (< L)$. In any case, $x^2 \in L$ since $\exp(G/L) = 2$ and so x induces an automorphism of order 2 on L such that $t^x = tu$, $\langle a^2 \rangle^x = \langle a^2 \rangle$ and x centralizes the subgroup $\langle v \rangle$ of order 4 which is contained in $\langle a^2 \rangle$. Therefore, we have $a^x = a^j t^i$, where $i = 0, 1$ and an integer j is odd (otherwise, $o(a^j t^i) < o(a)$). Since x normalizes $\langle a^2 \rangle$ and centralizes $\langle v \rangle \leq \langle a^2 \rangle$, we have either $(a^2)^x = a^2$ or $(a^2)^x = a^2 u$ (indeed, if x does not centralize a^2 , then $\langle x, a^2 \rangle / C_{\langle x \rangle}(a^2) \cong \mathrm{M}_{2^{m-1}}$, by Theorem 1.2); in particular, in the case under consideration, $m \geq 5$. If $(a^2)^x = a^2$, we obtain $a^x = at^i$ or $a^x = aut^i$. Indeed, $(a^2)^x = a^{2j}$ so $j \equiv 1 \pmod{2^{m-2}}$; then $a^j = a$ or $a^j = au$. If $(a^2)^x = a^2 u$, we get $a^x = avt^i$ or $a^x = auvt^i$, where we set $v = a^{2^{m-3}}$. Indeed, then $j \equiv 1 + 2^{m-2}$ so $a^j = av$ or $a^j = auv$. As we established above, we must have in the case where x does not centralize a^2 , $o(a^2) \geq 8$ and so $m \geq 5$.

Let $a^x = at^i$ or $a^x = aut^i$, where $m \geq 4$ and $o(a) = 2^{m-1}$. If $a^x = aut^i$, then replacing a with at , we get $(at)^x = aut^i tu = (at)t^i$. Note that $\langle at, b \rangle = Q_0 \cong \mathrm{Q}_{2^m}$ and also $C_G(t) = \langle t \rangle \times Q_0$. Hence we may assume from the start that $a^x = at^i$,

$i = 0, 1$. However, if $a^x = at$, then we compute $a = a^{x^2} = (at)^x = attu = au$, which gives $u = 1$ and this is a contradiction. It follows that $a^x = a$. If $x^2 = ta^j$ with an integer j , then $C_G(x) \geq \langle a, ta^j \rangle = L$, which is a contradiction since $x \notin L = C_G(L)$. Hence we have $x^2 \in \langle a \rangle$. If $b^x \in Q$, then $\langle x \rangle$ normalizes $Q = \langle a, b \rangle$ and since $x^2 \in \langle a \rangle$, so $Q\langle x \rangle$ would be a maximal subgroup of G which does not contain $t \in \Phi(G)$, a contradiction. It follows that $b^x = b't$, where b' is an element of order 4 contained in $Q - \langle a \rangle$. There are exactly two conjugacy classes of elements of order 4 in $Q - \langle a \rangle$ with the representatives b and ba . Thus, replacing x with xa^k for some integer k , we may assume that $b^x = bt$ or $b^x = bat$.

Let $b^x = bt$. We compute $b^{x^2} = (bt)^x = bttu = b^{-1}$ and so $x^2 \in \langle v \rangle$, where v is an element of order 4 in $\langle a \rangle$. Hence, we may set $x^2 = a^{2^{m-3}}$ or $x^2 = a^{2^{m-3}}u$ because these elements are the only elements of order 4 in $\langle a \rangle$. If $x^2 = a^{2^{m-3}}u$, then we replace x with xt . Then $xt \in G - T$, xt centralizes $\langle a \rangle$, $b^{xt} = (bt)^t = bt$ and finally $(xt)^2 = xttx = x^2t^xt = a^{2^{m-3}}utut = a^{2^{m-3}}$. Hence, we may assume from the start that $x^2 = a^{2^{m-3}}$ and so the structure of G is uniquely determined in this case. We see that here $\Phi(G) = \langle t \rangle \times \langle a^2 \rangle = G'$ and $G = \langle a, b, x \rangle$. Also, $xa^{2^{m-4}}t$ is an involution in $G - \langle a, b, t \rangle$. We have obtained the group stated in part (A2)(b).

Now let $b^x = bat$. We compute $b^{x^2} = (bat)^x = batatu = ba^2u$. On the other hand, by setting $v = a^{2^{m-3}}$, we see that $b^{a^{1+2^{m-3}}} = b^{av} = ba^2u$. Hence, we may set $x^2 = av$ or $x^2 = avu$. Note that the group $\langle a \rangle / \langle u \rangle$ produces by conjugation exactly 2^{m-3} distinct conjugates of b . However, if $x^2 = avu$, then similarly as before, we replace x with xt so that we obtain $(xt)^2 = xttx = x^2t^xt = avutut = av$ and all other relations remain unchanged. Hence, we may assume that $x^2 = av = a^{1+2^{m-3}}$ and the group G is again uniquely determined. Here we have $\Phi(G) = \langle t \rangle \times \langle a \rangle = L$ and our group $G = \langle x, b \rangle$ is 2-generated. Also, we see that $G' = \langle at \rangle$ and there are no involutions in $G - T$. Therefore G has exactly 3 involutions. We have obtained the group stated in part (A2)(c).

Now let $a^x = avt^i$ or $a^x = auvt^i$, where $v = a^{2^{m-3}}$, $m \geq 5$. If $a^x = auvt^i$, then replacing a with at (as above) we get $(at)^x = auvt^itu = (at)vt^i$. Hence we may assume from the start that $a^x = avt^i$, $i = 0, 1$. However, if $a^x = av$, then $a = a^{x^2} = (av)^x = (av)v = av^2 = au$, which gives $u = 1$ and this is a contradiction. It remains only the case $a^x = avt$. We note that $x^2 \in L$ and $C_L(x) = \langle a^4, x^2 \rangle$, where $\langle v \rangle \leq \langle a^4 \rangle$ since $o(a) = 2^{m-1} \geq 16$. All elements in $T - L$ are of order 4. There are exactly four conjugate classes of such elements in $T - L$ and under the action of $\langle a \rangle$ each such element is conjugate to one of the following four elements: b , ba , bt , bat , where $\langle a, b \rangle = Q \cong Q_{2^m}$. So replacing x with xa^k for some integer k (note that xa^k also centralizes v), we may assume that we have one of the following four possibilities: $b^x = b$, $b^x = bt$, $b^x = ba$ or $b^x = bat$. If $b^x = ba$, then $b^{x^2} = (ba)^x = baavt = ba^2vt$, which is a contradiction since $x^2 \in L < T$ and Q is normal in T . Similarly, if $b^x = bat$, then $b^{x^2} = (bat)^x = batavttu = ba^2vut$, which is a contradiction since Q is normal in T . If $b^x = bt$, then we replace b with $b' = ba$

and x with $x' = xa^{-2^{m-4}}$ (which also centralizes $v = a^{2^{m-3}}$). We compute $(b')^{x'} = (ba)^{xa^{-2^{m-4}}} = (btavt)a^{-2^{m-4}} = bb^{-1}a^{2^{m-4}}ba^{-2^{m-4}}av = ba^{-2^{m-4}}a^{-2^{m-4}}av = bv^{-1}av = ba = b'$. Hence we may assume from the start that $b^x = b$. In this case $x^2 \in C_L(b) = \langle t, u \rangle = U$. Since $C_G(U) = T$, we must have $x^2 \in \langle u \rangle = Z(G)$. If $x^2 = u$, then replacing x with xt , we get $(xt)^2 = xtvt = x^2t^xt = utut = 1$ and other relations remain unchanged: $a^{xt} = (avt)^t = avt$ and $b^{xt} = b^t = b$, Hence we may assume that $x^2 = 1$ and so the structure of G is uniquely determined as given in part (A2)(d). \square

2°. The case $t \notin U$. In this subsection we examine the difficult case, where our 2-group G has a normal four-subgroup U such that an involution $t \in G$ is not contained in U and $C_G(t) = \langle t \rangle \times Q$ with $Q \cong Q_{2^m}$, $m \geq 3$.

In order to formulate our main result, we shall define three types of 2-groups: $A(m, n)$, $B(m, n)$ and $C(m, n)$, $m, n \in N$.

Definition. Let $S = QL$ be a product of two normal subgroups $Q = \langle a, b \mid a^{2^{m-1}} = b^4 = z^2 = 1, a^{2^{m-2}} = b^2 = z, a^b = a^{-1} \rangle \cong Q_{2^m}$ and $L = \langle c, t \mid c^{2^{n-1}} = t^2 = z^2 = 1, c^{2^{n-2}} = z, c^t = c^{-1} \rangle \cong D_{2^n}$, where $m \geq 3, n \geq 3$ and $Q \cap L = Z(Q) = Z(L) = \langle z \rangle$.

If $[Q, L] = 1$, then $S = Q * L$ is the central product of Q and L which we denote with $A(m, n)$ for $m \geq 3, n \geq 3$.

If $C_Q(L) = \langle a \rangle$ and $t^b = t, c^b = cz$, then so determined group S we denote with $B(m, n)$ for $m \geq 3, n \geq 4$.

If $C_Q(L) = \langle a^2, b \rangle \cong Q_{2^{m-1}}$, $m \geq 4$ and $t^a = t, c^a = cz$, then so determined group S we denote with $C(m, n)$ for $m \geq 4, n \geq 4$.

Obviously, $|G| = 2^{m+n-1}$.

Theorem 49.2. *Let G be a 2-group containing an involution t such that $C_G(t) = \langle t \rangle \times Q$, where Q is a generalized quaternion group of order 2^m , $m \geq 3$. We assume, in addition, that G has a normal four-subgroup U such that $t \notin U$. Then G has a normal subgroup S containing $UC_G(t)$ such that $|G/S| \leq 4$ and S is isomorphic to one of the groups $A(m, n)$, $B(m, n)$ or $C(m, n)$. If $S \cong B(m, n)$, then we must have $S = G$. If $S \cong C(m, n)$, then $|G/S| \leq 2$ and if, in addition, $|G/S| = 2$, then we have $m = n$. Finally, if $|G/S| = 4$, then we must have $S \cong A(m, m)$ and G acts transitively on the set of involutions in $S - U$.*

Proof. Let $E_4 \cong U \triangleleft G$ with $t \notin U$. Set $T = C_G(U)$ and then we have obviously $t \notin T$. This gives $|G : T| = 2$ and so $G = \langle t \rangle T$. By the modular law, $G_0 = C_G(t) = \langle t \rangle \times Q$, where $Q = C_T(t) \cong Q_{2^m}$, $m \geq 3$, and so $Z = \langle z \rangle = \Omega_1(Q) = Z(Q) = C_U(t) = Z(G)$. Set $G_1 = N_G(G_0)$. Since $|UG_0| : |G_0| = 2$, we have $UG_0 \leq G_1$. It follows from $\Omega_1(G_0) = \langle t, z \rangle$ that t has exactly two conjugates t and tz in G_1 . Therefore, $|G_1 : C_{G_1}(t)| = |G_1 : G_0| = 2$ so $G_1 = UG_0$. Set $D_0 = U\langle t \rangle$ so that $D_0 \cong D_8$, $[Q, D_0] = \{1\}$ with $Q \cap D_0 = \langle z \rangle$ and $U = \langle z, u \rangle <$

D_0 so $G_1 = Q * D_0$, by the product formula. Let v be an element of order 4 in D_0 and let y be an element of order 4 in $\langle a \rangle$, where $Q = \langle a, b \mid a^{2^{m-1}} = b^4 = z^2 = 1, a^{2^{m-2}} = b^2 = z, a^b = a^{-1} \rangle \cong Q_{2^m}$, $m \geq 3$. Since $y^2 = v^2 = z$, we get $(yv)^2 = y^2v^2 = y^4 = 1$ so $x = yv$ is an involution in $G_1 - D_0$. But $x^t = (yv)^t = yv^{-1} = yvv^2 = yvz = xz$ and therefore $D_1 = \langle x, t \rangle \cong D_8$ and $D_1 \cap U = Z(D_1) = \langle z \rangle$. We see that $C_{G_1}(D_1) = \langle a, bt \rangle = Q_1 \cong Q_{2^m}$ because $x^{bt} = (yv)^{bt} = y^{-1}v^{-1} = yv = x$, $(bt)^2 = z$ and $a^{bt} = a^{-1}$. Thus we have $G_1 = Q_1 * D_1$ with $Q_1 \cong Q$, $Q_1 \cap D_1 = \langle z \rangle$, $C_G(t) = \langle t \rangle \times Q = \langle t \rangle \times Q_1$ and $U = \langle z, u \rangle \not\leq D_1$. Denoting again Q_1 with Q and bt with b , we have obtained the following initial result.

(R) Supposing that $U = \langle z, u \rangle$ is a normal four-subgroup of our 2-group G possessing an involution t with $t \notin U$ and $C_G(t) = \langle t \rangle \times Q$, where $Q \cong Q_{2^m}$, $m \geq 3$, then $G_1 = UC_G(t)$ has the following structure. We have $G_1 = Q * D_1$, where $D_1 \cong D_8$, $t \in D_1$, $Q \cap D_1 = \langle z \rangle = Z(G)$ and $U \not\leq D_1$.

The next step in the proof is to “blow up” the subgroup $G_1 = UC_G(t)$ as much as possible so that the structure of a large subgroup S containing G_1 remains “about” the same as the structure of G_1 .

In the rest of the proof, we denote with S a subgroup of G of the maximal possible order subject to the following conditions:

- (i) $S \geq G_1 = UC_G(t) = Q * D_1$, where $Q \cong Q_{2^m}$, $m \geq 3$, $D_1 \cong D_8$, $t \in D_1$.
- (ii) $S = QL$, where L is normal in S , $L \cong D_{2^n}$, $n \geq 3$, $Q \cap L = \langle z \rangle = Z(Q) = Z(L)$, $L \geq D_1$.
- (iii) $U = \langle z, u \rangle \not\leq L$.

In the sequel, we fix the following notation. We set $Q = \langle a, b \mid a^{2^{m-1}} = b^4 = z^2 = 1, a^{2^{m-2}} = b^2 = z, a^b = a^{-1} \rangle \cong Q_{2^m}$ and $L = \langle c, t \mid c^{2^{n-1}} = t^2 = z^2 = 1, c^{2^{n-2}} = z, c^t = c^{-1} \rangle \cong D_{2^n}$, where $m \geq 3$, $n \geq 3$ and $Q \cap L = Z(Q) = Z(L) = \langle z \rangle$. Then we have $u = yv$, where y is an element of order 4 in $\langle a \rangle$ and v is an element of order 4 in $\langle c \rangle$. If $a^4 = 1$, then we put $y = a$. Similarly, if $c^4 = 1$, then we put $v = c$.

At first we shall determine the structure of S . Act with Q on the dihedral group L . Since $\text{Aut}(L)/\text{Inn}(L)$ is abelian of type $(2^{n-3}, 2)$ (see Theorem 34.8), so $Q' = \langle a^2 \rangle$ centralizes L . Also, we know that Q centralizes $\langle v, t \rangle = D_1 \cong D_8$. It follows that either Q centralizes L and then $S = Q * L \cong A(m, n)$, $m \geq 3$, $n \geq 3$ or $M = C_Q(L)$ is a maximal subgroup of Q , in which case $n \geq 4$. We have essentially two different possibilities for M . First possibility is $M = \langle a \rangle$, $t^b = t$, $c^b = cz$ and then $S \cong B(m, n)$, $m \geq 3$, $n \geq 4$. Second possibility is $M = \langle a^2, b \rangle \cong Q_{2^{m-1}}$, $m \geq 4$, $t^a = t$, $c^a = cz$ and then $S \cong C(m, n)$, $m \geq 4$, $n \geq 4$. We see that we have in any case $[Q, L] \leq \langle z \rangle$ and so Q is a normal subgroup in S .

Suppose that $S \cong B(m, n)$. Then S has exactly six conjugacy classes of involutions contained in $S - U$ with the representatives t , tc , bv , bav , btc , $batc$. The

corresponding centralizers are:

$$\begin{aligned}
 C_S(t) = C_G(t) &= \langle t \rangle \times Q && \text{with} && Q \cong Q_{2^m}, \quad m \geq 3, \\
 C_S(tc) &= \langle tc \rangle \times \langle a, bv \rangle && \text{with} && \langle a, bv \rangle \cong D_{2^m}, \\
 C_S(bv) &= \langle bv \rangle \times \langle cy, tc \rangle && \text{with} && \langle cy, tc \rangle \cong SD_{2^n}, \\
 C_S(bav) &= \langle bav \rangle \times \langle cy, tc \rangle && \text{with} && \langle cy, tc \rangle \cong SD_{2^n}, \\
 C_S(btc) &= \langle btc \rangle \times \langle by, u \rangle && \text{with} && \langle by, u \rangle \cong D_8, \\
 C_S(batc) &= \langle batc \rangle \times \langle bay, u \rangle && \text{with} && \langle bay, u \rangle \cong D_8.
 \end{aligned}$$

It follows that t cannot be fused in $N_G(S)$ to any of the other five conjugacy classes of involutions in $S - U$. But $C_S(t) = C_G(t)$ then forces that $S = G$.

We make here the following simple observation. Since $t \in G - T$, where $T = C_G(U)$ and $|G : T| = 2$, t cannot be conjugate (fused) in G to any involution t' which centralizes U . Therefore, with respect to that fusion, it is enough to consider only those involutions in S which act faithfully on U .

Now suppose that $S \cong C(m, n)$. Then S has exactly four conjugacy classes of involutions contained in $S - U$ acting faithfully on U with the representatives t , tc , bv , and bav . The corresponding centralizers in S are:

$$\begin{aligned}
 C_S(t) = C_G(t) &= \langle t \rangle \times Q && \text{with} && Q \cong Q_{2^m}, \quad m \geq 4, \\
 C_S(tc) &= \langle tc \rangle \times \langle av, bav \rangle && \text{with} && \langle av, bav \rangle \cong SD_{2^m}, \\
 C_S(bv) &= \langle bv \rangle \times \langle c, yt \rangle && \text{with} && \langle c, yt \rangle \cong Q_{2^n}, \\
 C_S(bav) &= \langle bav \rangle \times \langle cy, ct \rangle && \text{with} && \langle cy, ct \rangle \cong SD_{2^n}.
 \end{aligned}$$

We may assume that $N_G(S) \neq S$ (otherwise we are finished). Then $N_G(S)$ can fuse the conjugacy class of t only with the conjugacy class of bv under the assumption that $m = n$ and then $|N_G(S) : S| = 2$. Then $\text{ccls}(t)$, the conjugacy class of t in S containing t , equals $\{tc^{2^i}, 1 \leq i \leq 2^{m-2}\}$ and $C_S(tc^{2^i}) = \langle tc^{2^i} \rangle \times Q$ so that $(C_S(tc^{2^i}))' = \langle a^2 \rangle$. Similarly, we have $\text{ccls}(bv) = \{ba^{2^j}v, 1 \leq j \leq 2^{m-2}\}$, $C_S(ba^{2^j}v) = \langle ba^{2^j}v \rangle \times \langle c, yt \rangle$, where $\langle c, yt \rangle \cong Q_{2^m}$ so that $(C_S(ba^{2^j}v))' = \langle c^2 \rangle$. Hence for any $x \in N_G(S) - S$, we have $t^x = ba^{2^j}v$ for some j and so, by the above, $\langle a^2 \rangle^x = \langle c^2 \rangle$. Assume now that $N_G(S) \neq G$ (otherwise we are finished). Since $C_S(t) = C_G(t)$ and $N_G(S)$ already fuses the involutions in $\text{ccls}(t)$ with involutions in $\text{ccls}(bv)$, so there is an element $s \in N_G(N_G(S)) - N_G(S)$ with $s^2 \in N_G(S)$ and $t^s = t^s \in N_G(S) - S$. Indeed, $t^s \in \text{ccls}(tc)$ or $t^s \in \text{ccls}(bav)$ is not possible since a semi-dihedral group is not a subgroup of a generalized quaternion group. However, if $t^s \in \text{ccls}(t) \cup \text{ccls}(bv)$, then there is an $n \in N_G(S)$ such that $t^s = t^n$. But then $t^{sn-1} = t$, which contradicts the fact that $C_G(t) \leq N_G(S)$. By the above, we have $\langle a^2 \rangle^{t'} = \langle c^{2k} \rangle$ with k odd. Since y is an element of order 4 contained in $\langle a^2 \rangle$ and v is an element of order 4 contained in $\langle c^2 \rangle$, we get that $y^{t'} = vz^l$ with $l = 0, 1$. But

then $(yvz^l)^{t'} = yvz^l$ which gives $(uz^l)^{t'} = uz^l$, recalling that $yv = u$. We have proved that t' centralizes $U = \langle z, u \rangle$ and so $C_G(t')$ contains a subgroup isomorphic to E_8 . This is a contradiction, since t' is conjugate in G to t . Hence, we must have $N_G(S) = G$ and so $|G : S| = 2$, as required.

Suppose, finally, that $S \cong A(m, n)$, $m \geq 3$, $n \geq 3$, i.e. $S = Q * L$ is the central product of Q and L . Then S has exactly four conjugacy classes of involutions contained in $S - U$ with the representatives t, tc, bv and bav and all these involutions act faithfully on U . The corresponding centralizers are:

$$C_S(t) = C_G(t) = \langle t \rangle \times Q \quad \text{with} \quad Q \cong Q_{2^m}, \quad C_S(tc) = \langle tc \rangle \times Q,$$

$$C_S(bv) = \langle bv \rangle \times \langle c, yt \rangle \quad \text{with} \quad \langle c, yt \rangle \cong Q_{2^n} \quad \text{and} \quad C_S(bav) = \langle bav \rangle \times \langle c, yt \rangle.$$

Note that all 2^{n-2} conjugates of t in S lie in the dihedral subgroup $L = \langle c, t \rangle$ and also all 2^{n-2} conjugates of tc in S lie in L . Similarly, all 2^{m-2} conjugates of bv in S lie in the dihedral subgroup $K = \langle bv, bav \rangle \cong D_{2^m}$ and also all 2^{m-2} conjugates of bav in S lie in K . These are all $2 \cdot 2^{n-2} + 2 \cdot 2^{m-2}$ involutions in $S - U$. Also, we see that $K = \langle a, bv \mid a^{2^{m-1}} = (bv)^2 = 1, a^{bv} = a^{-1} \rangle$.

We want to determine all dihedral subgroups of S which are generated by a pair of distinct involutions in $S - U$. We recall that any two distinct involutions always generate a dihedral subgroup. Any two distinct involutions in $\text{ccl}_S(t) \cup \text{ccl}_S(tc)$ generate a dihedral subgroup which is contained in L . Similarly, any two distinct involutions in $\text{ccl}_S(bv) \cup \text{ccl}_S(bav)$ generate a dihedral subgroup which is contained in K . We note that $\langle c \rangle$ fuses (by conjugation) all involutions in $\text{ccl}_S(t)$ to t and all involutions in $\text{ccl}_S(tc)$ to tc . Similarly, $\langle a \rangle$ fuses all involutions in $\text{ccl}_S(bv)$ to bv and all involutions in $\text{ccl}_S(bav)$ to bav . We have $[c, a] = 1$ and a centralizes t and both tc and c centralize bv and bav . All this means that it is enough to see what is the order of the following four dihedral subgroups: $\langle bv, t \rangle$, $\langle bv, tc \rangle$, $\langle bav, t \rangle$ and $\langle bav, tc \rangle$. The computation shows: $(bv \cdot t)^2 = (bv \cdot tc)^2 = (bav \cdot t)^2 = (bav \cdot tc)^2 = z$, and so all these four dihedral subgroups have order 8.

Suppose that t is not conjugate in $N_G(S)$ to any involution in $S - L$. That will certainly happen if (for example) $m \neq n$. Supposing, in addition, that $S \neq G$, we see that $N_G(S)$ fuses t with tc and so $|N_G(S) : S| = 2$, since $C_G(t) = C_S(t)$. If $N_G(S) = G$, then we are finished. Therefore, we assume that $N_G(S) \neq G$. Take an element $s \in G - N_G(S)$ such that s normalizes $N_G(S)$ and $s^2 \in N_G(S)$. If an involution $x \in N_G(S) - S$, then $(\text{ccl}_L(t))^x = \text{ccl}_L(tc)$ implies that $L_0 = L\langle x \rangle \cong D_{2^{n+1}}$. If $|C_S(x)| = 2^m$, then $C_L(x) = \langle z \rangle$ and $C_{N_G(S)}(x) = \langle x \rangle \times C_S(x)$ imply that $C_S(x)$ covers S/L and so Q normalizes $L_0 \cong D_{2^{n+1}}$ and $QL_0 = N_G(S)$, which contradicts the maximality of S . Hence there is no such involution x in $N_G(S) - S$ with $|C_S(x)| = 2^m$. Set $P = \text{ccl}_S(t) \cup \text{ccl}_S(tc) \cup \text{ccl}_S(bv) \cup \text{ccl}_S(bav)$ so that $\langle P \rangle = S$ and $P \subseteq G - T$. If $t' = t^s \in N_G(S) - S$, then $C_{N_G(S)}(t') = \langle t' \rangle \times C_S(t')$ and so $|C_S(t')| = 2^m$, a contradiction. If $t' \in \text{ccl}_S(t) \cup \text{ccl}_S(tc)$, then there is $n \in N_G(S)$ such that $t' = t^s = t^n$ and so $C_G(t) \not\leq N_G(S)$, a contradiction. Hence $t' \in \text{ccl}_S(bv)$ or $t' \in \text{ccl}_S(bav)$. If $N_G(S)$ fuses bv and bav , then all elements in P are conjugate in

$\langle y \rangle N_G(S)$ to t , and since $\langle P \rangle = S$, there is $x' \in P$ such that $x_0 = (x')^s \in N_G(S) - S$ and so $C_{N_G(S)}(x_0) = \langle x_0 \rangle \times C_S(x_0)$ and $|C_S(x_0)| = 2^m$, a contradiction. Suppose that $N_G(S)$ does not fuse bv and bav . Then $|C_{N_G(S)}(bv)| = |C_{N_G(S)}(bav)| = 2^{m+2}$ and so $n + 2 = m + 1$ because $t' \in \text{ccl}_S(bv)$ or $t' \in \text{ccl}_S(bav)$. There is $x' \in P$ such that $x_0 = (x')^s \in N_G(S) - S$ and so $|C_{N_G(S)}(x_0)| = 2^{n+2} = 2^{m+1}$ which gives $|C_S(x_0)| = 2^m$, a contradiction. This gives $N_G(S) = G$ and so $|G : S| = 2$, as required.

Now suppose that t is not conjugate in $N_G(S)$ to $tc \in L$ but $S \neq G$. Then $N_G(S)$ must fuse t to an involution in $S - L - U$. Without loss of generality, we may assume that t is fused in $N_G(S)$ to bv . This gives $|N_G(S) : S| = 2$ and $m = n$ because $C_S(bv) \cong C_2 \times Q_{2^n}$. Supposing $N_G(S) \neq G$, we take an element $s \in G - N_G(S)$ such that s normalizes $N_G(S)$ and $s^2 \in N_G(S)$. Set again $P = \text{ccl}_S(t) \cup \text{ccl}_S(tc) \cup \text{ccl}_S(bv) \cup \text{ccl}_S(bav)$ so that $\langle P \rangle = S$ and $P \subseteq G - T$. There is an $x' \in P$ such that $t' = (x')^s \in N_G(S) - S$ and t' acts faithfully on U . Suppose at first that $m = n \geq 4$. Then $L = \langle c, t \rangle$ and $K = \langle a, bv \rangle$ are the only dihedral subgroups of order 2^m in S and so for each $x \in N_G(S) - S$ we have $L^x = K$ and so $\langle c \rangle^x = \langle a \rangle$. In particular, $v^{t'} = yz^\mu$, $\mu = 0, 1$. It follows that t' centralizes $yvz^\mu = uz^\mu$ and since $z^\mu \in Z(G)$, so t' centralizes u . Hence, t' centralizes $U = \langle z, u \rangle$, a contradiction. We get in this case $N_G(S) = G$ and so $|G : S| = 2$, as required. Suppose now that $m = n = 3$ so that S is extraspecial of order 2^5 and $S \cong Q_8 * D_8$. Then t (fused with bv) lies in a conjugacy class of length 4 in $N_G(S)$. We have $t'^t \in \{bv, bvz\}$ and $\langle t, bv \rangle = D \cong D_8$. Hence $D\langle t' \rangle = D_0 \cong D_{16}$ and so t' acts fixed-point-free on $D - \langle z \rangle$. For each involution t_0 in $S - U$, we have $C_S(t_0) = \langle t_0 \rangle \times Q_0$ with $Q_0 \cong Q_8$. Since t' is a conjugate of an involution in $S - U$ under the action of s (normalizing $N_G(S)$), it follows that $C_{N_G(S)}(t') = \langle t' \rangle \times C_S(t')$ contains a subgroup isomorphic to Q_8 and so $C_S(t') = Q^* \cong Q_8$ because $Q^* \cap D = \langle z \rangle$. Since $N_{N_G(S)}(D) \geq \langle S, t' \rangle = N_G(S)$, it follows that Q^* normalizes $D_0 = D\langle t' \rangle \cong D_{16}$ and so D_0 is normal in $N_G(S)$ (since Q^* covers S/D). Note that $t \in D$ and so we have obtained a contradiction with the maximality of S . Hence, also in this case, we have $N_G(S) = G$ and so $|G : S| = 2$.

It remains to consider the case where t is fused in $N_G(S)$ to each involution in $S - U$. This gives at once that $m = n$ and $|N_G(S) : S| = 4$ so that $N_G(S)/S$ acts regularly on the four S -classes of involutions which are contained in $S - U$.

Let $m = n \geq 4$. Then S has exactly two dihedral subgroups $L = \langle c, t \rangle$ and $K = \langle a, bv \rangle$ of order 2^m and L and K contain all involutions from $S - U$. Therefore, for each $x \in N_G(S) - S$, we have either $K^x = K$ and $L^x = L$ or $K^x = L$. Supposing again that $N_G(S) \neq G$, we take an element $s \in N_G(N_G(S)) - N_G(S)$ with $s^2 \in N_G(S)$. Then we have $t' = t^s \in N_G(S) - S$. If $L^{t'} = L$ and $K^{t'} = K$, then t' fuses the two classes of involutions in $L - \langle c \rangle$ and also t' fuses the two classes of involutions in $K - \langle a \rangle$. This gives that $c^{t'} = c^{-1}$ and $a^{t'} = a^{-1}$. In particular, we get $u^{t'} = (yv)^{t'} = y^{-1}v^{-1} = yz \cdot vz = yv = u$. Hence, the elementary abelian subgroup $\langle z, u, t' \rangle \cong E_8$ is contained in $C_G(t')$ and this is a contradiction. Now assume that $L^{t'} = K$. Then $\langle c \rangle^{t'} = \langle a \rangle$ and, in particular, $v^{t'} = yz^\mu$, $\mu = 0, 1$.

But then $(yvz^\mu)^{t'} = yvz^\mu$ and consequently $(uz^\mu)^{t'} = uz^\mu$. Hence t' centralizes $U = \langle z, u \rangle$, which is a contradiction, since t' is conjugate in G to t .

Finally, we assume that $m = n = 3$ so that $S \cong Q_8 * D_8$ is an extraspecial group of order 2^5 . We recall that $N_G(S)$ acts transitively on the set of 8 involutions contained in $S - U$. Again assuming that $N_G(S) \neq G$, we take an element $s \in N_G(N_G(S) - N_G(S))$ with $s^2 \in N_G(S)$. Then we have $t' = t^s \in N_G(S) - S$. Set $M = \langle s \rangle N_G(S)$ so that $|M : N_G(S)| = 2$. We shall determine $V = S^M$ and we note that $S < V \leq N_G(S)$. Consider at first the possibility $V < N_G(S)$ which gives $|V : S| = 2$. Then $V = SS^s$, $t' = t^s \in S^s - S$ and $V = S\langle t' \rangle$. By the modular law, $C_G(t') = C_V(t') = \langle t' \rangle \times \hat{Q}$, where $C_S(t') = \hat{Q} \cong Q_8$. Then $C_S(\hat{Q}) = \hat{D} \cong D_8$ and S is the central product of \hat{Q} and \hat{D} . Since \hat{D} is t' -invariant and t' acts fixed-point-free on $\hat{D} - \langle z \rangle$, so $\hat{D}\langle t' \rangle \cong D_{16}$, $V = (\hat{D}\langle t' \rangle) * \hat{Q}$, V fuses all four involutions in $\hat{D} - \langle z \rangle$ and other V -classes of involutions in $S - U$ have length 2. This contradicts the fact that $N_G(S)/S$ acts regularly on the four S -classes of involutions in $S - U$. It follows that $V = S^M = N_G(S)$. Since SS^s is normal in M , so we get $V = SS^s = N_G(S)$. Thus $F = S \cap S^s$ is a normal subgroup of M of order 8. If F is nonabelian, then $S = F * C_S(F)$, where $F_1 = C_S(F)$ is nonabelian and normal in $N_G(S)$. Since $S \cong Q_8 * D_8$, so $\{F, F_1\} = \{D_8, Q_8\}$. But this contradicts the fact that $N_G(S)$ acts transitively on all 8 involutions from $S - U$. We have proved that F is abelian. Since $Q_8 * D_8$ does not possess a subgroup isomorphic to E_8 , it follows that F must be of type $(4, 2)$ and consequently we have $z \in F$. Again, because $N_G(S)$ acts transitively on all involutions from $S - U$, so we have $U \leq F$. Furthermore, $S' = (S^s)' = \langle z \rangle$ and so if $\langle f \rangle$ is a cyclic subgroup of order 4 in F , so $N_G(\langle f \rangle) \geq \langle S, S^s \rangle = N_G(S)$. Also, we have $S_1 = C_S(f) \cong C_4 * Q_8$ and $|S : S_1| = 2$. Hence, S_1 contains exactly 6 involutions which are different from z . This implies that there exist involutions in $S - S_1$. Let t_1 be an involution in $S_1 - F$ and let t_2 be an involution in $S - S_1$. Then t_1 centralizes f but t_2 inverts f . This is a contradiction because $N_G(S)$ normalizes $\langle f \rangle$ and $N_G(S)$ acts transitively on all involutions in $S - U$. We have proved again that $N_G(S) = G$ and so $|G : S| = 4$, as required. \square

3^o. Groups with subgroup isomorphic to E_{16} . As an application of Theorems 49.1 and 49.2, we shall determine up to isomorphism all 2-groups with an involution t such that $C_G(t) = \langle t \rangle \times Q$, where $Q \cong Q_{2^m}$, $m \geq 3$ and which have an elementary abelian subgroup E_{16} of order 16. We obtain exactly two classes of 2-groups and we present them in terms of generators and relations. More precisely, we shall prove the following result.

Theorem 49.3. *Let G be a 2-group containing an involution t such that $C_G(t) = \langle t \rangle \times Q$, where Q is a generalized quaternion group of order 2^m , $m \geq 3$. We assume in addition that G has an elementary abelian subgroup of order 16. Then G is isomorphic to one of the following groups.*

$$(E_1) \quad G = \langle a, b, z, c, t, x \mid a^{2^{m-1}} = b^4 = z^2 = c^{2^{m-1}} = t^2 = x^2 = 1, m \geq 4, a^{2^{m-2}} = b^2 = c^{2^{m-2}} = z, b^{-1}ab = a^{-1}, tct = c^{-1}, bc = cb, bt = tb, a^{-1}ca =$$

$cz, at = ta, xcx = a, xtx = bc^{2^{m-3}}\rangle$. Here $\langle z, x, a^{2^{m-3}}c^{2^{m-3}}, ba^{1+2^{m-3}}tc \rangle \cong E_{16}$ and $\langle a, b \rangle \cong Q_{2^m}, \langle c, t \rangle \cong D_{2^m}, \langle a, b, c, t \rangle \cong C(m, m)$.

(E₂) $G = \langle a, b, z, c, t, x, s \mid a^{2^{m-1}} = b^4 = z^2 = c^{2^{m-1}} = t^2 = x^2 = s^2 = 1, m \geq 3, a^{2^{m-2}} = b^2 = c^{2^{m-2}} = z, b^{-1}ab = a^{-1}, tct = c^{-1}, bc = cb, bt = tb, ac = ca, at = ta, sx = xs, xtx = tc, xcx = c^{-1}, xbx = ba, xax = a^{-1}, scs = az, sts = bc^{2^{m-3}} \rangle$. Here $\langle a, b \rangle \cong Q_{2^m}, \langle c, t \rangle \cong D_{2^m}, \langle a, b, c, t \rangle \cong A(m, m), \langle z, x, s, a^{2^{m-3}}c^{2^{m-3}} \rangle \cong E_{16}$. Finally, for $m = 3$, our group G is isomorphic to a Sylow 2-subgroup of the simple group J_2 .

Proof. Suppose that a 2-group G satisfies the assumptions of Theorem 49.3 and let E be an elementary abelian subgroup of order 16 in G . Using theorems 49.1 and 49.2, we see that we have exactly two possibilities:

- (E₁) G has a normal subgroup $S \cong C(m, m), m \geq 4$ of index 2 in $G, |E \cap S| = 8$ and so $G = SE$.
- (E₂) G has a normal subgroup $S \cong A(m, m), m \geq 3$ of index 4 in $G, E \cap S = U$ is a normal four-subgroup of G and so $G = SE$.

Case (E₁). Assume that $S \cong C(m, m), m \geq 4$, is given with generators and relations as in the definition. Let $U = \langle z, yv \rangle$ be the normal four-subgroup of G , where y is an element of order 4 in $\langle a \rangle$ and $v = c^{2^{m-3}}$ is an element of order 4 in $\langle c \rangle$. In the proof of Theorem 49.2 we have found all five conjugacy classes of involutions (and their centralizers) in $S - U$. Their representatives are the involutions: t, tc, bv, bav and bav . It follows that t can be fused in G only to an involution in the conjugacy class of bv . We see also that S has exactly two normal subgroups isomorphic to D_{2^m} which do not contain any conjugate of $bav : L = \langle t, c \rangle$ and $K = \langle bv, a \rangle$. Take an involution $x \in E - S$. Since x cannot fuse t with tc , it follows that x does not normalize the dihedral subgroup L . Hence we have $L^x = K$. The involution x sends the conjugacy class of t in L onto the conjugacy class of bv in K . Replacing t with tc^{2j} (j is an integer), we may assume that $t^x = bv = bc^{2^{m-3}}$. Also we have $\langle c \rangle^x = \langle a \rangle$ and so replacing c with c^k (k is an odd integer), we may assume that $c^x = a$. We note that these replacements of generators did not effect the defining relations for $S \cong C(m, m)$. The structure of G is uniquely determined.

Case (E₂). Assume that $S \cong A(m, m)$ is given with generators and relations as in of $A(m, n)$. Then we have $S = Q * L$, where $Q \cong Q_{2^m}$ and $L \cong D_{2^m}$. Let $U = \langle z, yv \rangle$ be the normal four-subgroup of G , where y is an element of order 4 in $\langle a \rangle$ and $v = c^{2^{m-3}}$ is an element of order 4 in $\langle c \rangle$. In the proof of Theorem 49.2 we have found all four conjugacy classes of involutions (and their centralizers which are all isomorphic to $C_2 \times Q_{2^m}$) in $S - U$. Their representatives are the involutions: t, tc, bv , and bav . Since $|G : S| = 4$, so G fuses all involutions in $S - U$ into a single conjugacy class in G . This gives that $E \cap S = U$.

Assume for a moment that $m \geq 4$. Then we have seen in the proof of Theorem 49.2 that S has exactly two subgroups isomorphic to D_{2^m} . They are $L = \langle t, c \rangle$ and

$K = \langle bv, a \rangle$ and both are normal in S . If we set $E = U \times \langle x, s \rangle$, where $\langle x, s \rangle \cap S = 1$, then the four-subgroup $\langle x, s \rangle$ acts on $\{L, K\}$. We may assume that x normalizes L and K and $L^s = K$. The involution x must induce outer automorphisms on L and K and so $c^x = c^{-1}$ and $a^x = a^{-1}$ since x fuses two conjugacy classes of non-central involutions in L and also in K . Replacing s with sx (if necessary), we may assume that s sends t to an involution in the conjugacy class of bv (instead of bav) in K . Replacing t with tc^{2j} (where j is an integer) we may assume that $t^s = bv = bc^{2^{m-3}}$. Also we have $\langle c \rangle^s = \langle a \rangle$. Let $t^x = t'$, where $t' = tc^k$ with k an odd integer. Then replacing c with c^k , we see that we may assume from the start that $t^x = tc$. Here it might happen that $(c^k)^{2^{m-3}} = v^{-1} = vz$ and then the previous relation $t^s = bv$ is changed into $t^s = bv^{-1} = bvz$. In that case we replace b with $b^{-1} = bz$ so that we may assume again $t^s = bv$. Replacing a with a^l , where l is an odd integer, we may assume $c^s = az$. (Here we have taken az rather than a so that the last relation looks simpler!) Act on the relation $xtx = tc$ with s . We get $x^s t^s x^s = t^s az$ and so since $[x, s] = 1$ we have $xbvx = bvaz$ or $b^x v^{-1} = bavz$ and finally $b^x = ba$. We note that these replacements of generators did not effect the defining relations for $S \cong A(m, m)$. The structure of G is uniquely determined.

In the remaining case $m = 3$ we have $S \cong Q_8 * D_8$. We shall determine the group G almost in the same way as above for $m \geq 4$. The only difference is that here S has exactly six subgroups isomorphic to D_8 which do not contain the normal four-subgroup U of G (see the proof of Theorem 49.2). They are:

$$\begin{aligned} L &= \langle t, tc \rangle, & K &= \langle bv, bav \rangle, & D_1 &= \langle t, bv \rangle, \\ D_2 &= \langle t, bav \rangle, & D_3 &= \langle tc, bv \rangle, & D_4 &= \langle tc, bav \rangle. \end{aligned}$$

In $S - U$ lie exactly eight involutions which are distributed in four S -classes: $\{t, tz\}$, $\{tc, tcz\}$, $\{bv, bvz\}$, $\{bav, bavz\}$. We set again $E = U \times \langle x, s \rangle$, where $\langle x, s \rangle \cap S = 1$. Then the four-group $\langle x, s \rangle$ acts transitively (and so regularly) on the above four S -classes. This follows from the fact that G acts transitively on the eight involutions in $S - U$ since $C_G(t)$ has index 8 in G . If τ is any involution in $\langle x, s \rangle$, then we must have either $L^\tau = L$ and $K^\tau = K$ or $L^\tau = K$. Indeed, if $L^\tau = D_i$, where $i \in \{1, 2, 3, 4\}$, then $L \cap D_i = \langle t, z \rangle$ or $\langle tc, z \rangle$ and $L \cap D_i$ is τ -invariant. But then the S -class $\{t, tz\}$ or the S -class $\{tc, tcz\}$ is τ -invariant which is a contradiction. Similarly, if $K^\tau = D_j$, where $j \in \{1, 2, 3, 4\}$, then the S -class $\{bv, bvz\}$ or the S -class $\{bav, bavz\}$ is τ -invariant which is again a contradiction. Hence the four-group $\langle x, s \rangle$ acts on $\{L, K\}$. We may assume that x normalizes L and K and $L^s = K$. Then we determine the group G uniquely in exactly the same way as above. The proof is complete. \square

4^o. *Groups without subgroups isomorphic to E_8 .* As a direct application of the above results, we shall prove the following

Theorem 49.4. *Let G be a 2-group which is not of maximal class and such that $|\Omega_1(G)| > 4$. If G has no elementary abelian subgroups of order 8, then G is*

isomorphic to one of the following groups:

- (a) A group G from (A1)(c) of Theorem 48.1 with involutions in $G - T$.
- (b) A group G from (A1)(d) of Theorem 48.1.
- (c) A group G from (A1) of Theorem 49.1.
- (d) A group G from (A2)(b) of Theorem 49.1.
- (e) A group G from (A2)(d) of Theorem 49.1.
- (f) A group G with a normal subgroup S of index at most 4 in G so that S is isomorphic to the central product of Q_{2^m} and D_{2^n} , where $m > 2$, $n > 2$ and $\Omega_1(G) \leq S$ (see Theorem 49.2).

Proof. Let G be a 2-group which has more than 3 involutions and which is not of maximal class. Also assume that G has no subgroups isomorphic to E_8 . Let U be a normal four-subgroup of G and set $T = C_G(U)$. By assumption we have $\Omega_1(T) = U$ and so there is an involution $t \in G - T$. We have $G = \langle t \rangle T$ and so $C_G(t) = \langle t \rangle \times Q$, where $Q = C_T(t)$. Since t does not centralize U , it follows that Q has only one involution. Therefore, Q is either cyclic or a generalized quaternion group. Such groups G are then described in this and previous subsection. A simple inspection yields the above result. \square

Exercise 1 (Alperin [Alp3]). Suppose that a nonabelian 2-group G has no normal elementary abelian subgroups of order 8. Suppose that G is neither cyclic nor of maximal class. Then one of the following holds:

- (a) G has a normal abelian subgroup A of type $(4, 2)$ with $C_G(A)$ abelian of type $(2, 2^n)$, $n \geq 2$. In that case, $G/C_G(A)$ is isomorphic to a subgroup of $\text{Aut}(A) \cong D_8$.
- (b) G has a normal abelian subgroup A of type $(4, 4)$ with metacyclic $C_G(A)$. In that case, $|G/C_G(A)| \leq 2^5$.

Solution. Let A be the greatest normal noncyclic abelian subgroup of G of exponent ≤ 4 . Since G is not of maximal class, either A is abelian of type $(2, 4)$ or $(4, 4)$ (Lemma 1.4). By Corollary 10.2, $\Omega_2(C_G(A)) = A$. It follows from Theorem 41.1 that $C_G(A)$ is metacyclic. Note that $\text{Aut}(C_4 \times C_2) \cong D_8$ and $|\text{Aut}(C_4 \times C_4)| = 3 \cdot 2^5$. It remains to show that, if G has not G -invariant abelian subgroup of type $(4, 4)$, then $C_G(A)$ is abelian of type $(2, 2^n)$ for some $n > 1$. Indeed, $\Omega_2(C_G(A)) = A$ is of order 8 so our claim follows from Lemma 42.1.

Exercise 2. Let $Q \cong Q_{2^m}$, where $m \geq 5$ and let H be the holomorph of the cyclic group $C \cong C_{2^n}$, $n > 2$. Set $G = Q * H$ with $Q \cap H = Z(Q)$. Show that G has a normal elementary abelian subgroup of order 8.

Solution (Janko). Let $\langle y \rangle$ be a normal (cyclic) subgroup of order 4 in Q , let $\langle v \rangle < C$ be of order 4 and set $\langle z \rangle = Z(G)$; then $(yv)^2 = y^2v^2 = zz = 1$. Let a be an

involution in $A = \text{Aut}(C)$ such that $\langle a, C \rangle \cong M_{2^{n+1}}$ ($\Omega_1(A) \cdot C$ has exactly three maximal subgroups containing C ; these subgroups are isomorphic to $D_{2^{n+1}}$, $SD_{2^{n+1}}$ and $M_{2^{n+1}}$, respectively). Then a centralizes $v \in Z(\langle a, C \rangle)$ and $D = \langle z, yv, a \rangle$ is the desired normal elementary abelian subgroup of order 8 in G . Indeed, $V = \langle z, yv \rangle$ is a normal four-subgroup of G , since $\langle z \rangle$, $\langle y \rangle$, $\langle v \rangle$ are normal in G and $o(yv) = 2$. Next, $|\langle a, V \rangle| = 8$ and $W = \langle z, a \rangle = \Omega_1(\langle a, C \rangle)$ is characteristic in a normal subgroup $\langle a, C \rangle$ of G . It follows that $D = VW$ is also normal in G . Since a centralizes V , $D \cong E_8$, and we are done.

Exercise 3. Let G be a p -group containing an elementary abelian subgroup of order p^3 and let E be the subgroup generated by all elementary abelian subgroups of G of order p^3 . Suppose that $G - E$ contains an element x of order p . Then $C_{\langle x, E \rangle}(x) = \langle x \rangle \times Q$, where Q is cyclic or generalized quaternion.

Exercise 4. Classify the 2-groups G such that

- (i) $\Omega_2(G) = C \times M$, where $|C| = 2$ and M is of maximal class and order > 8 ,
- (ii) $\Omega_i(G) = C * M$, where $i = 1$ or 2 , $C \cong C_4$ and M is of maximal class.

§50

Janko's theorem on 2-groups without normal elementary abelian subgroups of order 8

The main part of this section coincides with [Jan5]. Theorem 50.1 yields a deep insight in the structure of 2-groups without normal elementary abelian subgroups of order 8. The proof is fairly difficult, however elementary. In the analogous case, for $p > 2$, we have to classify the p -groups G without normal subgroup of order p^{p+1} and exponent p ; it seems that this problem is far from a solution.

The first important result about the groups of the title is the 4-generator theorem from [MacW] which asserts that any subgroup of such groups can be generated by four elements. However, this result does not say anything more about the structure of such groups. In [Kon3], the groups of the title are determined under the additional assumption that the Frattini subgroup contains an elementary abelian subgroup of order 8. This determination is somewhat unfortunate, because the resulting groups are given in terms of generators and relations without any comments and from these it is difficult to disclose the structure of such groups.

In his long paper [Ust], Ustjuzaninov has asserted that the groups G of the title must have a normal metacyclic subgroup N such that G/N is isomorphic to a subgroup of the dihedral group D_8 of order 8. But this paper is completely unreadable. With any attempt to read it, computational errors were discovered. However, it turns out that this result is correct after all!

We shall give here a relatively short proof of a stronger result. For example, in the case where G/N is isomorphic to D_8 , we shall determine completely the structure of N by showing at first that N is either abelian or minimal nonabelian. In our proof the computations are reduced to a minimum. The proof is based on a method of “pushing up” normal metacyclic subgroups of G combined with a very detailed knowledge of $\text{Aut}(C_4 \times C_4)$ (Proposition 50.5). We also note that our proof of the 4-generator theorem is character-free, i.e., it is completely elementary.

We state now our main result.

Theorem 50.1 (Janko [Jan5]). *Let G be a 2-group which has no normal subgroups isomorphic to E_8 . Suppose that G is neither abelian nor of maximal class. Then G has a normal metacyclic subgroup N such that $C_G(\Omega_2(N)) \leq N$ and one of the following holds:*

- (a) $|G/N| \leq 4$ and either $\Omega_2(N)$ is abelian of type $(4, 4)$ or N is abelian of type $(2^j, 2)$, $j \geq 2$.
- (b) $G/N \cong D_8$ and
 - (b1) N is either abelian of type $(2^k, 2^{k+1})$, $k \geq 1$ or of type $(2^l, 2^l)$, $l \geq 2$ or
 - (b2) N is minimal nonabelian, $\Omega_2(N)$ is abelian of type $(4, 4)$ and more precisely $N = \langle a, b \mid a^{2^m} = b^{2^n} = 1, a^b = a^{1+2^{m-1}} \rangle$, where $m = n$ with $n \geq 3$ or $m = n + 1$ with $n \geq 2$.

We prove here the following easy special case of the above theorem.

Theorem 50.2. Suppose that a 2-group G has no normal elementary abelian subgroups of order 8 and has two distinct normal four-subgroups U and V . Then $D = UV \cong D_8$ and G is the central product $G = D * C$ of D and C with $D \cap C = Z(D)$ and C is either cyclic or of maximal class $\not\cong D_8$. Conversely, if $G = D * C$, where $D \cong D_8$, C is cyclic or of maximal class $\not\cong D_8$ and $D \cap C = Z(D)$, then G has no normal subgroups isomorphic to E_8 .

Proof. By hypothesis, $[U, V] \neq \{1\}$. Hence $|U \cap V| = 2$ which gives $D = UV \cong D_8$. We have $C = C_G(D) = C_G(U) \cap C_G(V)$ so $|G : C| = 4$. It follows that $G = D * C$ with $D \cap C = Z(G)$, where $C = C_G(D)$. If W is a normal four-subgroup in C , then UW would be an elementary abelian normal subgroup of order ≥ 8 in G . This is a contradiction and so C is either cyclic or a group of maximal class (Lemma 1.4) which is not isomorphic to D_8 .

Now assume that $G = D * C$, where D, C and $D \cap C$ are the same as in the previous paragraph. Clearly, $Z(G) = Z(C)$ is cyclic. Assume that G has a normal elementary abelian subgroup E of order 8. Since $C \not\cong D_8$ and $Z(G)$ is cyclic, we get $E \cap C = Z(D)$. By the product formula, $G = EC$. Let U, V be two distinct four-subgroups in D ; then they are normal in G . Since $C_G(U) = U * C$ and $C_G(V) = V * C$, we get $U \not\leq E$ and $V \not\leq E$ (recall that $G = EC$). It follows that $E \cap D = Z(D)$. Then G/D is noncyclic since it contains a four-subgroup $DE/D \cong E/Z(D)$; it follows that C is of maximal class. Clearly, U is the only G -invariant four-subgroup in $U * C$ since $C \not\cong D_8$ and $U * C = Z \times C$, where Z is a subgroup of order 2 in U . However, $E \cap (U * C)$ is a G -invariant four-subgroup. It follows that $U < E$, which is a contradiction. The proof is complete. \square

In view of Theorem 50.2, in what follows we may confine our approach to the case where G has exactly one normal four-subgroup.

Remark 1. Let $G = D * C$ be a 2-group from Theorem 50.2 with $G \neq D$. Let Z_1 be the cyclic subgroup of order 4 in D ($\cong D_8$) and let Z_2 be a maximal cyclic subgroup of index ≤ 2 in C . Then $N = Z_1Z_2$ is an abelian normal subgroup of type $(2^j, 2)$, $j \geq 2$, and G/N is elementary abelian of order ≤ 4 . Hence this is a special case of groups occurring in Theorem 50.1(a).

The 4-generator theorem follows as a trivial consequence of Theorem 50.1.

Theorem 50.3 (4-generator theorem). *Let G be a 2-group which has no normal elementary abelian subgroups of order 8. Then every subgroup U of G is generated by four elements.*

Proof. By Theorem 50.1, G has a normal metacyclic subgroup N such that G/N is isomorphic to a subgroup of D_8 . Since $U/(U \cap N)$ is isomorphic to a subgroup of G/N , we have $d(U/(U \cap N)) \leq 2$. Also, $U \cap N$ is metacyclic and therefore $d(U \cap N) \leq 2$. Hence $d(U) \leq 4$ and we are done. \square

We prove three important preliminary results.

Proposition 50.4. *Let G be a 2-group with a metacyclic normal subgroup N . Suppose that N has a G -invariant four-subgroup N_0 which is not contained in $Z(G)$ but there is no G -invariant cyclic subgroup of order 4 contained in N . If N is abelian, it is of type $(2^n, 2^n)$ or $(2^{n+1}, 2^n)$, where $n \geq 1$. If N is nonabelian, it is minimal nonabelian and moreover $N = \langle a, b \mid a^{2^m} = b^{2^n} = 1, a^b = a^{1+2^{m-1}} \rangle$, where $n \geq 2$ and $m = n$ or $m = n + 1$.*

Proof. If N is abelian (of rank 2), the result is clear since N cannot contain a characteristic cyclic subgroup of order 4. Suppose that $N' \neq 1$. Since N' is cyclic, we must have $|N'| = 2$. By Example 10.14, N is minimal nonabelian. Then a result of Rédei (Exercise 1.8a) implies that $N = \langle a, b \mid a^{2^m} = b^{2^n} = 1, a^b = a^{1+2^{m-1}}, m \geq 2, n \geq 1 \rangle$. If $n = 1$, then $N \cong D_8$ or $N \cong M_{2m+1}$ with $m \geq 3$. In both cases N has a characteristic cyclic subgroup of order 4, which is a contradiction. Hence we have $n \geq 2$. It follows that $N' = \langle a^{2^{m-1}} \rangle$ and $Z(N) = \langle a^2, b^2 \rangle$. If $m < n$, then $Z_0 = \langle b^{2^{n-1}} \rangle = \mathfrak{V}_{n-2}(Z(N))$ is a G -invariant subgroup of order 2. In that case, $N_0 = N' \times Z_0$ lies in $Z(G)$, contrary to our assumption. Thus $m \geq n$. However, if $m > n + 1$, then $\mathfrak{V}_{n-1}(Z(N))$ is a characteristic cyclic subgroup of N of order ≥ 4 , which is a contradiction. Thus, $m = n$ or $m = n + 1$. \square

Remark 2. Let W_0 be a normal subgroup of a group W and $\exp(W_0) = n$. Let $A \leq \text{Aut}(W)$ stabilize the chain $W > W_0 \geq \{1\}$. Then $\exp(A)$ divides n . Indeed, take $w \in W$ and $\phi \in A$. Then $w^\phi = ww_0$ for some $w_0 \in W_0$ so $w^{\phi^n} = ww_0^n = w$. It follows that $\phi^n = \text{id}_W$ so $\exp(A)$ divides n , as claimed.

Exercise 1. Let $W = \langle a, b \mid a^{2^n} = b^{2^n} = [a, b] = 1, n > 1 \rangle$ be abelian of type $(2^n, 2^n)$ and let Y be a subgroup of index 2 in W . Then $A = \{\phi \in \text{Aut}(W) \mid Y^\phi = Y\}$ is of order 2^{4n-3} . In particular, if $n = 2$, $|A| = 2^5$.

Exercise 2. Let W be an abelian group of type $(4, 4)$ and A the stabilizer of the chain $W > \Omega_1(W) > \{1\}$. Then $|A| = 2^4$.

Exercise 3. Let W be abelian of type $(4, 4)$. Suppose that $\phi \in \text{Aut}(W)$ stabilizes the chain $W > \Omega_1(W)$. Then ϕ stabilizes the chain $W > \Omega_1(W) > \{1\}$. (*Hint.* Use Proposition 4.9.)

Proposition 50.5. *The automorphism group $\text{Aut}(W)$ of the group $W = \langle u, y \mid u^4 = y^4 = [u, y] = 1 \rangle \cong C_4 \times C_4$ is of order $2^5 \cdot 3$. The subgroup A of $\text{Aut}(W)$ of all automorphisms fixing the subgroup $Y = \langle u^2, y \rangle \cong C_2 \times C_4$ is of order 2^5 and so is a Sylow 2-subgroup of $\text{Aut}(W)$. We have*

$$A = \langle \lambda, \sigma, \rho \mid \lambda^4 = \sigma^4 = \rho^2 = [\sigma^2, \lambda] = 1, [\sigma, \lambda] = \sigma^2 \lambda^2, [\rho, \lambda] = \sigma^2 = [\sigma, \rho] \rangle.$$

where the automorphisms λ, σ, ρ are induced with: $u^\lambda = u^{-1}y, y^\lambda = u^2y; u^\sigma = uy, y^\sigma = y; u^\rho = u^{-1}, y^\rho = y$. We have $A' = Z(A) = \Phi(A) = \langle \sigma^2, \lambda^2 = \eta \rangle \cong E_4$ and so A is a special 2-group. Set $W_0 = \Omega_1(W) = \langle u^2, y^2 \rangle$. Then the stabilizer A_0 of the chain $W > W_0 > 1$ is elementary abelian of order 2^4 (Exercise 2 and Remark 50.2) and $A_0 = \langle \rho, \lambda\sigma = \rho', \eta, \sigma^2 \rangle = C_A(W_0)$. The subgroup A_0 contains the “special” subset $S = \{\sigma^2, \xi, \zeta, \mu, \nu\}$ of five automorphisms defined by:

$$\begin{aligned} u^\xi &= u, & y^\xi &= yu^2; & u^\zeta &= uu^2y^2, & y^\zeta &= yu^2y^2; \\ u^\mu &= uu^2y^2, & y^\mu &= yu^2; & u^\nu &= uy^2, & y^\nu &= yu^2y^2. \end{aligned}$$

If X is any maximal subgroup of A_0 , then $X \cap S$ is nonempty. Each $\tau \in S$ has the property that τ does not invert any element of order 4 in W . In addition, the “superspecial” automorphisms μ and ν have also the property that they do not fix (centralize) any element of order 4 in W . We have $C_A(Y) = \langle \rho, \sigma^2 \rangle \cong E_4$ is normal in A and $A/\langle \rho, \sigma^2 \rangle \cong D_8$. In fact A is a splitting extension of $\langle \rho, \sigma^2 \rangle$ by $\langle \sigma\rho, \lambda \rangle \cong D_8$. Finally, if U is any subgroup of A covering $A/\langle \rho, \sigma^2 \rangle$ (i.e. $U\langle \rho, \sigma^2 \rangle = A$), then U does not normalize any of the six cyclic subgroups of order 4 in W .

Proof. The number of elements x, x' of order 4 in W such that $\langle x, x' \rangle = W$ (by the product formula, $\{x, x'\}$ is a basis of W) is $12 \cdot 8$ and so $|\text{Aut}(W)| = 2^5 \cdot 3$. By Exercise 1, $|A| = 2^5$ and therefore A is a Sylow 2-subgroup of $\text{Aut}(W)$. The stabilizer A_0 of the chain $W > W_0 > 1$ is elementary abelian (Remark 50.2) of order 2^4 (Exercise 2) and so $|A : A_0| = 2$. Any automorphism from $A - A_0$ acts faithfully on W/W_0 (and so also on W_0 ; see Exercise 3) and so we see that $A_0 = C_A(W_0)$ (recall that $W_0 = \Omega_1(W)$). Defining the automorphisms $\lambda, \sigma, \rho, \eta = \lambda^2, \rho' = \lambda\sigma$ as above, we verify the defining relations for A . Since $\rho, \rho', \eta, \sigma^2$ all lie in A_0 and generate a subgroup of order 2^4 , we get $A_0 = \langle \rho, \rho', \eta, \sigma^2 \rangle$. For any $x \in A - A_0, x^2 \in Z(A)$ which gives $\Phi(A) \leq Z(A)$. We have $\langle \sigma^2, \lambda^2 \rangle \leq \Phi(A) \leq Z(A)$ and so the four-subgroup $\langle \sigma^2, \lambda^2 \rangle$ is normal in G . On the other hand, the relations for A show that $A/\langle \sigma^2, \lambda^2 \rangle$ is elementary abelian and $\langle \sigma^2, \lambda^2 \rangle \leq A'$. Hence $\langle \sigma^2, \lambda^2 \rangle = \Phi(A) = A'$. Also, $\langle \sigma^2, \lambda^2 \rangle \leq Z(A) < A_0$ and we check that no element in $A_0 - \langle \sigma^2, \lambda^2 \rangle$ lies in $Z(A)$. Hence $Z(A) = A'$ and so A is special.

Since $C_A(Y) \leq A_0$, so for each $\tau \in C_A(Y)$ we have $u^\tau = uw_0$ with $w_0 \in W_0$. It follows that $|C_A(Y)| \leq 4$. On the other hand, $\langle \rho, \sigma^2 \rangle \leq C_A(Y)$ and so $C_A(Y) = \langle \rho, \sigma^2 \rangle \cong E_4$. Hence $\langle \rho, \sigma^2 \rangle$ is normal in A and since $A/\langle \rho, \sigma^2 \rangle$ acts faithfully on $Y \cong C_4 \times C_2$, it follows that $A/\langle \rho, \sigma^2 \rangle \cong \text{Aut}(C_4 \times C_2) \cong D_8$. Since $\sigma\rho$ is an involution and $\lambda^{\sigma\rho} = \lambda^{-1}$, it follows that $\langle \sigma\rho, \lambda \rangle \cong D_8$. Because $\langle \sigma\rho, \lambda \rangle \cap \langle \rho, \sigma^2 \rangle = 1$, A is a splitting extension of the four-group $\langle \rho, \sigma^2 \rangle$ by $\langle \sigma\rho, \lambda \rangle$.

Let U be any subgroup of A covering $A/\langle \rho, \sigma^2 \rangle$. Then we have $U/(U \cap \langle \rho, \sigma^2 \rangle) \cong D_8$ and so there exists an element α of order 4 in U . Since $\alpha \in A - A_0$ (recall that $\exp(A_0) = 2$), α acts faithfully on W/W_0 . But α fixes $Y = W_0\langle y \rangle$ (since Y is A -invariant) and so α sends two cyclic subgroups of order 4 in $W_0\langle u \rangle$ onto two cyclic subgroups of order 4 in $W_0\langle uy \rangle$ since $W_0\langle u \rangle$ is not A -invariant. It remains to be shown that U does not fix the cyclic subgroup $\langle y \rangle$ contained in Y . Suppose that U fixes $\langle y \rangle$ so that $|U : C_U(y)| \leq 2$. Since $c_1(Y) = 3$, we get $|U : C_U(u^2)| \leq 2$ and so $C_U(Y) = C_U(y) \cap C_U(u^2)$ has index ≤ 4 in U . This is a contradiction, since $|U : (U \cap \langle \rho, \sigma^2 \rangle)| = 8$ (recall that $C_A(Y) = \langle \rho, \sigma^2 \rangle$). We have proved that U does not fix any cyclic subgroup of order 4 in W .

Let X be any maximal subgroup of A_0 . Suppose that $S \cap X$ is empty, where $S = \{x_1, \dots, x_5\}$ is the “special” subset of automorphisms in A_0 with $x_1 = \sigma^2$, $x_2 = \xi$, $x_3 = \zeta$, $x_4 = \mu$ and $x_5 = \nu$. Then we verify that the 10 products $x_i x_j$ ($1 \leq i < j \leq 5$) give 10 pairwise distinct elements in A_0 . But all these products lie in X . This is a contradiction since $|X| = 2^3$. Other statements about “special” and “extraspecial” elements in A_0 are self-explanatory. \square

Proposition 50.6. *Let a 2-group G have no normal elementary abelian subgroups of order 8. Suppose that G is neither abelian nor of maximal class. The one of the following holds:*

- (a) *G has a normal abelian subgroup A of type $(4, 2)$ with $C_G(A)$ abelian of type $(2^n, 2)$, $n \geq 2$. In that case, $G/C_G(A)$ is isomorphic to a subgroup of $\text{Aut}(A) \cong D_8$. If $G/C_G(A) \cong D_8$, then $C_G(A) = A$.*
- (b) *G has a normal abelian subgroup W of type $(4, 4)$ with metacyclic $C_G(W)$. In that case $\Omega_2(C_G(W)) = W$ and $G/C_G(W)$ is isomorphic to a subgroup of $\text{Aut}(W)$, i.e., $|G/C_G(W)| \leq 2^5$ (see Proposition 50.5).*

Proof. Let A be a greatest normal noncyclic abelian subgroup of G of exponent ≤ 4 . Since G is not of maximal class, A is abelian of type $(4, 2)$ or $(4, 4)$. By Corollary 10.2, $\Omega_2(C_G(A)) = A$. Then Theorem 41.1 implies that $C_G(A)$ is metacyclic.

Suppose that $A \cong C_4 \times C_2$. Then $|\Omega_2(C_G(A))| = 8$ and Lemma 42.1 gives that $C_G(A)$ is abelian of type $(2^n, 2)$, $n \geq 2$. Suppose in addition that $G/C_G(A) \cong D_8$. If $C_G(A) > A$, then $C_G(A)$ contains a characteristic cyclic subgroup Z of order 4. We have $Z < A$ and Z is normal in G . But $G/C_G(A) \cong \text{Aut}(A)$ and $\text{Aut}(A) \cong D_8$ contains an automorphism α which permutes two cyclic subgroups of order 4 in A (Remark 50.3), a contradiction and so we must have $C_G(A) = A$. \square

Proof of Theorem 50.1. Let a 2-group G have no normal elementary abelian subgroups of order 8. Assume that G is neither abelian nor of maximal class. The starting point is Proposition 50.6. If we are in case (a) of Proposition 50.6, then G has a normal abelian subgroup A of type $(4, 2)$ with $N = C_G(A)$ abelian of type $(2^j, 2)$, $j \geq 2$. In that case G/N is isomorphic to a subgroup of D_8 and if $G/N \cong D_8$, then $N = A$ and we are done.

We assume that we are in case (b) of Proposition 50.6. Then G has a normal abelian subgroup $W = \langle u, y \mid u^4 = y^4 = [u, y] = 1 \rangle \cong C_4 \times C_4$ with metacyclic $C = C_G(W)$ and $\Omega_2(C) = W$. Set $W_0 = \Omega_1(W) = \langle u^2, y^2 \rangle$ so that W_0 is a normal four-subgroup of G . Let Y be a normal subgroup of G such that $W_0 < Y < W$. Then Y is abelian of type $(4, 2)$ and we may choose the generators u and y of W so that $Y = \langle u^2, y \rangle$. Also set $D = C_G(Y)$ so that G/D is isomorphic to a subgroup of $\text{Aut}(Y) \cong D_8$. It follows from $\langle y^2 \rangle = \mathcal{V}_1(Y)$ that $y^2 \in Z(G)$. Now, G/C is isomorphic to a subgroup of $A = \langle \lambda, \sigma, \rho \rangle$ which is the Sylow 2-subgroup of $\text{Aut}(W)$ fixing Y . In what follows we use freely Proposition 50.5 about the structure of A and the action on W together with the notation introduced there. It follows that D/C is elementary abelian of order ≤ 4 since D/C induces on W a subgroup of $\langle \rho, \sigma^2 \rangle \cong E_4$. We note that $A/\langle \rho, \sigma^2 \rangle \cong D_8$ and $W_0 \leq Z(G)$ if and only if G/C induces on W a subgroup of A_0 in which case G/C is elementary abelian of order $\leq 2^4$. If $C = D$, then G/C is isomorphic to a subgroup of D_8 . Suppose in addition that $G/C \cong D_8$. Then $W_0 \not\leq Z(G)$ and G/C induces on W a subgroup $U \cong D_8$ of automorphisms which covers $A/\langle \rho, \sigma^2 \rangle$. By Proposition 50.5, there is no cyclic G -invariant subgroup of order 4 contained in C . Using Proposition 50.4, we see that the structure of the normal metacyclic subgroup C is completely determined, as stated in Theorem 50.1.

From now on, let $D/C \neq \{1\}$. Suppose at first that D/C contains a subgroup F/C of order 2 such that F/C induces the automorphism σ^2 on W , where $u^{\sigma^2} = uy^2$, $y^{\sigma^2} = y$ and $(uy)^{\sigma^2} = uyy^2$. Since σ^2 does not invert any element of order 4 in W , it follows that σ^2 does not invert any element in $C - W_0$. Because $\sigma^2 \in Z(A)$, so F is normal in G . We claim that $\Omega_2(F) = W$ and so, by Theorem 41.1, F is metacyclic. If not, then $\Omega_2(F) \neq W$ and so $\Omega_2(F) \not\leq C$. There exists an element $s \in F - C$ so that $o(s) \leq 4$ which gives $s^2 \in W_0$. It is easy to see that there exist involutions in $(W\langle s \rangle) - W$. Indeed, we have $y^s = y$, $u^s = uy^2$. If $s^2 = 1$, then we are finished. If $s^2 = y^2$, then $(sy)^2 = s^2y^2 = 1$. If $s^2 = u^2$, then $(syu)^2 = s^2(yu)^syu = u^2 \cdot yuy^2 \cdot yu = 1$. If $s^2 = y^2u^2$, then $(su)^2 = s^2u^su = y^2u^2 \cdot uy^2 \cdot u = 1$. Hence we may assume that $s \in F - C$ is an involution. For any $c \in C$, sc is an involution if and only if $(sc)^2 = 1$ or $c^s = c^{-1}$, i.e., s inverts c . But s inverts in C only the elements in W_0 . (Actually, s centralizes W_0 .) It follows that there are exactly 4 involutions in $F - C$ and they all lie in the elementary abelian subgroup $E = \langle s \rangle \times W_0$. Thus E is characteristic in F and so E is normal in G , which is a contradiction. We have proved that $\Omega_2(F) = W$ and so $F \triangleleft G$ is metacyclic.

Assume now that $|D/C| = 2$. If D/C induces the automorphism σ^2 on W , then by the above, $D = F$ is a normal metacyclic subgroup of G with $\Omega_2(D) = W$.

If $|G/D| \leq 4$, then we are done. It remains to consider the case where $G/D \cong D_8$. In this case G/C induces on W a subgroup U of automorphisms which covers $A/\langle \rho, \sigma^2 \rangle$. In fact, we have in addition $U \cap \langle \rho, \sigma^2 \rangle = \langle \sigma^2 \rangle$. Again by Proposition 50.5, there is no cyclic G -invariant subgroup of order 4 contained in D . In this case, $W_0 \not\leq Z(G)$. By Proposition 50.4, the structure of the normal metacyclic subgroup D is uniquely determined, as stated in Theorem 50.1.

It remains to consider here (where $|D/C| = 2$) the case that D/C induces on W the automorphism ρ or $\rho\sigma^2$. Note that neither ρ nor $\rho\sigma^2$ is central in A and so $N_A(\langle \rho \rangle) = A_0$ and $N_A(\langle \rho\sigma^2 \rangle) = A_0$. Hence G/C induces on W a subgroup of A_0 which does not contain σ^2 . If $|G/C| \leq 4$, we are done. Hence we may assume that G/C induces on W a maximal subgroup X of A_0 which does not contain σ^2 . In that case $G/C \cong E_8$. By Proposition 50.5, X contains a “special” element $\tau \in \{\xi, \zeta, \nu, \mu\}$, where τ does not invert any element of order 4 in W .

Let H/C be a subgroup of order 2 in $G/C \cong E_8$ so that H/C induces the automorphism $\tau = \xi$ on W , where $y^\xi = yu^2$ and $u^\xi = u$. If $\Omega_2(H) > W$, then there is an element $s \in H - C$ with $s^2 \in W_0$. By replacing s with sw for a suitable $w \in W$, we may assume that s is an involution. Indeed, if $s^2 = u^2$, then $u^s = u$ and $y^s = yu^2$ imply that $(su)^2 = s^2u^2 = 1$. If $s^2 = y^2$, then $(syu)^2 = s^2(yu)^syu = y^2 \cdot yu^2u \cdot yu = 1$. If $s^2 = y^2u^2$, then $(sy)^2 = s^2(y)^sy = y^2u^2 \cdot yu^2 \cdot y = 1$. Then sc (with $c \in C$) is an involution if and only if s inverts c and so there are exactly 4 involutions in $H - C$ and therefore they all lie in $E = \langle s \rangle \times W_0 \cong E_8$. Hence E is characteristic in H and so E is normal in G , which is a contradiction. Thus $\Omega_2(H) = W$ and so H must be metacyclic. Since $G/H \cong E_4$, we are done.

Let K/C be a subgroup of order 2 in $G/C \cong E_8$ so that K/C induces the automorphism $\tau = \zeta$ on W , where $y^\zeta = yu^2y^2$ and $u^\zeta = uu^2y^2$. If $\Omega_2(K) > W$, then there is an element $s \in K - C$ with $s^2 \in W_0$. By replacing s with sw for a suitable $w \in W$, we may assume that s is an involution. If $s^2 = y^2$, then $(su)^2 = 1$. If $s^2 = u^2$, then $(sy)^2 = 1$. If $s^2 = y^2u^2$, then $(suy)^2 = 1$. Then sc (with $c \in C$) is an involution if and only if s inverts c and so there are exactly 4 involutions in $K - C$ and therefore they all lie in $E = \langle s \rangle \times W_0 \cong E_8$. Hence E is characteristic in K and so E is normal in G , which is a contradiction. Thus $\Omega_2(K) = W$ and so K must be metacyclic. Since $G/K \cong E_4$, we are done.

Let L/C be a subgroup of order 2 in $G/C \cong E_8$ so that L/C induces a “super-special” automorphism $\tau \in \{\nu, \mu\}$ on W . Then τ has the additional property that it does not fix (centralize) any element of order 4 in W . Suppose that $\Omega_2(L) = W$ so that L is metacyclic. In that case an element $l \in L - C$ commutes with an element of order 4 in W , which contradicts the above property of τ . Hence there is $s \in L - C$ so that $s^2 \in W_0$. Again we may assume that s is an involution. If $\tau = \nu$, then $u^s = uy^2$, $y^s = yu^2y^2$. In this case, if $s^2 = u^2$, then $(sy)^2 = 1$. If $s^2 = y^2u^2$, then $(su)^2 = 1$ and if $s^2 = y^2$, then $(suy)^2 = 1$. If $\tau = \mu$, then $u^s = uu^2y^2$, $y^s = yu^2$. In this case, if $s^2 = u^2y^2$, then $(sy)^2 = 1$. If $s^2 = u^2$, then $(suy)^2 = 1$ and if $s^2 = y^2$, then $(su)^2 = 1$. It follows that $L - C$ contains exactly 4 involutions

and so $E = \langle s \rangle \times W_0 \cong E_8$ (being characteristic in L) is normal in G , which is a contradiction. This finishes completely the case $|D/C| = 2$.

We make here the following observation. If $G/C \cong E_{16}$ and G/C induces on W the group A_0 of automorphisms, then we get a contradiction. Indeed, we consider a subgroup L/C of order 2 in G/C so that L/C induces the automorphism ν on W . Then exactly the same proof as above shows that L has an elementary abelian subgroup E of order 8 which contains all involutions in L and so E would be normal in G , which is a contradiction.

It remains to consider the case where D/C is a four-group inducing on W the four-group $\langle \rho, \sigma^2 \rangle$. If $C < F < D$ and F/C induces σ^2 on W , then we have already proved that $\Omega_2(F) = W$ and F is a normal metacyclic subgroup of G . If $|G/D| \leq 2$, then $|G/F| \leq 4$ and we are finished. Hence we may assume that $|G/D| \geq 4$ and so G induces on W either the whole group A (in which case $G/D \cong D_8$) or one of the maximal subgroups of A containing $\langle \rho, \sigma^2 \rangle$:

- A. $\langle \rho, \sigma^2, \eta, \rho' = \lambda\sigma \rangle = A_0$,
- B. $\langle \rho, \sigma^2, \eta, \sigma \rangle = \langle \eta \rangle \times \langle \sigma, \rho \rangle \cong C_2 \times D_8$ with $\sigma^\rho = \sigma^{-1}$,
- C. $\langle \rho, \sigma^2, \eta, \lambda \rangle$, where $\lambda^2 = \eta$ and $[\rho, \lambda] = \sigma^2$.

Case A is impossible, by the previous paragraph.

Suppose that we are in case B. We note that $\langle \sigma \rangle$ is normal in $\langle \rho, \sigma^2, \eta, \sigma \rangle$. Let K_0 be a subgroup of G such that $F < K_0 < G$ and K_0/C induces the cyclic group $\langle \sigma \rangle \cong C_4$ on W . Hence $K_0/C \cong C_4$ and K_0 is normal in G . Suppose that $\Omega_2(K_0) > W$. Since $\Omega_2(F) = W$, it follows that there is an element $x \in K_0 - F$ so that $o(x) \leq 4$ and $\langle x \rangle C = K_0$. But then $o(x^2) \leq 2$ and $x^2 \in F$ and so $x^2 \in W_0 \leq C$. This is a contradiction since $K_0/C \cong C_4$. Hence $\Omega_2(K_0) = W$ and so K_0 is a normal metacyclic subgroup of G with $|G/K_0| = 4$ and so we are finished in this case.

Finally, we assume that we are in case C or $G/D \cong D_8$ (in which case G induces the full group A on W). In any case, there is an element $k \in G$ such that k induces the automorphism λ on W and so $u^k = u^{-1}y$ and $y^k = yu^2$. Hence k does not normalize any cyclic subgroup of order 4 in W . Also, $W_0 \not\leq Z(G)$. We know that F is a G -invariant nonabelian metacyclic subgroup with $\Omega_2(F) = W$. By Proposition 50.4, F is minimal nonabelian and we may set: $F = \langle a, b \mid a^{2^m} = b^{2^n} = 1, a^b = a^{1+2^{m-1}} \rangle$, where $n \geq 2$ and $m = n$ or $m = n + 1$. If $n \geq 3$, then $W \leq \langle a^2, b^2 \rangle = Z(F)$. This is a contradiction since F/C induces the automorphism σ^2 on W . It follows that $n = 2$. But we have $F > C \geq W$ and so $m = n + 1 = 3$. In particular, $W = C$ and so W is self-centralizing in G . Since $C_W(a) = Y = \langle y, u^2 \rangle$, we have $a^2 \in Y - W_0$. Replacing y with some other element of order 4 in Y (if necessary), we may assume that $a^2 = y$. The structure of F is uniquely determined. We have $F = \langle a, u \mid a^8 = u^4 = 1, a^u = aa^4 \rangle$ and $W = \langle u, y \rangle$, where $y = a^2$ and $C_G(W) = C = W$. Set $y^2 = z$ so that $\langle z \rangle = Z(G)$ because $C_W(k) = \langle y^2 \rangle$. The element k^2 induces the automorphism $\eta = \lambda^2$ on W and so k^2 inverts W . Set $S = F\langle k \rangle$ so that $S/F \cong C_4$ and $k^4 \in C = W$. Since $\langle \sigma^2, \lambda \rangle$ is normal in A , so S is normal in G .

Since $k^4 \in C_W(k) = \langle z \rangle$, we have $k^4 = 1$ or $k^4 = z$. Because $\Omega_2(F) = W$, it follows that all elements in $F - W$ have the order 8. We shall determine the action of k on F . We have $a^k = au^i y^j$, where i, j are some integers and so $u^i y^j$ is an arbitrary element in W . We get

$$\begin{aligned} (a^2)^k &= y^k = yu^2 = (a^k)^2 = (au^i y^j)^2 = au^i y^j au^i y^j \\ &= a^2(u^i y^j)^a u^i y^j = y(uz)^i y^j u^i y^j = yu^{2i} y^{2j} z^i. \end{aligned}$$

Thus $u^2 = u^{2i} y^{2j} z^i$ and so $(u^2)^{1-i} = z^{i+j}$. Hence $1-i \equiv 0 \pmod{2}$ and $i+j \equiv 0 \pmod{2}$. This gives that we must have $i \equiv j \equiv 1 \pmod{2}$. Let x be an element in G inducing the automorphism ρ on W . Then x normalizes S , $x^2 \in W$, $y^x = y$ and $u^x = u^{-1}$. Since $(\sigma^2)^\rho = \sigma^2$ and $\lambda^\rho = \lambda\sigma^2$, we may set $a^x = au^m y^n$ and $k^x = kau^p y^q$, where m, n, p, q are some integers. We get

$$\begin{aligned} (a^2)^x &= y^x = y = (a^x)^2 = (au^m y^n)^2 = au^m y^n \cdot au^m y^n \\ &= a^2(u^m y^n)^a u^m y^n = y(uy^2)^m y^n u^m y^n = yu^{2m} y^{2m+2n}. \end{aligned}$$

Thus $u^{2m} y^{2m+2n} = 1$ and so $m \equiv n \equiv 0 \pmod{2}$. Then the relation $a^k = au^i y^j$ with $i \equiv j \equiv 1 \pmod{2}$ should hold under the action of x , i.e. $(a^x)^{k^x} = a^x (u^x)^i (y^x)^j$. Since m and n are even and $a^u = ay^2$ and so $a^{u^p} = ay^{2p}$, this gives:

$$\begin{aligned} (au^m y^n)^k a u^p y^q &= au^m y^n u^{-i} y^j = au^{m-i} y^{n+j} = (au^i y^j (u^{-1} y)^m y^n u^{2n})^{au^p y^q} \\ &= (a(uy^2)^i y^j u^{-m} y^m y^n)^{au^p y^q} = ay^{2p} u^i y^{2i} y^j u^{-m} y^m y^n \\ &= au^{i-m} y^{2p+2i+j+m+n}. \end{aligned}$$

Hence $u^{m-i} = u^{i-m}$ and so $u^{2i-2m} = 1$. Since $m \equiv 0 \pmod{2}$, we get $u^{2i} = 1$ and so $i \equiv 0 \pmod{2}$, which contradicts the above statement. \square

Exercise 4. Let W be a homocyclic p -group of exponent 2^n and rank d and let L be a subgroup of index 2 in W . Find the order of $\text{Aut}_L(G) = \{\phi \in \text{Aut}(W) \mid L^\phi = L\}$.

Exercise 5. Suppose that a 2-group G has a subgroup isomorphic to E_8 . If G has no subgroups isomorphic to $C_2 \times D_8$, it has an odd number of subgroups isomorphic to E_8 .

2-groups with self centralizing subgroup isomorphic to E_8

In §§48, 49 the 2-groups G have been described which have the property that they possess an involution t such that $C_G(t) = \langle t \rangle \times C$, where C is either a non-trivial cyclic group or a generalized quaternion group. It is natural to ask what happens if C is isomorphic to one of the other two groups of maximal class, i.e., C is isomorphic to D_{2n} (dihedral group) or to SD_{2n} (semi-dihedral group) (Question 49.4). It is easy to see that in that case the 2-group G has a self-centralizing elementary abelian subgroup E of order 8 but the problem of classifying 2-groups G which possess such a subgroup E is far more general.

In this section we classify 2-groups G which possess a self-centralizing elementary abelian subgroup E of order 8. If E is normal in G , then G/E is isomorphic to a subgroup of $GL(3, 2)$ and therefore G/E is isomorphic to a subgroup of the dihedral group D_8 of order 8. We determine here the unique 2-group G such that $E = \Phi(G)$ (Theorem 51.3). There are exactly five 2-groups G , where E is normal in G and $E \leq \Phi(G)$. We shall present these groups in terms of generators and relations (Theorems 51.3 and 51.4). All these groups exist because we find some faithful transitive permutation representation of degree 8 or 16 for these groups. We assume in the sequel that E is not normal in G . Then we have two essentially different possibilities according to $E \leq \Phi(G)$ or $E \not\leq \Phi(G)$, where $\Phi(G)$ is the Frattini subgroup of G .

Suppose that $E \leq \Phi(G)$. Then our first non-trivial result is that G has no normal elementary abelian subgroups of order 8 (Theorem 51.5). We are now in a position to use the main theorem in §50 which allows us to describe the structure of G very accurately (Theorem 51.6).

Suppose that $E \not\leq \Phi(G)$. In that case, we see easily that for each involution $t \in E - \Phi(G)$, we have $C_G(t) = \langle t \rangle \times M_0$, where M_0 is isomorphic to one of the following groups: E_4 , D_{2^n} ($n \geq 3$), or SD_{2^m} ($m \geq 4$). Then we try to pin down the structure of G by using the structure of $C_G(t)$. Assume in addition that G has normal elementary abelian subgroups of order ≥ 8 . In that special case we see that M_0 is isomorphic to E_4 or D_8 (Theorem 51.7). An exceptional case is treated in Theorem 51.8. The group G could possess also a normal elementary abelian subgroup B of order 16 such that $G/B \cong D_8$ (Theorem 51.9). In all other cases, the structure of G is described

in Theorem 51.10. Finally, the example produces a group of order 2⁸ (in terms of generators and relations) which satisfies the assumptions of Theorem 51.10.

It remains to consider the case $E \not\leq \Phi(G)$ and G has no normal elementary abelian subgroups of order 8. In this case Theorem 50.1 does not give a very precise information about the structure of G . Therefore, we use here the fusion arguments for involutions which have been introduced in §§48,49. In this way we show that G has in most cases a large normal subgroup S with $|G/S| \leq 4$ and for the structure of S we have exactly seven possibilities (Theorems 51.14 and 51.15). The exceptional cases are treated in Theorems 51.11–51.13.

We use here the standard notation introduced in §§48, 49. In particular, for $x \in G$ we denote with $\text{ccl}_G(x)$ the conjugacy class of x in G .

For the sake of completeness, we give here some known results which will be used often in this book.

Proposition 51.1. *Let τ be an involutory automorphism acting on an elementary abelian 2-group A . Then we have $|\text{C}_A(\tau)| \geq |A : \text{C}_A(\tau)|$.*

Proof. Consider the Jordan normal form of the linear transformation induced by τ on A (considered as a vector space over GF(2)). Then the result follows. \square

Proposition 51.2. *Let τ be an involutory automorphism acting on an abelian 2-group B so that $\text{C}_B(\tau) = W_0 \leq \Omega_1(B)$. Then τ inverts $\mathfrak{U}_1(B)$ and B/W_0 .*

Proof. If $x \in B$, then $(xx^\tau)^\tau = x^\tau x^{\tau^2} = x^\tau x = xx^\tau$. Hence, $xx^\tau = w_0$ with $w_0 \in W_0$ and so $x^\tau = x^{-1}w_0$. This gives $(x^2)^\tau = (x^\tau)^2 = (x^{-1}w_0)^2 = x^{-2}w_0^2 = x^{-2}$ and our result follows. \square

1°. *The case $E \leq \Phi(G)$.* In this subsection we suppose that a 2-group G contains a self-centralizing elementary abelian subgroup E of order 8 which is contained in $\Phi(G)$. Obviously, $Z(G) \leq E$ and also $Z(\Phi(G)) \leq E$. If $|Z(\Phi(G))| = 2$ then, by Proposition 1.13, we get that $\Phi(G)$ is cyclic, which is not the case. It follows that $4 \leq |Z(\Phi(G))| \leq 8$.

We consider at first the possibility $|Z(\Phi(G))| = 8$ which gives that $Z(\Phi(G)) = E$ and since $\text{C}_G(E) = E$, it follows that $E = \Phi(G)$ is a normal self-centralizing elementary abelian subgroup of order 8 of G . On the other hand, G/E is an elementary abelian subgroup of D_8 and so G/E is a four-group. Thus $|G| = 2^5$. For each $x \in G - E$, we must have $|\text{C}_E(x)| = 4$ (since x acts faithfully on E and $\langle x, E \rangle$ is not of maximal class according to Theorem 1.7, Propositions 1.8 and 51.1), $\text{C}_G(x) = \langle x \rangle \text{C}_E(x)$ with $x^2 \in \text{C}_E(x)$. Otherwise, $\text{C}_G(x)$ would cover G/E , which is not possible since $E = \Phi(G)$. It follows that for each $x \in G - E$, $|\text{ccl}_G(x)| = 4$ and so $|G'| \geq 4$. If $G' = E$, then by the Taussky's theorem (Proposition 1.6), G is of maximal class, which is not the case. Thus $|G'| = 4$. Suppose that $|Z(G)| = 4$. Then for each $x \in G - E$ we have $\text{C}_G(x) = \langle x \rangle Z(G)$ which gives $x^2 \in Z(G)$. But then $E = \Phi(G) = \mathfrak{U}_1(G) \leq Z(G)$, a contradiction. Hence $Z(G) = \langle z \rangle$ is of

order 2 and $Z(G) < G'$. Since $Z(G) < G' < E$, we have $[G, G'] = Z(G)$, so G is a 2-group of class 3. The group G/G' is abelian of type $(4, 2)$ and so there is an element $x \in G - E$ so that $x^2 = v \in E - G'$. Since x centralizes z and $v = x^2$, and $E = \langle v, G' \rangle$, it follows that x does not centralize G' (otherwise x would centralize E). Let $y \in G - (E\langle x \rangle)$ which centralizes G' so that $y^2 \in G'$ and $G = \langle x, y \rangle$. Note that $|G : C_G(G')| = 2$. If $[x, y] \in \langle z \rangle$, then $G/\langle z \rangle$ is abelian, a contradiction. Hence we may put $[x, y] = u$, where $G' = \langle z, u \rangle$. From $[x, y] = u$ we get $x^y = xu$ and so $v^y = (x^2)^y = (x^y)^2 = (xu)^2 = xuxu = x^2(x^{-1}ux)u = v(uz)u = vz$. Hence we get $z^y = z$, $u^y = u$, $v^y = vz$, $x^y = xu$, $x^2 = v$, $z^x = z$, $u^x = uz$, $v^x = v$. The relation $[x, y] = u$ gives also $y^x = yu = uy$ since y centralizes $u \in G'$. From this we get $(y^2)^x = (y^x)^2 = (uy)^2 = y^2$. Hence x centralizes $y^2 \in G'$. But x acts faithfully on G' and so we must have $y^2 \in \langle z \rangle$. Suppose now that $y^2 = z$. Then we replace y with $y' = yv$. We get $(y')^2 = (yv)^2 = yvyv = y^2v^yv = z(vz)v = 1$ and other relations remain unchanged $z^{y'} = z$, $u^{y'} = u$, $v^{y'} = vz$, $x^{y'} = x^{yv} = (xu)^v = xu$, and so we may assume from the start that $y^2 = 1$. The structure of G is uniquely determined. It is easy to see that this group G is isomorphic to a subgroup of A_8 . It is enough to set $x = (2, 7, 6, 8)(4, 5)$, $y = (1, 2)(3, 6)(4, 7)(5, 8)$, and we compute further permutations $x^2 = v = (2, 6)(7, 8)$, $[v, y] = z = (1, 3)(2, 6)(4, 5)(7, 8)$, $[x, y] = u = (1, 4)(2, 7)(3, 5)(6, 8)$. Then we simply check that all above relations are satisfied for these permutations. Since z is represented with a non-trivial permutation, so the induced permutation representation of degree 8 is faithful. Note that all above permutations are even. Hence our group G exists and is isomorphic to a subgroup of A_8 . We have proved the following result.

Theorem 51.3. *Suppose that a 2-group G contains a self-centralizing elementary abelian subgroup E of order 8 and $E = \Phi(G)$. Then G is uniquely determined and we have $G = \langle x, y, z, u, v \mid x^4 = y^2 = z^2 = u^2 = v^2 = [z, u] = [z, v] = [z, x] = [z, y] = [u, v] = [u, y] = [v, x] = 1, x^2 = v, v^y = vz, x^y = xu, u^x = uz \rangle$. Here $E = \langle z, u, v \rangle$ is a self-centralizing normal elementary abelian subgroup of order 8 of G , $E = \Phi(G)$, $G = \langle x, y \rangle$ is of order 2^5 , $G' = \langle z, u \rangle$, and $Z(G) = [G, G'] = \langle z \rangle$ is of order 2. The group G exists and is isomorphic to a subgroup of A_8 .*

It remains to consider the second possibility $|Z(\Phi(G))| = 4$. We set $Z(\Phi(G)) = W_0$ so that W_0 is a G -invariant four-group contained in E . Therefore the subgroup $T = C_G(W_0)$ is of index ≤ 2 in G . Since $C_G(E) = E$, so for each $t \in E - W_0$ we have $C_T(t) = E$. Assume that $T = G$, in which case $W_0 = Z(G)$. Let A be a G -invariant subgroup so that $W_0 < A \leq \Phi(G)$ and $|A : W_0| = 2$. Then A is abelian of order 8 and G stabilizes the chain $A > W_0 > 1$ so that $G/C_G(A)$ is elementary abelian (of order ≤ 4). In particular, $\Phi(G) \leq C_G(A)$ and so $A \leq Z(\Phi(G))$, which is a contradiction. It follows that $|G : T| = 2$ and so $Z(G) = \langle z \rangle$ is of order 2 and we set $W_0 = \langle z, u \rangle$. For each $x \in G - T$, $u^x = uz$. Since $|\Phi(G)| \geq 2^4$, so $|G| \geq 2^6$.

Assume now in addition that E is normal in G . Since G/E is isomorphic to a subgroup of D_8 and $|G| \geq 2^6$, so $|G| = 2^6$ and $G/E \cong D_8$. The subgroup T

stabilizes the chain $E > W_0 > 1$ and $|G : T| = 2$, so T/E is a 4-group. We have $Z(T) = W_0$. For each $x \in T - E$, $x^2 \in W_0$ since x acts non-trivially on E . Thus $\Phi(T) = \mathfrak{U}_1(T) \leq W_0$ and so $T' \leq W_0$. On the other hand, if $t \in E - W_0$, then $C_T(t) = E$ implies that $|\text{ccl}_T(t)| = 4$ and so $\text{ccl}_T(t) = E - W_0$ and $|T'| \geq 4$. It follows that $Z(T) = T' = \Phi(T) = W_0$ and therefore T is a special 2-group of order 2^5 . Let $x, y \in T - E$ be such that Ex and Ey are two distinct elements in $T/E \cong E_4$. Then $M = W_0\langle x, y \rangle$ is a maximal subgroup of T not containing E . If M is nonabelian, then $[x, y] = v$ is an involution in W_0 . Let $t \in E - W_0$. We know that $C_T(t) = E$ and so $[x, t]$, $[y, t]$, and $[xy, t] = [x, t][y, t]$ are three distinct involutions in W_0 . Note that T is of class 2. If, for example, $[x, t] = [y, t]$, then $[xy, t] = [x, t][y, t] = 1$, a contradiction. Therefore, we may assume that $[x, t] = v$. It follows $[x, ty] = [x, t][x, y] = v^2 = 1$. Hence, replacing y with $ty \in Ey$, we may assume from the start that $[x, y] = 1$ and so $M = W_0\langle x, y \rangle$ is abelian. We claim that M is the unique abelian maximal subgroup of T . Indeed, if $M_0 \neq M$ is another abelian maximal subgroup of T , then $M \cap M_0 \leq Z(T)$ and $|M \cap M_0| = 2^3$, a contradiction. Since $T = C_G(W_0)$ and $Z(\Phi(G)) = W_0$, so T is a characteristic subgroup of G . Hence M is also a characteristic subgroup of G . Since $G/E \cong D_8$ and D_8 has five involutions, there is an element $s \in G - T$ such that $s^2 \in E$. Note that s normalizes M and so if $s^2 \in W_0 \leq M$, then $M\langle s \rangle$ is a maximal subgroup of G which does not contain E , a contradiction. Thus, we must have $s^2 = t \in E - W_0$. Since $G/E \cong D_8$, s acts non-trivially on $M/W_0 \cong T/E \cong E_4$. Hence, there is an element $x \in M - W_0$ such that $y = x^s$ has the property $M = W_0\langle x, y \rangle$. Also, $x^{-1}y = x^{-1}x^s = [x, s] \in \Phi(G)$ and so $x^2(x^{-1}y) = xy \in \Phi(G)$. Hence $\Phi(G) = E\langle xy \rangle$ and $G = \langle s, x \rangle$. Now, $y^s = x^{s^2} = x^t = xu$, where $u \in W_0 - \langle z \rangle$. Indeed, if $x^t = txt = xz$, then we act on this relation with s . We get $t^s x^s t^s = x^s z^s$ which gives $tyt = yz$ and then $(xy)^t = xzyz = xy$. But this contradicts the fact that $C_T(t) = E$ and so we must have $y^s = xu$, with $u \in W_0 - \langle z \rangle$. Also note that $u^s = uz$ since s acts non-trivially on W_0 . It remains to determine x^2 and y^2 . There are exactly three possibilities for the structure of the abelian group M .

(a) $\Omega_1(M) = M_0$ is of order 2^3 . Since M_0 is normal in G , so x and $y = x^s$ are elements of order 4 contained in $M - M_0$. On the other hand, $|\mathfrak{U}_1(M)| = 2$ and so $\mathfrak{U}_1(M) = \langle z \rangle = Z(G)$. This gives $x^2 = y^2 = z$. If we set

$$s = (2, 5, 8, 12)(4, 6, 10, 11)(7, 9)(13, 15, 14, 16),$$

$$x = (1, 2, 3, 4)(5, 13, 6, 14)(7, 8, 9, 10)(11, 15, 12, 16),$$

then we see (in the same way as in the proof of Theorem 51.3) that G exists in this case and is isomorphic to a subgroup of A_{16} .

(b) $\Omega_1(M) = M$ is of order 2^4 . Here we have $x^2 = y^2 = 1$. If we set $s = (1, 4, 3, 5)(2, 7, 6, 8)$, $x = (4, 7)$, then we see easily that G exists in this case as a subgroup of S_8 .

(c) $\Omega_1(M) = W_0$ is of order 2^2 and so $M \cong C_4 \times C_4$. Here we have $\mathfrak{U}_1(M) = W_0 = \langle x^2, y^2 \rangle$ and $\langle x, x^s \rangle = M$ so that we have two possibilities for x^2 and y^2 .

(c1) If $x^2 = u$, then $y^2 = uz$ and so $y^s = xu = x^{-1}$. This gives $y^t = y^{s^2} = (x^{-1})^s = y^{-1}$ and $x^t = x^{s^2} = y^s = x^{-1}$ and so t inverts M . If we set $s = (1, 5)(2, 8, 4, 7)(3, 6)$, $x = (5, 7, 6, 8)$, then we see easily that G exists in this case as a subgroup of S_8 .

(c2) If $x^2 = uz$, then $y^2 = u$ and then $y^s = xu = (xuz)z = x^{-1}z$. This gives $y^t = y^{s^2} = (x^{-1}z)^s = y^{-1}z$ and $x^t = x^{s^2} = y^s = x^{-1}z$ and so t does not invert M . If we set

$$s = (2, 5, 12, 10)(3, 6)(4, 7, 14, 15)(9, 13, 16, 11),$$

$$x = (1, 2, 3, 4)(5, 9, 10, 11)(6, 12, 8, 14)(7, 13, 15, 16),$$

then we see as before that G exists in this case as a subgroup of A_{16} .

We have proved the following result.

Theorem 51.4. Suppose that a 2-group G contains a self-centralizing elementary abelian subgroup E of order 8, $E < \Phi(G)$, and E is normal in G . Then we have $G = \langle x, y, u, z, t, s \rangle$ with the following initial relations

$$\begin{aligned} u^2 &= z^2 = t^2 = s^4 = [x, y] = [x, u] = [x, z] = [y, u] = [y, z] = [u, z] \\ &= [u, t] = [z, t] = [z, s] = 1, \quad s^2 = t, \quad u^s = uz, \quad x^s = y, \quad y^s = xu. \end{aligned}$$

Here $E = \langle t, z, u \rangle$ is a self-centralizing elementary abelian normal subgroup of order 8 in G , $G/E \cong D_8$, $Z(G) = \langle z \rangle$ is of order 2, G is of order 2^6 , $\Phi(G) = E\langle xy \rangle$ and $G = \langle s, x \rangle$. Also, $Z(\Phi(G)) = W_0 = \langle z, u \rangle$ is a four-group, $M = \langle x, y, z, u \rangle$ is a characteristic abelian subgroup of G of order 2^4 and exponent at most 4 and M is the unique abelian maximal subgroup of $T = C_G(W_0)$, $|G : T| = 2$ and $T/E \cong E_4$. There are exactly four possibilities for the structure of G (with two additional relations).

(a) $x^2 = y^2 = z$, M is abelian of type $(4, 2, 2)$, and the group G is in this case isomorphic to a subgroup of A_{16} .

(b) $x^2 = y^2 = 1$, M is abelian of type $(2, 2, 2, 2)$, and the group G is in this case isomorphic to a subgroup of S_8 .

(c1) $x^2 = u$, $y^2 = uz$, $M \cong C_4 \times C_4$, t inverts M , and the group G is in this case isomorphic to a subgroup of S_8 .

(c2) $x^2 = uz$, $y^2 = u$, $M \cong C_4 \times C_4$, t does not invert on M , and the group G is in this case isomorphic to a subgroup of A_{16} .

In what follows, we assume that E is not normal in G . We recall that $W_0 = Z(\Phi(G))$ is a four-group and $|G : T| = 2$, where $T = C_G(W_0)$. We set $W_0 = \langle z, u \rangle$ and we know that $Z(G) = \langle z \rangle$ is of order 2. Finally, for each involution $t \in E - W_0$, $C_T(t) = E$ and $|G| \geq 2^6$ since $|\Phi(G)| \geq 2^4$. Our aim is to prove that G does not possess in this case a normal elementary abelian subgroup of order 8.

Suppose that A_1 is a normal elementary abelian subgroup of order 16 in T . Let $t \in E - W_0$. No involution in $E - W_0$ could be contained in A_1 and, by Proposition 51.1, $|C_{A_1}(t)| \geq 2^2$. Hence, $|C_{A_1}(t)| = 4$ and $C_{A_1}(t) = W_0$ so that $E \cap A_1 = W_0$. Set $C = EA_1$ and so $|C| = 2^5$ with $|C : A_1| = 2$. Take any $a \in A_1$. Then ta is an involution if and only if $(ta)^2 = 1$ or equivalently $a^t = a^{-1} = a$. It follows that all involutions in $C - A_1$ lie in $E - W_0$. Since $\langle E - W_0 \rangle = E$, we see that E is normal in $N_G(C)$. If $C = T$, then E would be normal in G , a contradiction. Let D/C be a subgroup of order 2 in $N_T(C)/C$. Then E is normal in D and note that all involutions in $E - W_0$ lie in a single conjugacy class in C since $C_G(t) = E$ and $|C : E| = 4$. But then $C_D(t) \not\leq C$, a contradiction. We have proved that T has no normal elementary abelian subgroups of order 16.

Let A_2 be a normal elementary abelian subgroup of order 16 in G . By the previous paragraph, $A_2 \not\leq T$ and so $B_2 = A_2 \cap T$ is a normal elementary abelian subgroup of order 8 in G . If $W_0 \not\leq B_2$, then W_0B_2 is a normal elementary abelian subgroup of order ≥ 16 contained in T , a contradiction. Hence we must have $W_0 \leq B_2$. But then $C_G(W_0) \geq \langle T, A_2 \rangle = G$, which is a contradiction. We have proved that G has no normal elementary abelian subgroups of order 16.

Suppose that A_0 is a normal elementary abelian subgroup of order 8 in G but $A_0 \not\leq T$. Then $\tilde{A}_0 = A_0 \cap T$ is a G -invariant 4-subgroup. If $W_0 = \tilde{A}_0$, then $C_G(W_0) \geq \langle A_0, T \rangle = G$, a contradiction. Hence $W_0 \neq \tilde{A}_0$ and so \tilde{A}_0W_0 is a G -invariant elementary abelian subgroup of order 8 contained in T . We have proved that if G has a normal subgroup isomorphic to E_8 , then G has also such one which is contained in T .

Now assume that G has a normal subgroup $A \cong E_8$. By the previous paragraph, we may assume that $A \leq T$. Since E is not normal in G , so we get $E \neq A$. If $W_0 \not\leq A$, then W_0A would be a G -invariant elementary abelian subgroup of order ≥ 16 , a contradiction. Hence $W_0 \leq A$ and so $E \cap A = W_0$. It is well known that there is a self-centralizing normal abelian subgroup B of T such that $A \leq B$ and B is normal in G . We have $\Omega_1(B) = A$ and $E \cap B = E \cap A = W_0$. Since G/T acts faithfully on W_0 (and so on B), B is also self-centralizing in G . For any $x \in B$, tx is an involution if and only if t inverts x .

Suppose that $B = A$. In this special case, A is a self-centralizing normal elementary abelian subgroup of order 8 of G and so $G/A \cong D_8$ since $|G| \geq 2^6$. Set $V_0 = EA$ and note that $V_0 - A$ contains exactly four involutions and they are contained in $E - W_0$. Hence E is normal in $N_G(V_0)$ and so V_0/A does not lie in $Z(G/A)$ since E is not normal in G . Let R/A be the cyclic subgroup of index 2 in G/A so that we have $R \cap V_0 = A$ and R is a maximal subgroup of G . Hence $E \not\leq R$ and this is a contradiction since $E \leq \Phi(G)$. We have proved that $B \neq A$ and so $|B| \geq 2^4$.

We shall determine now the structure of B . If an involution $e \in A - W_0$ would be a square in B , then t would centralize e , since t inverts on $\Omega_1(B)$ (Proposition 51.2). This is a contradiction. Suppose that all three involutions in W_0 are squares in B . Then $\Omega_2(B) = \langle b_1 \rangle \times \langle b_2 \rangle \times \langle e \rangle q$, where $o(b_1) = o(b_2) = 4$, e is an involution

in $A - W_0$, and $W_0 = \langle b_1^2, b_2^2 \rangle$. We act with $t \in E - W_0$ on $\Omega_2(B)$. By Proposition 51.2, $b_1^t = b_1^{-1}w$ with $w \in W_0$. This gives $b_1^t = b_1(b_1^2 w)$, where $b_1^2 w = w_1 \in W_0$. Similarly, $b_2^t = b_2 w_2$ with $w_2 \in W_0$ and so $(b_1 b_2)^t = (b_1 b_2)(w_1 w_2)$. Here w_1, w_2 , and $w_3 = w_1 w_2$ must be three pairwise distinct involutions in W_0 since $C_{\Omega_2(B)}(t) = \langle b_1^2, b_2^2 \rangle = W_0$. But then $e^t = ew_j$ with $j \in \{1, 2, 3\}$ and so t centralizes one of the elements $b_1 e, b_2 e$, or $b_1 b_2 e$ of order 4, which is a contradiction. We have proved that at most one involution in W_0 is a square in B . Hence, we have obtained the following result. The subgroup $B (> A)$ is abelian of type $(2^m, 2, 2)$, $m \geq 2$, and so $B = \langle b \rangle \times \langle w \rangle \times \langle e \rangle$, where $o(b) = 2^m \geq 4$, $b^{2^{m-1}} = z$, $\langle z \rangle = Z(G) = \mathcal{V}_{m-1}(B)$, $W_0 = \langle z, w \rangle$, $e \in A - W_0$.

Set $V = EB = \langle t \rangle B$, where t is an involution in $E - W_0 = E - B$. Our aim is to show that $V = T$. Therefore, we assume $V \neq T$ and set $\tilde{V} = N_T(V)$ so that $|\tilde{V}/V| \geq 2$. We note that $|B| = 2^{m+2}$ ($m \geq 2$) and so $V - B$ is a normal subset of \tilde{V} and $|V - B| = 2^{m+2} = |tB|$. If $|\tilde{V}/V| \geq 4$, then $|\tilde{V} : C_{\tilde{V}}(t)| = |\tilde{V} : E| \geq 2^{m+2}$ and so $|\tilde{V}/V| = 4$ and all elements in $V - B$ are involutions since they are all conjugate in \tilde{V} to t . This is not the case since te is not an involution in view of $[t, e] \neq 1$. Hence we must have $|\tilde{V}/V| = 2$. Assume for a moment that $\tilde{V} = N_G(V)$. By Theorem 1.7 and Proposition 1.8, G/B is of maximal class and V/B is a non-central subgroup of order 2 in G/B . In fact G/B must be dihedral of order ≥ 8 or semi-dihedral. Let R^*/B be the cyclic subgroup of index 2 in G/B . Then $|G : R^*| = 2$ and $R^* \cap V = B$. But then $E \not\leq R^*$ and so $E \not\leq \Phi(G)$, a contradiction. Hence we must have $N_G(V) > \tilde{V}$. We set $V^* = N_G(V)$ so that $|V^* : \tilde{V}| = 2$ and $V^*T = G$. If $C_{V^*}(t) = E$, then we see (since $|V^* : E| = 2^{m+2}$) that all 2^{m+2} elements in the normal subset $V - B$ in V^* are conjugate to t and so they are all involutions. But this is not the case, since te (as above) is not an involution. Thus $C_{V^*}(t) = \tilde{E}$ is of order 2^4 , $|\tilde{E} : E| = 2$ and $\tilde{E} \cap T = E$. Hence all elements $y \in \tilde{E} - E$ lie in $G - T$, $y^2 \in E$ and $w^y = wz$, where $W_0 = \langle z, w \rangle$. Suppose at first that there is $y \in \tilde{E} - E$ with $y^2 \in W_0$. In this case $W_0\langle y \rangle \cong D_8$ and since there are involutions in $(W_0\langle y \rangle) - W_0$, we may assume that $y^2 = 1$. We act with the involution y on A . Since $C_{W_0}(y) = \langle z \rangle$ and $|C_A(y)| \geq 4$ (Proposition 51.1), we see that there is an element $e \in A - W_0$ so that $[y, e] = 1$. We have $1 \neq [t, e] \in W_0$ and since $[t, e]^y = [t^y, e^y] = [t, e]$, so $[t, e] = z$ which gives $e^t = ez$. Set $v = b^{2^{m-2}}$ so that $\langle v \rangle$ is the cyclic subgroup of order 4 in $\langle b \rangle$. Since $e^t = ez$, we must have $v^t = vw$ for an element $w \in W_0 - \langle z \rangle$. Otherwise, t would centralize ve , which is not possible. In particular, t does not invert v , and so $v \notin \mathcal{V}_1(B)$. Recall that, by Proposition 51.2, t inverts $\mathcal{V}_1(B)$. But this forces that $o(b) = 4$, $\langle v \rangle = \langle b \rangle$, $|B| = 2^4$, and E is normal in V . The last statement follows from the fact that there are only four involutions in $V - B$ (since t inverts in B only the involutions in W_0) and they lie in $E - W_0$. Suppose now that for each $y \in \tilde{E} - E$, $y^2 \in E - W_0$ and so we may assume in this case that $y^2 = t \in E - W_0$. The cyclic group $\langle y \rangle$ of order 4 acts faithfully on A and $\langle y \rangle$ acts fixed-point-free on the set $A - W_0$. If $e^y = ez$ with $e \in A - W_0$, then $e^{y^2} = (ez)^y = ezz = e$ and so $e^t = e$, a contradiction. Hence, $e^y = ew$

with $w \in W_0 - \langle z \rangle$. This gives $e^{y^2} = e^t = (ew)^y = ewwz = ez$. It follows that $v^t = vw_1$ with some $w_1 \in W_0 - \langle z \rangle$, where again $\langle v \rangle$ is the cyclic subgroup of order 4 in $\langle b \rangle$. Otherwise, t would centralize ve . But this means that t does not invert $\langle v \rangle$. As before, this forces that $o(b) = 4$, $\langle b \rangle = \langle v \rangle$, $|B| = 2^4$, and E is normal in V . Again, the last statement follows from the fact that there are only four involutions in $V - B$ (since t inverts in B only the involutions in W_0) and these lie in $E - W_0$. In both cases for the structure of $\tilde{E} = \langle y \rangle E$, we have $|B| = 2^4$, $|\tilde{V}| = 2^6$, and \tilde{V} normalizes the subset $V - B$ containing exactly four involutions. On the other hand, $|\tilde{V} : C_{\tilde{V}}(t)| = |\tilde{V} : E| = 2^3$ which means that $V - B$ contains eight conjugates of t , which is the final contradiction in this paragraph. We have proved that we must have $V = T$ and so $T = \langle t \rangle B$, where $t \in E - W_0$.

Set again $v = b^{2^{m-2}}$ so that $o(v) = 4$ and $v^2 = z$. Since $t \in \Phi(G)$ and $\Phi(G) = \mathfrak{V}_1(G)$, there is an element $x \in G - T$ such that $x^2 = t' \in T - B$. Because $t' = lt$ with $l \in B$, we have for all $y \in B$, $y^{t'} = y^{lt} = y^t$ and $(t')^2 \in B$. Hence x induces an automorphism of order 4 on $\Omega_2(B) = A\langle v \rangle$ since x^2 induces the same involutory automorphism on $\Omega_2(B)$ as the automorphism induced by t . Since t acts fixed-point-free on $A - W_0$, so x induces a 4-cycle on $A - W_0$ and so $e^x = ew$, where $w \in W_0 - \langle z \rangle$. Indeed, if $e^x = ez$, then $e^t = e^{t'} = e^{x^2} = (ez)^x = ezz = e$, which is a contradiction. From $e^x = ew$ follows $e^{x^2} = e^{t'} = e^t = (ew)^x = (ew)(wz) = ez$. But then we must have $v^t = vw'$ with $w' \in W_0 - \langle z \rangle$. Namely, if $v^t = vz = v^{-1}$, then $(ve)^t = (vz)(ez) = ve$, a contradiction. It follows from $v^t = vw'$ that t does not invert v . By Proposition 51.2, t inverts $\mathfrak{V}_1(B)$. Hence v is not a square in B and so $\Omega_2(B) = B$ is of order 2^4 . Since t inverts in B only the elements in W_0 , so there are exactly four involutions in tB and they lie in $E - W_0$. It follows that $E^x = E$ and so E is normal in G . This is the final contradiction.

We have proved the following major result.

Theorem 51.5. *Suppose that a 2-group G contains a self-centralizing elementary abelian subgroup E of order 8, $E \leq \Phi(G)$, and E is not normal in G . Then G has no normal elementary abelian subgroups of order 8.*

In the rest of this subsection, we study the structure of a 2-group G satisfying the assumptions of Theorem 51.5.

We recall that $W_0 = Z(\Phi(G))$ is a normal four-subgroup contained in E and $|G : T| = 2$, where $T = C_G(W_0)$. We set $W_0 = \langle z, u \rangle$ and we know that $Z(G) = \langle z \rangle$ is of order 2. Finally, for each involution $t \in E - W_0$, $C_T(t) = E$ and $|G| \geq 2^6$. Since G has no normal elementary abelian subgroups of order 8, we may apply Theorems 50.1 and 50.2.

Suppose that G has two distinct normal 4-subgroups. Then Theorem 50.2 implies that $G = D * C$, where $D \cong D_8$, $D \cap C = Z(D)$ and C is either cyclic or of maximal class but not isomorphic to D_8 . We get $\Phi(G) \leq C$ and so $E \leq C$, which is not possible. We have proved that W_0 is the unique normal four-subgroup of G .

Since G is neither abelian nor of maximal class, we may apply Proposition 50.1. It follows that G has a normal metacyclic subgroup N such that $C_G(\Omega_2(N)) \leq N$, G/N is isomorphic to a subgroup of D_8 and $W = \Omega_2(N)$ is abelian of type $(4, 2)$ or $(4, 4)$. In any case, $W_0 = \Omega_1(N)$ is the unique normal four-subgroup of G and $W_0 \not\leq Z(G)$. It follows that $E \cap N = W_0$. Since $E \leq \Phi(G)$, G/N is not elementary abelian. Hence G/N is either cyclic of order 4 or $G/N \cong D_8$.

Assume that $G/N \cong C_4$. If N is abelian of type $(2^j, 2)$, $j \geq 2$, then G/N acts faithfully on $\Omega_2(N) \cong C_4 \times C_2$. If, in addition, $N > \Omega_2(N)$, then there is a characteristic cyclic subgroup Z of order 4 contained in $\Omega_2(N)$ so that Z is normal in G . But then acting with G/N on Z , we see that $t \in E - W_0$ centralizes $Z \leq T = C_G(W_0)$, which is a contradiction. Thus, $N = \Omega_2(N)$ and so $|G| = 2^5$, which is again a contradiction. It follows that $\Omega_2(N) = W$ is abelian of type $(4, 4)$. We want to show that N does not possess a G -invariant cyclic subgroup Z of order 4. Suppose that there is such Z so that $Z \leq W \leq T$. But $|G : C_G(Z)| \leq 2$ and so E centralizes Z since $E \leq \Phi(G)$, a contradiction. It follows that we may use Proposition 50.4. Hence in case $G/N \cong C_4$, N is either abelian of type $(2^n, 2^n)$ or $(2^{n+1}, 2^n)$ with $n \geq 2$ or N is minimal nonabelian and more precisely $N = \langle a, b \mid a^{2^m} = b^{2^n} = 1, a^b = a^{1+2^{m-1}} \rangle$, where $m = n$ with $n \geq 3$ or $m = n + 1$ with $n \geq 2$.

Assume that $G/N \cong D_8$. Then the structure of N is determined by Theorem 50.1. We shall show here that the minimal case with $N \cong C_4 \times C_2$ cannot occur. Indeed, suppose that N is abelian of type $(4, 2)$. Let $L/N = Z(G/N)$ so that $|L/N| = 2$ and $E \leq L$ since $E \leq \Phi(G)$. Set $W_0 = \Omega_1(N)$ so that $W_0 = Z(\Phi(G))$, $W_0 < E$ and since $E < \Phi(G)$, we get $\Phi(G) = L$. By the structure of $G/N \cong D_8 \cong \text{Aut}(N)$, we know that $t \in E - W_0$ inverts N . Thus, all elements in $L - N$ are involutions. Set $N = \langle y, w \mid y^4 = w^2 = [y, w] = 1, y^2 = z \rangle$ so that $W_0 = \langle z, w \rangle$, $E = \langle t, z, w \rangle$ with $\langle z \rangle = Z(G)$. Let k be any element in G such that $\langle k \rangle N/N \cong C_4$. Set $K = \langle k \rangle N$. It follows that $k^2 \in L - N$ and since k^2 is an involution, so $k^4 = 1$. By the structure of $\text{Aut}(N) \cong D_8$, we have $y^k = yw, w^k = wz$. Then we see that $\Omega_1(K) = \Phi(K) = \langle k^2, w, z \rangle$. Hence the elementary abelian subgroup $\langle k^2, w, z \rangle$ of order 8 is normal in G . But then the other elementary abelian subgroup $\langle k^2y, w, z \rangle$ of order 8 in K must be also normal in G . Note that K has exactly two elementary abelian subgroups of order 8 since there are exactly eight involutions in $L - N$. In particular, E is normal in G , a contradiction. This proves that the case $G/N \cong D_8$ with $N \cong C_4 \times C_2$ cannot occur.

We have proved the following final result of this subsection.

Theorem 51.6. *Let G be a 2-group which has a self-centralizing elementary abelian subgroup E of order 8. Assume that $E \leq \Phi(G)$ and E is not normal in G . Then the group G has the following properties.*

- (a) *G has no normal elementary abelian subgroups of order 8.*
- (b) *G has the unique normal four-subgroup W_0 and $W_0 < E$.*

- (c) G has a normal metacyclic subgroup N such that $\Omega_2(N) = W$ is abelian of type $(4, 4)$, $C_G(W) \leq N$, $\Omega_1(W) = W_0$, and G/N is either cyclic of order 4 or $G/N \cong D_8$.
- (d) N is either abelian of type $(2^k, 2^{k+1})$ or $(2^k, 2^k)$, $k \geq 2$, or N is minimal nonabelian and more precisely $N = \langle a, b \mid a^{2^m} = b^{2^n} = 1, a^b = a^{1+2^{m-1}} \rangle$, where $m = n$ with $n \geq 3$ or $m = n + 1$ with $n \geq 2$.

2°. The case $E \not\subseteq \Phi(G)$ and G has a normal elementary abelian subgroup of order ≥ 8 . We suppose throughout this subsection that our 2-group G contains a self-centralizing non-normal elementary abelian subgroup E of order 8 such that $E \not\subseteq \Phi(G)$. (If E is normal in G , then G/E is isomorphic to a subgroup of D_8 .) Also, we assume that G has a normal elementary abelian subgroup of order ≥ 8 .

Let $t \in E - \Phi(G)$ and let M be a maximal subgroup of G such that $t \notin M$. Then $C_G(t) = \langle t \rangle \times C_M(t)$. But $M_0 = C_M(t)$ contains the four-subgroup $E_0 = E \cap M$ and $C_{M_0}(E_0) = E_0$. If $E_0 \neq M_0$, then Theorem 1.7 and Proposition 1.8 imply that $M_0 \cong D_{2^n}$ or $M_0 \cong SD_{2^n}$. Let A be a normal elementary abelian subgroup of order 8 in G . If $t \in A$, then A is a normal subgroup of $C_G(t)$. If $t \notin A$, then Proposition 51.1 implies that $C_A(t) = A_0$ is of order ≥ 4 and so $\langle t \rangle \times A_0$ is a normal elementary abelian subgroup of order ≥ 8 of $C_G(t)$. In any case, M_0 has a normal 4-subgroup and so $E_0 \neq M_0$ implies that $M_0 \cong D_8$.

We have proved the following result.

Theorem 51.7. *Let G be a 2-group which has a self-centralizing elementary abelian subgroup E of order 8 which is not contained in $\Phi(G)$. Assume that G has a normal elementary abelian subgroup of order ≥ 8 . Then for each $t \in E - \Phi(G)$, we have either $C_G(t) = E$ or $C_G(t) = \langle t \rangle \times M_0$, where $M_0 \cong D_8$.*

Suppose that there is an involution $t \in E - \Phi(G)$ such that $C_G(t)$ contains an elementary abelian G -invariant subgroup A of order 8. Since E is not normal in G , so $E \neq A$ and therefore $C = C_G(t) = \langle E, A \rangle = \langle t \rangle \times D$, where $D \cong D_8$. The subgroup C has exactly two elementary abelian subgroups of order 8 and so they are A and E . Also, $t \in A \cap E$. Since $C_C(A) = A$, so A is self-centralizing in G and therefore G/A is isomorphic to a subgroup of D_8 . Obviously, E is normal in $N_G(C)$. But E is not normal in G and so $N_G(C) \neq G$. This forces that $|G : C| \geq 4$ and therefore $G/A \cong D_8$.

We have proved the following result which describes an exceptional case.

Theorem 51.8. *Let G be a 2-group which has a self-centralizing non-normal elementary abelian subgroup E of order 8 which is not contained in $\Phi(G)$. Suppose that there is an involution $t \in E - \Phi(G)$ such that $C_G(t)$ contains an elementary abelian G -invariant subgroup A of order 8. Then A is self-centralizing in G and $G/A \cong D_8$.*

We assume in the rest of this subsection that there is no involution $t \in E - \Phi(G)$ such that $C_G(t)$ contains an elementary abelian G -invariant subgroup of order 8.

Suppose that G has a normal elementary abelian subgroup B of order ≥ 16 . Let t be an involution in $E - \Phi(G)$. By the structure of $C_G(t)$, we have $|C_B(t)| \leq 4$. Then Proposition 51.1 forces that $|B| = 16$ and $C_B(t) = W_0$ is of order 4. Let C be a maximal normal abelian subgroup of G containing B . Then $B = \Omega_1(C)$ and, by the structure of $C_G(t)$, we have $C_C(t) = C_B(t) = W_0$. Also, G/C acts faithfully on C . Set $W_0 = \langle z_1, z_2 \rangle$ and let $W_1 = \langle u_1, u_2 \rangle$ be a complement of W_0 in B . Set $z_3 = z_1 z_2$ and $u_3 = u_1 u_2$. We claim that we may choose the generators of W_0 and W_1 in such a way that $u_i^t = u_i z_i$ for $i = 1, 2, 3$. Indeed, suppose that there exist two elements $u \neq u' \in W_1$ so that $u^t = uz$ and $(u')^t = u'z$, where $1 \neq z \in W_0$. Then $uu' \neq 1$ and $(uu')^t = (uz)(u'z) = uu'$, which contradicts the fact that $C_C(t) = W_0$. Hence $u^t = uz$ and $(u')^t = u'z'$, where z, z' are distinct involutions in W_0 . This gives $(uu')^t = (uu')(zz')$, where $uu' \neq 1$ and $zz' \neq 1$. It remains to set $u_1 = u$, $u_2 = u'$, $u_3 = uu'$, $z_1 = z$, $z_2 = z'$, $z_3 = zz'$, and we see that the above claim is proved. Suppose that $C \neq B$. Let v be an element of order 4 contained in $C - B$. Then $v^2 \in B$ and, by Proposition 51.2, $(v^2)^t = v^{-2} = v^2$ and so $v^2 \in W_0$. By Proposition 51.2, $v^t = v^{-1}w_0$ with $w_0 \in W_0$ and so $v^t = v(v^2w_0) = vz_j$, where $j \in \{1, 2, 3\}$. But then $(vu_j)^t = vz_j u_j z_j = vu_j$, which is a contradiction. We have proved that $C = B$ is a self-centralizing normal elementary abelian subgroup of order 16 of G . Set $E_1 = \langle t \rangle \times W_0$ and $L = \langle t \rangle B$. Then all elements in $L - (E_1 \cup B)$ have order 4 and four involutions in $E_1 - W_0$ form a single conjugacy class in L since $|L : C_L(t)| = 4$. It follows $L' = Z(L) = \Phi(L) = W_0$. If $L = G$, then $C_G(t) = E_1 = E$ is normal in G . This is a contradiction and so $L \neq G$. Set $K = N_G(L)$. Then K normalizes the L -class $E_1 - W_0$. Hence $C_K(t)$ must cover K/L . Since $N = C_K(t) = C_G(t) \cong C_2 \times D_8$, so $|K/L| = 2$ and $N \cap L = E_1$. We have $N_G(E_1) \geq \langle N, L \rangle = K$ and so $K \neq G$ by our last assumption. Indeed, if $K = G$, then $N = C_G(t)$ would contain the G -invariant subgroup E_1 . Now, Theorem 1.7 and Proposition 1.8 imply that G/B is of maximal class (acting faithfully on B). Also, L/B is a non-central subgroup of order 2 in G/B and so G/B is not a generalized quaternion group. On the other hand, $GL(4, 2)$ does not possess elements of order 8 and so $|G/B| = 8$ and consequently $G/B \cong D_8$. We have $Z(G) \leq C_G(t) = N$ and so $Z(G) \leq Z(N) = \langle t, z' \rangle$, where $\langle z' \rangle = N' < W_0$. Hence $Z(G) \leq Z(L) = W_0$ and so $Z(G) = \langle t, z' \rangle \cap W_0 = \langle z' \rangle$ is of order 2.

We have proved the following result.

Theorem 51.9. *Let G be a 2-group which has a self-centralizing non-normal elementary abelian subgroup E of order 8 which is not contained in $\Phi(G)$. Assume that there is no involution $t \in E - \Phi(G)$ such that $C_G(t)$ contains an elementary abelian G -invariant subgroup of order 8. Suppose that G has a normal elementary abelian subgroup B of order ≥ 16 . Then $|B| = 16$, B is self-centralizing in G , $G/B \cong D_8$, and $Z(G)$ is of order 2.*

We suppose also in the rest of this subsection that G has no normal elementary abelian subgroups of order ≥ 16 .

Let A be a normal elementary abelian subgroup of order 8 in G . Let B be a maximal normal abelian subgroup of G containing A . Then G/B acts faithfully on B and we have $\Omega_1(B) = A$. Let t be any involution in $E - \Phi(G)$. By our assumptions, $C_G(t)$ does not contain a G -invariant elementary abelian subgroup of order 8. Hence $t \notin B$. By Theorem 51.7, we have either $C_G(t) = E$ or $C_G(t) = \langle t \rangle \times D$, where $D \cong D_8$. By Proposition 51.1, $|C_A(t)| \geq 4$ and so $C_B(t) = C_A(t) = W_0$ is a four-group.

Assume that $B = A$. Then G/A is isomorphic to a subgroup of D_8 . Set $\langle t \rangle A = L$ and $\langle t \rangle \times W_0 = E_1$. All elements in $L - (E_1 \cup A)$ are of order 4 and so E_1 is normal in $N_G(L)$ since $\langle E_1 - W_0 \rangle = E_1$. If L is normal in G , then E_1 is normal in G . But then $C_G(t)$ contains a G -invariant elementary abelian subgroup of order 8, which contradicts our assumptions. It follows that L/A is a non-central subgroup in G/A and so $G/A \cong D_8$. In what follows we shall assume that $B \neq A$.

By Proposition 51.2, no element in $A - W_0$ is a square in B . Assume that all three involutions in W_0 are squares in B . Then $\Omega_2(B) = \langle b_1 \rangle \times \langle b_2 \rangle \times \langle e \rangle$, where $o(b_1) = o(b_2) = 4$, $e \in A - W_0$, and $W_0 = \langle b_1^2, b_2^2 \rangle$. By Proposition 51.2, $b_1^t = (b_1)^{-1}w_0$ with $w_0 \in W_0$ and so $b_1^t = b_1(b_1^2 w_0)$, where $1 \neq w_1 = b_1^2 w_0 \in W_0$. Similarly, $b_2^t = b_2 w_2$ with $1 \neq w_2 \in W_0$ and so $(b_1 b_2)^t = (b_1 b_2)(w_1 w_2)$. Since $C_{\Omega_2(B)}(t) = W_0$, so $w_1, w_2, w_3 = w_1 w_2$ must be pairwise distinct involutions in W_0 . But then $e^t = ew_j$ with $j \in \{1, 2, 3\}$ and so t centralizes one of the elements b_1e, b_2e , or b_1b_2e (all of order 4), which is a contradiction. It follows that exactly one involution in W_0 is a square in B . We have proved that $B = \langle b \rangle \times \langle w \rangle \times \langle e \rangle$, where $o(b) = 2^m, m \geq 2, b^{2^{m-1}} = z, \langle z \rangle \leq Z(G), W_0 = \langle z, w \rangle$, and $e \in A - W_0$.

Set $V = \langle t \rangle B$ and suppose that $C_G(t) = \langle t \rangle \times D$, where $D \cong D_8$. Then W_0 is normal in $C_G(t)$, $Z(C_G(t)) = \langle t, z \rangle$ and $(C_G(t))' = \langle z \rangle$. Hence $C_G(t)$ contains an involution $u \in G - V$ so that $w^u = wz$ and so $W_0 \langle u \rangle = D \cong D_8$. Acting with u on A , we see that $|C_A(u)| \geq 4$ (Proposition 51.1). Since $C_{W_0}(u) = \langle z \rangle$, so u centralizes an involution in $A - W_0$. We may assume $e^u = e$ and so $C_A(u) = \langle z, e \rangle$. If $[t, e] = w_0$ with $w_0 \in W_0 - \langle z \rangle$, then $[t, e]^u = [t^u, e^u] = [t, e] = w_0 = w_0^u = w_0z$ and so $z = 1$, a contradiction. Hence, we must have $[t, e] = z$. If $m \geq 3$, then t inverts the element $v = b^{2^{m-2}}$ of order 4 (Proposition 51.2) and so $v^t = v^{-1} = vz$. But then $(ve)^t = (vz)(ez) = ve$, which is a contradiction since $C_B(t) = W_0$. Hence we must have $m = 2, o(b) = 4, b^2 = z, b^t = bw$ with $w \in W_0 - \langle z \rangle$, and $e^t = ez$. It follows that t inverts in B exactly four elements, namely the elements in W_0 (which are actually centralized by t). Hence there are exactly four involutions in $V - B$ and they all lie in $E_1 = \langle t \rangle \times W_0$. These four involutions in $E_1 - W_0$ lie in a single conjugacy class in V since $|V : C_V(t)| = 4$. Set $\tilde{V} = VC_G(t) = V\langle u \rangle$ so that $N_G(V) = \tilde{V}$ (since $C_G(t)$ must cover $N_G(V)/V$) and E_1 is normal in \tilde{V} because $\langle E_1 - W_0 \rangle = E_1$. If $\tilde{V} = G$, then $C_G(t)$ would contain a G -invariant elementary abelian subgroup E_1 of order 8, contrary to our assumptions. Hence $\tilde{V} \neq G$ and then Theorem 1.7 and Proposition 1.8 imply that G/B is of maximal class and $\tilde{V}/B \cong \langle t, u \rangle \cong E_4$. Replacing u with ut (if necessary), we may assume that $\langle u \rangle B/B = Z(G/B)$. We claim that $C_G(A) = B$. Set $C_G(A) = \tilde{B}$ so that $\tilde{B} \geq B$ and \tilde{B} is normal in G .

If $\tilde{B} \neq B$, then $\tilde{B} \geq \langle u \rangle B$. This is a contradiction since $w^u = wz$ and so u acts faithfully on A . Hence we have $C_G(A) = B$ and so $G/B \cong D_8$ since $\tilde{V} \neq G$.

It remains to consider the case where $C_G(t) = E = \langle t \rangle \times W_0$ for each $t \in E - \Phi(G)$. We set again $V = \langle t \rangle B$. Since $|B| = 2^{m+2}$, $m \geq 2$, so also $|V - B| = |Bt| = 2^{m+2}$. Set $\tilde{V} = N_G(V)$. If $|\tilde{V}/V| \geq 4$, then $|\tilde{V} : C_{\tilde{V}}(t)| = |\tilde{V} : E| \geq 2^{m+2}$ and so all 2^{m+2} elements in $V - B$ are involutions. This is a contradiction since te is not an involution in view of $[t, e] \neq 1$. Therefore we must have $|\tilde{V}/V| \leq 2$. If $\tilde{V} = G$, then $|G/B| = 2$ or 4.

We assume that $G \neq \tilde{V}$ and so in this case $|\tilde{V}/V| = 2$. Since B is abelian, so the set B_0 of elements of B which are inverted by t is a subgroup of B . The number of involutions in $V - B$ is equal to $|B_0|$. Since t does not invert $e \in A - W_0$, so $|B_0| \leq 2^{m+1}$. On the other hand, $|\text{ccl}_{\tilde{V}}(t)| = |\tilde{V} : E| = 2^{m+1}$ and so $|B_0| = 2^{m+1}$, $V - B$ has exactly 2^{m+1} involutions and they lie in a single \tilde{V} -class. By Proposition 51.2, $\mathfrak{V}_1(B) = \langle b^2 \rangle \leq B_0$ and so $B_1 = \mathfrak{V}_1(B)W_0 = \langle b^2, w \rangle \leq B_0$, where $w \in W_0 - \langle z \rangle$. Since $B/B_1 \cong E_4$ and $\langle B_1, e \rangle \not\leq B_0$, so $B_0 = \langle B_1, b \rangle$ or $B_0 = \langle B_1, be \rangle$. Replacing b with be (if necessary), we may assume that t inverts b and so $B_0 = \langle B_1, b \rangle = \langle b, w \rangle$. Since t inverts $v = b^{2^{m-2}}$ with $v^2 = z$, so $v^t = v^{-1} = vz$. Then $e^t = ez$ would imply $(ve)^t = (vz)(ez) = ve$, which is a contradiction since $C_B(t) = W_0 = \langle z, w \rangle$. Therefore $e^t = ew$ with $w \in W_0 - \langle z \rangle$.

Since $N_G(V)/B$ is of order 4 and $G \neq N_G(V) = \tilde{V}$, Theorem 1.7 and Proposition 1.8 imply that G/B is of maximal class. The subgroup V/B (of order 2) is non-central in G/B and so G/B is dihedral or semi-dihedral. In particular, \tilde{V}/B is a 4-group. Let $x \in G - \tilde{V}$ be such that x normalizes \tilde{V} and $x^2 \in \tilde{V}$. Set $D^* = \langle \tilde{V}, x \rangle$ so that (by the structure of G/B) $D^*/B \cong D_8$ and therefore we may assume that $x^2 \in B$. Since V/B is noncentral in D^*/B , $u = t^x \in \tilde{V} - V$.

We claim that $W_0 = \langle z, w \rangle$ is normal in G . Obviously $Z(G) \leq C_B(t) = W_0$. If $Z(G) = W_0$, then our claim is clear. Suppose that $Z(G) < W_0$ so that $Z(G) = \langle z \rangle$ is of order 2. Let U be a normal 4-subgroup contained in A and assume that $U \neq W_0$. Then we have $U > \langle z \rangle = Z(G)$ and so $U \cap W_0 = \langle z \rangle$. But then for an element $u \in U - \langle z \rangle$, we have $u^t = uz$ since $C_A(t) = W_0$. This gives $(vu)^t = (vz)(uz) = vu$, where v is the cyclic subgroup of order 4 in $\langle b \rangle$. This is a contradiction and so $W_0 = \langle z, w \rangle$ is normal in G .

Since $C_A(t) = W_0$ and x normalizes A and W_0 , it follows $C_A(u) = W_0$. Hence $C_G(u) = \langle u \rangle \times W_0$ and $Z(\tilde{V}) = W_0$ since $\tilde{V} = B\langle t, u \rangle$. Note that $\langle t, b \rangle \cong D_{2^{m+1}}$ and $t^e = tw$. There are exactly two V -classes of involutions contained in $V - B$ with the representatives t and tb containing 2^m elements each. The V -class of t is the set $\{tw^i b^{2^j}\}$ and the V -class of tb is the set $\{tbw^i b^{2^j}\}$, where i, j are any integers. Now u fuses these two V -classes and so $t^u = tbw^r b^{2^s}$ for suitable integers r, s . This gives $(tu)^2 = tutu = tt^u = bw^r b^{2^s} = b^{2s+1}w^r$ and so $o(tu) = 2^{m+1}$ and $\langle t, u \rangle \cong D_{2^{m+2}}$. Since u inverts $\langle tu \rangle$, so u inverts $(tu)^2$ and w . But $\langle (tu)^2, w \rangle = B_0$ and so u inverts B_0 . It follows that $b^u = b^{-1}$ and $w^u = w$. Thus tu centralizes $B_0 = \langle b, w \rangle$. Since tu acts faithfully on B and $B = B_0A$, tu must act faithfully

on A . Note that $\langle tu \rangle B / B = Z(D^* / B) = Z(G / B)$. If $\tilde{B} = C_G(A) > B$, then $tu \in \tilde{B}$ since \tilde{B} is normal in G and G / B is of maximal class. This is a contradiction and so $C_G(A) = B$, $D^* = G$, and $G / B \cong D_8$.

We have proved the following final result of this subsection.

Theorem 51.10. *Let G be a 2-group which has a self-centralizing non-normal elementary abelian subgroup E of order 8 which is not contained in $\Phi(G)$. Assume that there is no involution $t \in E - \Phi(G)$, such that $C_G(t)$ contains an elementary abelian G -invariant subgroup of order 8. Suppose that G has a normal elementary abelian subgroup of order 8 but none of order 16. Then G has a maximal normal abelian subgroup B of type $(2^m, 2, 2)$, $m \geq 1$ such that G / B is isomorphic to a non-trivial subgroup of D_8 .*

Example. We give here an example of a 2-group G of order 2^8 satisfying the assumptions of Theorem 51.10. We set $G = \langle b, z, w, e, t, u, x \mid b^8 = z^2 = w^2 = e^2 = t^2 = u^2 = x^2 = [b, w] = [b, e] = [w, e] = [t, w] = [u, w] = [e, x] = 1, b^4 = z, u = t^x, b^t = b^{-1}, b^u = b^{-1}, e^t = ew, e^u = ewz, (tu)^2 = b, b^x = b^{-1}, w^x = wz \rangle$. Here $B = \langle b, w, e \rangle$ is abelian of type $(8, 2, 2)$ and $G / B \cong D_8$. A coset enumeration computer program assures that such a group G exists!

3°. *The case $E \not\leq \Phi(G)$ and G has no normal elementary abelian subgroups of order ≥ 8 .* We suppose throughout this subsection that a 2-group G contains a self-centralizing elementary abelian subgroup E of order 8 which is not contained in $\Phi(G)$. We assume in addition that G has no normal elementary abelian subgroups of order 8.

Let $t \in E - \Phi(G)$ and M be a maximal subgroup of G such that $t \notin M$. Then (by modular law) $C_G(t) = \langle t \rangle \times M_0$, where $M_0 = C_M(t)$ contains the four-subgroup $E_0 = E \cap M$ and $C_{M_0}(E_0) = M_0$. Hence we have either $C_G(t) = E$ or (by Theorem 1.7 and Proposition 1.8) $M_0 \cong D_{2^n}$, $n \geq 3$ or $M_0 \cong SD_{2^m}$, $m \geq 4$.

Suppose that G has (at least) two distinct normal 4-subgroups. Then Theorem 50.2 implies that G is the central product $G = D * C$ of $D \cong D_8$ and C with $D \cap C = Z(D)$ and C is either cyclic or of maximal class different from D_8 . However, if C is cyclic or generalized quaternion, then G does not possess a self-centralizing elementary abelian subgroup of order 8. Hence $C \cong D_{2^n}$ or $C \cong SD_{2^n}$, $n \geq 4$.

We have proved the following result.

Theorem 51.11. *Let G be a 2-group which has a self centralizing elementary abelian subgroup E of order 8 with $E \not\leq \Phi(G)$. Assume in addition that G has no normal elementary abelian subgroups of order 8. Then for each involution $t \in E - \Phi(G)$, we have $C_G(t) = \langle t \rangle \times M_0$, where M_0 is isomorphic to one of the following groups: E_4 , D_{2^n} ($n \geq 3$), or SD_{2^m} ($m \geq 4$). If G has (at least) two distinct normal 4-subgroups, then $G = D * C$ is the central product of D and C , where $D \cong D_8$, $D \cap C = Z(D)$, and $C \cong D_{2^n}$ or $C \cong SD_{2^n}$ with $n \geq 4$.*

In view of Theorem 51.11, we assume in the rest of this subsection that G has the unique normal four-subgroup U (see Lemma 1.4).

Suppose that $C_G(t) = E$ for an involution $t \in E - \Phi(G)$. This is an exceptional case. Since G is neither abelian nor of maximal class, we may apply Theorem 50.1. Let N be a metacyclic normal subgroup of G such that G/N is isomorphic to a subgroup of D_8 , $W = \Omega_2(N)$ is abelian of type $(4, 4)$ or $(4, 2)$, and $C_G(W) \leq N$. Set $W_0 = \Omega_1(W)$ so that W_0 is the unique normal four-subgroup of G . Suppose that $|E \cap N| \leq 2$. In that case $|E \cap N| = 2$ and $E \cap N = E \cap W_0$. Since $C_G(t) = E$, $t \in E - N$ induces on W an involutory automorphism, where $W^* = C_W(t)$ is of order 2. We may apply Proposition 51.2 which shows that t inverts $\Omega_1(W)$ and also on W/W^* . If $W \cong C_4 \times C_4$, then t inverts $\Omega_1(W) = W_0$ contrary to the fact that $|C_W(t)| = 2$. Suppose that $W = \langle a, s \mid a^4 = s^2 = [a, s] = 1, a^2 = z \rangle \cong C_4 \times C_2$. In this case $W^* = C_W(t) = \langle z \rangle = \Omega_1(W)$. We must have $s^t = sz$ and $a^t = a^{-1}z^\epsilon$ with $\epsilon = 0, 1$. If $\epsilon = 1$, then $a^t = a^{-1}z = a$, a contradiction. If $\epsilon = 0$, then $a^t = a^{-1} = az$ and so $(as)^t = (az)(sz) = as$, a contradiction. We have proved that in this special case $|E \cap N| = 4$ and so $E > W_0$, which gives the following result.

Theorem 51.12. *Let G be a 2-group which has a self-centralizing elementary abelian subgroup E of order 8 with $E \not\leq \Phi(G)$. Assume that G has no normal elementary abelian subgroups of order 8. Suppose in addition that G has the unique normal 4-subgroup W_0 and that for an involution $t \in E - \Phi(G)$, $C_G(t) = E$. Then we have $E > W_0$ and Theorem 50.1 gives further information about the structure of G .*

In the rest of this subsection we assume also that there is an involution $t \in E - \Phi(G)$ such that $G \neq C_G(t) = \langle t \rangle \times D$ with $D \cong D_{2^m}$, $m \geq 3$ or $D \cong SD_{2^n}$, $n \geq 4$.

Remark. If G is a 2-group possessing an involution t such that $C_G(t) = \langle t \rangle \times D$ with $D \cong D_{2^m}$ or $D \cong SD_{2^m}$, where $m \geq 4$, then G has no normal elementary abelian subgroup A of order 8. Indeed, if A is such a subgroup, then Proposition 51.1 implies that $|C_A(t)| \geq 4$ and so $C_G(t)$ would contain a normal elementary abelian subgroup of order 8, which is not the case.

Let U be the unique normal 4-subgroup of G . Set $T = C_G(U)$ so that $|G : T| \leq 2$. Suppose at first that $t \in U$. Since $G \neq C_G(t)$, we have $|G : T| = 2$ and $T = C_G(t) = \langle t \rangle \times D$ with $D \cap U = \langle u \rangle = Z(D) = Z(G)$ and $D \cong D_{2^m}$, $m \geq 3$ or $D \cong SD_{2^n}$, $n \geq 4$. Let M be a maximal subgroup of G such that $t \notin M$. Set $M_0 = T \cap M$ so that $C_G(t) = \langle t \rangle \times M_0$ and $M_0 \cong D$. If M were not of maximal class, then Lemma 1.4 implies that M contains a G -invariant 4-subgroup U_0 . Since $U_0 \neq U$, we have obtained a contradiction. Hence M is of maximal class and therefore $M \cong D_{2^{m+1}}$ or $M \cong SD_{2^{m+1}}$ and $M_0 \cong D \cong D_{2^m}$, $m \geq 3$. There is an element $y \in M - M_0$ such that $y^2 \in \langle u \rangle = Z(M) = Z(M_0)$. We get $t^y = tu$ so that $y^t = yu$ and this determines the action of t on M .

We have proved the following result.

Theorem 51.13. *Let G be a 2-group which has a self-centralizing elementary abelian subgroup E of order 8 with $E \not\leq \Phi(G)$. Assume that G has no normal elementary*

abelian subgroups of order 8. Suppose in addition that G has the unique normal 4-subgroup U and there is an involution $t \in E - \Phi(G)$ such that $t \in U$ and $G \neq C_G(t) = \langle t \rangle \times D$ with $D \cong D_{2^m}$, $m \geq 3$ or $D \cong SD_{2^n}$, $n \geq 4$. Then G has a maximal subgroup M such that $G = \langle t \rangle M$, where $M \cong D_{2^{m+1}}$ or $M \cong SD_{2^{m+1}}$ and $C_M(t) \cong D_{2^m}$, $m \geq 3$.

In what follows we assume also that $t \notin U$, where U is the unique normal four-subgroup of G .

Suppose for a moment that $t \in T - U$, where $T = C_G(U)$. Then $C_G(t)$ has the normal elementary abelian subgroup $E_1 = \langle t \rangle \times U$ of order 8. This forces $C_G(t) = \langle t \rangle \times D$, where $D \cong D_8$. Since $E_1 \not\leq Z(C_G(t))$, it follows $C_G(t) \not\leq T$ and $C_T(t) = E_1$. In particular, $|G : T| = 2$ and there is an involution $t' \in C_G(t) - T$. Set $\langle z \rangle = C_U(t')$ so that $z \in Z(G)$. It follows that $E_2 = \langle t', t, z \rangle$ is another elementary abelian subgroup of order 8 contained in $C_G(t)$ and so $C_G(E_2) = E_2$. Also, t' is an involution in $E_2 - \Phi(G)$. If $C_G(t') = E_2$, then applying Theorem 51.12 we get a contradiction since E_2 does not contain U . It follows that $G \neq C_G(t') = \langle t' \rangle \times M_0$ with $M_0 \cong D_{2^m}$, $m \geq 3$ or $M_0 \cong SD_{2^n}$, $n \geq 4$. Replacing E with E_2 and t with t' , we see that we may assume from the start that $t \in G - T$.

It remains to consider only the case $t \in G - T$, where $C_G(t) = \langle t \rangle \times M_0$ with $M_0 \cong D_{2^m}$, $m \geq 3$ or $M_0 \cong SD_{2^n}$, $n \geq 4$. Here $T = C_G(U)$, $|G : T| = 2$, where U is the unique normal four-subgroup of G . It follows that $G = \langle t \rangle T$ and so, by the modular law, $G_0 = C_G(t) = \langle t \rangle \times D$, where $D = C_T(t) \cong M_0$. We have $\langle z \rangle = Z(D) = C_U(t) = Z(G)$ is of order 2. Set $G_1 = N_G(G_0)$. Since $|(UG_0) : G_0| = 2$, we have $UG_0 \leq G_1$. But $Z(G_0) = \langle t, z \rangle$, so t has exactly two conjugates t and tz in G_1 . It follows $G_1 = UG_0$. Set $D_0 = U\langle t \rangle$ and so $D_0 \cong D_8$ and $G_1 = D * D_0$ with $D \cap D_0 = \langle z \rangle$ and $U = \langle z, u \rangle < D_0$. We fix in the rest of this subsection the notation for the structure of D . We set

$$D = \langle a, b \mid a^{2^{m-1}} = b^2 = z^2 = 1, a^{2^{m-2}} = z, a^b = a^{-1}z^\epsilon, \epsilon = 0, 1 \rangle,$$

where $m \geq 3$, and if $\epsilon = 1$, then $m \geq 4$. Let v be an element of order 4 in D_0 and let y be an element of order 4 in $\langle a \rangle$. Since $y^2 = v^2 = z$, so $x = yv$ is an involution in $G_1 - (D_0 \cup D)$. We compute $x^t = (yv)^t = yv^{-1} = yvz = xz$, and so $D_1 = \langle x, t \rangle \cong D_8$ and $D_1 \cap U = Z(D_1) = Z(G) = \langle z \rangle$. We see that $C_{G_1}(D_1) = \langle a, bt \rangle = D^* \cong D$ because $x^{bt} = (yv)^{bt} = y^{-1}v^{-1} = yv = x$, $(bt)^2 = 1$ and $a^{bt} = a^{-1}z^\epsilon$. Thus $G_1 = D^* * D_1$ with $D^* \cong D$, $D^* \cap D_1 = \langle z \rangle$, $C_G(t) = \langle t \rangle \times D = \langle t \rangle \times D^*$ and $U = \langle z, u \rangle \not\leq D_1$. Denoting again D^* with D and bt with b , we have obtained the following initial configuration.

(R) The subgroup $G_1 = UC_G(t)$ is the central product $G_1 = D * D_1$, where $D_1 \cong D_8$, $t \in D_1$, $D \cap D_1 = \langle z \rangle = Z(G)$, $C_G(t) = \langle t \rangle \times D$ with $D \cong D_{2^m}$ or $D \cong SD_{2^m}$, $m \geq 3$, and $U \not\leq D_1$, $U \not\leq D$.

In the rest of this subsection we denote with S a subgroup of G of the maximal possible order subject to the following three conditions.

- (i) $S \geq G_1 = UC_G(t) = D * D_1$, where $D \cong D_{2^m}$ or $D \cong SD_{2^m}$, $m \geq 3$, $D_1 \cong D_8$, $t \in D_1$.
- (ii) $S = DL$, where L is normal in S , $L \cong D_{2^n}$, $n \geq 3$, $D \cap L = \langle z \rangle = Z(D) = Z(L)$ and $L \geq D_1$.
- (iii) $U = \langle z, u \rangle \not\leq L$ and $U \not\leq D$.

We set for the rest of this subsection:

$$L = \langle c, t \mid c^{2^{n-1}} = t^2 = z^2 = 1, c^{2^{n-2}} = z, c^t = c^{-1}, n \geq 3 \rangle \cong D_{2^n}.$$

We may set $u = yv$, where y is an element of order 4 in $\langle a \rangle$ and v is an element of order 4 in $\langle c \rangle$. If $a^4 = 1$, then we put $a = y$ and if $c^4 = 1$, then we set $c = v$.

It is now easy to determine all possibilities for the structure of S . Act with D on the dihedral subgroup L . Since $\text{Aut}(L)/\text{Inn}(L)$ is abelian of type $(2^{n-3}, 2)$, it follows that $D' = \langle a^2 \rangle$ centralizes L . Also we know that D centralizes $\langle v, t \rangle = D_1 \cong D_8$, where $D_1 \leq L$ and so by the structure of $\text{Aut}(L)$ either D centralizes L (and so $S = D * L$) or $M = C_D(L)$ is a maximal subgroup of D in which case $n \geq 4$. In that case D/M induces such an involutory automorphism on L so that $C_L(D/M) = \langle c^2, t \rangle \cong D_{2^{n-1}}$. In any case, $[D, L] \leq \langle z \rangle$ and so D is also normal in S . If $\epsilon = 1$ (i.e. D is semi-dihedral), then we have three possibilities for the maximal subgroup M of D . If $\epsilon = 0$ (i.e. D is dihedral), then two distinct maximal subgroups of D are isomorphic and so we have in this case only two possibilities for the maximal subgroup M of D . This gives (together with central products) exactly seven possibilities \mathcal{S}_i , $i = 1, 2, \dots, 7$ for the structure of S and they are given explicitly (in terms of generators and relations) in the following definition.

Definition 1. Let $S = DL$ be a product of two normal subgroups

$$D = \langle a, b \mid a^{2^{m-1}} = b^2 = z^2 = 1, a^{2^{m-2}} = z, a^b = a^{-1}z^\epsilon, \epsilon = 0, 1, m \geq 3,$$

and if $\epsilon = 1$, then $m \geq 4 \rangle$

and

$$L = \langle c, t \mid c^{2^{n-1}} = t^2 = z^2 = 1, c^{2^{n-2}} = z, c^t = c^{-1}, n \geq 3 \rangle \cong D_{2^n},$$

where $D \cap L = Z(D) = Z(L) = \langle z \rangle$ and $[a, t] = [b, t] = 1$ so that $C_S(t) = \langle t \rangle \times D$. Here if $\epsilon = 1$, then $D \cong SD_{2^m}$, $m \geq 4$, and if $\epsilon = 0$, then $D \cong D_{2^m}$, $m \geq 3$.

- (1) If $\epsilon = 1$ and $[a, c] = [b, c] = 1$, then $S = D * L = \mathcal{S}_1$, $m \geq 4$, $n \geq 3$.
- (2) If $\epsilon = 1$, $C_D(L) = \langle a \rangle$, and $c^b = cz$, then $S = \mathcal{S}_2$, $m \geq 4$, $n \geq 4$.
- (3) If $\epsilon = 1$, $C_D(L) = \langle a^2, b \rangle \cong D_{2^{m-1}}$, and $c^a = cz$, then $S = \mathcal{S}_3$, $m \geq 4$, $n \geq 4$.
- (4) If $\epsilon = 1$, $C_D(L) = \langle a^2, ba \rangle \cong Q_{2^{m-1}}$, then $S = \mathcal{S}_4$, $m \geq 4$, $n \geq 4$.
- (5) If $\epsilon = 0$, $C_D(L) = \langle a \rangle$, and $c^b = cz$, then $S = \mathcal{S}_5$, $m \geq 3$, $n \geq 4$.

(6) If $\epsilon = 0$, $C_D(L) = \langle a^2, b \rangle \cong E_4$ or $D_{2^{m-1}}$, and $c^a = cz$, then $S = \mathcal{S}_6$, $m \geq 3, n \geq 4$.

(7) If $\epsilon = 0$, and $C_D(L) = D$, then $S = D * L = \mathcal{S}_7, m \geq 3, n \geq 3$.

We make here the following simple observation. Since $t \in G - T$, where $T = C_G(U)$ and $|G : T| = 2$, t cannot be conjugate (fused) in G to any involution t' which centralizes U . Therefore, with respect to that fusion, it is enough to consider only those involutions in S which act faithfully on U . We want to show in the sequel that S must be a normal subgroup of G and $|G/S| \leq 4$. In some cases for the structure of S this is difficult.

4°. The case $S \cong \mathcal{S}_1$. We have exactly four conjugacy classes of involutions contained in $S - U$ which act faithfully on U with the representatives t, tc, b , and bav . The corresponding centralizers in S are $C_S(t) = C_G(t) = \langle t \rangle \times D$ with $D \cong SD_{2^m}$, $m \geq 4$; $C_S(tc) = \langle tc \rangle \times D$ with $D \cong SD_{2^m}$ $m \geq 4$; $C_S(b) = \langle b \rangle \times L$ with $L \cong D_{2^n}$, $n \geq 3$; $C_S(bav) = \langle bav \rangle \times \langle c, ty \rangle$ with $\langle c, ty \rangle \cong Q_{2^n}, n \geq 3$.

We may assume $N_G(S) \neq S$ (otherwise we are finished). Then $N_G(S)$ can fuse $ccl_S(t)$ (the conjugacy class of t in S) only with $ccl_S(tc)$ and so $|N_G(S) : S| = 2$. Obviously, $L - \langle c \rangle$ is a normal subset of involutions in $N_G(S)$ and $L = \langle L - \langle c \rangle \rangle$ which implies that L is normal in $N_G(S)$. Suppose that $N_G(S) \neq G$ (otherwise we are finished). Note that each x in $N_G(S) - S$ sends (by conjugation) $ccl_S(t)$ onto $ccl_S(tc)$. By the above, $N_G(S)$ cannot fuse $ccl_S(b)$ and $ccl_S(bav)$ to any other conjugate class of involutions in S . This gives that $C_{N_G(S)}(b)$ covers $N_G(S)/S$ and also $C_{N_G(S)}(bav)$ covers $N_G(S)/S$. In particular $|C_{N_G(S)}(b)| = |C_{N_G(S)}(bav)| = 2^{n+2}$. The subgroup $K = \langle b, bav \rangle$ is dihedral of order 2^m and $S = KL$. Since both K and L are generated by its non-central involutions, we have $\langle ccl_S(t), ccl_S(tc), ccl_S(b), ccl_S(bav) \rangle = S$.

Let x be any involution in $N_G(S) - S$. Since $(ccl_L(t))^x = ccl_L(tc)$, so x induces an outer involutory automorphism on L which inverts $\langle c \rangle$. Indeed, if $t^x = tc^k$ (k odd), then x inverts $t(tc^k) = c^k$ and so x inverts c . Hence $C_L(x) = \langle z \rangle$ and so, by Theorem 1.7 and Proposition 1.8, $L\langle x \rangle = L_0$ is of maximal class. Since L_0 is generated by its involutions, it follows $L_0 \cong D_{2^{n+1}}$. We have $N_G(S) = S\langle x \rangle$ and so $C_{N_G(S)}(x) = \langle x \rangle \times C_S(x)$. On the other hand $C_L(x) = \langle z \rangle$ and so if $|C_S(x)| = 2^m$, then $C_S(x)$ covers S/L which implies that $L_0 \cong D_{2^{n+1}}$ is normal in $N_G(S) = DL_0 > S$. This contradicts the maximality of S . (See the construction of S .) It follows that there is no involution $x \in N_G(S) - S$ with the property $|C_S(x)| = 2^m$.

Let y' be an element in $G - N_G(S)$ such that y' normalizes $N_G(S)$ and $(y')^2 \in N_G(S)$. If $x = t^{y'} \in N_G(S) - S$, then $C_{N_G(S)}(x) = \langle x \rangle \times C_S(x) \cong \langle t \rangle \times D$ and so $|C_S(x)| = 2^m$, which is a contradiction. If $t^{y'} \in ccl_S(t) \cup ccl_S(tc)$, then there is an $n \in N_G(S)$ such that $t^{y'} = t^n$. But then $t^{y'n^{-1}} = t$ and so $C_G(t) \not\subset N_G(S)$, a contradiction. Hence we must have $t^{y'} \in ccl_S(b)$ or $t^{y'} \in ccl_S(bav)$. We know that $|C_{N_G(S)}(b)| = |C_{N_G(S)}(bav)| = 2^{n+2}$ and on the other hand $|C_{N_G(S)}(t^{y'})| = |C_{N_G(S)}(t)| = 2^{m+1}$. Hence $m = n + 1$. It follows that for each $x \in (ccl_S(t) \cup ccl_S(tc) \cup ccl_S(b) \cup ccl_S(bav)) = P$, we have $|C_{N_G(S)}(x)| = 2^{n+2} = 2^{m+1}$.

Finally, since $S^{y'} \neq S$, there is an $x \in P$ such that $x' = x^{y'} \in N_G(S) - S$. But then $C_{N_G(S)}(x') = \langle x' \rangle \times C_S(x')$ and $|C_S(x')| = 2^m$, which is the final contradiction. It follows that $N_G(S) = G$ and so in case $S \cong \mathcal{S}_1$, the subgroup S is normal in G and $|G/S| \leq 2$.

5°. The case $S \cong \mathcal{S}_2$. We have exactly four conjugacy classes of involutions contained in $S - U$ which act faithfully on U with the representatives t, tc, b , and bav . The corresponding centralizers in S are $C_S(t) = C_G(t) = \langle t \rangle \times D$ with $D \cong SD_{2^m}$, $m \geq 4$; $C_S(tc) = \langle tc \rangle \times \langle a, bav \rangle$ with $\langle a, bav \rangle \cong SD_{2^m}$, $m \geq 4$; $C_S(b) = \langle b \rangle \times \langle yc, t \rangle$ with $\langle yc, t \rangle \cong SD_{2^n}$, $n \geq 4$; $C_S(bav) = \langle bav \rangle \times \langle cy, tc \rangle$ with $\langle cy, tc \rangle \cong SD_{2^n}$, $n \geq 4$.

We assume $N_G(S) \neq S$ (otherwise we are finished). Set $P = \text{ccl}_S(t) \cup \text{ccl}_S(tc) \cup \text{ccl}_S(b) \cup \text{ccl}_S(bav)$. Obviously, $\langle P \rangle = S$ and $P \subseteq G - T$, where $T = C_G(U)$ and $|G : T| = 2$. Suppose also that t is conjugate in $N_G(S)$ to tc but t is not conjugate in $N_G(S)$ to any involution in $S - L$. Then $|N_G(S) : S| = 2$ and since $N_G(S)$ normalizes the set $L - \langle c \rangle$ and $\langle L - \langle c \rangle \rangle = L$, so L is normal in $N_G(S)$. Let x be any involution in $N_G(S) - S$. Since $(\text{ccl}_L(t))^x = \text{ccl}_L(tc)$, we get (as in case $S \cong \mathcal{S}_1$) $L_0 = L\langle x \rangle \cong D_{2^{n+1}}$. We have $C_{N_G(S)}(x) = \langle x \rangle \times C_S(x)$ and $C_L(x) = \langle z \rangle$. If $|C_S(x)| = 2^m$, then $C_S(x)$ covers S/L and so L_0 is normal in $DL_0 > S$. This contradicts the maximality of S . Hence there is no involution $x \in N_G(S) - S$ with $|C_S(x)| = 2^m$. Suppose in addition that $N_G(S) \neq G$ (otherwise we are finished). Let y' be an element in $G - N_G(S)$ such that y' normalizes $N_G(S)$ and $(y')^2 \in N_G(S)$. If $x = t^{y'} \in N_G(S) - S$, then $|C_{N_G(S)}(x)| = 2^{m+1}$ and so $|C_S(x)| = 2^m$, a contradiction. If $t^{y'} \in \text{ccl}_S(t) \cup \text{ccl}_S(tc)$, then $C_G(t) \not\subseteq N_G(S)$ (as in case $S \cong \mathcal{S}_1$), which is a contradiction. Hence we must have $t^{y'} \in \text{ccl}_S(b)$ or $t^{y'} \in \text{ccl}_S(bav)$. Since y' does not normalize S , there is $x' \in P$ such that $x_0 = (x')^{y'} \in N_G(S) - S$. If $N_G(S)$ fuses b with bav , then all involutions in P are fused in $\langle y' \rangle N_G(S)$ to t and so $|C_{N_G(S)}(x_0)| = 2^{m+1}$ and $|C_S(x_0)| = 2^m$, a contradiction. If $N_G(S)$ does not fuse b with bav , then $|C_{N_G(S)}(b)| = |C_{N_G(S)}(bav)| = 2^{n+2}$. Since $|C_{N_G(S)}(t^{y'})| = 2^{m+1}$, so $n+2 = m+1$ and therefore $|C_{N_G(S)}(x_0)| = 2^{n+2} = 2^{m+1}$ and so again $|C_S(x_0)| = 2^m$, a contradiction. Hence we must have $N_G(S) = G$ and so we are done in this case.

Suppose now that t is not conjugate to tc in $N_G(S)$. Then t must be conjugate in $N_G(S)$ to b or to bav . This implies $|N_G(S) : S| = 2$ and $m = n \geq 4$. Each element $x \in N_G(S) - S$ sends $(C_S(t))' = \langle a^2 \rangle$ onto $(C_S(t^x))' = \langle c^2 \rangle$. Suppose that $N_G(S) \neq G$ and let y' be an element in $G - N_G(S)$ such that y' normalizes $N_G(S)$ and $(y')^2 \in N_G(S)$. Since y' does not normalize S , there is an $x' \in P$ such that $x_0 = (x')^{y'} \in N_G(S) - S$, $x_0 \in G - T$, and so x_0 does not centralize U . On the other hand, x_0 sends $\langle y \rangle$ (contained in $\langle a^2 \rangle$) onto $\langle v \rangle$ (contained in $\langle c^2 \rangle$). We have $y^{x_0} = vz^\epsilon$ with $\epsilon = 0, 1$. But then $(yvz^\epsilon)^{x_0} = yvz^\epsilon$ and so x_0 centralizes $U = \langle z, u = yv \rangle$. This is a contradiction and so we have $N_G(S) = G$ also in this case.

It remains to consider the case that t is fused in $N_G(S)$ to all three involutions tc , b , and bav . In that case $m = n \geq 4$ and $|N_G(S) : S| = 4$. Note that L and $K = \langle b, bav \rangle$ are two dihedral normal subgroups both of order 2^m of S containing $\text{ccl}_S(t)$, $\text{ccl}_S(tc)$, $\text{ccl}_S(b)$, and $\text{ccl}_S(bav)$ with $N_G(S)/S$ acting regularly on those four S -classes. Hence for each $x \in N_G(S) - S$ we have either $L^x = L$ and $K^x = K$ or $L^x = K$. Suppose now that $N_G(S) \neq G$ and let y' be an element in $G - N_G(S)$ such that y' normalizes $N_G(S)$ and $(y')^2 \in N_G(S)$. Then $t' = t^{y'} \in N_G(S) - S$. Indeed, if $t' \in S$, then $t' \in P$ and so there is an $n \in N_G(S)$ such that $t' = t^{y'} = t^n$. But then $t^{y'n^{-1}} = t$ and so $C_G(t) \not\leq N_G(S)$, a contradiction. If $L^{t'} = L$ and $K^{t'} = K$, then $(\text{ccl}_L(t))^{t'} = \text{ccl}_L(tc)$ and $(\text{ccl}_K(b))^{t'} = \text{ccl}_K(bav)$. This gives (as in case $S \cong \mathcal{S}_1$) $L\langle t' \rangle \cong D_{2^{m+1}}$ and $K\langle t' \rangle \cong D_{2^{m+1}}$. In particular, t' inverts $\langle c \rangle$ and on $\langle av \rangle$. Hence t' inverts $v \in \langle c^{2^{m-3}} \rangle$ and on $y \in \langle (av)^{2^{m-3}} \rangle = \langle a^{2^{m-3}} \rangle$. From $y^{t'} = y^{-1}$ and $v^{t'} = v^{-1}$, we get $u^{t'} = (yv)^{t'} = y^{-1}v^{-1} = yv = u$. Hence t' centralizes $U = \langle z, u \rangle$ and so $t' \in T$. But $t \in G - T$ and $|G : T| = 2$, which is a contradiction. If $L^{t'} = K$, then $\langle c \rangle^{t'} = \langle av \rangle$ and so $v^{t'} = yz^\mu$, $\mu = 0, 1$. This gives $(yvz^\mu)^{t'} = yvz^\mu$ and $(uz^\mu)^{t'} = uz^\mu$ and so t' centralizes U , which is a contradiction. It follows that we must have $N_G(S) = G$ also in this case. We have proved that in case $S \cong \mathcal{S}_2$, the subgroup S is normal in G , $|G : S| \leq 4$, and if $|G/S| = 4$, then $m = n \geq 4$.

6°. Cases $S \cong \mathcal{S}_3$ and $S \cong \mathcal{S}_4$. We have exactly four conjugacy classes of involutions contained in $S - U$ which act faithfully on U with the representatives t , tc , b , and bav . The corresponding centralizers in S in case $S \cong \mathcal{S}_3$ are $C_S(t) = C_G(t) = \langle t \rangle \times D$ with $D \cong \text{SD}_{2^m}$, $m \geq 4$; $C_S(tc) = \langle tc \rangle \times \langle av, b \rangle$ with $\langle av, b \rangle \cong D_{2^m}$, $m \geq 4$; $C_S(b) = \langle b \rangle \times L$ with $L \cong D_{2^n}$, $n \geq 4$; $C_S(bav) = \langle bav \rangle \times \langle cy, tc \rangle$ with $\langle cy, tc \rangle \cong \text{SD}_{2^n}$, $n \geq 4$.

The centralizers in S in case $S \cong \mathcal{S}_4$ are $C_S(t) = C_G(t) = \langle t \rangle \times D$ with $D \cong \text{SD}_{2^m}$, $m \geq 4$; $C_S(tc) = \langle tc \rangle \times \langle av, ba \rangle$ with $\langle av, ba \rangle \cong Q_{2^m}$, $m \geq 4$; $C_S(b) = \langle b \rangle \times \langle cy, t \rangle$ with $\langle cy, t \rangle \cong \text{SD}_{2^n}$, $n \geq 4$; $C_S(bav) = \langle bav \rangle \times \langle c, ty \rangle$ with $\langle c, ty \rangle \cong Q_{2^n}$, $n \geq 4$.

Suppose that $S \neq N_G(S)$. Then $N_G(S)$ can fuse t only with an involution in $\text{ccl}_S(bav)$ when $S \cong \mathcal{S}_3$ and only with an involution in $\text{ccl}_S(b)$ when $S \cong \mathcal{S}_4$. This gives $m = n$ and $|N_G(S)/S| = 2$. Set $P = \text{ccl}_S(t) \cup \text{ccl}_S(tc) \cup \text{ccl}_S(b) \cup \text{ccl}_S(bav)$. Obviously, $\langle P \rangle = S$ and $P \subseteq G - T$, where $T = C_G(U)$ and $|G : T| = 2$. Assume that $N_G(S) \neq G$ and let y' be an element in $G - N_G(S)$ such that y' normalizes $N_G(S)$ and $(y')^2 \in N_G(S)$. Since y' does not normalize S , there is $x' \in P$ such that $x_0 = (x')^{y'} \in N_G(S) - S$, $x_0 \in G - T$ and so x_0 does not centralize U . Since $(\text{ccl}_S(t))^{x_0} = \text{ccl}_S(t^{x_0})$, where $t^{x_0} \in \text{ccl}_S(bav)$ in case $S \cong \mathcal{S}_3$ and $t^{x_0} \in \text{ccl}_S(b)$ in case $S \cong \mathcal{S}_4$, so x_0 sends $(C_S(t))' = \langle a^2 \rangle$ onto $(C_S(t^{x_0}))' = \langle c^2 \rangle$. Indeed, $(C_S(bav))' = \langle c^2 \rangle$ in case $S \cong \mathcal{S}_3$ and $(C_S(b))' = \langle c^2 \rangle$ in case $S \cong \mathcal{S}_4$ and in both cases $\langle c^2 \rangle$ is normal in S . We get $\langle a^2 \rangle^{x_0} = \langle c^2 \rangle$ and so, in particular, $y^{x_0} = vz^\epsilon$, $\epsilon = 0, 1$ and so $(yvz^\epsilon)^{x_0} = yvz^\epsilon$ or $(uz^\epsilon)^{x_0} = uz^\epsilon$ and so x_0 centralizes $U =$

$\langle z, u = yv \rangle$. This is a contradiction and so we must have $N_G(S) = G$. We have obtained in both cases $S \cong \mathcal{S}_3$ and $S \cong \mathcal{S}_4$ that $|G : S| \leq 2$ and if $|G : S| = 2$, then $m = n \geq 4$. We have proved the following result.

Theorem 51.14. *Let G be a 2-group which has a self-centralizing elementary abelian subgroup E of order 8 with $E \not\subseteq \Phi(G)$. We assume that G has the unique normal four-subgroup U and set $T = C_G(U)$. Suppose that there is an involution $t \in E - \Phi(G)$ such that $C_G(t) = \langle t \rangle \times D$ with $D \cong SD_{2^m}$, $m \geq 4$. Finally, assume $t \notin U$ and in that case we have proved that we may assume $t \in G - T$. Then G has a (large) normal subgroup S containing $UC_G(t)$ which is isomorphic to one of the groups \mathcal{S}_i for $i = 1, 2, 3, 4$ (see Definition 1) so that $|G/S| \leq 4$. More precisely,*

- (a) if $S \cong \mathcal{S}_1$, then $|G/S| \leq 2$;
- (b) if $S \cong \mathcal{S}_2$, then $|G/S| \leq 4$ and if $|G/S| = 4$, then $m = n \geq 4$;
- (c) if $S \cong \mathcal{S}_3$, then $|G/S| \leq 2$ and if $|G/S| = 2$, then $m = n \geq 4$;
- (d) if $S \cong \mathcal{S}_4$, then $|G/S| \leq 2$ and if $|G/S| = 2$, then $m = n \geq 4$.

We have to analyze three remaining cases \mathcal{S}_5 , \mathcal{S}_6 , and \mathcal{S}_7 for the structure of S .

7^o. *The case $S \cong \mathcal{S}_5$.* We have exactly four conjugacy classes of involutions contained in $S - U$ which act faithfully on U with the representatives t , tc , b , and ba . The corresponding centralizers in S are $C_S(t) = C_G(t) = \langle t \rangle \times D$ with $D \cong D_{2^m}$, $m \geq 3$; $C_S(tc) = \langle tc \rangle \times \langle a, bv \rangle$ with $\langle v, bv \rangle \cong Q_{2^m}$, $m \geq 3$; $C_S(b) = \langle b \rangle \times \langle yc, t \rangle$ with $\langle yc, t \rangle \cong SD_{2^n}$, $n \geq 4$; $C_S(ba) = \langle ba \rangle \times \langle yc, t \rangle$ with $\langle yc, t \rangle \cong SD_{2^n}$, $n \geq 4$.

We see that t cannot be fused in $N_G(S)$ to any of the involutions tc , b , or ba and this implies $S = G$. By our assumption, G has the unique normal 4-subgroup U and so $m \geq 4$.

8^o. *The case $S \cong \mathcal{S}_6$.* We have exactly four conjugacy classes of involutions contained in $S - U$ which act faithfully on U with the representatives t , tc , b , and ba . The corresponding centralizers in S are $C_S(t) = C_G(t) = \langle t \rangle \times D$ with $D \cong D_{2^m}$, $m \geq 3$; $C_S(tc) = \langle tc \rangle \times \langle av, b \rangle$ with $\langle av, b \rangle \cong SD_{2^m}$, $m \geq 4$ and $\langle av, b \rangle \cong D_8$ if $m = 3$ (in which case tc centralizes U), $C_S(b) = \langle b \rangle \times L$ with $L \cong D_{2^n}$, $n \geq 4$; $C_S(ba) = \langle ba \rangle \times \langle cy, t \rangle$ with $\langle cy, t \rangle \cong SD_{2^n}$, $n \geq 4$.

Suppose that $N_G(S) \neq S$. Since $N_G(S)$ can fuse t only with an involution in $ccl_S(b)$, we have $m = n \geq 4$ and $|N_G(S)/S| = 2$. Set $P = ccl_S(t) \cup ccl_S(tc) \cup ccl_S(b) \cup ccl_S(ba)$. Obviously, $\langle P \rangle = S$ and $P \subseteq G - T$, where $T = C_G(U)$ and $|G : T| = 2$. Assume that $N_G(S) \neq G$ and let y' be an element in $G - N_G(S)$ such that y' normalizes $N_G(S)$ and $(y')^2 \in N_G(S)$. Since y' does not normalize S , there is an $x' \in P$ such that $x_0 = (x')^{y'} \in N_G(S) - S$, $x_0 \in G - T$ and so x_0 does not centralize U . Then x_0 sends (by conjugation) t onto an S -conjugate of b and so x_0 sends $(C_S(t))' = \langle a^2 \rangle$ onto $(C_S(b))' = \langle c^2 \rangle$. Indeed, each S -conjugate b' of b has the property $C_S(b') = \langle b' \rangle \times L$ because L is normal in S . In particular, $y^{x_0} = vz^\epsilon$, $\epsilon = 0, 1$ and so $yvz^\epsilon = uz^\epsilon$ is centralized by x_0 . Hence x_0 centralizes $U = \langle z, u \rangle$,

which is a contradiction. Hence we must have $N_G(S) = G$ which implies that in case $S \cong \mathcal{S}_6$ we get $|G/S| \leq 2$ and if $|G/S| = 2$, then $m = n \geq 4$.

It remains to consider the case $S \cong \mathcal{S}_7$ which is rather difficult since there are several possibilities for the fusion of the involution t with other involutions in $S - U$ which act faithfully on U .

9°. *The case $S \cong \mathcal{S}_7$.* We have exactly four conjugacy classes of involutions contained in $S - U$ which act faithfully on U with the representatives t , tc , b , and ba . The corresponding centralizers in S are $C_S(t) = C_G(t) = \langle t \rangle \times D$ with $D \cong D_{2^m}$, $m \geq 3$; $C_S(tc) = \langle tc \rangle \times D$ with $D \cong D_{2^m}$, $m \geq 3$; $C_S(b) = \langle b \rangle \times L$ with $L \cong D_{2^n}$, $n \geq 3$; $C_S(ba) = \langle ba \rangle \times L$ with $L \cong D_{2^n}$, $n \geq 3$.

Suppose that $N_G(S) \neq S$ (otherwise we are finished). Set $P = \text{ccl}_S(t) \cup \text{ccl}_S(tc) \cup \text{ccl}_S(b) \cup \text{ccl}_S(ba)$. Obviously, $\langle P \rangle = S$ and $P \subseteq G - T$, where $T = C_G(U)$ and $|G : T| = 2$. Suppose also that t is not fused in $N_G(S)$ to any involution in $S - L$. Then $N_G(S)$ fuses t with tc and so $|N_G(S) : S| = 2$ and L is normal in $N_G(S)$ since $L - \langle c \rangle$ is a normal subset in $N_G(S)$. Let x be any involution in $N_G(S) - S$. Since $(\text{ccl}_L(t))^x = \text{ccl}_L(tc)$, we get $L_0 = L\langle x \rangle \cong D_{2^{n+1}}$ (as in case $S \cong \mathcal{S}_1$). We have $C_{N_G(S)}(x) = \langle x \rangle \times C_S(x)$ and $C_L(x) = \langle z \rangle = Z(L) = Z(L_0)$. If $|C_S(x)| = 2^m$, then $C_S(x)$ covers S/L and so L_0 is normal in $DL_0 > L$. This contradicts the maximality of S . Hence there is no involution $x \in N_G(S) - S$ such that $|C_S(x)| = 2^m$. Suppose in addition that $N_G(S) \neq G$. Let y' be an element in $G - N_G(S)$ such that y' normalizes $N_G(S)$ and $(y')^2 \in N_G(S)$. If $x = t^{y'} \in N_G(S) - S$, then $|C_{N_G(S)}(x)| = 2^{m+1}$ and so $|C_S(x)| = 2^m$, a contradiction. If $t^{y'} \in \text{ccl}_S(t) \cup \text{ccl}_S(tc)$, then (as before) $C_G(t) \not\subseteq N_G(S)$, a contradiction. Hence $t^{y'} \in \text{ccl}_S(b)$ or $t^{y'} \in \text{ccl}_S(ba)$. Since $y' \notin N_G(S)$, there is an $x' \in P$ with $x_0 = (x')^{y'} \in N_G(S) - S$. If $N_G(S)$ fuses b and ba , then all involutions in P are fused in $\langle y' \rangle N_G(S)$ to t and so $|C_{N_G(S)}(x_0)| = 2^{m+1}$ and $|C_S(x_0)| = 2^m$, a contradiction. If $N_G(S)$ does not fuse b and ba , then $|C_{N_G(S)}(b)| = |C_{N_G(S)}(ba)| = 2^{n+2}$ and since $|C_{N_G(S)}(t^{y'})| = 2^{m+1}$, so we get $n + 2 = m + 1$ and therefore $|C_{N_G(S)}(x_0)| = 2^{n+2} = 2^{m+1}$ and so again $|C_S(x_0)| = 2^m$, a contradiction. Hence we must have $N_G(S) = G$ in this case.

Suppose that t is not conjugate to tc in $N_G(S)$. Then t must be conjugate in $N_G(S)$ to b or ba . This implies $|N_G(S) : S| = 2$ and $m = n \geq 3$.

We make here the following simple observation. All involutions in $S - (D \cup L)$ centralize U and so lie in T . All noncentral involutions in D and L lie in $G - T$. Since S is the central product $S = D * L$ of D and L , it follows that D and L are the only dihedral normal subgroups of order 2^m of S all of whose noncentral involutions belong to $G - T$. Therefore for each element $x \in N_G(S) - S$, we have $L^x = D$ since $t^x \in \text{ccl}_S(b)$ or $t^x \in \text{ccl}_S(ba)$. In particular, $\langle c \rangle^x = \langle a \rangle$.

Suppose again that $N_G(S) \neq G$. Let y' be an element in $G - N_G(S)$ such that y' normalizes $N_G(S)$ and $(y')^2 \in N_G(S)$. Since $y' \notin N_G(S)$, there is an $x' \in P$ such that $x_0 = (x')^{y'} \in N_G(S) - S$ and $x_0 \in G - T$ and so x_0 does not centralize U . Note that $\langle P \rangle = S$ and $P \subseteq G - T$. On the other hand (by the above), $\langle c \rangle^{x_0} = \langle a \rangle$

and so $v^{x_0} = yz^\mu$, $\mu = 0, 1$. But then $(yvz^\mu)^{x_0} = yvz^\mu$, where $yv = u$. Hence x_0 centralizes $U = \langle z, u \rangle$, a contradiction. Thus in this case we have also $N_G(S) = G$.

It remains to analyze the case that t is fused in $N_G(S)$ to all three involutions tc, b , and ba . In that case $m = n \geq 3$ and $|N_G(S) : S| = 4$. By the above observation, for each $x \in N_G(S) - S$, we have either $L^x = L$ and $D^x = D$ or $L^x = D$. Suppose now that $N_G(S) \neq G$. Let y' be an element in $G - N_G(S)$ such that y' normalizes $N_G(S)$ and $(y')^2 \in N_G(S)$. Then $t' = t^{y'} \in N_G(S) - S$. Otherwise, $t^{y'} \in P$ and so there is an $n \in N_G(S)$ with $t^{y'} = t^n$ and so $t^{y'n^{-1}} = t$, which is a contradiction since $y'n^{-1} \notin N_G(S)$. If $L^{t'} = L$ and $D^{t'} = D$, then $(\text{ccl}_L(t))^{t'} = \text{ccl}_L(tc)$ and $(\text{ccl}_D(b))^{t'} = \text{ccl}_D(ba)$ imply (as before) that $L\langle t' \rangle \cong D\langle t' \rangle \cong D_{2m+1}$. In particular, t' inverts v and y which gives $u^{t'} = (yv)^{t'} = y^{-1}v^{-1} = yv = u$ and so t' centralizes U . This is not possible since t' (together with t) lies in $G - T$. If $L^{t'} = D$, then $\langle c \rangle^{t'} = \langle a \rangle$ and so in particular $v^{t'} = yz^\epsilon$, $\epsilon = 0, 1$. But then t' centralizes $yv = u$ and so t' centralizes U , which is again a contradiction. Hence we must have also in this case $N_G(S) = G$.

We have proved the following final result.

Theorem 51.15. *Let G be a 2-group which has a self-centralizing elementary abelian subgroup E of order 8 with $E \not\leq \Phi(G)$. We assume that G has the unique normal 4-subgroup U and set $T = C_G(U)$. Suppose that there is an involution $t \in E - \Phi(G)$ such that $C_G(t) = \langle t \rangle \times D$ with $D \cong D_{2m}$, $m \geq 3$. Also, in case $D \cong D_8$ we assume in addition that G does not possess a normal elementary abelian subgroup of order 8. Finally, assume $t \notin U$ and in that case we have proved that we may assume $t \in G - T$. Then G has a (large) normal subgroup S containing $UC_G(t)$ which is isomorphic to one of the groups \mathcal{S}_i for $i = 5, 6, 7$ (see Definition 1) so that $|G/S| \leq 4$. More precisely,*

- (a) *If $S \cong \mathcal{S}_5$, then $S = G$ and $m \geq 4, n \geq 4$;*
- (b) *if $S \cong \mathcal{S}_6$, then $|G/S| \leq 2$ and if $|G/S| = 2$, then $m = n \geq 4$;*
- (c) *if $S \cong \mathcal{S}_7$, then $|G/S| \leq 4$ and if $|G/S| = 4$, then $m = n \geq 3$.*

§52

2-groups with Ω_2 -subgroup of small order

The main results of this section are due to Janko [Jan6].

In Lemma 42.1 finite 2-groups G have been determined with $|\Omega_2(G)| \leq 8$. In this section we do the next step and determine the finite 2-groups G with $|G| > 16$ and $|\Omega_2(G)| = 16$ ($= \Omega_2$ -groups). All nonmetacyclic Ω_2 -groups will be given in terms of generators and relations. For more general result, see §55.

If $|G| = 16$, then $\Omega_2(G) < G$ if and only if $G \notin \{C_{16}, C_8 \times C_2, M_{16}\}$. Therefore, we consider in this section only groups of order > 16 .

If $|\Omega_2(G)| = 16$, then the numbers $c_1(G)$ and $c_2(G)$ are small. This observation allows us to generalize the main result of this section (see §55).

In subsection 1^o we study Ω_2 -groups G which have no normal subgroups isomorphic to E_8 . Using the main theorem from §50, we obtain three classes of such 2-groups and one exceptional group of order 2^5 (Theorem 52.1).

In subsection 2^o we study nonabelian Ω_2 -groups G with normal subgroup isomorphic to E_8 . It is easy to see that then G/E is either cyclic or generalized quaternion. If G/E is cyclic, then we get three classes of groups (Theorem 52.2). If G/E is generalized quaternion and $E \not\leq \Phi(G)$, then we get one class of groups (Theorem 52.4). If G/E is generalized quaternion and $E \leq \Phi(G)$, we get two classes of groups (Theorem 52.5).

In subsection 3^o we investigate 2-groups G with $|G| > 16$ which have exactly one subgroup of order 16 and exponent 4. It turns out that a 2-group G has this property if and only if $|G| > 16$ and $|\Omega_2(G)| = 16$ (Theorem 52.6).

It is interesting to note that, for a Ω_2 -group G , there are exactly five possibilities for the structure of $\Omega_2(G)$: $Q_8 * C_4$, $Q_8 \times C_2$, $D_8 \times C_2$, $C_4 \times C_2 \times C_2$, $C_4 \times C_4$ (note that $Q_8 * C_4 \cong D_8 * C_4$). In fact, if $\Omega_2(G) \cong Q_8 \times C_2$ or $D_8 \times C_2$ and $|G| > 16$, then we get exactly one group of order 2^5 in each case (see Theorem 52.1(d) and Theorem 52.2(a) for $n = 2$). In other three cases for the structure of $\Omega_2(G)$ we get infinitely many groups.

In subsection 4^o we consider a similar problem. In [Ber25, §48] the 2-groups G have been considered which have exactly one abelian subgroup of type $(4, 2)$. It was shown that either $|\Omega_2(G)| = 8$ (and then G is isomorphic to one of the groups in Lemma 42.1) or G has a self-centralizing elementary abelian subgroup of order 8 (see §51). We improve this result by determining completely the groups of the second possibility (Theorem 52.7). Finally, Theorem 52.8 shows that our result also slightly

improves the classification of 2-groups with exactly two cyclic subgroups of order 4 given in Theorem 43.4.

Lemma A ([Ber25, §48]). *Let G be a metacyclic 2-group of order $> 2^4$. If $|\Omega_2(G)| = 2^4$, then $\Omega_2(G) \cong C_4 \times C_4$.*

Proof. Let $|G| = 2^m > 2^4$. Assume that $\Omega_2(G) = H$ is nonabelian. We want to show that this assumption leads to a contradiction. If H is not minimal nonabelian, then Proposition 10.19 implies that G is of maximal class. But then $\Omega_2(G) = G$, a contradiction. Suppose that H has a cyclic subgroup of index 2. Since in that case H is minimal nonabelian, $H \cong M_{24}$ (Theorem 1.2). But then $\Omega_2(G) = \Omega_2(H)$ is abelian of type $(4, 2)$ which contradicts the fact that $H = \Omega_2(G)$. Exercise 1.8A implies $H = \langle a, b \mid a^4 = b^4 = 1, a^b = a^{-1} \rangle$. It follows that $Z(H) = \langle a^2, b^2 \rangle = \Omega_1(H) = \Omega_1(G)$, $H' = \langle a^2 \rangle$, and $Z = \langle b^2 \rangle$ is a characteristic subgroup of order 2 in H so $Z \triangleleft G$. Indeed, b^2 is a square in H , a^2b^2 is not a square in H (check!), and $Z(H) - H' = \{b^2, a^2b^2\}$. Thus Z is central in G . Since $H/Z \cong D_8$, Proposition 10.19 implies that G/Z is of maximal class. All involutions in G/Z lie in H/Z and so $G/Z \cong SD_{16}$ and $|G| = 2^5$. But there are elements of order 4 in $(G/Z) - (H/Z)$ whose square lies in $Z(G/Z) = \langle a^2, b^2 \rangle / Z$. Hence there is an element $x \in G - H$ such that $x^2 \in \langle a^2, b^2 \rangle$ and so $o(x) \leq 4$, which is the final contradiction. Thus, $H \cong C_4 \times C_4$. \square

1^o. *G has no normal elementary abelian subgroups of order 8.* In this subsection we prove the following result.

Theorem 52.1. *Let G be a 2-group of order $> 2^4$ satisfying $|\Omega_2(G)| = 2^4$. Suppose, in addition, that G has no normal elementary abelian subgroups of order 8. Then we have one of the following four possibilities:*

- (a) *$G = D * C$ (the central product) with $D \cong D_8$, $D \cap C = Z(D)$, and C is cyclic of order ≥ 8 . Here we have $\Omega_2(G) \cong Q_8 * C_4 \cong D_8 * C_4$. (For such groups, see Appendix 16; it is proved there, that also $G \cong Q_8 * C$.)*
- (b) *G is metacyclic of order $\geq 2^5$ (in that case, by Lemma A, $\Omega_2(G) \cong C_4 \times C_4$).*
- (c) *$G = QS$, where $Q \cong Q_8$, Q is normal in G , S is cyclic of order ≥ 16 , $Q \cap S = Z(Q)$, and if C is the subgroup of index 2 in S , then $C_G(Q) = C$. Setting $Q = \langle a, b \rangle$ and $S = \langle s \rangle$, we have $a^s = a^{-1}$ and $b^s = ba$. Here we have $\Omega_2(G) \cong Q_8 * C_4$.*
- (d) *The exceptional group G of order 2^5 has a maximal subgroup $M = \langle u \rangle \times Q$, where u is an involution, $Q \cong Q_8$, $C_G(u) = M$ and G is isomorphic to the group $A2(a)$ from Theorem 49.1. We have $\Omega_2(G) = M \cong Q_8 \times C_2$.*

Proof. We may assume that G is nonabelian. If G were of maximal class, then $\Omega_2(G) = G$, a contradiction since $|G| > 2^4$. Since G is neither abelian nor of maximal class, we may apply main theorem from §50 about 2-groups without nor-

mal elementary abelian subgroup of order 8. Then G has a normal metacyclic subgroup N such that $C_G(\Omega_2(N)) \leq N$, G/N is isomorphic to a subgroup of D_8 , and $W = \Omega_2(N)$ is either abelian of type $(4, 4)$ or N is abelian of type $(2^j, 2)$, $j \geq 2$. However, if $W \cong C_4 \times C_4$, then $W = \Omega_2(G)$ since $|\Omega_2(W)| = 2^4 = |\Omega_2(G)|$, and Theorem 41.1 and Remark 41.2 imply that G is metacyclic. This gives the case (b) of our theorem, by Lemma A. In what follows we assume that G is not metacyclic.

We assume in the sequel that N is abelian of type $(2^j, 2)$, $j \geq 2$ and so $W = \Omega_2(N)$ is abelian of type $(4, 2)$. By hypothesis, $|\Omega_2(G) : W| = 2$.

Suppose that G has at least two distinct normal four-subgroups. Then it follows from Theorem 50.2 that $G = D * C$, where D is dihedral of order 8 and C is either cyclic or of maximal class and $D \cap C = Z(D)$. In view of $|\Omega_2(G)| = 16$, C must be cyclic of order ≥ 8 since $|G| > 2^4$, and this gives the case (a) of our theorem.

Next we assume that G has the unique normal four-subgroup $W_0 = \Omega_1(W) = \Omega_1(N)$. Also we have $C_G(W) = N$ (N is abelian of type $(2^j, 2)$, $j \geq 2$).

Set $\tilde{W} = \Omega_2(G)$ so that $\tilde{W} \cap N = W$, $|\tilde{W} : W| = 2$, and \tilde{W} is nonabelian (the last assertion follows from $C_G(W) = N \not\leq \tilde{W}$). If \tilde{W} is metacyclic, then Theorem 41.1 and Remark 41.2 imply that G is metacyclic. But then Lemma A gives a contradiction. Thus \tilde{W} is nonabelian non-metacyclic. In particular, $\exp(\tilde{W}) = 4$ (see Theorem 1.2). Proposition 1.6 gives $|\tilde{W}/\tilde{W}'| = 8$ and so $|\tilde{W}'| = 2$. By Lemma 1.1, $|\tilde{W}| = 2|\tilde{W}'||Z(\tilde{W})|$ and so $|Z(\tilde{W})| = 4$ and $Z(\tilde{W}) < W$.

First assume that $Z(\tilde{W}) = \langle v \rangle \cong C_4$ is cyclic and set $z = v^2$, $W_0 = \langle z, u \rangle = \Omega_1(W)$. Since $\{1\} < \tilde{W}' < \langle v \rangle$ (by the previous paragraph, $|\tilde{W}| = 2$), we have $\tilde{W}' = \langle z \rangle$. For any $x \in \tilde{W} - W$, we have $x^2 \in Z(\tilde{W}) = \langle v \rangle$ (indeed, $\tilde{W}/Z(\tilde{W})$ is elementary abelian). But \tilde{W} has no elements of order 8 and so $x^2 \in \langle z \rangle$ and $u^x = uz$ since $C_{\tilde{W}}(u) = W$. It follows that the nonabelian subgroup $W_0\langle x \rangle \cong D_8$ (it is nonabelian since $W_0 \not\leq Z(\tilde{W})$) and so, since D_8 has five involutions, we may assume that x is an involution. Then \tilde{W} is the central product of $\langle u, x \rangle \cong D_8$ and $\langle v \rangle = Z(\tilde{W}) \cong C_4$ with $\langle v \rangle \cap \langle u, x \rangle = \langle z \rangle$ and $(ux)^2 = z$. We set $Q = \langle ux, vx \rangle \cong Q_8$ and see that $\tilde{W} = Q * \langle v \rangle$ is also the central product of Q_8 and C_4 (see also Appendix 16, subsection 1^o). All six elements in $\tilde{W} - (Q \cup \langle v \rangle)$ are involutions and therefore Q is the unique quaternion subgroup of $\tilde{W} = \Omega_2(G)$ and so Q is characteristic in \tilde{W} hence normal in G (see also Appendix 16). There are exactly three four-subgroups in \tilde{W} and one of them is $W_0 = \langle z, u \rangle$ and this one is normal in G . Since G has exactly one normal four-subgroup, it follows that the other two four-subgroups in \tilde{W} are conjugate to each other in G . Set $C = C_G(Q)$. Obviously C is normal in G and $C \cap \tilde{W} = \langle v \rangle$. But $\langle v \rangle$ is the unique subgroup of order 4 in C (indeed, all subgroups of G of order 4 are contained in \tilde{W}) so C is cyclic, by Proposition 1.3, and $\tilde{W}C = Q * C$ with $Q \cap C = \langle z \rangle$. Set $Q = \langle a, b \rangle$, where we choose the generator a so that $u = av$. Since $W_0 = \Omega_1(W) = \langle z, u \rangle$ and $\langle v \rangle = Z(\tilde{W})$ are both normal in G , it follows that $\langle a \rangle$ ($\leq W$) is normal in G (indeed, W has exactly three subgroups of order 4). Every four-subgroup L is normal in \tilde{W} . Indeed, L is characteristic in $LZ(\tilde{W})$, which is normal in \tilde{W} ; it follows that all four-subgroups are normal in $Q * C$. The four-

subgroups $\langle bv, z \rangle$ and $\langle bav, z \rangle$ must be conjugate in G since they are not normal in G and are contained in \tilde{W} ($\leq Q * C$) (\tilde{W} has exactly three four-subgroups and exactly one of them is normal in G). Therefore $Q * C < G$ so $|G : (Q * C)| = 2$, by the product formula, and $G/(Q * C)$ induces an outer automorphism α on Q normalizing $\langle a \rangle$ and sending $\langle b \rangle$ onto $\langle ba \rangle$. A Sylow 2-subgroup of $\text{Aut}(Q)$ is isomorphic to D_8 . It follows that $G/C \cong D_8$ and so there is an element $s \in G - (Q * C)$ such that $s^2 \in C$ and $b^s = ba$. If $a^s = a$, then $(ba)^s = ba^2 = b^{-1}$ and so $ba = (b^s)^{-1} = (ba)^{-1}$, which is a contradiction. It follows that $a^s = a^{-1}$. It remains to determine s^2 . Set $\langle s \rangle C = S$ and we see that C is a cyclic subgroup of index 2 in S . Since $o(s) \geq 8$ (indeed, all elements of G of order ≤ 4 are contained in $\tilde{W} \leq Q * C$), we have $o(s^2) \geq 4$ and therefore $|\text{Z}(S)| \geq 4$. The same argument shows that all elements in $S - C$ have order ≥ 8 . It follows from Theorem 1.2 that S is cyclic. We may set $s^2 = c$, where $\langle c \rangle = C$. We compute

$$(sb)^2 = sbsb = s^2b^s b = cbab = cabzb = cab^2z = cazz = ca.$$

If $|C| = 4$, then $C = \langle v \rangle$ and so ca is an involution. But then $o(sb) = 4$, by the displayed formula, and this is a contradiction since $sb \notin \tilde{W}$. Thus $|C| \geq 8$ and so $o(s) \geq 16$. We have obtained the groups stated in part (c) of our theorem.

Now suppose that $\text{Z}(\tilde{W}) \cong E_4$, the four-group, so that $\text{Z}(\tilde{W}) = W_0 = \Omega_1(W) = \Omega_1(N) = \langle z, u \rangle$, where $z = v^2$ and $W = \langle u \rangle \times \langle v \rangle \cong C_2 \times C_4$.

If \tilde{W} is minimal nonabelian, then the fact that \tilde{W} is nonmetacyclic implies with the help of Exercise 1.8A that $\tilde{W} = \langle a, b \mid [a, b] = c, a^4 = b^2 = c^2 = [a, c] = [b, c] = 1 \rangle$. We see that $\text{Z}(\tilde{W}) = \Phi(\tilde{W}) = \langle a^2, c \rangle \cong E_4$ and \tilde{W} has exactly three maximal subgroups $\langle a^2, c, b \rangle \cong E_8$, $\langle a, c \rangle \cong C_4 \times C_2$, $\langle ba, c \rangle \cong C_4 \times C_2$ since $(ba)^2 = a[a, b]a = aca = a^2c$. Hence $\langle a^2, c, b \rangle$ is normal in G , contrary to the assumption of this subsection.

We have proved that \tilde{W} is not minimal nonabelian. Let D be a minimal nonabelian subgroup of \tilde{W} (of order 8). If $u \in \text{Z}(\tilde{W}) - D$, then $\tilde{W} = \langle u \rangle \times D$ and $\Phi(\tilde{W}) = \tilde{W}' = \Phi(D) = \Omega_1(D) = \langle z \rangle$ since $z = v^2$.

Suppose first that $D \cong D_8$. Let t be an involution in $\tilde{W} - W$ (t exists since $c_1(\tilde{W}) = 7 > 5 = c_1(D) > 3 = c_1(W)$). Since $[v, t] = z = v^2$ ($\langle v \rangle$ is normal in \tilde{W} and it is not contained in $\text{Z}(\tilde{W}) \cong E_4$), t inverts $\langle v \rangle$ and so we may set $D = \langle v, t \rangle$, where $\tilde{W} = \langle u \rangle \times D$. Since t inverts $\Omega_2(N) = W$ (indeed, t centralizes $\Omega_1(N)$ and both cyclic subgroups of W of order 4 are t -invariant but not centralized by t), it follows that $C_N(t) = W_0 = \langle z, u \rangle$. Assume that $N - W$ contains an element x of order 8 (i.e., $j > 2$; by the above, N is abelian of type $(2^j, 2)$). Then Theorem 51.2 implies $x^t = x^{-1}w_0$ with $w_0 \in W_0$. But then $(tx)^2 = (txt)x = x^tx = x^{-1}w_0x = w_0$ and therefore $o(tx) \leq 4$ with $tx \notin \tilde{W}$, a contradiction. Thus, x does not exist so $N = W$ is abelian of type $(4, 2)$. Since t inverts $N = W$, all eight elements in $\tilde{W} - N = \tilde{W} - W$ are involutions: indeed, $\tilde{W} = \langle t \rangle \cdot W$. In particular, no involution in $\tilde{W} - N$ is a square in G (otherwise, G has an element of order 4 not contained in \tilde{W}) and so $G/N \cong E_4$ (indeed, G/N is isomorphic to a subgroup of

$\text{Aut}(W) \cong D_8$ and $|G : N| > 2$) and $|G| = 2^5$. All elements in $G - \tilde{W}$ must be of order 8 and so for any $y \in G - \tilde{W}$, $y^2 \in N - W_0 = W - W_0$ since $G/N \cong E_4$. Replacing $\langle uv \rangle$ with $\langle v \rangle$ and v with v^{-1} , if necessary, we may assume that $y^2 = v$ since $c_2(W) = 2$. Since $C_G(N) = N (= \langle y^2, u \rangle)$, we get $u^y = uz$, and so $y^u = yz$. Thus $\langle y, u \rangle \cong M_{24}$ and $\langle y, u \rangle > N$. The cyclic group $\langle v \rangle = Z(\langle y, u \rangle)$ of order 4 is normal in G and $C_G(v) = \langle y \rangle N \cong M_{24}$. Since ty is also an element of order 8, we have $(ty)^2 \in N - W_0$. If $(ty)^2 \in \langle v \rangle$, then $C_G(v) \geq \langle N, y, ty \rangle = G$, a contradiction. Thus $(ty)^2 \in \langle uv \rangle$. If $(ty)^2 = (uv)^{-1} = (uz)v$, then replacing u with uz , we may assume from the start that $(ty)^2 = uv$. We have $uv = tyty = ty^2t^y = tvt^y$. It follows that $t^y = v^{-1}tuv = t^v u^v = tuz$, and so y normalizes the elementary abelian subgroup $E = \langle z, u, t \rangle$ of order 8. Since E is normal in \tilde{W} , E is also normal in $G = \langle \tilde{W}, y \rangle$, contrary to the assumption of this subsection.

Finally, let $D \cong Q_8$ so that $\tilde{W} = \langle u \rangle \times D$, $Z(D) = \langle z \rangle$, $z = v^2$, and $D \cap N = \langle v \rangle$. Take $r \in D - \langle v \rangle$. We have $r^2 = z$ with $z \in Z(G)$ and so r induces an involutory automorphism on the abelian group N of type $(2^j, 2)$, $j \geq 2$. Since r inverts $W = \langle u, v \rangle = \Omega_2(N)$, it follows that $C_N(r) = W_0 = \langle u, z \rangle$. Then Theorem 51.2 implies that r inverts N/W_0 . Suppose that $W < N$ (i.e., $j > 2$) and let $x \in N - W$. We get $x^r = x^{-1}w_0$ with $w_0 \in W_0$ and so $(rx)^2 = rxrx = r^2x^r x = zx^{-1}w_0x = zw_0 \in W_0$. Since $rx \notin \tilde{W} = \Omega_2(G)$ and $o(rx) \leq 4$, we get a contradiction. We have proved that $N = W = C_G(N)$ is abelian of type $(4, 2)$. We have $|G| \leq 2^6$.

Set $S = C_G(W_0)$ so that $S \geq \tilde{W}$ and S/N stabilizes the chain $N > W_0 > \{1\}$ since $|N/W_0| = 2$. Hence S/N is elementary abelian of order ≤ 4 . Suppose that $S > \tilde{W}$; then S/N is a four-group. Let \tilde{S}/N be a subgroup of order 2 in S/N distinct from \tilde{W}/N . Thus $\tilde{S} \cap \tilde{W} = N$. Take an element $y \in \tilde{S} - N$ so that $o(y) = 8$ and therefore $y^2 \in N - W_0$. But then y centralizes $\langle y^2, W_0 \rangle = N$, a contradiction. Hence $S = \tilde{W} = C_G(W_0)$, $|G : \tilde{W}| = 2$ and $|G| = 2^5$. In particular, $C_G(u) = \langle u \rangle \times D$ with $D \cong Q_8$. Note that the involution u is contained in the unique normal four-subgroup W_0 of G and $C_G(u) \neq G$. Then our group G is isomorphic to the group A2(a) of the Theorem 49.1. The proof is complete. \square

2^o. G has a normal E_8 . Throughout this subsection we assume that G is a non-abelian 2-group of order $> 2^4$ satisfying $|\Omega_2(G)| = 2^4$. We assume in addition that G has a normal elementary abelian subgroup E of order 8. In that case, G/E has exactly one subgroup $\Omega_2(G)/E$ of order 2 so G/E is either cyclic of order ≥ 4 or generalized quaternion (see Proposition 1.3). In the case where G/E is cyclic, G is determined in Theorem 52.2. In the case where G/E is generalized quaternion and $E \not\leq \Phi(G)$, G is determined in Theorem 52.4. Finally, if G/E is generalized quaternion and $E \leq \Phi(G)$, then G is determined in Theorem 52.5.

Theorem 52.2. *Let G be a nonabelian 2-group of order $> 2^4$ satisfying $|\Omega_2(G)| = 2^4$. Suppose, in addition, that G has a normal subgroup $E \cong E_8$ such that G/E is cyclic of order 2^n , $n \geq 2$. Then one of the following holds:*

- (a) $G = \langle a, e_1 \mid a^{2^{n+1}} = e_1^2 = 1, n \geq 2, a^{2^n} = z, [a, e_1] = e_2, e_2^2 = [e_1, e_2] = 1, [a, e_2] = z \rangle$ is a group of order 2^{n+3} , $Z(G) = \langle a^4 \rangle$, $G' = \langle z, e_2 \rangle$, $\Phi(G) = \langle a^2, e_2 \rangle$, $E = \langle z, e_1, e_2 \rangle$ is a normal elementary abelian subgroup of order 8, and $\Omega_2(G) = E\langle a^{2^{n-1}} \rangle$ is abelian of type (4, 2, 2) for $n \geq 3$, and $\Omega_2(G) \cong C_2 \times D_8$ for $n = 2$.
- (b) $G \cong M_{2n+2} \times C_2$ with $n \geq 2$, and $\Omega_2(G)$ is abelian of type (4, 2, 2).
- (c) $G = \langle a, e_1 \mid a^{2^{n+1}} = e_1^2 = 1, n \geq 2, [a, e_1] = e_2, e_2^2 = [e_1, e_2] = [a, e_2] = 1 \rangle$ being minimal nonabelian, $|G| = 2^{n+3}$, $\Phi(G) = \langle a^2, e_2 \rangle$, $G' = \langle e_2 \rangle$, and $\Omega_2(G) = E\langle a^{2^{n-1}} \rangle$ is abelian of type (4, 2, 2), where $E = \langle a^{2^n}, e_1, e_2 \rangle$ is a normal elementary abelian subgroup of order 8.

Proof. By assumption, $G = E\langle a \rangle$ for some $a \in G - E$; let $|G/E| = 2^n > 2$. Obviously G does not split over E (otherwise, if $G = T \cdot E$, then $\Omega_2(G) = \Omega_2(T) \cdot E$ is of order $2^5 > 2^4$) and so $o(a) = 2^{n+1}$ and $\langle a \rangle \cap E = \langle z \rangle$ is of order 2, where $z = a^{2^n}$. Note that a Sylow 2-subgroup of $\text{Aut}(E)$ is isomorphic to D_8 , so a induces an automorphism of order ≤ 4 on E hence $a^4 \in Z(G)$. It is easy to check, that if $C_E(a)$ is a four-subgroup, then a induces an involutory automorphism on E . Indeed, then a stabilizes the chain $\{1\} < C_E(a) < E$ with factors of exponent 2.

Suppose that a induces an automorphism of order 4 on E . In that case, by what has been said in the previous paragraph, $C_E(a) = \langle z \rangle$ so that $Z(G) = \langle a^4 \rangle \geq \langle z \rangle$ and $C_G(E) = Z(G)E$. There are involutions $e_1, e_2 \in E$ such that $\langle z, e_1, e_2 \rangle = E$ and $e_1^a = e_1 e_2, e_2^a = e_2 z$. Then $C_E(a^2) = \langle z, e_2 \rangle = G'$, $G = \langle a, e_1 \rangle$, $\Phi(G) = \langle a^2, e_2 \rangle$, $\Omega_2(G) = E\langle a^{2^{n-1}} \rangle$. We have determined the groups stated in part (a).

Suppose that a induces an involutory automorphism on E . We have $C_E(a) = E_1 = \langle z, e_2 \rangle \cong E_4$ (see Exercise 19, below), $Z(G) = \langle a^2, e_2 \rangle$ and $G' = [a, E]$ is a subgroup of order 2 in E_1 (by Lemma 1.1, since G has an abelian subgroup $\langle a^2, E \rangle$ of index 2 and $Z(G)$ is of index 4 in G). If $G' = \langle z \rangle$, then $\langle a \rangle$ is normal in G . Let $e_1 \in E - E_1$. Then $\langle a, e_1 \rangle \cong M_{2n+2}$ and $G = \langle e_2 \rangle \times \langle a, e_1 \rangle$ which is the group stated in part (b) of our theorem. If $G' = \langle e_2 \rangle$, where $e_2 \in E_1 - \langle z \rangle$ and $e_1 \in E - E_1$, then $[a, e_1] = e_2$ and this group is stated in part (c) of our theorem. \square

In the rest of this subsection we assume that $G/E \cong Q_{2^n}$, $n \geq 3$. Then $C_G(E) > E$, since a Sylow 2-subgroup of $\text{Aut}(E)$ is isomorphic to D_8 . Therefore $\tilde{W} = \Omega_2(G)$ centralizes E , where $\tilde{W}/E = Z(G/E)$ (it is important that $|\Omega_2(G)| = 2^4$), \tilde{W} is abelian of type (4, 2, 2) and $\langle z \rangle = \mathcal{V}_1(\tilde{W})$ is of order 2. All elements in $\tilde{W} - E$ are of order 4 and so no involution in $E - \langle z \rangle$ is a square in G . Indeed, if $x^2 \in E - \langle z \rangle$, then $o(x) = 4$ and $x \notin \tilde{W}$ since z is the unique nontrivial square on \tilde{W} , and this is a contradiction. We first prove the following useful result.

Lemma 52.3. *Let, as above, $G/E \cong Q_{2^n}$, where G is an Ω_2 -group. We have $C_G(E) \geq \tilde{W} = \Omega_2(G)$, $C_G(E)/E$ is cyclic of order ≥ 2 , and $G/C_G(E)$ is isomorphic to C_2, E_4 or D_8 .*

Proof. Suppose that $C_G(E)$ contains a subgroup $H > E$ such that $H/E \cong Q_8$. Then $Z(H/E) = \tilde{W}/E$. Let A/E and B/E be two distinct cyclic subgroups of order 4 in H/E . Then A and B are abelian maximal subgroups of H . It follows that $A \cap B = \tilde{W} \leq Z(H)$ and therefore $\tilde{W} = Z(H)$ is of order 2^4 . Using Lemma 1.1, we get $2^6 = |H| = 2|Z(H)||H'|$, which gives $|H'| = 2$. Since $\Omega_1(H) = E$, we get $H' \leq E$ and H/E is abelian, a contradiction. It follows that $C_G(E)/E$ must be a normal cyclic subgroup of G/E and so $G/C_G(E)$ is isomorphic to a nonidentity epimorphic image of Q_{2^n} of order ≤ 8 such that $G/C_G(E) \not\cong Q_8$ (the last condition is superfluous if $n > 3$). We conclude that $G/C_G(E) \in \{C_2, E_4, D_8\}$. \square

Theorem 52.4. *Let G be a 2-group of order $> 2^4$ satisfying $|\Omega_2(G)| = 2^4$. Suppose, in addition, that G has a normal elementary abelian subgroup E of order 8 such that $G/E \cong Q_{2^n}$, $n \geq 3$, and $E \not\leq \Phi(G)$. Then we have*

$$\begin{aligned} G = \langle a, b, e \mid a^{2^n} = b^8 = e^2 = 1, n \geq 3, a^{2^{n-1}} = b^4 = z, a^b = a^{-1}, \\ [e, b] = 1, [e, a] = z^\mu, \mu = 0, 1 \rangle. \end{aligned}$$

Here G is a group of order 2^{n+3} , $G' = \langle a^2 \rangle$, $\Phi(G) = \langle a^2, b^2 \rangle$ is abelian of type $(2^{n-1}, 2)$. The subgroup $E = \langle e, a^{2^{n-2}}b^2, z \rangle$ is a normal elementary abelian subgroup of order 8 in G and $G/E \cong Q_{2^n}$. If $\mu = 0$, then $Z(G) = \langle e, b^2 \rangle$ is abelian of type $(4, 2)$. If $\mu = 1$, then $Z(G) = \langle b^2 \rangle \cong C_4$. Finally, $\Omega_2(G) = E\langle b^2 \rangle$ is abelian of type $(4, 2, 2)$.

Proof. Let $\tilde{W}/E = Z(G/E)$; then $\tilde{W} = \Omega_2(G)$ since $|\Omega_2(G)| = 16$ and the subgroup \tilde{W} has order 16 and exponent ≤ 4 . It follows from $\text{Aut}(E) = \text{GL}(3, 2)$ that a Sylow 2-subgroup of $\text{Aut}(E)$ is dihedral of order 8 so $C_G(E) > E$. We conclude that \tilde{W} is abelian of type $(4, 2, 2)$. Since $E \not\leq \Phi(G)$, there is a maximal subgroup M of G such that $E \not\leq M$; then $G = EM$. We have $E_0 = E \cap M \cong E_4$ (obviously, E_0 is normal in G since E and M are), $\tilde{W}_0 = \tilde{W} \cap M$ is abelian of type $(4, 2)$, $\tilde{W}_0 = \Omega_2(M)$, and $M/E_0 \cong Q_{2^n}$, $n \geq 3$. If $\Phi(\tilde{W}_0) = \langle z \rangle$, then $z \in E_0$. By Lemma 42.1, M is isomorphic to a group (c) in that proposition. Hence M is metacyclic with a cyclic normal subgroup $\langle a \rangle$ of order 2^n and the cyclic quotient group $M/\langle a \rangle$ of order 4 so that there is an element b of order 8 in $M - (E_0\langle a \rangle)$ with $b^2 \in \tilde{W}_0 - E_0$, $b^4 = z = a^{2^{n-1}}$, $\langle b \rangle \cap \langle a \rangle = \langle z \rangle$, $\tilde{W}_0 = \langle b^2 \rangle \langle a^{2^{n-2}} \rangle \leq \Phi(M)$. We have used the following facts: $\Omega_1(\tilde{W}) = E$, $\mathfrak{V}_1(\tilde{W}) = \langle z \rangle$, $\langle a \rangle \cap \langle b \rangle$ is of order 2 (by the product formula), $\Phi(G) = \mathfrak{V}_1(G)$. We have (see Lemma 42.1(c)) $\Phi(M) = \langle a^2, b^2 \rangle \geq \tilde{W}_0$, $M' = \langle a^2 \rangle$, $a^b = a^{-1}$. Also, $Z(M) = \langle b^2 \rangle$ is cyclic of order 4 and so $E_0\langle a \rangle = \langle b^2, a \rangle$ is abelian of index 2 in M , and $C_M(E_0) = E_0\langle a \rangle$ (again by Lemma 42.1(c)). The element b induces an involutory automorphism on E (because $b^2 \in Z(G)$). The element b does not centralize E_0 since $b \notin \langle a, E_0 \rangle = C_M(E_0)$. For every $u \in E_0 - \{1, z\}$, we have $\langle b, u \rangle \cong M_{16}$ (we have $|\langle b, E_0 \rangle| = 16$ so E_0 normalizes $\langle b \rangle$). We conclude that $Z(\langle b, E_0 \rangle) = \langle z \rangle$. The subgroup $\tilde{W} = \langle b^2, E \rangle$ is abelian so b induces an involutory automorphism on E . Therefore, by Exercise 19, $Z = C_E(b)$ is of order 4. By the

above, $Z \neq E_0$ so there is an element $e \in E - E_0$ such that b centralizes e . Set $u = a^{2^{n-2}}b^2 \in E_0 - \langle z \rangle$ and we have $u^b = uz$. We act with the cyclic group $\langle a \rangle$ on E . By the above, $\langle a, E_0 \rangle$ is abelian. It follows from $|E : E_0| = 2$ that $\langle a \rangle$ stabilizes the chain $E > E_0 > \{1\}$ and so a^2 centralizes E and $e^a = ey$ with $y \in E_0$. This gives $a^e = ay$. We may set $a^b = a^{-1}$. Then we act on $b^{-1}ab = a^{-1}$ with e . It follows $b^{-1}ayb = (ay)^{-1}$ and so $a^{-1}y^b = a^{-1}y$ which gives $y^b = y$ and $y \in \langle z \rangle$. If $y = 1$, then $G = \langle e \rangle \times M$. We set $a^e = az^\mu$, where $\mu = 0, 1$. The group G is completely determined. \square

Theorem 52.5. *Let G be a 2-group of order $> 2^4$ satisfying $|\Omega_2(G)| = 2^4$. Suppose, in addition, that G has a normal elementary abelian subgroup E of order 8 such that $G/E \cong Q_{2^n}$, $n \geq 3$, and $E \leq \Phi(G)$. Then one of the following holds:*

- (a) $G = \langle a, b \mid a^{2^n} = b^8 = 1, a^{2^{n-1}} = b^4 = z, b^2 = a^{2^{n-2}}e,$
 $a^b = a^{-1}ue^\epsilon, \epsilon = 0, 1,$
 $u^2 = e^2 = [e, u] = [e, z] = [u, z] = 1, e^a = ez,$
 $u^a = u, e^b = ez, u^b = uz, n \geq 3, \text{ and if } \epsilon = 1, \text{ then } n \geq 4\rangle.$

Here G is a group of order 2^{n+3} , $G' = \langle ue^\epsilon \rangle \times \langle a^2 \rangle$ is abelian of type $(2^{n-1}, 2)$, $\Phi(G) = E\langle a^2 \rangle$, where $E = \langle z, e, u \rangle$ is a normal elementary abelian subgroup of order 8 in G with $G/E \cong Q_{2^n}$. Finally, $Z(G) = \langle z \rangle$ is of order 2, and $\Omega_2(G) = E\langle a^{2^{n-2}} \rangle$ is abelian of type $(4, 2, 2)$.

- (b) $G = \langle a, b \mid a^{2^n} = b^8 = 1, n \geq 3, a^{2^{n-1}} = b^4 = z,$
 $b^2 = a^{2^{n-2}}u, a^b = a^{-1}e,$
 $u^2 = e^2 = [e, u] = [e, z] = [u, z] = [a, e] = [a, u] = [b, e] = 1,$
 $u^b = uz\rangle.$

Here G is a group of order 2^{n+3} , $G' = \langle a^2e \rangle$ is cyclic of order 2^{n-1} , $\Phi(G) = E\langle a^2 \rangle$, where $E = \langle z, e, u \rangle$ is a normal elementary abelian subgroup of order 8 in G with $G/E \cong Q_{2^n}$ and $C_G(E) = E\langle a \rangle$. Finally, $Z(G) = \langle e, b^2 \rangle$, and $\Omega_2(G) = E\langle b^2 \rangle$ is abelian of type $(4, 2, 2)$.

Proof. We have in this case $\Phi(G) \geq \tilde{W} = \Omega_2(G)$, $\tilde{W}/E = Z(G/E)$ and \tilde{W} is abelian of type $(4, 2, 2)$ since $C_G(E) > E$ (a Sylow 2-subgroup of $\text{Aut}(E)$ is isomorphic to D_8) and $|\tilde{W}| = 2^4$. Hence $\langle z \rangle = \mathcal{V}_1(\tilde{W})$ is a central subgroup of order 2 contained in E . By Lemma 52.3, since every normal cyclic subgroup of G/E is contained in a cyclic subgroup of index 2 in G/E , there is a subgroup M of index 2 in G such that M/E is cyclic and $C_G(E) \leq M$. (If $n > 3$, then M is unique since $G/E \cong Q_{2^n}$ has only one cyclic subgroup of index 2. However, if $n = 3$

and $C_G(E) = \tilde{W}$, then we have three possibilities for M since $G/E \cong Q_8$ has exactly three cyclic subgroups of index 2.) Let a be an element in $M - E$ such that $\langle a, E \rangle = M$. Then $o(a) = 2^n$ since $|M/E| = 2^{n-1}$ and M does not split over E (indeed, all involutions of G lie in E). Hence $a_0 = a^{2^{n-2}} \in \tilde{W} - E$, $a_0^2 = z \in E$. By the structure of $G/E \cong Q_{2^n}$, all elements in $(G/E) - (M/E)$ have order 4, so we have for each $x \in G - M$, $x^2 \in \tilde{W} - E$, $x^4 = z$, x induces an involutory automorphism on E since $C_G(E) \leq M$ and $x \notin M$, and so $C_E(x) \cong E_4$ (see Exercise 19). $C_E(x) > \langle z \rangle$, and $C_{\tilde{W}}(x) = \langle x^2 \rangle C_E(x)$ is abelian of type $(4, 2)$. It follows that all elements in $G - M$ have the same order 8. We have $M' < E$ (recall that M/E is cyclic) so $|M'| \leq 4$, and $M' = [\langle a \rangle, E]$. For each $a^i e \in M$, where $e \in E$ and i is an integer, we get $(a^i e)^2 = a^i e a^i e = a^{2i} (a^{-i} e a^i) e = a^{2i} [a^i, e]$ and so $\Phi(M) = \mathfrak{U}_1(M) = \langle a^2 \rangle M'$. We have exactly the following four cases for the action of the cyclic subgroup $\langle a \rangle$ of order 2^n on E :

- (1) a induces an automorphism of order 4 on E .
- (2) a induces an automorphism of order 2 on E and $[E, a] = \langle u \rangle$, where $u \in E - \langle z \rangle$.
- (3) a induces an automorphism of order 2 on E and $[E, a] = \langle z \rangle$.
- (4) a centralizes E (in that case, obviously, M is abelian).

Case (1). Since a induces an automorphism of order 4 on E , we get $n \geq 4$ (recall that $a^{2^{n-2}}$ centralizes E) and $C_E(a) = \langle z \rangle$ (see, in the first paragraph, the proof of the equality $C_G(x) \cong E_4$). In this case M' is a four-subgroup contained in E , $M' > \langle z \rangle$ (if $\langle z \rangle \not\leq M'$, then $\langle a \rangle \cap M' = \{1\}$ and a centralizes some element in $(M')^\#$, which is not the case) and for each $\tilde{e} \in E - M'$, $\tilde{e}^a = \tilde{e}\tilde{u}$ with some $\tilde{u} \in M' - \langle z \rangle$ and $\tilde{u}^a = \tilde{u}z$. We see that $\langle a, M' \rangle \cong M_{2^{n+1}}$ so $C_E(a^2) = M'$ (this is true again since a^2 induces an involutory automorphism on E). Since $|G : C_G(M')| = 2$, it follows that $C_G(M') = E\langle a^2, b' \rangle$, where $b' \in G - M$ and $E\langle a^2, b' \rangle$ is a maximal subgroup of G . Set $b = b'a$ so that $\tilde{u}^b = \tilde{u}z$ for each $\tilde{u} \in M' - \langle z \rangle$ and therefore $C_E(b) = \langle e, z \rangle$ for some $e \in E - M'$ (see the proof of Theorem 52.4), $e^a = eu$ with $u \in M' - \langle z \rangle$, $u^a = uz$, and $u^b = uz$. Since $G/E \cong Q_{2^n}$, $b^{-1}ab = a^{-1}y$ with $y \in E$. We have two subcases according to $y \in E - M'$ or $y \in M'$.

Subcase (1a). Here $y = e' \in E - M'$ and so $b^{-1}ab = a^{-1}e'$. We compute

$$a^{b^2} = (a^b)^b = (a^{-1}e')^b = (a^{-1}e')^{-1}(e')^b = e'a(e')^b = a(e')^a(e')^b = au.$$

Indeed, if $e' = ez^\mu$ ($\mu = 0, 1$), then $(e')^a = e'u$, $(e')^b = e'$, and if $e' = eu z^\mu$ ($\mu = 0, 1$), then $(e')^a = e^a u^a z^\mu = euuzz^\mu = e'uz$, $(e')^b = e'z$. On the other hand, $b^2 = a_0 x$ with $x \in E$. But $M'\langle a \rangle = \langle u, a \rangle$ is isomorphic to $M_{2^{n+1}}$ and so $a^{b^2} = au = a^{a_0 x} = a^x$ implies that $x \in E - M'$. We may set $x = eu'$ with $u' \in M'$ and so $b^2 = a_0 e u'$. We compute

$$\begin{aligned} b^{-1}a^2b &= (a^{-1}e')^2 = a^{-1}e'a^{-1}e' = (a^{-1}e'a)a^{-2}e' \\ &= (e')^a(e')^a a^{-2} = u_0za^{-2}, \end{aligned}$$

since $(e')^a = e'u_0$ ($u_0 \in M' - \langle z \rangle$) and $(e')^{a^2} = e'z$. Therefore $(a^4)^b = ((a^2)^b)^2 = (u_0za^{-2})^2 = a^{-4}$ because $C_E(a^2) = M'$. Since $a_0 = a^{2^{n-2}} \in \langle a^4 \rangle$ (recall that $n \geq 4$), we get $a_0^b = a_0^{-1}$. Obviously, b centralizes $b^2 = a_0eu'$ ($u' \in M'$) and so $a_0eu' = (a_0eu')^b = a_0^{-1}e(u')^b = a_0ze(u')^b$ which gives $(u')^b = u'z$ and $u' \in M' - \langle z \rangle$. Therefore $u' = uz^\epsilon$ ($\epsilon = 0, 1$) and $b^2 = a_0euuz^\epsilon$. On the other hand, $au = a^{b^2} = a^{a_0euuz^\epsilon} = a^{eu} = a(a^{-1}eua)eu = a(eu)(uz)eu = auz$, which is a contradiction.

Subcase (1b). Here $b^{-1}ab = a^{-1}y$ with $y \in M'$. This gives $(a^2)^b = (a^{-1}y)^2 = a^{-1}ya^{-1}y = (a^{-1}ya)a^{-2}y = y^a y^{a^2} a^{-2} = yz^\nu ya^{-2}$ ($\nu = 0, 1$), and so $(a^4)^b = (z^\nu a^{-2})^2 = a^{-4}$. Since $n \geq 4$, we get $a_0 \in \langle a^4 \rangle$ so $a_0^b = a_0^{-1}$. If $b^2 \in M'\langle a_0 \rangle$, then $S = M'\langle a, b \rangle$ is a maximal subgroup of G not containing E since $S \cap E = M'$, a contradiction (recall, that, by hypothesis, $E \leq \Phi(G)$). Thus $b^2 = a_0e_0$ with $e_0 \in E - M'$. Since b centralizes b^2 , we get $a_0e_0 = (a_0e_0)^b = a_0^{-1}e_0^b = a_0ze_0^b$ and so $e_0^b = e_0z$. Hence $e_0 = eu z^\epsilon$ ($\epsilon = 0, 1$) and $b^2 = a_0euuz^\epsilon$. From $b^{-1}ab = a^{-1}y$ with $y \in M'$, we get $b^{-2}ab^2 = (a^{-1}y)^b = (a^b)^{-1}y^b = yay^b = a(a^{-1}ya)y^b = a(yz^\eta)(yz^\eta) = a$, where $\eta = 0$ if $y \in \langle z \rangle$ and $\eta = 1$ if $y \in M' - \langle z \rangle$. On the other hand, we compute

$$a = a^{b^2} = a^{a_0euuz^\epsilon} = a^{eu} = euaeu = a(a^{-1}eua)eu = a(eu)(uz)eu = auz,$$

which is a contradiction.

Case (2). Here, by assumption, a induces an automorphism of order 2 on E and $M' = [E, a] = \langle u \rangle$, where $u \in E - \langle z \rangle$. It follows $\langle u, z \rangle \leq Z(G)$. For each $\tilde{e} \in E - \langle u, z \rangle$, $\tilde{e}^a = \tilde{e}u$. Since $\Phi(M) = \langle u \rangle \times \langle a^2 \rangle$ and $\Phi(G) \geq E$, there exists $b \in G - M$ such that $b^2 = a_0e$, where $e \in E - \langle u, z \rangle$ and $a_0 = a^{2^{n-2}}$. We have $a^b = a^{-1}y$ with $y \in E$ (see the last two sentences of the first paragraph of Case (1)). This gives $a^{b^2} = (a^{-1}y)^b = (a^b)^{-1}y^b = yay^b = ay^a y^b = a^{a_0e} = a^e = eae = a(a^{-1}ea)e = aeue = au$. Hence $y^a y^b = u$. If $y \in \langle u, z \rangle \leq Z(G)$, then $u = y^a y^b = y^2 = 1$, a contradiction. Therefore $y = es$ with $s \in \langle u, z \rangle$. But then $u = y^a y^b = (es)^a(es)^b = (eus)(e^b s) = uee^b$ and so $e^b = e$. Hence b centralizes $E = \langle e, u, z \rangle$, a contradiction.

Case (3). Here a induces an automorphism of order 2 on E and $M' = [E, a] = \langle z \rangle$. It follows $\Phi(M) = \langle a^2 \rangle \geq \langle a_0 \rangle$ and so $\langle a_0 \rangle$ is normal in G since the cyclic subgroup $\Phi(M)$ is G -invariant. Since $\mathfrak{V}_1(G) = \Phi(G) \geq \tilde{W} = E\langle a_0 \rangle$, it follows $\langle a_0, x^2 \mid x \in G - M \rangle = \tilde{W}$. Since $\langle x^2 \rangle$ is normal in G for each $x \in G - M$ and $x^4 = z$ (indeed, $M/M' = M/\langle z \rangle$ is an abelian maximal subgroup of G/M'), we get $\tilde{W}/\langle z \rangle \leq Z(G/\langle z \rangle)$. Set $U = C_E(a) \cong E_4$ and obviously $Z(M) = U\langle a^2 \rangle$. Also, $U = Z(M) \cap E$ is normal in G . Suppose that $U \leq Z(G)$. Then the four-group $G/E\langle a^2 \rangle$ acts as the full stability group of the chain $E > U > \{1\}$ since $G/E\langle a^2 \rangle$ acts faithfully on E . (Note that $C_G(E) \leq M$.) This is a contradiction since $E/\langle z \rangle < \tilde{W}/\langle z \rangle \leq Z(G/\langle z \rangle)$. Hence for each $x \in G - M$ and each $\tilde{u} \in U - \langle z \rangle$, we have $\tilde{u}^x = \tilde{u}z$. There exists $b \in G - M$ such that $b^2 = a_0e$ with $e \in E - U$.

Also, $a^b = a^{-1}y$ with $y \in E$. Then we compute $a^{b^2} = (a^{-1}y)^b = yay^b = a(a^{-1}ya)y^b = ay^a y^b = a^{a_0 e} = eae = a(a^{-1}ea)e = aeze = az$. This gives

$$(1) \quad y^a y^b = z.$$

On the other hand, b centralizes b^2 and so $a_0 e = (a_0 e)^b = a_0^b e^b$ which gives

$$(2) \quad a_0 e = a_0^b e^b.$$

We compute further $b^{-1}a^2b = (a^{-1}y)(a^{-1}y) = (a^{-1}ya)(a^{-2}ya^2)a^{-2} = y^a ya^{-2}$, and so we get

$$(3) \quad (a^2)^b = y^a ya^{-2}. \text{ There are two subcases according to } y \in U \text{ or } y \in E - U.$$

Subcase (3a). Suppose that $y \in U = C_E(a)$. Then (1) implies $y^b = yz$ and so $y = u \in U - \langle z \rangle$ and $b^{-1}ab = a^{-1}u$. From (3) we get $(a^2)^b = y^a ya^{-2} = yya^{-2} = a^{-2}$ and so $a_0^b = a_0^{-1}$ since a_0 is a power of a^2 . From (2) follows $e^b = a_0^{-b}a_0e = a_0^2e = ez$ and we have determined the group stated in part (a) of our theorem for $\epsilon = 0$.

Subcase (3b). Suppose that $y \in E - U$, where $a^b = a^{-1}y$. From (1) we get $yzy^b = z$ and so $y^b = y$. The relation (3) implies $(a^2)^b = a^{-2}z$. We compute, for each $x \in E$ and each integer i , $(b(a^2)^i x)^2 = b^2 z^\xi$ and $(ba(a^2)^i x)^2 = b^2 yz^\eta$, where $\xi, \eta = 0, 1$. Hence the square of each element in $G - M$ lies in $\langle b^2 \rangle = \langle a_0 e \rangle$ and in $\langle a_0 ey \rangle = \langle b^2 y \rangle$. Since $\Phi(G) \geq E$, we must have $y = eu$ with some $u \in U - \langle z \rangle$. From $y^b = y$ follows $eu = e^b uz$ (since $u^b = uz$) and so $e^b = ez$. Then (2) implies $a_0 e = a_0^b e z$ and so $a_0^b = a_0 z = a_0^{-1}$. From $(a^2)^b = a^{-2}z$ follows that $\langle a^2 \rangle > \langle a_0 \rangle$ which gives $n \geq 4$. We get the group stated in part (a) with $\epsilon = 1$ and $n \geq 4$.

Case (4). Here a centralizes E and so M is abelian of type $(2^n, 2, 2)$, $n \geq 3$, and $\langle a_0 \rangle$ is normal in G , where $a_0 = a^{2^{n-2}}$. Since $\Phi(G) \geq \tilde{W} = E\langle a_0 \rangle$, there exists $b \in G - M$ such that $b^2 = a_0 u$, where u is an involution in $E - \langle z \rangle$ (recall that all elements in $G - M$ have the same order 8). Indeed, if such b does not exist, we get $b^2 = a_0$ or a_0^3 for all $b \in G - M$. Then $\Phi(G) = \mathcal{U}_1(G) \not\geq E$, a contradiction. Since $C_G(b^2) \geq \langle M, b \rangle = G$, we get $b^2 \in Z(G)$, $\langle a_0, b^2 \rangle = \langle a_0 \rangle \times \langle u \rangle$ is abelian of type $(4, 2)$ and $\Phi(G) \geq \langle a^2, u \rangle$. Again $\Phi(G) \geq \tilde{W}$ and $\langle a^2, b^2 \rangle \not\geq \tilde{W}$ implies that there exists $c \in G - M$ such that $c^2 \in \tilde{W} - \langle a_0, b^2 \rangle$ and (as before) $c^2 \in Z(G)$. If $a_0 \in Z(G)$, then $\langle a_0, b^2, c^2 \rangle = \tilde{W}$ lies in $Z(G)$ contrary to Lemma 52.3. Hence $a_0 \notin Z(G)$ and therefore $a_0^b = a_0^{-1}$ and $u^b = uz$ (recall that $u = a_0^{-1}b^2 \notin Z(G)$). The subgroup $Z(G) = \langle b^2, c^2 \rangle$ is abelian of type $(4, 2)$. Lemma 1.1 implies $|G| = 2^{n+3} = 2|Z(G)||G'|$ and so $|G'| = 2^{n-1}$. Since $|(G/E)'| = 2^{n-2}$ and $\Phi(G) > G' > \langle z \rangle$, G' is cyclic of order 2^{n-1} , by the modular law. Set $a^b = a^{-1}e$ with $e \in E$. If $e \in \langle a_0, u \rangle = \langle a_0, b^2 \rangle$, then $\langle a, b \rangle$, a metacyclic maximal subgroup of G , does not contain E , a contradiction. Thus $e \in E - \langle z, u \rangle$ and we compute $(ba)^2 = baba = b^2(b^{-1}ab)a = b^2(a^{-1}e)a = b^2e$. Since both b^2 and b^2e lie in $Z(G)$, it follows $e \in Z(G)$ and therefore $Z(G) = \langle e, b^2 \rangle$. Finally, $G' = \langle a^2e \rangle$ is cyclic of order 2^{n-1} . We get the group from part (b). \square

3^o. 2-groups with exactly one subgroup of order 2⁴ and exponent 4.

Theorem 52.6. *The following two statements for a 2-group G of order $> 2^4$ are equivalent: (a) $|\Omega_2(G)| = 2^4$ and (b) G has exactly one subgroup of order 2⁴ and exponent 4.*

Proof. Suppose that (a) holds. The results of Subsections 1 and 2 imply that $\Omega_2(G)$ is isomorphic to one of the following groups $Q_8 * C_4$, $Q_8 \times C_2$, $D_8 \times C_2$, $C_4 \times C_2 \times C_2$, $C_4 \times C_4$. In particular, $\exp(\Omega_2(G)) = 4$ and so (b) holds.

Suppose now that (b) holds. Let H be the unique subgroup of order 2⁴ and exponent 4 in G , where $|G| > 2^4$. We want to show that $H = \Omega_2(G)$. Suppose that this is false. Then there exist elements of order ≤ 4 in $G - H$, where H is a characteristic subgroup of G . In particular, there is an element $a \in G - H$ such that $o(a) \leq 4$ and $a^2 \in H$. Set $\tilde{H} = H\langle a \rangle$ so that $|\tilde{H}| = 2^5$. Since H is neither cyclic nor a 2-group of maximal class, there exists a G -invariant four-subgroup W_0 contained in H , by Lemma 1.4.

Let x be any element in $\tilde{H} - H$ with $o(x) \leq 4$. Then $\langle x, W_0 \rangle$ is a subgroup of order $\leq 2^4$ in \tilde{H} and so there exists a maximal subgroup M of \tilde{H} containing $\langle x, W_0 \rangle$. Since $\exp(M \cap H) \leq 4$ and $M = \langle M \cap H, x \rangle$, we have $\Omega_2(M) = M$. But $|M| = 2^4$ and $M \neq H$, so M is either elementary abelian or $\exp(M) = 8$. Suppose that $\exp(M) = 8$. Then M is a nonabelian group of order 2⁴ with a cyclic subgroup of index 2. Since M has the normal four-subgroup W_0 , it follows that M is not of maximal class. Thus $M \cong M_{24}$. But $\Omega_2(M_{24})$ is abelian of type (4, 2) which contradicts the above fact that $\Omega_2(M) = M$.

We have proved that $M \cong E_{24}$. In particular, x must be an involution and $\exp(\tilde{H}) = 4$ because for each $y \in \tilde{H}$, $y^2 \in M$. Hence all elements in $\tilde{H} - H$ are of order ≤ 4 and so (by the above) all these elements must be involutions. In that case, every involution $x \in \tilde{H} - H$ inverts H . Let k be any element of order 4 in H . Since $k^x = k^{-1}$, $\langle k, x \rangle = D \cong D_8$. Let \tilde{M} be a maximal subgroup of \tilde{H} containing D . Then $|\tilde{M}| = 2^4$, $\exp(\tilde{M}) = 4$, $\tilde{M} \neq H$, and this is a final contradiction. \square

4^o. Generalization of Theorem 43.4. Here we improve Theorem 43.4 and some results of [Ber25, §48]. In Theorem 52.7 we classify the 2-groups with exactly one abelian subgroups of type (4, 2); the proof is independent of the proof of Theorem 43.4. The following remark shows that there are few 2-groups without abelian subgroups of type (4, 2).

Remarks. 1. Let us classify the 2-groups without abelian subgroup of type (4, 2). Of course, if G is cyclic, elementary abelian or of maximal class, it has no abelian subgroups of type (4, 2). So in what follows suppose that G is of exponent > 2 and is neither cyclic nor of maximal class. Let A be a cyclic subgroup of order 4 in G . Then $C_G(A) - A$ has no involutions. It follows that $C_G(A)$ is cyclic (Proposition 1.3). By Suzuki's theorem (Proposition 1.8), $|C_G(A)| > 4$. By Lemma 1.4, G has a normal abelian subgroup R of type (2, 2). Since $Z(G) < C_G(A)$, we get $R \cap C_G(A)$ is of

order 2. It follows that $H = RC_G(A) \cong M_{2^n}$ for some $n > 3$. Let B be a subgroup of order 4 in $Z(H)$. In that case, RB is abelian of type $(4, 2)$, which is not the case. Thus, our G is elementary abelian, cyclic or of maximal class.

2. Let G be a p -group without abelian subgroup of type (p^2, p) , $p > 2$, $\exp(G) > p$. Then, as in Remark 1, we obtain $\exp(G) = p^2$ and $C_G(x) = \langle x \rangle$ so G is of maximal class (Proposition 1.8). In particular, $|G| \leq p^{2p-1}$ (Theorem 9.6). We claim that $|G| \leq p^{p+1}$. Assume that this is false. Let G_1 be a fundamental subgroup of G . Then $\exp(G_1) > p$ and $Z(G_1)$ is noncyclic. In that case, obviously, G_1 contains an abelian subgroup of type (p^2, p) , a contradiction. Thus, $|G| \leq p^{p+1}$. It is easy to check that a Sylow p -subgroup of the symmetric group of degree p^2 has no abelian subgroups of type (p^2, p) .

Theorem 52.7. *Let G be a 2-group containing exactly one abelian subgroup of type $(4, 2)$. Then one of the following holds:*

- (a) $|\Omega_2(G)| = 8$ and G is isomorphic to one of the metacyclic groups (a), (b) or (c) in Lemma 42.1.
- (b) $G \cong C_2 \times D_{2n+1}$, $n \geq 2$.
- (c) $G = \langle b, t \mid b^{2^{n+1}} = t^2 = 1, b^t = b^{-1+2^{n-1}}u, u^2 = [u, t] = 1, bu = b^{1+2^n}, n \geq 2 \rangle$. Here $|G| = 2^{n+3}$, $Z(G) = \langle b^{2^n} \rangle$ is of order 2, $\Phi(G) = \langle b^2, u \rangle < \langle b, u \rangle \cong M_{2^{n+2}}$, $E = \langle b^{2^n}, u, t \rangle \cong E_8$ is self-centralizing in G , $\Omega_2(G) = \langle u \rangle \times \langle b^2, t \rangle \cong C_2 \times D_{2n+1}$, $G' = \langle b^{2^n}, u \rangle \cong E_4$ in case $n = 2$, and $G' = \langle b^2u \rangle \cong C_{2^n}$ for $n \geq 3$. Finally, the group G for $n = 2$ (of order 2^5) is isomorphic to the group (a) in Theorem 52.2 for $n = 2$ (since $\Omega_2(G) \cong C_2 \times D_8$).

Proof. Let G be a 2-group with exactly one abelian subgroup A of type $(4, 2)$; then A is characteristic in G . Set $C = C_G(A)$. Then C is normal in G and G/C is isomorphic to a subgroup of $\text{Aut}(A) \cong D_8$. We claim that $\Omega_2(C) = A$. Indeed, let $y \in C - A$ such that $o(y) \leq 4$ and $y^2 \in A$. Then $A\langle y \rangle$ is an abelian subgroup of order 2^4 and exponent 4. But then $A\langle y \rangle$ contains an abelian subgroup of type $(4, 2)$ distinct from A , a contradiction. Thus $\Omega_2(C) = A$, as claimed. Lemma 42.1 implies that C must be abelian of type $(2^n, 2)$, $n \geq 2$. If $\Omega_2(G) = \Omega_2(C) = A$, then G is metacyclic and G is isomorphic to one of the groups in Lemma 42.1.

We assume from now on that $\Omega_2(G) > A$. Set $U = \Omega_1(A)$ and $\langle z \rangle = \Phi(A)$ so that $z \in Z(G)$ and U is a normal four-subgroup of G . Let $a \in G - C$ be such that $o(a) \leq 4$ and $a^2 \in C$. Obviously, $a^2 \in U$ since $U = \Omega_1(C)$. Let $D = \langle a \rangle C$; then $|D : C| = 2$. Since D is a nonabelian group (of order $\geq 2^4$) containing a normal four-subgroup U , it follows that D is not of maximal class. If $o(a) = 4$, then a does not centralize U (otherwise $U\langle a \rangle$ would be abelian of type $(4, 2)$ distinct from A) and so $U\langle a \rangle \cong D_8$. But then there exists an involution in $(U\langle a \rangle) - U$. In any case the coset Ca ($\supset Ua$) contains involutions and let t be one of them. If t centralizes an element s of order 4 in C , then $\langle s, t \rangle$ is an abelian subgroup of type $(4, 2)$ distinct from A , a

contradiction. Hence $C_C(t)$ is of exponent 2 and (since D is not of maximal class) $C_C(t) = U$ (Proposition 1.8) and $E = C_D(t) = U \times \langle t \rangle \cong E_8$. It is easy to check that, for each $x \in D - C = Ct$, $C_C(x) = U$. Hence $x^2 \in U$ and $\langle U, x \rangle$ is elementary abelian (of order 8). Thus, all elements in $D - C$ are involutions and therefore t inverts C . Let B be a cyclic subgroup of index 2 in C and an involution $u \in C - B$. Then $\langle B, t \rangle \cong D_{2n+1}$ and $D \cong C_2 \times D_{2n+1}$, $n \geq 2$, where $C_2 = \langle u \rangle$. Obviously, we may choose $a \in G - C$ so that $D = \langle a, C \rangle \triangleleft G$.

Suppose that G/C has a cyclic subgroup K/C of order 4. Then $K > D$ since D/C , in the case under consideration, is contained in $\Phi(G/C)$, and let $k \in K$ be such that $K = \langle k, C \rangle$. We have $k^2 \in D - C$ and so k^2 is an involution. It follows $o(k) = 4$ and so $\langle k, z \rangle$ is an abelian subgroup of type (4, 2) distinct from A since $\langle k \rangle \cap C = \{1\}$, and this is a contradiction. We have proved that G/C is elementary abelian. If $|G/C| = 2$, then $G = D$ and we are done.

It remains to study the possibility $G/C \cong E_4$. By the above, if $y \in G - D$ and $o(y) \leq 4$, then $y^2 \in C$ and y is an involution inverting C (indeed, as in the second paragraph of the proof, all elements in $\langle y, C \rangle - C$ are involutions). But then $yt \notin C$ and yt centralizes C , a contradiction ($C = C_G(A)$ is self centralizing in G). Hence, for each element $y \in G - D$, $o(y) \geq 8$ and $y^2 \in C$. This gives $\Omega_2(G) = D$, $C_G(t) = E = \langle t \rangle \times \Omega_1(A)$ and so E is a self-centralizing elementary abelian subgroup of order 8 in G .

For each $y \in G - D$, we have $y^2 \in C$ and $o(y^2) \geq 4$ and so y centralizes a cyclic subgroup of order 4 in A . Since y does not centralize A , it follows that y does not centralize $U = \Omega_1(A)$ since $y \notin C = C_G(A)$. Hence $D = C_G(U)$ and so $Z(G) = \langle z \rangle = \Phi(A)$ is of order 2. Since $\Omega_2(\langle y \rangle C) = A$ and $\langle y \rangle C$ is nonabelian, Lemma 42.1 implies that $\langle y \rangle C$ is isomorphic to a group (a) or (c) of that lemma.

Assume that there is $b \in G - D$ such that $\langle b \rangle C$ is isomorphic to a group of Lemma 42.1(c). In particular, $|\langle b \rangle C| \geq 2^5$, C is the unique abelian maximal subgroup of $\langle b \rangle C$ (since $Z(\langle b \rangle C) \cong C_4$), $o(b) = 8$, $Z(\langle b \rangle C) = \langle b^2 \rangle < A$, $\langle b^4 \rangle = \langle z \rangle = \Phi(A)$, C contains a cyclic subgroup $\langle a \rangle$ of index 2 such that $\langle a \rangle$ is normal in $\langle b \rangle C$, $o(a) \geq 2^3$, $A \cap \langle a \rangle \cong C_4$, $\langle b \rangle \cap \langle a \rangle = \langle z \rangle$, and $a^b = a^{-1}$. Also, we see that for each $y \in (\langle b \rangle C) - C$, $C_C(y) = \langle b^2 \rangle \cong C_4$, and y is of order 8. Since t inverts C , we get $a^{bt} = a$ and so $|C_C(bt)| \geq 2^3$. This implies that $\langle bt \rangle C \cong M_{2n+2}$ because $C_C(bt) \leq Z(\langle bt \rangle C)$.

Replacing b with bt (if necessary), we may assume from the start that there is an element $b \in G - D$ such that $\langle b \rangle C \cong M_{2n+2}$ ($n \geq 2$), which is a group in part (a) of Lemma 42.1. We have $o(b) = 2^{n+1}$, $\langle b \rangle$ is a cyclic subgroup of index 2 in $\langle b \rangle C$, $z = b^{2^n}$, $U = \langle z, u \rangle = \Omega_1(\langle b \rangle C)$, and $u^b = uz$. This gives also $b^u = bz = b^{1+2^n}$, $Z(\langle b \rangle C) = \langle b^2 \rangle \cong C_{2^n}$, $A = \langle b^{2^{n-1}} = v, u \rangle$, $C = \langle b^2 \rangle \times \langle u \rangle$. We see that $C_C(bt) = \langle vu \rangle \cong C_4$ and so $Z(\langle bt \rangle C) = \langle vu \rangle$. It follows that $\langle bt \rangle C \cong M_{24}$ for $n = 2$ and $\langle bt \rangle C$ is isomorphic to a group (c) of Lemma 42.1 for $n > 2$. In any case, $(bt)^2 \in \langle vu \rangle - \langle z \rangle$ and so $(bt)^2 = vu$ or $(bt)^2 = v^{-1}u = vu$. Replacing u with uz (if necessary), we may assume that $(bt)^2 = vu$, where $v = b^{2^{n-1}}$. From this crucial

relation follows $b^t = b^{-1+2^{n-1}}u$. The structure of $G = \langle b, t \rangle$ is determined and our theorem is proved. \square

Theorem 52.8. *The following two statements for a 2-group G are equivalent: (a) $c_2(G) = 4$; (b) G has exactly one abelian subgroup of type $(4, 2)$.*

Proof. Suppose that G is a 2-group having exactly two cyclic subgroups U, V of order 4. Then $|G : N_G(U)| \leq 2$ and so $V \leq N_G(U)$. Similarly, $U \leq N_G(V)$. We get $[U, V] \leq U \cap V$. Since $A = \langle U, V \rangle$ has exactly two cyclic subgroups of order 4, A must be abelian of type $(4, 2)$. But A is generated by its two cyclic subgroups of order 4 and so (b) holds.

Let (b) hold. Then the group G is completely determined by Theorem 52.7. Looking at $\Omega_2(G)$, we see that G has exactly two cyclic subgroups of order 4. \square

Exercise 1. Let G be a 2-group, $\exp(G) \geq 2^n$ with $n > 1$. Let $H < G$ contains all cyclic subgroups of G of order 2^n . If $x \in H$ with $o(x) = 2^n$, then $\Omega_{n-1}(C_G(x)) \leq H$.

Exercise 2. Let G be a 2-group with $|\Omega_2(G)| \leq 2^5$. Prove that $\text{dl}(G)$, the derived length of G , is at most 5.

Solution. If G has no normal elementary abelian subgroups of order 8, then the $\text{dl}(G) \leq 4$, by §50. Now let E be a normal elementary abelian subgroup of G of order 8. Then $|\Omega_1(G/E)| \leq 4$ so $\text{dl}(G/E) \leq 4$, and we are done.

Exercise 3. Let G be a 2-group and $n > 3$. Denote by \mathfrak{M}_n the set of noncyclic subgroups of order 2^n in G which are abelian of type $(2^{n-1}, 2)$ or M_{2^n} . Study the structure of G in the case $|\mathfrak{M}_n| = 1$.

Exercise 4. Study the 2-groups without abelian subgroups (i) of type $(4, 4)$, (ii) of type $(4, 2, 2)$.

Exercise 5. Suppose that a noncyclic p -group G has no abelian subgroups of type (p^2, p) . If $\exp(G) > p$, then either G is a 2-group of maximal class or $p > 2$ and G is of maximal class and order $\leq p^{p+1}$.

Exercise 6. Let G be a noncyclic p -group of order $> p^4$ and exponent $> p$, $p > 2$. Prove that if G has no subgroups of order p^4 and exponent $\leq p^2$, then G has a cyclic subgroup of index p .

5^o. 2-groups G with $|\Omega_3(G)| = 2^5$. The ultimate goal is to classify finite 2-groups G of order $> 2^6$ with $|\Omega_3(G)| = 2^6$ (see #525 in Research problems and themes I). However, if $\Omega_3(G) \not\leq \Phi(G)$, there is a maximal subgroup M of G such that $|\Omega_3(M)| \leq 2^5$ and without the exact knowledge of the structure of M there is no chance to determine G in that case.

All results of this subsection are due to Z. Bozikov [Boz].

In this subsection we determine up to isomorphism all 2-groups G with $|\Omega_3(G)| \leq 2^5$ and $G > \Omega_3(G)$. The cases $|\Omega_3(G)| = 2^3$ and $|\Omega_3(G)| = 2^4$ are easy (Proposition 52.9). If $|\Omega_3(G)| = 2^5$, we show first that $\exp(\Omega_3(G)) = 2^3$ and $|\Omega_2(G)| = 2^4$ (Proposition 52.10). This allows us to use the classification of 2-groups G with $|\Omega_2(G)| = 2^4$ and $|G| > 2^4$ given in first two subsections. Indeed, in Theorem 52.11 we consider nonmetacyclic 2-groups G and get our result almost immediately. In Theorem 52.12 we consider metacyclic 2-groups G with the above property. This case is difficult since in §50 there is no single information for metacyclic groups but we have to determine the groups G up to isomorphism also in this case.

In conclusion, we classify the 2-groups G containing exactly one subgroup of order 2^5 and exponent ≤ 8 (see #437 in Research problems and themes I). We show that such groups satisfy $|\Omega_3(G)| = 2^5$. In fact, we get a more general result (Theorem 52.14).

5.1^o. For the convenience we prove two preliminary results (Propositions 52.9 and 52.10).

Proposition 52.9. *Let G be a 2-group with $G > \Omega_3(G)$. If $|\Omega_3(G)| \leq 2^3$, then $|\Omega_3(G)| = 2^3$ and G is cyclic. If $|\Omega_3(G)| = 2^4$, then $\Omega_3(G)$ is abelian of type $(8, 2)$ and G is either abelian of type $(2^m, 2)$ or $G \cong M_{2^m+1}$, $m \geq 4$.*

Proof. Set $\Omega_3(G) = H$. Assume that G is noncyclic. If G is of maximal class, then $H \geq \Omega_2(G) = G$, which is a contradiction. Therefore, G has a normal abelian subgroup R of type $(2, 2)$. By hypothesis, H/R is cyclic of order 4 so G/R cyclic. It follows that $R = \Omega_1(G)$ so G contains a cyclic subgroup of index 2. Now the result follows from Theorem 1.2. \square

Proposition 52.10. *Let G be a 2-group with $G > \Omega_3(G)$. If $|\Omega_3(G)| = 2^5$, then $\exp(\Omega_3(G)) = 2^3$ and $|\Omega_2(G)| = 2^4$.*

Proof. Set $\Omega_3(G) = H$ so that $|H| = 2^5$ and $G > H$. If H is cyclic, then $\Omega_3(H) < H$, a contradiction. If H is of maximal class so G is since $c_1(G) = c_1(H)$ (see Theorem 1.17); then $H \geq \Omega_2(G) = G$, a contradiction. If $\exp(H) = 2^4$, then (Theorem 1.2) H is either abelian of type $(16, 2)$ or $H \cong M_{32}$. In any case, $\Omega_3(H) < H$ which is again a contradiction.

We have proved that $\exp(H) = 2^3$ (since $\exp(H) \leq 2^2$ is obviously impossible). Since H is neither cyclic nor of maximal class, there is a G -invariant four-subgroup R contained in H . We assume (by way of contradiction) that $H = \Omega_2(G)$. Then $\Omega_2(G/R) = H/R$ is of order 2^3 and $|G/R| > 2^3$. Lemma 42.1 implies that H/R is abelian of type $(4, 2)$. In particular, $H' \leq R$ and H' is elementary abelian. If the class $\text{cl}(H)$ of H is ≤ 2 , then for each $x, y \in H$ with $o(x) \leq 4$, $o(y) \leq 4$, we get $(xy)^4 = x^4y^4[y, x]^6 = 1$, which implies that $\exp(H) \leq 4$, a contradiction. Thus (since H is not of maximal class) $\text{cl}(H) = 3$ and so $H' = R$ and $R \not\leq Z(H)$. We set $C = C_H(R)$ and $D = C_G(R)$. Since $|H : C| = 2$, D covers G/H and $G = HD$.

If $\exp(C) \leq 4$, then taking $x \in D - C$ such that $x^2 \in C$, we get $o(x) \leq 8$, a contradiction. It follows $\exp(C) = 8$. Let $a \in C$ with $o(a) = 8$. Then $C = R\langle a \rangle$, $|R \cap \langle a \rangle| = 2$, and so C is abelian of type $(8, 2)$. Since $\Omega_3(D) = C$, our Proposition 52.9 implies that D is either abelian of type $(2^m, 2)$ or $D \cong M_{2m+1}$, $m \geq 4$. In any case, $\Phi(D)$ is cyclic of order 2^{m-1} and so $\Phi(D)$ contains a characteristic cyclic subgroup Z of order 8. It follows that $Z \leq C$ and Z is normal in G . But $|H/Z| = 4$ and so $H' \leq Z$. This contradicts the fact that $H' = R$ and $|R \cap Z| = 2$.

We have proved that $\Omega_2(G) < H$. On the other hand, $R < \Omega_2(G)$ and so $|\Omega_2(G)| = 8$ or 16. Set $K = \Omega_2(G)$ and assume $|K| = 8$. Then Lemma 42.1 shows that either $|\Omega_3(G)| = 2^4$ (in cases (a) or (b)) or $\Omega_3(G) = G$ (in case (c)). This is a contradiction and so $|K| = 16$ and we are done. \square

5.2^o. Now let G be a nonmetacyclic 2-group of order $> 2^5$ with $|\Omega_3(G)| = 2^5$. We set $H = \Omega_3(G)$ and apply Proposition 52.10. We see that $\exp(H) = 2^3$ and $\Omega_2(G) = K$ is of order 2^4 so that $|H : K| = 2$. By Theorem 41.1, K is nonmetacyclic. We are in a position to use the first part of this section. Since $|G| > 2^5$, we get either $K \cong Q_8 * C_4$ or $K \cong C_4 \times C_2 \times C_2$. All elements in $H - K$ are of order 8.

Assume first that $K = Q * Z$, where $Q \cong Q_8$, $Z \cong C_4$, and $Q \cap Z = Z(Q)$. All elements in $K - (Q \cup Z)$ are involutions and so Q is the unique quaternion subgroup in K . Thus Q is normal in G and so also $C = C_G(Q)$ is normal in G . Since $|G/(QC)| \leq 2$ and $|G| > 2^5$, we have $|C| \geq 2^3$ and $C \cap K = Z$. Also, $\Omega_2(C) = Z$ and so Lemma 42.1 implies that C is cyclic and $H = Q * \Omega_3(C)$. Suppose that $|G/(QC)| = 2$. Since $G/C \cong D_8$, there is an element $c \in G - (QC)$ such that $c^2 \in C$. Set $P = C\langle c \rangle$. Again, $\Omega_2(P) = Z$ and so $P = \langle c \rangle$ is cyclic. But $\langle c \rangle$ induces on Q an “outer” involutory automorphism and so we may set $Q = \langle a, b \rangle$ so that $a^c = a^{-1}$ and $b^c = ba$.

Assume now $K \cong C_4 \times C_2 \times C_2$ so that $E = \Omega_1(K)$ is a normal elementary abelian subgroup of order 8 in G . We have $\Omega_1(K) = \langle z \rangle$ is a central subgroup of order 2 in G . Obviously, K/E is the unique subgroup of order 2 in G/E and so G/E is either cyclic (of order ≥ 8) or generalized quaternion. Suppose that G/E is generalized quaternion and let L/E be a cyclic subgroup of index 2 in G/E . For each $x \in G - L$, $x^2 \in K - E$ and so $o(x) = 8$ which forces $\Omega_3(G) = G$, a contradiction.

We have proved that G/E is cyclic. Let $a \in G - K$ be such that $\langle a \rangle$ covers G/E . Then $\langle a \rangle$ is cyclic of order 2^m , $m \geq 4$, $G = E\langle a \rangle$, $K \cap \langle a \rangle \cong C_4$, and $E \cap \langle a \rangle = \langle z \rangle$. We may set $E = \langle e, u, z \rangle$ so that we have the following possibilities for the action of $\langle a \rangle$ on E :

- (i) $e^a = eu$, $u^a = uz$ (here a induces an automorphism of order 4 on E);
- (ii) $e^a = e$, $u^a = uz$ (here $G = \langle e \rangle \times \langle a, u \rangle \cong C_2 \times M_{2m+1}$);
- (iii) $e^a = eu$, $u^a = u$ (here G is minimal nonabelian);
- (iv) $[E, a] = 1$ (here G is abelian of type $(2^m, 2, 2)$).

We have proved the following result.

Theorem 52.11 ([Boz]). *Let G be a non-metacyclic 2-group of order $> 2^5$ with $|\Omega_3(G)| = 2^5$. Then one of the following holds.*

- (a) $G = QP$, where $Q = \langle a, b \rangle$ is a normal quaternion subgroup of G , $P = \langle c \rangle$ is cyclic of order 2^m , $m \geq 4$, $Q \cap P = Z(Q)$ and c either centralizes Q or $a^c = a^{-1}$ and $b^c = ba$.
- (b) $G = EP$, where $E = \langle e, u, z \rangle$ is a normal elementary abelian subgroup of order 8, $P = \langle a \rangle$ is cyclic of order 2^m , $m \geq 4$, and $E \cap P = \langle z \rangle$ with $z = a^{2^{m-1}}$. For the action of $\langle a \rangle$ on E we have one of the following possibilities:
 - (i) $e^a = eu$, $u^a = uz$, and here a induces an automorphism of order 4 on E ;
 - (ii) $e^a = e$, $u^a = uz$, and here $G \cong C_2 \times M_{2^m+1}$;
 - (iii) $e^a = eu$, $u^a = u$, and here G is minimal nonabelian;
 - (iv) $e^a = e$, $u^a = u$, and here G is abelian of type $(2^m, 2, 2)$.

5.3^o. Now we assume that G is a metacyclic 2-group of order $> 2^5$ with $|\Omega_3(G)| = 2^5$. We set $H = \Omega_3(G)$. By Proposition 52.10, $\exp(H) = 2^3$ and $\Omega_2(G) = K$ is of order 2^4 . The first part of this section implies that $K \cong C_4 \times C_4$ and all elements in $H - K$ are of order 8. It follows that $R = \Omega_1(K)$ is a normal 4-subgroup. Suppose that $C_H(R) = K$. Since $C_G(R)$ covers G/H , there is an element $x \in C_G(R) - H$ with $x^2 \in K$. But then $o(x) \leq 8$, a contradiction. We have proved that $R \leq Z(H)$.

Let Y/K be a subgroup of order 2 in G/K . Since $Y \leq \Omega_3(G)$, we get $Y = H$. Hence H/K is the unique subgroup of order 2 in G/K . This implies that G/K is either cyclic (of order ≥ 4) or generalized quaternion.

We study first the case, where G/K is cyclic. Let $a \in G - K$ be such that $\langle a \rangle$ covers G/K . Then $\langle a \rangle \cap H \cong C_{2^3}$, $\langle a \rangle \cap K \cong C_{2^2}$, and $\langle a \rangle \cap R = \langle z \rangle \leq Z(G)$. Thus a is of order 2^m , $m \geq 4$, and we set $s = a^{2^{m-3}}$ and $v = a^{2^{m-2}}$ so that $s^2 = v$, $v^2 = z$, and $o(s) = 8$. Set $C = C_G(K)$. Since G/C is cyclic and acts faithfully on K , we have $|G/C| \leq 4$. For the structure of $\text{Aut}(C_4 \times C_4)$ see Proposition 50.5. Also, $G' \leq K$ and G' is cyclic which implies that $|G'| \leq 4$.

If $G' = \{1\}$, then G is abelian of type $(2^m, 4)$, $m \geq 4$.

Suppose $|G'| = 2$. Then Exercise 10.13 implies that G is minimal nonabelian. Since $|G| > 8$, Exercise 1.8a together with the fact that $|\Omega_3(G)| = 2^5$ gives $G = \langle a, b \mid a^{2^m} = b^4 = 1, m \geq 4, a^b = a^{1+2^{m-1}} \text{ or } b^a = b^{-1} \rangle$.

Suppose $|G'| = 4$ and $|G : C| = 2$. Then a induces an involutory automorphism on K , $H = \langle K, s \rangle \leq C$, and so H is abelian of type $(8, 4)$. If a centralizes K/R , then $G' \leq R$. But G' is cyclic and so $|G'| \leq 2$, a contradiction. Hence a acts non-trivially on K/R and so a acts also non-trivially on $R = \Omega_1(K)$. There is an element $w \in K - R$ such that $w^2 = u \in R - \langle z \rangle$, $w^a = w'$, $(w')^2 = uz$, $K = \langle w \rangle \times \langle w' \rangle$, and $u^a = uz$. Since a induces an involutory automorphism on K , $(w')^a = w^{a^2} = w$

and therefore $C_K(a) = \langle ww' \rangle = \langle v \rangle$ with $(ww')^2 = z$. From $w^a w^{-1} = [a, w^{-1}] = w' w^{-1} = w' w u = w w' u$ follows that $G' = \langle w w' u \rangle \cong C_4$, $(w w' u)^2 = z$, and $G' \not\leq Z(G)$. From the above, $w w' = v z^\epsilon$ ($\epsilon = 0, 1$) and set $l = s w u^{\epsilon+1}$. Then $l^2 = s^2 w^2 = v u = w w' u z^\epsilon \in G'$, $(v u)^2 = z$, and so $\langle l \rangle \cong C_8$ is normal in G with $\langle l \rangle \cap \langle a \rangle = \langle z \rangle$. We compute

$$\begin{aligned} l^a &= (s w u^{\epsilon+1})^a = s w' u^{\epsilon+1} z^{\epsilon+1} = s^{-1} s^2 w' u^{\epsilon+1} z^{\epsilon+1} \\ &= s^{-1} v w' u^{\epsilon+1} z^{\epsilon+1} = s^{-1} (w w' z^\epsilon) w' u^{\epsilon+1} z^{\epsilon+1} \\ &= s^{-1} w^{-1} w^2 (w')^2 u^{\epsilon+1} z = s^{-1} w^{-1} u u z u^{\epsilon+1} z \\ &= s^{-1} w^{-1} u^{\epsilon+1} = l^{-1}. \end{aligned}$$

We have obtained the following metacyclic group $G = \langle a, l \mid a^{2^m} = l^8 = 1, a^{2^{m-1}} = l^4, l^a = l^{-1}, m \geq 4 \rangle$, where $H = \langle l, s \rangle = \langle l, a^{2^{m-3}} \rangle$ is abelian of type $(8, 4)$.

It remains to study here the case $|G'| = 4$ and $|G : C| = 4$. Hence a induces on K an automorphism of order 4 and so, in particular, a acts nontrivially on R . This implies that $C_K(a) = \langle v \rangle$, where $\langle v^2 \rangle = \langle z \rangle = C_R(a)$. We may set $K = \langle w \rangle \times \langle w' \rangle$, where $w^a = w'$, $w^2 = u \in R - \langle z \rangle$, $(w')^2 = u z$, $u^a = u z$, and $(w')^a = w s_0$ with $s_0 \in R$. We have $s_0 \neq 1$ (otherwise a induces on K an involutory automorphism). Since $(w w')^2 = w^2 (w')^2 = u u z = z$, it follows that $w w' \in R \langle v \rangle$. We compute $(w w')^a = w' w s_0 = (w w') s_0$, which implies $\langle w w' \rangle \neq \langle v \rangle$ and so $\langle w w' u \rangle = \langle v \rangle$. Here we have used the fact that $R \langle v \rangle$ contains exactly two cyclic subgroups of order 4 and they are $\langle v \rangle$ and $\langle v u \rangle$. This gives (since a centralizes v) $w w' u = (w w' u)^a = w' w s_0 u z$, and consequently $s_0 = z$. Hence $(w')^a = w z$ and so the action of $\langle a \rangle$ on K is uniquely determined. We see that $[a, w^{-1}] = w^a w^{-1} = w' w^{-1} = w' w u = w w' u$ and so $G' = \langle w w' u \rangle$. But $\langle w w' u \rangle = \langle v \rangle \leq \langle a \rangle$ and so $\langle a \rangle$ is normal in G . Also, $\langle w \rangle$ induces on $\langle a \rangle$ an automorphism of order 4 with $\langle w \rangle \cap \langle a \rangle = 1$ and $|\langle a \rangle : C_{\langle a \rangle}(w)| = 4$. This determines uniquely the structure of our “splitting” metacyclic group $G = \langle a, w \mid a^{2^m} = w^4 = 1, m \geq 4, a^w = a^{1+2^{m-2}} \rangle$, where $H = \langle w, a^{2^{m-3}} \rangle$. For $m = 4$, H is nonabelian and for $m > 4$, H is abelian of type $(8, 4)$. Here $G' = \langle a^{2^{m-2}} \rangle \leq Z(G) = \langle a^4 \rangle$.

We have to study the difficult case, where G/K is generalized quaternion. Since a generalized quaternion group is not a subgroup of $\text{Aut}(K)$ (see Proposition 50.5), we have $C_G(K) \geq H$ and consequently H is abelian of type $(8, 4)$. Note that $H/K = Z(G/K)$. We set $L/K = (G/K)' = \Phi(G/K)$ so that L/K is cyclic containing H/K . We have $G/L \cong E_4$ and since G is metacyclic (and so $d(G) = 2$), we get $L = \Phi(G)$ and G' is cyclic. On the other hand, G' covers L/K and all elements in $H - K$ are of order 8. Hence $G' \cap H \cong C_8$, $G' \cap K \cong C_4$, and $|L : G'| = 4$. Again, since G is metacyclic, there is a cyclic normal subgroup S of G such that $G' < S$ and $|S : G'| = 2$. If $S \leq L$, then $|S \cap K| = 8$. But a maximal subgroup $S \cap K$ of K is not cyclic since $\exp(K) = 4$. This contradiction shows that $S \cap L = G'$. Set $T = K S = L S$ so that T/K is a cyclic subgroup of index 2 in G/K . For each

$x \in G - T$, we have $x^2 \in H - K$ and so all elements in $G - T$ are of order 16. Now, $\Phi(T) \leq L$ and $\Phi(T) \geq \langle G', \mathfrak{V}_1(K) = R \rangle$ since $G' = \mathfrak{V}_1(S)$. But $|L : (G'R)| = 2$ and T is noncyclic and so $\Phi(T) = G'R$. Then $F = \Phi(T) \cap H$ is abelian of type $(8, 2)$ and $F_1 = \Phi(T) \cap K$ is abelian of type $(4, 2)$.

Set $S = \langle a \rangle$, where $o(a) = 2^m$, $m \geq 4$. Also, set $s = a^{2^{m-3}}$, $v = a^{2^{m-2}}$, and $z = a^{2^{m-1}}$ so that $z \in Z(G)$, $\langle s \rangle = S \cap H$, $\langle v \rangle = S \cap K$, and $\langle z \rangle = S \cap R$. Obviously, $\langle s \rangle$ and $\langle v \rangle$ are normal subgroups in G . Since $\Phi(G) = L$, there is an element $b \in G - T$ (of order 16) such that $b^2 \in H - K$ and $b^2 \notin F$. Then $b^2 = ws$, where $w \in K - F_1$ and $K = \langle w \rangle \times \langle v \rangle$. We set $w^2 = u$ and so $R = \Omega_1(K) = \langle u, z \rangle$. We compute $b^4 = w^2s^2 = uv$ and $b^8 = z$. Hence $G = \langle a \rangle \langle b \rangle$, where $\langle a \rangle$ is a cyclic normal subgroup of order 2^m ($m \geq 4$) of G , $\langle b \rangle$ is cyclic of order 16, and $\langle a \rangle \cap \langle b \rangle = \langle z \rangle$ (of order 2).

It remains to determine the action of $\langle b \rangle$ on $\langle a \rangle$. Now, $\langle b \rangle$ induces a cyclic automorphism group on $\langle a \rangle$ so that b inverts $\langle a \rangle / \langle v \rangle$ since G/K is generalized quaternion. Thus $a^b = a^{-1}v_0$ with $v_0 \in \langle v \rangle$ and so $(a^4)^b = (a^b)^4 = (a^{-1}v_0)^4 = a^{-4}$. In particular, b inverts $\langle v \rangle$. On the other hand, b centralizes $b^4 = uv$ and so $uv = (uv)^b = u^b v^b = u^b v^{-1}$, which gives $u^b = uz$. We compute $a^{b^2} = (a^{-1}v_0)^b = (a^{-1}v_0)^{-1}v_0^{-1} = av_0^{-2} = az^\epsilon$, $\epsilon = 0, 1$. Since $b^2 = sw$, this gives $a^{sw} = a^w = az^\epsilon$ and $a^u = a^{w^2} = (az^\epsilon)^w = az^\epsilon z^\epsilon = a$ and so $[a, u] = 1$. Replacing a with au we get $o(au) = o(a) = 2^m$ and $(au)^b = a^{-1}v_0uz = (au)^{-1}v_0z$. Hence replacing a with au (if necessary), we may assume that $v_0 = v = a^{2^{m-2}}$ or $v_0 = 1$. We have obtained exactly two possibilities for our group $G = \langle a, b \mid a^{2^m} = b^{16} = 1, m \geq 4, a^{2^{m-1}} = b^8, a^b = a^{-1+\epsilon \cdot 2^{m-2}}, \epsilon = 0, 1 \rangle$. The following result was proved.

Theorem 52.12 ([Boz]). *Let G be a metacyclic 2-group of order $> 2^5$ with $|\Omega_3(G)| = 2^5$. Then one of the following holds.*

- (a) G is abelian of type $(2^m, 4)$, $m \geq 4$.
- (b) $G = \langle a, b \mid a^{2^m} = b^4 = 1, m \geq 4, a^b = a^{1+2^{m-1}} \text{ or } b^a = b^{-1} \rangle$ is minimal nonabelian.
- (c) $G = \langle a, l \mid a^{2^m} = l^8 = 1, m \geq 4, a^{2^{m-1}} = l^4, l^a = l^{-1} \rangle$, where $\Omega_3(G) = \langle l, a^{2^{m-3}} \rangle$ is abelian of type $(8, 4)$, $G' = \langle l^2 \rangle \cong C_4$, $Z(G) = \langle a^2 \rangle \cong C_{2^{m-1}}$, and $G' \not\leq Z(G)$.
- (d) $G = \langle a, w \mid a^{2^m} = w^4 = 1, m \geq 4, a^w = a^{1+2^{m-2}} \rangle$, where $\Omega_3(G) = \langle w, a^{2^{m-3}} \rangle$, $G' = \langle a^{2^{m-2}} \rangle \cong C_4$, $Z(G) = \langle a^4 \rangle$, and so $G' \leq Z(G)$. Also, for $m = 4$, $\Omega_3(G)$ is nonabelian and for $m > 4$, $\Omega_3(G)$ is abelian of type $(8, 4)$.
- (e) $G = \langle a, b \mid a^{2^m} = b^{16} = 1, m \geq 4, a^{2^{m-1}} = b^8, a^b = a^{-1+\epsilon \cdot 2^{m-2}}, \epsilon = 0, 1 \rangle$, where $\Omega_3(G) = \langle b^2, a^{2^{m-3}} \rangle$ is abelian of type $(8, 4)$ and $G/\Omega_2(G) \cong Q_{2^{m-1}}$. If $\epsilon = 0$, then $|G : C_G(\Omega_2(G))| = 2$ and if $\epsilon = 1$, then $|G : C_G(\Omega_2(G))| = 4$.

5.4^o . We prove here the following result.

Theorem 52.13 ([Boz]). *Let G be a 2-group containing exactly one subgroup of order 2^5 and exponent ≤ 8 . Then we have $|\Omega_3(G)| = 2^5$.*

In fact, with the similar proof, we get the following more general result.

Theorem 52.14 ([Boz]). *Let G be a 2-group containing exactly one subgroup of order 2^{n+2} and exponent $\leq 2^n$, where $n \geq 2$ is a fixed integer. Then we have $|\Omega_n(G)| = 2^{n+2}$.*

Proof. Let H be the unique subgroup of order 2^{n+2} and exponent $\leq 2^n$ ($n \geq 2$). Then H is a characteristic subgroup of G and $H \leq \Omega_n(G)$. Suppose that the theorem is false. Then there exists an element $a \in G - H$ of order $\leq 2^n$ with $a^2 \in H$. Set $\tilde{H} = H\langle a \rangle$ so that $|\tilde{H}| = 2^{n+3}$. Since H is neither cyclic nor of maximal class, H has a G -invariant four-subgroup R . We have $|R\langle a \rangle| \leq 2^{n+2}$ and so there is a maximal subgroup M of \tilde{H} such that $M \geq R\langle a \rangle$. We have $\exp(M \cap H) \leq 2^n$ and since $M = (M \cap H)\langle a \rangle$, we get $\Omega_n(M) = M$, $|M| = 2^{n+2}$, $M \neq H$, and $\exp(M) \leq 2^{n+1}$.

The uniqueness of H forces $\exp(M) = 2^{n+1}$ so M has a cyclic subgroup of index 2. But $|M| \geq 2^4$ (since $n \geq 2$) and M has the normal 4-subgroup R . This implies that M is not of maximal class and so M is either abelian of type $(2^{n+1}, 2)$ or $M \cong M_{2^{n+2}}$. In both cases $\Omega_n(M) < M$ and this contradicts our result in the previous paragraph. The theorem is proved. \square

2-groups G with $c_2(G) = 4$

For a finite 2-group G and a fixed integer $n \geq 1$ we denote with $c_n(G)$ the number of cyclic subgroups of order 2^n . The starting point is the following result: if a 2-group G is neither cyclic nor of maximal class and $n > 1$, then $c_n(G)$ is even. Thus, for any 2-group G we have $c_2(G) = 1$ if and only if G is either cyclic or dihedral and $c_2(G) = 3$ if and only if $G \in \{Q_8, SD_{16}\}$.

In this section we shall determine (up to isomorphism) all 2-groups G of order $> 2^4$ with $c_2(G) = 4$. If, in addition, $|\Omega_2(G)| = 2^4$, then such groups G have been determined in §52. In the sequel we assume that $|\Omega_2(G)| > 2^4$. If moreover G has a quaternion subgroup, then we get an infinite class of 2-groups and they have the properties $\Omega_2(G) = G$ and $|Z(G)| = 2$ (Theorem 53.6). Therefore we assume also in what follows that G has no quaternion subgroups. Then we show first that $A = \langle U_1, U_2, U_3, U_4 \rangle \cong C_4 \times C_2 \times C_2$, where $\{U_1, U_2, U_3, U_4\}$ is the set of four cyclic subgroups of order 4 in G (Theorem 53.7). It is interesting to note here that each subgroup U_i turns out to be normal in G . If in addition $\Omega_2(G) = G$, then $G = B\langle t \rangle$, where B is abelian of type $(2^m, 2, 2)$, $m \geq 2$, and t is an involution inverting B and here $Z(G) \cong E_8$ (Theorem 53.8). If $|G : \Omega_2(G)| \geq 4$, then $|G : \Omega_2(G)| = 4$ and G is a uniquely determined group of order 2^7 with $|Z(G)| = 2$ (Theorem 53.9). Finally, if $|G : \Omega_2(G)| = 2$, then we get an infinite class of 2-groups G with the properties $|G| \geq 2^7$, $G' \not\leq \Omega_1(A)$, and $Z(G) \cong E_4$ (Theorem 53.10(a)) and we get an exceptional group G of order 2^6 with $Z(G) \cong E_4$ and $G' \leq \Omega_1(A)$ (Theorem 53.10(b)). All groups will be given in terms of generators and relations. The above exceptional groups of orders 2^6 and 2^7 have peculiar structure but they exist as subgroups of the alternating group A_{16} .

Exercise 1 (see Theorem 6.10). Let A be an abelian 2-group of type $(2^n, 2, \dots, 2)$ and of order 2^{n+d-1} , $n > 1$, $d > 1$. Prove that $|\text{Aut}(A)| = 2^{n+d-2}(2^d - 2)(2^d - 2^2) \dots (2^d - 2^{d-1})$.

We need the following information about the structure of $\text{Aut}(C_4 \times C_2 \times C_2)$.

Proposition 53.1. *Let $S \in \text{Syl}_2(\text{Aut}(A))$, where $A \cong C_4 \times C_2 \times C_2$. Let F be the stability group of the chain $A > \Omega_1(A) > \{1\}$. Then $F \cong E_8$ is normal in $\text{Aut}(A)$ and $S = D \cdot F$, where $F \cap D = \{1\}$ and $D \cong D_8$. If X is any subgroup of S such that $X \cap F = \langle t \rangle$ is of order 2, then t is either a square in X or $t \notin \Phi(X)$.*

Proof. By Exercise 1 with $n = 2$ and $d = 3$, we get $|\text{Aut}(A)| = 8 \cdot 6 \cdot 4 = 2^6 \cdot 3$ and so $|S| = 2^6$. Let $A = \langle v, u, e \rangle$, where $o(v) = 4$, $o(u) = 2 = o(e)$. The stability group F of the chain $A > \Omega_1(A) > \{1\}$ is normal in $\text{Aut}(A)$, $F \cong E_8$, and so $F \leq S$. Consider the automorphisms α and β of A given by $v^\alpha = v$, $u^\alpha = uz$, $e^\alpha = eu$; $v^\beta = v$, $u^\beta = uz$, $e^\beta = e$, where $z = v^2$. Then $o(\alpha) = 4$, $o(\beta) = 2$, $\alpha^\beta = \alpha^{-1}$, and so $D = \langle \alpha, \beta \rangle \cong D_8$ with $D \cap F = \{1\}$. Since $|FD| = 2^6 = |S|$, we may set $S = D \cdot F$.

Let $X \leq S$ be such that $X \cap F = \langle t \rangle$ is of order 2 and assume that t is not a square in X . Since F is normal in S , $\langle t \rangle \leq Z(X)$ and $X/\langle t \rangle$ is isomorphic to a subgroup of $S/F \cong D_8$. If $X/\langle t \rangle$ is elementary abelian, then $\Phi(X) \leq \langle t \rangle$ and therefore $\Phi(X) = \{1\}$ since t is not a square in X ; in that case $t \notin \Phi(X)$. If $X/\langle t \rangle$ is cyclic of order 4, then, since X is not cyclic, we get $t \notin \Phi(X) (= \mathfrak{V}_1(X))$. Finally, suppose that $X/\langle t \rangle \cong D_8$. Let $U/\langle t \rangle$ be the cyclic subgroup of index 2 in $X/\langle t \rangle$. Then U is noncyclic so $t \notin \Phi(U) = \mathfrak{V}_1(U)$. For each $x \in X - U$, $x^2 \in \langle t \rangle$ (indeed, $\langle x, t \rangle/\langle t \rangle$ is of order 2), and so (by our assumption) $x^2 = 1$. It follows that $\Phi(X) = \mathfrak{V}_1(U)$. Hence in any case $t \notin \Phi(X)$. \square

Theorems 52.7 and 52.8 imply the following

Proposition 53.2. *Let K be a 2-group possessing exactly two cyclic subgroups of order 4 and assume that neither of them is a characteristic subgroup of K . Then one of the following holds: (a) $K \cong C_4 \times C_2$; (b) $K \cong D_8 \times C_2$; (c) $K = \langle b, t \mid b^8 = t^2 = 1, b^t = bu, u^2 = [u, t] = 1, b^u = bz, z = b^4 \rangle$ and this is a group of order 2^5 with $\Omega_2(K) = \langle b^2, t \rangle \times \langle u \rangle \cong D_8 \times C_2$.*

The following two propositions describe the results from §52 (see Theorems 52.4 and 52.5 for the Proposition 53.3 and Theorem 52.2 for Proposition 53.4) adopted for an application in the proofs of Theorems 53.9 and 53.10. Since the notation introduced in these propositions will be used in the proofs (which are quite involved), the explicit statement of these results is unavoidable.

Proposition 53.3. *Let H be a 2-group of order $> 2^4$ and suppose that $A = \Omega_2(H) \cong C_4 \times C_2 \times C_2$. We set $E = \Omega_1(A) \cong E_8$, $\mathfrak{V}_1(A) = \langle z \rangle$, $B = C_H(A)$. Then $C_H(E)/E$ is cyclic and so B is abelian and H/E is either cyclic or generalized quaternion. Suppose that $H/E \cong Q_{2^n}$, $n \geq 3$, and set $E = \langle z, u, e \rangle$, $H = \langle E, a, b \rangle$, where $\langle E, a \rangle/E$ is a cyclic subgroup of index 2 in H/E , $o(a) = 2^n$, $a^{2^{n-1}} = z$, $a^{2^{n-2}} = v$ is of order 4, $b^2 \in A - E$, $o(b) = 8$, and $A = \langle E, v \rangle$. Then we have one of the following possibilities:*

- (a) *If $E \not\leq \Phi(H)$, then $b^2 = uv$, $[a, u] = 1$, $[a, e] = z^\mu$, $\mu = 0, 1$, $[b, e] = 1$, $u^b = uz$, and $a^b = a^{-1}$. If $\mu = 0$, then $B = \langle E, a \rangle$, and if $\mu = 1$, then $B = \langle E, a^2 \rangle$.*
- (b) *If $E \leq \Phi(H)$ and $[E, a] \neq \{1\}$, then $b^2 = ev$, $[a, u] = 1$, $[a, e] = z$, $[b, e] = z$, $[b, u] = z$, $a^b = a^{-1}ue^\epsilon$, $\epsilon = 0, 1$, and if $\epsilon = 1$, then $n \geq 4$. Here $B = \langle E, a^2 \rangle$.*

(c) If $E \leq \Phi(H)$ and $[E, a] = \{1\}$, then $b^2 = uv$, $[b, e] = 1$, $u^b = uz$, and $a^b = a^{-1}e$. Here $B = \langle E, a \rangle$.

Proposition 53.4. Let H be a nonabelian 2-group of order $> 2^4$ and suppose that $A = \Omega_2(H) \cong C_4 \times C_2 \times C_2$. We set $E = \Omega_1(A) \cong E_8$, $\mathfrak{U}_1(A) = \langle z \rangle$, and $B = C_H(A)$. Suppose that $H/E \cong C_{2^{n-1}}$, $n \geq 3$, and set $E = \langle z, u, e \rangle$, $H = \langle E, a \rangle$, where $o(a) = 2^n$, $a^{2^{n-1}} = z$, $a^{2^{n-2}} = v$ is of order 4, and $A = \langle E, v \rangle$. Then we have one of the following possibilities:

- (a) If $|[E, a]| = 4$, then $[a, e] = u$, $[a, u] = z$, $n \geq 4$, and $B = \langle E, a^4 \rangle$.
- (b) If $|[E, a]| = 2$ and $[E, a] = \langle z \rangle$, then $[a, e] = 1$, $[a, u] = z$, and $B = \langle E, a^2 \rangle$.
- (c) If $|[E, a]| = 2$ and $[E, a] \neq \langle z \rangle$, then $[a, e] = u$, $[a, u] = 1$, and $B = \langle E, a^2 \rangle$.

Let G be a 2-group of order $> 2^4$ with $c_2(G) = 4$. Then $|\Omega_2(G)| \geq 2^4$. If $|\Omega_2(G)| = 2^4$, then from results of §52 follows that $\Omega_2(G)$ is isomorphic to $Q_8 * C_4$ or $C_4 \times C_2 \times C_2$ and the following result follows at once.

Theorem 53.5. Let G be a 2-group of order $> 2^4$ with $c_2(G) = 4$ and $|\Omega_2(G)| = 2^4$. Then one of the following holds:

- (a) $\Omega_2(G) \cong Q_8 * C_4$ and G is isomorphic to a group (a) or (c) of Theorem 52.1.
- (b) $\Omega_2(G) \cong C_4 \times C_2 \times C_2$ and G is isomorphic to a group described in Propositions 53.3 and 53.4 or $G \cong C_{2^m} \times C_2 \times C_2$, $m \geq 2$.

In the rest of this section we assume that $|\Omega_2(G)| > 2^4$. First we prove the following easy special result.

Theorem 53.6. Let G be a 2-group of order $> 2^4$ with $c_2(G) = 4$ and $|\Omega_2(G)| > 2^4$. If G has a subgroup $Q \cong Q_8$, then $Q \triangleleft G$, $C = C_G(Q)$ is cyclic of order 2^n , $n \geq 2$, $G = (Q * C)\langle t \rangle$, where t is an involution such that $Q\langle t \rangle \cong SD_{2^4}$ and $\langle t \rangle C \cong D_{2^{n+1}}$. We have $|Z(G)| = 2$, $|G| = 2^{n+3}$ and $\Omega_2(G) = G$.

Proof. If Q were not normal in G , there is $g \in G$ such that $Q \neq Q^g$. But then $|Q \cap Q^g| \leq 4$ and so $Q \cup Q^g$ contains at least five cyclic subgroups of order 4, a contradiction. Hence Q is normal in G . If $C_G(Q) \leq Q$, then $|G| \leq 2^4$, a contradiction. Therefore $C = C_G(Q) > Z(Q)$ and C is normal in G . If t_0 is an involution in $C - Z(Q)$, then $c_2(Q \times \langle t_0 \rangle) = 6$, a contradiction. Since C cannot be generalized quaternion (otherwise $c_2(G) \geq 6$), C is cyclic of order 2^n , $n \geq 2$. We see that $c_2(Q * C) = 4$ and $\Omega_2(Q * C) = Q * \Omega_2(C)$ is of order 2^4 . But $|\Omega_2(G)| > 2^4$ and so there is an involution $t \in G - (QC)$, $G = (QC)\langle t \rangle$ and t induces an “outer” automorphism on Q . It follows $Q\langle t \rangle \cong SD_{2^4}$. Since there are no elements of order 4 in $G - (QC)$, $C_{QC}(t)$ is elementary abelian. Hence $C_C(t) = Z(Q)$ and so $\langle t \rangle \cdot C$ is of maximal class. The only possibility is that $\langle t \rangle \cdot C$ is dihedral of order 2^{n+1} . The structure of G is completely determined. \square

Remark. Here we will give another proof of Theorem 53.6, retaining the same notation. Since G is not of maximal class, $C = C_G(Q) \not\leq Q$, by Proposition 10.17. If z is an involution in $C - Z(Q)$, then $c_2(Q \times \langle z \rangle) = 6 > 4 = c_2(G)$, a contradiction. If $c_2(C) > 1$, then, obviously, $c_2(QC) \geq 5 > 4 = c_2(G)$. Thus, $c_1(C) = c_2(C) = 1$ so, by Theorem 1.17(b), C is cyclic, $C \cap Q = Z(Q)$. We have $c_2(Q * \Omega_2(C)) = 4 = c_2(G)$ so $Q * \Omega_2(C)$ is normal in G . Since Q is characteristic in $Q * \Omega_2(C)$ (Appendix 16), it is normal in G . Since $|\text{Aut}(Q)|_2 = 8$, we have $|G : (Q * C)| \leq 2$. Since $|\Omega_2(G)| > 16 = |Q * \Omega_2(C)|$, there exists an involution t in $G - (Q * C)$, and we get $G = \langle t \rangle \cdot (QC)$. Using the condition $c_2(G) = 4$, we get $\langle t \rangle \cdot Q \cong SD_{16}$ and $\langle t \rangle \cdot C \cong D_{2^n}$ for some $n \in \mathbb{N}$. The group G is completely determined.

Next we assume also that G has no subgroups isomorphic to Q_8 . The subgroup generated by four cyclic subgroups of order 4 will be determined in our next basic result.

Theorem 53.7. *Let G be a 2-group of order $> 2^4$ with $c_2(G) = 4$ and $|\Omega_2(G)| > 2^4$. Suppose that G has no subgroups isomorphic to Q_8 . Then $A = \langle U_1, U_2, U_3, U_4 \rangle$ is abelian of type $(4, 2, 2)$, where $U_1, U_2, U_3, U_4 < G$ are cyclic of order 4.*

Proof. We first show the following easy fact. If a cyclic subgroup V of order 4 normalizes another cyclic subgroup U of order 4, then $|U \cap V| = 2$ and $\langle U, V \rangle$ is abelian of type $(4, 2)$. Indeed, if $U \cap V = \{1\}$, then $|(UV)'| \leq 2$ and so UV is metacyclic of order 2^4 and class ≤ 2 . This implies that $\exp(UV) = 4$ and $\Omega_1(UV)$ is abelian of type $(2, 2)$. If N is a maximal subgroup of UV containing U , then all eight elements in $(UV) - N$ are of order 4 and so $c_2(UV) > 4$, a contradiction. Hence $|U \cap V| = 2$ and $|UV| = 8$. But UV cannot be nonabelian, i.e., quaternion or dihedral, and so UV is abelian of type $(4, 2)$.

If each U_i is normal in G , then (by the above) $A = \langle U_1, U_2, U_3, U_4 \rangle$ is abelian of type $(4, 2, 2)$, and we are done. Therefore we may assume that U_1 is not normal in G . Set $K = N_G(U_1)$ and we have $2 \leq |G : K| \leq 4$. By Theorem 1.17(b), $c_2(K)$ is even. Let M be a subgroup of G such that $K < M$, $|M : K| = 2$ and $|G : M| \leq 2$. For each $m \in M - K$, $U_1^m = U_2 \neq U_1$ and $N_G(U_2) = K$. By the above, $A_0 = \langle U_1, U_2 \rangle \cong C_4 \times C_2$ and A_0 is normal in M . If there is a further cyclic subgroup U_3 of order 4 contained in K , then $U_3 \not\leq A_0$, U_3 normalizes U_1 and U_2 and so, by the above, U_3 centralizes U_1 and U_2 and $|A_0 \cap U_3| = 2$. Hence $A_0 U_3$ is abelian of type $(4, 2, 2)$ and we are done.

We assume in the sequel that K has exactly two cyclic subgroups U_1 and U_2 of order 4. Since U_1 and U_2 are conjugate in M , it follows that neither U_1 nor U_2 is a characteristic subgroup of K . By Proposition 53.2, we have exactly three possibilities for the structure of K .

Assume (by way of contradiction) that $K > A_0$ and set $L = \Omega_2(K)$. By Lemma 42.1, $|L| > 2^3$ (if $|L| = 2^3$, then $Z(L)$ is a characteristic cyclic subgroup of order 4 in

K , which is not the case). Therefore, by Proposition 53.2, we have $L \cong D_8 \times C_2$ and L is normal in M . If $K > L$, then $|K : L| = 2$ (Proposition 53.2(c)) and all elements in $K - L$ are of order 8. In any case, by Proposition 53.2, $C_K(A_0) = A_0$ and K/A_0 is elementary abelian of order 2 or 4.

Suppose that $K > L$. Then $M/A_0 \cong \text{Aut}(A_0) \cong D_8$ since $|M/A_0| = 8$. Since $L/A_0 = \Phi(M/A_0)$, there is an element $k \in M - K$ such that $k^2 \in L - A_0$ (if $k^2 \in A_0$ for all $k \in M - K$, then $A_0 \geq \Phi(M)$, a contradiction since $M/A_0 \cong D_8$). All elements in $L - A_0$ are involutions and so k is an element of order 4. In fact, all 16 elements in $(\langle k \rangle A_0) - L$ are of order 4. But then $c_2(\langle k \rangle A_0) \geq 8$, a contradiction.

We have $K = L \cong D_8 \times C_2$; in that case, $|M| = 2^5$. Assume that $M/A_0 \cong C_4$. Let $x \in M - K$. If $o(x) = 8$, then $\langle x \rangle \cap K$ is cyclic of order 4, say U_1 . Then $N_G(U_1) \geq \langle x, K \rangle > K$, which is a contradiction. Thus, $M - K$ has no elements of order 8. Suppose that $o(x) = 2$. Then $\langle x, A_0 \rangle = K$ since M/A_0 is cyclic; in that case $x \in K$, again a contradiction. Thus, in the case under consideration, all 16 elements in $M - K$ are of order 4, a contradiction. Thus $M/A_0 \cong E_4$. For each $m \in M - K$, $U_1^m = U_2$ and so $m^2 \in \Omega_1(A_0)$ and m is an element of order 2 or 4. Since $c_2(A_0) = 2$, it follows that $M - K$ contains at most four elements of order 4. Hence there exists an involution $s \in M - K$ since $|M - K| = 16$ (in fact, there are at least 12 involutions in $M - K$). Let t be an involution in $K - A_0$. We set $A_0 = \langle a, u \mid a^4 = u^2 = [a, u] = 1, a^2 = z \rangle$ and so $\Omega_1(A_0) = \langle u, z \rangle$ and $a^t = a^{-1}, u^t = u, a^s = au, u^s = u$, because $U_1^s = U_2$ and s induces an involutory automorphism on A_0 . Since s inverts (actually centralizes) exactly the elements in $\Omega_1(A_0)$, it follows that A_0s has exactly four involutions. Hence the other four elements in A_0s are of order 4. This means that we have found all four elements of order 4 in $M - K$. Hence the coset $A_0(st)$ consists only of involutions. But then the involution st must invert A_0 . On the other hand, we have $a^{st} = (au)^t = a^{-1}u$, which is a contradiction.

We have proved that $K = A_0$. Since $|G| > 2^4$, it follows $|G : M| = 2$ and $|G| = 2^5$. In this case $|G : K| = 4$ and so $\{U_1, U_2, U_3, U_4\}$ forms a single conjugacy class in G . This implies that $N_G(A_0) = M$ (otherwise, A_0 is normal in G so U_1 and U_3 are not conjugate in G) and $M - A_0$ contains exactly four elements of order 4, and the other four elements in $M - A_0$ are involutions. Since $|\Omega_2(G)| > 2^4$, there are involutions in $G - M$.

Let m be an involution in $M - A_0$. We set again $A_0 = \langle a, u \mid a^4 = u^2 = [a, u] = 1, a^2 = z \rangle$. Since M is not of maximal class (see Proposition 1.8), $U_1^m = U_2$, and m induces an involutory automorphism on A_0 , we may set $a^m = a^\mu u$ ($\mu = \pm 1$) and $u^m = u$. Thus $C_{A_0}(m) = \Omega_1(A_0) = \langle u, z \rangle$ and so $E = \langle u, z, m \rangle = \Omega_1(M)$ (indeed, $|\langle u, z, m \rangle - |\langle u, z \rangle| = 4$ is the number of involutions in $M - K = M - A_0$) is a normal elementary abelian subgroup of order 8 in G .

Let v be an involution in $G - M$. If v does not centralize E , then Ev would contain some elements of order 4, a contradiction since $M \cap Ev \subseteq M \cap Mv = \emptyset$. Thus $\langle E, v \rangle = E \times \langle v \rangle$ is an elementary abelian maximal subgroup of G . But then $\exp(G) = 4$ and so all elements in $G - M$ must be involutions. It follows that v

inverts M and so M is abelian. In this case, as it is easy to check since $|M| = 2^4$, M is abelian of type $(4, 2, 2)$, and the theorem is proved. \square

In the rest of this section we set $A = \langle U_1, U_2, U_3, U_4 \rangle \cong C_4 \times C_2 \times C_2$, where $\{U_1, U_2, U_3, U_4\}$ is the set of four cyclic subgroups of order 4 in G , $E = \Omega_1(A) \cong E_8$, $\langle z \rangle = \mathcal{O}_1(A) \leq Z(G)$, $B = C_G(A)$. Let $v \in A - E$ so that $v^2 = z$. If there is an involution $s \in B - A$, then sv is an element of order 4 in $B - A$, a contradiction. Hence $A = \Omega_2(B)$ and Proposition 53.3 implies that B/E is cyclic and so B is abelian of type $(2^m, 2, 2)$, $m \geq 2$. It follows that $C_G(B) = B$. If $c \in B$ with $o(c) = 2^m$, then $c^{2^{m-1}} = \langle z \rangle$, $B = E\langle c \rangle$, $E \cap \langle c \rangle = \langle z \rangle$, $A = E\langle c^{2^{m-2}} \rangle$. Since $|\Omega_2(G)| > 2^4$, there exists an involution $t \in G - B$. If there is an element $x \in Bt$ with $o(x) > 2$, then $o(x) \geq 8$ since $B \cap Bx = \emptyset$, and so $o(x^2) \geq 4$ and $x^2 \in B$. Thus $C_B(t) = C_B(x)$ is not elementary abelian and so Bt would contain elements of order 4, a contradiction (namely, if y is an element of order 4 in $C_B(t)$, then $yt \in Bt$ is of order 4). Hence all elements in Bt are involutions and consequently t inverts B . If there is an involution $t' \in G - B\langle t \rangle$, then t' also inverts B and so $tt' \in G - B$ would centralize B , a contradiction since $C_G(B) = B$. Thus $D = B\langle t \rangle = \Omega_2(G)$. If $\Omega_2(G) = G$, the structure of G is determined and we have proved the following

Theorem 53.8. *Let G be a 2-group of order $> 2^4$ with $c_2(G) = 4$ and $|\Omega_2(G)| > 2^4$. Suppose that G has no subgroups isomorphic to Q_8 . Then $D = \Omega_2(G) = B\langle t \rangle$, where B is abelian of type $(2^m, 2, 2)$, $m \geq 2$, and t is an involution inverting B . We have $Z(D) = E = \Omega_1(B)$, $C_G(t) = \langle t \rangle \times E = F$, and so F is a self-centralizing elementary abelian subgroup of order 16. If $\Omega_2(G) = G$, the structure of G is completely determined.*

In what follows we assume, in addition, that $G > \Omega_2(G)$. We show next that $C_G(E) = D = \Omega_2(G)$. Indeed, suppose that $C_G(E) > D$. Since $C_G(E)$ stabilizes the chain $A > E > \{1\}$ in view of $|A : E| = 2$, it follows that $C_G(E)/B (= C_G(E)/C_G(A))$ is elementary abelian and $4 \leq |C_G(E)/B| \leq 8$. Let F_0/B be a subgroup of order 2 in $C_G(E)/B$ such that $D \cap F_0 = B$. Then $\Omega_2(F_0) = A$ (otherwise, $c_2(F_0) > 4 = c_2(G)$) and F_0 is nonabelian of order $> 2^4$ since $F_0 \not\leq B = C_G(A)$. Proposition 53.3 implies, however, that F_0/E is cyclic and so F_0 is abelian, a contradiction.

We have proved that $C_G(E) = D (= \Omega_2(G))$. Hence $X = G/B$ is a subgroup of $\text{Aut}(A)$ (see Proposition 53.1) and if $F_1 (\cong E_8)$ is the stability group of $A > E > \{1\}$ (note that $F_1 < \text{Aut}(A)$), then $X \cap F_1 = D/B$ is of order 2. Suppose that the involution in D/B is a square in X . Then there exists $x \in G$ such that $x^2 = t' \in D - B$. But t' is an involution (indeed, all elements in $D - B$, by the above, are involutions) and so x is an element of order 4 in $G - B$, a contradiction since $A \leq B$. Proposition 53.1 implies that there exists a maximal subgroup H of G containing B such that $H \cap D = B$ (indeed, by the above proposition, $D/B \not\leq \Phi(G/B)$), and so $G/B = (D/B) \times (H/B)$ since D is normal in G . Note that $\Omega_2(H) = A$ (indeed, $H \cap \Omega_2(G) = H \cap D = B$ and $\Omega_2(B) = A$) and $H > B$ is nonabelian of order $> 2^4$,

where $B = C_G(A) = C_H(A)$. In this situation we shall apply Propositions 53.3 and 53.4 which describe all possibilities for the structure of H . Also we shall use freely the notation introduced in these propositions. In particular, $2 \leq |H/B| \leq 4$ and so $G/B(= (D/B) \times (H/B))$ is abelian of order ≥ 4 . We also set $D = B\langle t \rangle$, where t is an involution inverting B .

It is possible at this stage to eliminate the possibility (c) of Proposition 53.3 and the possibilities (a) and (c) of Proposition 53.4 (thus, we intend to consider these three possibilities using the notation introduced in corresponding parts).

Suppose that H is isomorphic to a group (c) of Proposition 53.3. Consider the subgroup $K = B\langle tb \rangle$, where $(tb)^2 \in B$ and $\Omega_2(K) = A$. We compute $a^{tb} = (a^{-1})^b = (a^b)^{-1} = (a^{-1}e)^{-1} = ae$ and so tb centralizes B/E and $|B/E| \geq 4$. Hence K/E cannot be generalized quaternion and so K/E is cyclic. It follows that $\langle tb \rangle$ covers K/E which gives $(tb)^2 = a^i s$, where $s \in E$ and i is an odd integer. On the other hand, tb centralizes $(tb)^2$ and so $a^i s = (a^i s)^{tb} = (a^{-i}s)^b = (a^{-1}e)^{-i}s^b = a^i e s^b$. Thus $s^b = se$ and $[b, s] = e$. This is a contradiction since $[b, E] = \langle z \rangle$ according to Proposition 53.3(c).

Suppose that H is isomorphic to a group (a) of Proposition 53.4; in that case, $H/B \cong C_4$ since $H = \langle E, a \rangle$ and $B = \langle E, a^4 \rangle$. Consider the subgroup $K = B\langle ta \rangle$. Since $G/B \cong C_2 \times C_4$, it follows $K/B \cong C_4$ and $\Omega_2(K) = A$. We compute $(a^4)^{ta} = (a^4)^{-1}$ and so if $|B/E| \geq 4$, K/E is nonabelian and so K/E is generalized quaternion. But K/E has the cyclic factor group $(K/E)/(B/E) \cong K/B$ of order 4, a contradiction. Hence we must have $B = A$, $n = 4$, $|G| = 2^7$, and K/E is cyclic of order 8. Since $\langle ta \rangle$ covers K/E , we get $(ta)^4 = sv$ with $s \in E$. But ta centralizes $(ta)^4$ and so we get (recall that $v = a^4$) $sv = (sv)^{ta} = (sv^{-1})^a = s^a v^{-1} = s^a v z$ which implies $s^a = sz$. This gives $s = uz^\eta$ with $\eta = 0, 1$, and $(ta)^4 = uz^\eta v$. On the other hand, $(ta)^2 \in (B\langle a^2 \rangle) - B$, and so $(ta)^2 = a^2 s'$, where $s' \in A$. Indeed, G/B is abelian and so $(ta)^2 = t^2 a^2 s'$ with $s' \in B = A$. We compute $uz^\eta v = (ta)^4 = (a^2 s')^2 = a^2 s' a^2 s' = a^4 (a^{-2} s' a^2) s' = v(s')^{a^2} s'$, which gives $(s')^{a^2} = (s')^{-1} u z^\eta$ and $[a^2, (s')^{-1}] = u(z^\eta (s')^{-2})$ with $z^\eta (s')^{-2} \in \langle z \rangle$. This is a contradiction since, according to Proposition 53.4(a), $[a^2, A] = \langle z \rangle$.

Suppose that H is isomorphic to a group (c) of Proposition 53.4. Here $B = \langle E, a^2 \rangle$ and we consider the subgroup $K = B\langle ta \rangle$. We see $(a^2)^{ta} = (a^2)^{-1}$ and so ta inverts B/E . Note that $\Omega_2(K) = A$ and so in case $|B/E| \geq 4$, K/E is generalized quaternion and consequently $(ta)^2 \in A - E$ (since $A/E = Z(K/E)$). If $|B/E| < 4$, then $B = A$ and again $(ta)^2 \in A - E$ (since $o(ta) \geq 8$). It follows $(ta)^2 = sv$ with $s \in E$ and $v = a^{2^{n-2}}$. Since ta centralizes $(ta)^2$, we get $sv = (sv)^{ta} = (sv^{-1})^a = s^a v^{-1} = s^a v z$. This gives $s^a = sz$ and $[a, s] = z$. But Proposition 53.4(c) implies $[a, E] = \langle u \rangle \neq \langle z \rangle$, a contradiction.

We are now ready to prove the following deep result.

Theorem 53.9. *Let G be a 2-group of order $> 2^4$ with $c_2(G) = 4$ and $|\Omega_2(G)| > 2^4$. Suppose that G has no subgroups isomorphic to Q_8 and $|G : \Omega_2(G)| \geq 4$. Then we*

have $|G : \Omega_2(G)| = 4$ and G is a uniquely determined group of order 2^7 :

$$\begin{aligned} G = \langle a, b, t \mid a^8 &= b^8 = t^2 = 1, a^2 = v, a^4 = z, b^2 = ev, a^b = a^{-1}u, \\ e^2 &= u^2 = [e, v] = [u, v] = [e, u] = [a, u] = [t, e] = [t, u] = 1, \\ e^a &= ez, e^b = ez, u^b = uz, v^t = v^{-1}, a^t = eva^{-1}, \\ b^t &= euvb^{-1} \rangle. \end{aligned}$$

Here $E = \langle z, u, e \rangle$ is a normal elementary abelian subgroup of order 8. Four cyclic subgroups of order 4 in G generate the abelian subgroup $A = \langle E, v \rangle$ of type $(4, 2, 2)$ which is self-centralizing in G and each cyclic subgroup of order 4 is normal in G . We have $D = \Omega_2(G) = A\langle t \rangle$, where the involution t inverts A and $C_G(t) = E \times \langle t \rangle \cong E_{16}$ is self-centralizing in G . We have $\Phi(G) = A$, all elements in $G - D$ are of order 8, and $Z(G) = \langle z \rangle$ is of order 2. For one of the four maximal subgroups M of G which do not contain D we have $M/E \cong Q_8$ and $E < \Phi(M)$ (so this M is generated by two elements) but for the other three such maximal subgroups M we have $M/E \cong Q_8$ and $E \not\leq \Phi(M)$ (so these M are not generated by two elements). For each of the three maximal subgroups N of G which contain D we have $N/E \cong D_8$. The group G exists as a subgroup of the alternating group A_{16} and 16 is the smallest degree for any faithful permutation representation of G .

Proof. Since $G/B = (D/B) \times (H/B)$ we get $G/\Omega_2(G) = G/D \cong H/B$, so we have to examine here only the cases, where H is isomorphic to a group (b) of Proposition 53.3 or to a group (a) with $\mu = 1$ of Proposition 53.3. In these cases we have $|H/B| = 4$ and so we have already proved that $|G : \Omega_2(G)| = 4$.

Suppose first that H is isomorphic to a group (b) of Proposition 53.3. Note that in this case $H/E \cong Q_{2^n}$, $n \geq 3$, $E \leq \Phi(H)$, and if $n = 3$, then $\epsilon = 0$, i.e., $a^b = a^{-1}ue^\epsilon = a^{-1}u$. We have here $G/B \cong E_8$. Consider the subgroup $L = B\langle ta \rangle$, where $(ta)^2 \in B$ and $\Omega_2(L) \leq D \cap L \leq A$ so $\Omega_2(L) = A$ (recall that $A\langle t \rangle = D = \Omega_2(G)$ and involution t inverts A). We compute $(a^2)^{ta} = (a^{-2})^a = (a^2)^{-1}$, and so ta inverts B/E (recall that $B = \langle E, a^2 \rangle$). If $n \geq 4$, then $|B/E| \geq 4$, L/E is generalized quaternion, and consequently $(ta)^2 \in A - E$ (since $o(ta) \geq 8$). If $n = 3$, then $B = A$ and $o(ta) \geq 8$ implies again $(ta)^2 \in A - E$. Thus $(ta)^2 = sv$, where $s \in E$ and $v = a^{2^{n-2}}$. From this relation we get $sv = tata = a^ta$ so $a^t = sva^{-1}$. Since ta centralizes $(ta)^2$, we have $sv = (sv)^{ta} = (sv^{-1})^a = s^a v^{-1} = s^a v v^2 = s^a v z$ and $s^a = sz$, which gives $s = eu_0$ with $u_0 \in \langle u, z \rangle$ since $E = \langle e, u, z \rangle$.

On the other hand, set $B_1 = B\langle a \rangle = E\langle a \rangle$ and consider the subgroup $L_1 = B_1\langle tb \rangle$; then $\Omega_2(L_1) = A$ since $L \neq D = \Omega_2(G)$ and $A \leq \Omega_2(L)$. We compute, taking into account the above obtained equalities, $a^{tb} = (sva^{-1})^b = s^b v^b (a^b)^{-1} = (s^b v^b e^\epsilon u)a = a_0 a$, where $\epsilon = 0, 1$ and $a_0 = s^b v^b e^\epsilon u \in A - E$. If $n \geq 4$, then B_1/E is cyclic of order ≥ 8 and so $L_1/E \cong M_{2^n}$. This is a contradiction since L_1/E must be either cyclic or generalized quaternion. It follows (see Proposition 53.3(b)) $n = 3$, $B = A$, $\epsilon = 0$, $a^2 = v$, $b^2 = ve$, $a^b = a^{-1}u$, and $|G| = 2^7$. We get $v^b = (a^2)^b =$

$(a^b)^2 = (a^{-1}u)^2 = a^{-2} = v^{-1}$, and so $v^b = v^{-1}$. Since $(tb)^2 \in B = A$ and $o(tb) \geq 8$ (indeed, $tb \in G - D = G - \Omega_2(G)$), we have $(tb)^2 = s_0v$, where $s_0 \in E$. Since tb centralizes $(tb)^2$, we get $s_0v = (s_0v)^{tb} = (s_0v^{-1})^b = s_0^b v$, and therefore $s_0^b = s_0$, which implies $s_0 \in \langle eu, z \rangle$. We get $s_0v = tb tb = b^t b$ and $b^t = s_0vb^{-1}$.

The above elements $s, s_0 \in E$ are connected with a relation which we obtain in the following way. We act with t (by conjugation) on the relation $b^{-1}ab = a^{-1}u$ and get (taking into account the above obtained equalities)

$$\begin{aligned} (s_0vb^{-1})^{-1}(sva^{-1})(s_0vb^{-1}) &= (sva^{-1})^{-1}u, \\ bs_0sa^{-1}s_0vb^{-1} &= av^{-1}su, \\ s_0sa^{-1}s_0v &= b^{-1}(av^{-1}su)b = a^{-1}uvs^buz = a^{-1}vs^bz, \\ (as_0sa^{-1})s_0v &= vs^bz, \end{aligned}$$

and since $s_0^{a^{-1}} = s_0^a, s^{a^{-1}} = sz$, we get $s_0^a sz s_0 v = vs^bz$, and this implies the desired relation

$$(1) \quad s_0^a s^b = s_0 s.$$

Note that $s = eu_0$ with $u_0 \in \langle u, z \rangle$ and $s_0 \in \langle eu, z \rangle$.

If $s_0 = euz^\alpha$ ($\alpha = 0, 1$), then (1) gives $s^b = sz$ and so $s = ez^\beta$ ($\beta = 0, 1$). If $s_0 = z^\alpha$ ($\alpha = 0, 1$), then (1) gives $s^b = s$ and so $s = euz^\beta$ ($\beta = 0, 1$). We consider again the relations $a^t = sva^{-1}, b^t = s_0vb^{-1}$, where s, s_0 are the above elements in E . Replacing t with tue , we get $a^{tue} = (sva^{-1})^{ue} = sva^{-1}z = (sz)va^{-1}, b^{tue} = (s_0vb^{-1})^{ue} = s_0vb^{-1}$. Replacing t with tu , we get $a^{tu} = (sva^{-1})^u = sva^{-1}, b^{tu} = (s_0vb^{-1})^u = (s_0z)vb^{-1}$. The above facts show that in our expressions for s and s_0 we may choose $\alpha = \beta = 0$. Hence we get either $s = e$ and $s_0 = eu$ or $s = eu$ and $s_0 = 1$.

We have obtained exactly two groups G_1 and G_2 (of order 2⁷) which differ only in the last two relations:

- (a) G_1 with relations $a^t = eva^{-1}, b^t = evvb^{-1}$;
- (b) G_2 with relations $a^t = euva^{-1}, b^t = vb^{-1}$.

For both groups G_1 and G_2 we have obtained the following common relations:

- (c) $a^8 = b^8 = t^2 = 1, a^2 = v, a^4 = z, b^2 = ev, a^b = a^{-1}u, e^2 = u^2 = [e, v] = [u, v] = [e, u] = [a, u] = [t, e] = [t, u] = 1, e^a = ez, e^b = ez, u^b = uz, v^t = v^{-1}$.

It is possible to show that the groups G_1 and G_2 are isomorphic. In the group G_1 we first obtain by computation (using the relations for G_1)

$$(2) \quad (ab)^t = zv(ab)^{-1}.$$

Then in G_1 we replace the elements a, v, b, e, t with $a' = a^{-1}, v' = v^{-1}, b' = ab, e' = eu, t' = te$, and see that these new elements satisfy the same common relations

(c). But from the relations (a) and (2), we get $(a')^{t'} = e'uv'(a')^{-1}$, $(b')^{t'} = v'(b')^{-1}$, which are the last two relations (b) for the group G_2 . Hence the groups G_1 and G_2 are isomorphic and we have obtained the unique group $G = G_1$ of order 2^7 as stated in our theorem.

We have $\Phi(G) = A$. In order to investigate the structure of seven maximal subgroups M of G , we first see $a^2 = v$, $b^2 = ev$, $(ab)^2 = euzev$, $(ta)^2 = ev$, $(tb)^2 = euv$, and $(tab)^2 = zv$. If $M = \langle A, a, b \rangle = H$, then $\Phi(M) = A \cong C_4 \times C_2 \times C_2$ and so $E \leq \Phi(M)$. If $M = \langle A, a, tb \rangle$, then $\Phi(M) = \langle v, eu \rangle \cong C_4 \times C_2$. If $M = \langle A, b, ta \rangle$, then $\Phi(M) = \langle v, e \rangle \cong C_4 \times C_2$. If $M = \langle A, ta, tb \rangle$, then $\Phi(M) = \langle ev, u \rangle \cong C_4 \times C_2$. Hence in the last three cases we have $E \not\leq \Phi(M)$. For these four maximal subgroups M (which do not contain $D = A\langle t \rangle$) we have $M/E \cong Q_8$. For the other three maximal subgroups N (which contain D) we see that $N/E \cong D_8$.

We get a faithful permutation representation of degree 16 of G in the following way. We set:

$$\begin{aligned} a &= (1, 2, 3, 4, 5, 6, 7, 8)(9, 16, 12, 13, 11, 14, 10, 15), \\ b &= (1, 9, 3, 10, 5, 11, 7, 12)(2, 13, 8, 14, 6, 15, 4, 16), \\ t &= (3, 7)(4, 8)(10, 12)(14, 16). \end{aligned}$$

We see that the above permutations a, b, t are even and check that they satisfy the defining relations for G . The obtained representation is faithful since

$$z = a^4 = (1, 5)(2, 6)(3, 7)(4, 8)(9, 11)(14, 16)(10, 12)(13, 15) \neq 1.$$

It remains to show that $\delta(G)$, the minimal degree of a faithful permutation representation of G (minimal representation), equals 16 (in the previous paragraph we have showed that $\delta(G) \leq 16$). Assume that this is false. Since $Z(G)$ is cyclic, every minimal representation of G , is transitive so $\delta(G)$ is a power of 2. Then G is isomorphic to a 2-subgroup of $S_{\delta(G)}$ so $\delta(G) = 8$. Moreover, $G \cong \Sigma_3 \in \text{Syl}_2(S_{2^3})$. However, $c_1(G) = c_1(\Omega_2(G)) = |D - A| + c_1(A) = 23$ (note that $c_1(A) = 7$). On the other hand, $c_1(\Sigma_3) = |D_8| + [c_1(D_8) + 1]^2 - 1 = 8 + 6^2 - 1 = 43 > 23$, and this is a contradiction. Thus, $\delta(G) = 16$.

In the second half of the proof we investigate the remaining possibility, where H is isomorphic to a group (a) with $\mu = 1$ of Proposition 53.3. Note that in this case $H/E \cong Q_{2^n}$, $n \geq 3$, and $E \not\leq \Phi(H)$. In exactly the same way as in the first part of the proof we get $n = 3$, $B = A$, $|G| = 2^7$, $a^2 = v$, $b^2 = vu$, and $a^b = a^{-1}$. Also we get $a^t = sva^{-1}$ where $s \in E$, $s^a = sz$, $s = eu_0$ with $u_0 \in \langle u, z \rangle$, $b^t = s_0vb^{-1}$, where $s_0 \in E$, $s_0^b = s_0$, and $s_0 \in \langle e, z \rangle$.

We conjugate the relation $b^{-1}ab = a^{-1}$ with the element t and obtain $(b^t)^{-1}a^t b^t = (a^t)^{-1}$ which gives (as in the first part of the proof) the following connection between s and s_0 :

$$(3) \quad s_0^a s^b = s_0 s z.$$

If $s_0 = ez^\alpha$ ($\alpha = 0, 1$), then (3) gives $s^b = s$ and $s = ez^\beta$ ($\beta = 0, 1$). If $s_0 = z^\alpha$ ($\alpha = 0, 1$), then (3) gives $s^b = sz$ and so $s = eu z^\beta$ ($\beta = 0, 1$). Replacing t with te , we get $a^{te} = (sva^{-1})^e = (sz)va^{-1}$, $b^{te} = (s_0vb^{-1})^e = s_0vb^{-1}$. Replacing t with tu , we get $a^{tu} = (sva^{-1})^u = sva^{-1}$, $b^{tu} = (s_0vb^{-1})^u = (s_0z)vb^{-1}$. This shows that in our expressions for s and s_0 we may choose $\alpha = \beta = 0$ and so we have either $s = e$ and $s_0 = e$ or $s = eu$ and $s_0 = 1$.

We have obtained again exactly two new groups G_1 and G_2 (of order 2^7) which differ only in the last two relations:

(a') G_1 with relations $a^t = eva^{-1}$, $b^t = evb^{-1}$;

(b') G_2 with relations $a^t = euva^{-1}$, $b^t = vb^{-1}$.

It is possible to show that the new groups G_1 and G_2 are isomorphic. In G_1 we replace the elements e, b, t with $e' = eu$, $b' = ab$, $t' = tu$, respectively, and see that the common relations for G_1 and G_2 remain valid. But from the relations (a') we get $(a)^{t'} = e'uv(a)^{-1}$, $(b')^{t'} = v(b')^{-1}$, which are the last two relations (b') for the group G_2 . Hence the groups G_1 and G_2 are isomorphic and we have to study further only the new group $G = G_1$.

We consider the maximal subgroup $H^* = \langle A, b, ta \rangle$ and see that $\Phi(H^*) = \langle uv, ev, v \rangle = A$. We have $\Omega_2(H^*) = A$, $H^*/E \cong Q_8$, and $E \leq \Phi(H^*)$. But this is exactly the starting point for the first part of the proof with the subgroup H^* instead of H . It follows that our new group $G = G_1$ must be isomorphic to the unique group of order 2^7 stated in our theorem. \square

Remark. Let us show that every subgroup $T \leq G$ of order $\geq 2^4$ contains z (here G is the group of Theorem 53.9). Since $Z(G) = \langle z \rangle$, it suffices to show that $T_G = \{1\}$. Assume that this is false. Then $|G : T| = 8$ and G is isomorphic to a Sylow 2-subgroup of the symmetric group S_8 . As the proof of Theorem 53.9 shows, G and a Sylow 2-subgroup of S_8 have distinct numbers of involutions, and this is a contradiction. Thus, $z \in T$.

In our next result the remaining 2-groups G with $c_2(G) = 4$ will be determined.

Theorem 53.10. *Let G be a 2-group of order $> 2^4$ with $c_2(G) = 4$ and $|\Omega_2(G)| > 2^4$. Suppose that G has no subgroups isomorphic to Q_8 and $|G : \Omega_2(G)| = 2$. Then we have the following two possibilities:*

(a) $G = \langle b, e, t \rangle$ with

$$\begin{aligned} b^8 &= e^2 = t^2 = 1, \quad (tb)^2 = a, \quad a^{2^n} = 1, \quad n \geq 3, \\ a^{2^{n-2}} &= v, \quad a^{2^{n-1}} = z, \quad b^2 = uv, u^2 = 1 \\ [b, e] &= [a, e] = [a, u] = [u, e] = [t, e] = [t, u] = 1, \\ u^b &= uz, \quad a^b = a^{-1}, \quad a^t = a^{-1}. \end{aligned}$$

Here $|G| = 2^{n+4}$, $n \geq 3$, $G = \langle e \rangle \times \langle a, b, t \rangle$, and $E = \langle z, u, e \rangle$ is a normal elementary abelian subgroup of order 8 in G . Four cyclic subgroups of order 4 generate the abelian subgroup $A = \langle E, v \rangle$ of type $(4, 2, 2)$ and each cyclic subgroup of order 4 is normal in G . We have $B = C_G(A) = \langle E, a \rangle$ is abelian of type $(2^n, 2, 2)$, $\Omega_2(G) = B\langle t \rangle$ is of order 2^{n+3} , where the involution t inverts B , and $C_G(t) = E \times \langle t \rangle \cong E_{16}$ is self-centralizing in G . We have $\Phi(G) = \langle u \rangle \times \langle a \rangle \cong C_2 \times C_{2^n}$, $G' \not\leq E$, $Z(G) = \langle e, z \rangle \cong E_4$. Finally, $(E\langle a, b \rangle)/E \cong Q_{2^n}$ and $(E\langle tb \rangle)/E \cong C_{2^n}$.

(b) $G = \langle a, t, e \rangle$ with

$$\begin{aligned} a^8 &= e^2 = t^2 = 1, & a^2 &= v, & a^4 &= z, & (ta)^2 &= uv, \\ u^2 &= [a, e] = [u, e] = [t, e] = [t, u] = 1, & u^a &= uz. \end{aligned}$$

Here $|G| = 2^6$ and $E = \langle z, u, e \rangle$ is a normal elementary abelian subgroup of order 8 in G . Four cyclic subgroups of order 4 generate the abelian subgroup $A = \langle E, v \rangle$ of type $(4, 2, 2)$ and each cyclic subgroup of order 4 is normal in G . We have $A = C_G(A)$, $\Omega_2(G) = A\langle t \rangle$ is a maximal subgroup of G , where the involution t inverts A . We have $\Phi(G) = \langle u, v \rangle \cong C_4 \times C_2$, $G' = \langle z, u \rangle \leq E$, $Z(G) = \langle e, z \rangle \cong E_4$. This exceptional group exists as a subgroup of A_{16} . The subgroup $\langle e \rangle$ is a direct factor of G . The minimal degree of a faithful permutation representation of G equals 10 (obviously, this representation is intransitive: every permutation representation of a 2-group G such that its degree does not equal to a power of 2, is intransitive).

Proof. Here H is isomorphic to a group (a) with $\mu = 0$ of Proposition 53.3 or to a group (b) of Proposition 53.4 since these are the only remaining possibilities with $|H/B| = 2$, where $B = C_G(A)$ and $G/\Omega_2(G) \cong H/B$.

Suppose that H is isomorphic to a group (a) with $\mu = 0$ of Proposition 53.3. Here $C_G(A) = B = \langle E, a \rangle$ is abelian of type $(2^n, 2, 2)$, $n \geq 3$, and $H/E \cong Q_{2^n}$. We have $a^{tb} = (a^{-1})^b = a$ and so looking at $K = B\langle tb \rangle$ with $\Omega_2(K) = A$, we get that K/E must be cyclic. Thus $\langle tb \rangle$ covers K/E and so $(tb)^2 = a^i s$, where $s \in E$ and i is an odd integer. Replacing a with a^i we may assume from the start $(tb)^2 = as$ which gives $b^t = asb^{-1}$. Since tb centralizes $(tb)^2$ we obtain $as = (as)^{tb} = (a^{-1}s)^b = as^b$, which gives $s^b = s$ and so $s \in \langle e, z \rangle$. We compute $b^{tu} = (asb^{-1})^u = asb^{-1}z = a(sz)b^{-1}$, and so replacing t with the involution tu (if necessary), we may assume that $s = 1$ or $s = e$. Suppose that $s = e$ and so $(tb)^2 = ae$. But then replacing a with $a' = ae$, all other relations remain unchanged and the last relation is transformed into $(tb)^2 = a'$. Hence we may assume from the start that $(tb)^2 = a$ and our group G is uniquely determined as stated in part (a) of our theorem.

Suppose, finally, that H is isomorphic to a group (b) of Proposition 53.4. Here $C_G(A) = B = \langle E, a^2 \rangle$ is abelian of type $(2^{n-1}, 2, 2)$, $n \geq 3$, and $H/E \cong C_{2^{n-1}}$. We set $K = B\langle ta \rangle$ and see that $(a^2)^{ta} = (a^2)^{-1}$ and therefore ta inverts B/E . If $|B/E| \geq 4$, then $\Omega_2(K) = A$ implies that K/E is generalized quaternion. But then replacing H with K , we know that such groups have been determined before.

It follows that we may assume that $|B/E| = 2$ and so $B = A$, $K/E \cong C_4$, and $|G| = 2^6$. Hence $o(ta) = 8$ and $(ta)^2 = sv$, where $s \in E$ and $a^t = sva^{-1}$. Since ta centralizes $(ta)^2$, we get $sv = (sv)^{ta} = (sv^{-1})^a = s^a v^{-1} = s^a vz$, which gives $s^a = sz$ and so $s = ue'$ with $e' \in \langle e, z \rangle$. We note that $a^{tu} = (sva^{-1})^u = (sz)va^{-1}$ and so replacing t with tu (if necessary), we may set $s = u$ or $s = ue$. However, if $s = ue$, then $(ta)^2 = uev$. In this case we replace u with $u' = eu$ and see that all other relations remain valid (with u' instead of u) and only the last relation is transformed in $(ta)^2 = u'$. Hence we may assume from the start that $(ta)^2 = u$. Our group G is uniquely determined as stated in part (b) of our theorem.

We get a faithful representation of degree 16 of G in the following way. We set

$$\begin{aligned} a &= (1, 2, 3, 4, 5, 6, 7, 8)(9, 10, 11, 12, 13, 14, 15, 16), \\ e &= (1, 9)(2, 10)(3, 11)(4, 12)(5, 13)(6, 14)(7, 15)(8, 16), \\ t &= (2, 6)(3, 7)(10, 14)(11, 15). \end{aligned}$$

We see that the permutations a, e, t are even and they satisfy the defining relations for G . The obtained representation is faithful since the central permutations $z = a^4, e$, and ez are nontrivial.

Since $e \notin \Phi(G)$, we get $G = \langle e \rangle \times M$ for some maximal subgroup M of G . The subgroup $Z(M) = \langle z \rangle$ is cyclic so a faithful permutation representation of minimal degree $\delta(M)$ is transitive, i.e., $\delta(M)$ is a power of 2. We claim that $\delta(M) = 8$. Clearly, $\delta(M) \geq 8$. Set $U = \langle a \rangle$ and $V = \langle u, e, t \rangle$. Since $U \cap V = \{1\}$, we have $\delta(M) \leq |M : U| + |M : V| = 4 + 4 = 8$. It follows that $\delta(M) = 8$. We get $\delta(G) = \delta(M \times \langle e \rangle) \leq \delta(M) + \delta(\langle a \rangle) = 8 + 2 = 10$. Since, by [Ber26, page 740],

$$\delta(G) \geq \delta(\langle a \rangle \times \langle e \rangle) = \delta(\langle a \rangle) + \delta(\langle e \rangle) = o(a) + o(e) = 8 + 2 = 10,$$

we get $\delta(G) = 10$. The proof is complete. \square

Problem. Classify the 2-groups G such that $c_2(G) \not\equiv 0 \pmod{4}$. In particular, classify the 2-groups G with $c_2(G) = 6$.

§54

2-groups G with $c_n(G) = 4, n > 2$

In this section we study a 2-group G with $c_n(G) = 4, n > 2$ [Jan8]. If $\{U_1, U_2, U_3, U_4\}$ is the set of four cyclic subgroups of order 2^n , then we describe first the structure of the subgroup $X = \langle U_1, U_2, U_3, U_4 \rangle$ (Theorems 54.1 and 54.2). It is interesting to note that always $|X| = 2^{n+2}$. If G has a normal elementary abelian subgroup of order 8, the structure of G is described in Theorem 54.6. If G has no normal elementary abelian subgroups of order 8, the structure of G is described in Theorem 54.7. The proofs of these theorems are quite involved and therefore we prepare the stage with Propositions 54.3, 54.4, and Theorem 54.5 which are also of independent interest.

If $c_n(G) = 2$, then the 2-groups are known (Corollary 43.6). The next interesting and important case is $c_n(G) = 4$ (see Research Problems #188 and #425). However, this problem is essentially more difficult.

Throughout this section we assume that G is a 2-group with $c_n(G) = 4, n > 2$. We consider first the case that G has a normal subgroup isomorphic to E_8 .

Theorem 54.1. *Let G be a 2-group with $c_n(G) = 4, n > 2$, and suppose that G has a normal subgroup $E \cong E_8$. Let $\{U_1, U_2, U_3, U_4\}$ be the set of four cyclic subgroups of order 2^n in G . Then $X = \langle U_1, U_2, U_3, U_4 \rangle = EU_1$, where $E \cap U_1 > \{1\}$ and so $|X| = 2^{n+2}$. Moreover, $\Omega_2(X) \cong C_4 \times C_2 \times C_2$ or $\Omega_2(X) \cong D_8 \times C_2$ in which case $n = 3$.*

Proof. Assume that for each cyclic subgroup U of order 2^n , $U \cap E = 1$. Let $U = \langle a \rangle$ be one of them. Then $(EU)/E \cong C_{2^n}$ and all 2^{n+2} elements in $(EU) - (E\langle a^2 \rangle)$ are of order 2^n . Indeed, if $x \in (EU) - (E\langle a^2 \rangle)$ and $o(x) = 2^{n+1}$, then $o(x^2) = 2^n$ and $\langle x^2 \rangle \cap E \neq \{1\}$, a contradiction. But then $c_n(G) \geq \frac{2^{n+2}}{\varphi(2^n)} = 8$ which contradicts our assumption (here $\varphi(*)$ is Euler's totient function; $\varphi(2^n)$ is the number of generators of a cyclic group of order 2^n).

We have proved that there is a cyclic subgroup $\langle b \rangle$ of order 2^n with $|\langle b \rangle \cap E| = 2$ so that $(E\langle b \rangle)/E \cong C_{2^{n-1}}$. Let $H = E\langle b \rangle$, $z = b^{2^{n-1}}$, and $v = b^{2^{n-2}}$; then $\langle b \rangle \cap E = \langle z \rangle$.

Assume that $C_H(E) = E$. Then $n = 3$, $H/E \cong C_4$ acts faithfully on E , and we may set $E = \langle e, u, z \rangle$, $e^b = eu$, $u^b = uz$. The structure of H is uniquely determined, $H = \langle b, e \rangle$. We have $u^v = (u^b)^b = (uz)^b = uzz = u$, $e^v = (eu)^b = eu \cdot uz = ez$, $v^e = eve = ve^v e = veze = vz = vv^2 = v^{-1}$. It follows that $E\langle v \rangle = \langle e, v \rangle \times \langle u \rangle \cong D_8 \times C_2$. Let us check that $\Omega_2(H) = E\langle v \rangle$, $\Phi(H) =$

$\langle u \rangle \times \langle v \rangle \cong C_4 \times C_2$. We have $(be)^2 = b^2e^b e = veue = vu \in \Phi(G)$. Since $v = b^2 \in \Phi(G)$ we get $u = v^{-1} \cdot vu \in \Phi(G)$. It follows from $d(H) = 2$ that $\Phi(G)$ has order 2^3 so is abelian, and the second isomorphism in the displayed formula is proved. It remains to prove the first equality in the displayed formula. Assume that it is false. Then there exists an element y of order 4 in $H - (E\langle v \rangle)$. We may assume that $y \in \{be, bu, beu, bez, buz, beuz\}$. However, it is easy to check that all these six elements have order 8. Thus, $\Omega_2(H) = E\langle v \rangle \cong D_8 \times C_2$, and we see that all 16 elements in $H - (E\langle v \rangle)$ are of order 8. Thus $c_3(H) = c_3(G) = 4$ and therefore, by the product formula, $X = EU_1$, where $U_1 = \langle b \rangle$.

Suppose now that $C_H(E) > E$. Then $A = E\langle v \rangle$ is abelian of type $(4, 2, 2)$, all elements in $A - E$ are of order 4, and $\Omega_1(A) = \langle z \rangle$. For each element $y \in H - (E\langle b^2 \rangle)$, we have $y^{2^{n-2}} \in A - E$ and so $o(y) = 2^n$. Hence all 2^{n+1} elements in $H - (E\langle b^2 \rangle)$ are of order 2^n which gives $c_n(H) = \frac{2^{n+1}}{\varphi(2^n)} = 4 = c_n(G)$. We get again $X = EU_1$ and $\Omega_2(X) = E\langle v \rangle \cong C_4 \times C_2 \times C_2$. \square

We assume now that G is a nonabelian 2-group which has no normal subgroups isomorphic to E_8 . Since G is not of maximal class, we may apply the main theorem in §50 to conclude that G has a normal subgroup W which is either abelian of type $(4, 4)$ with $C_G(W)$ being metacyclic or W is abelian of type $(4, 2)$ with $C_G(W)$ being abelian of type $(2^j, 2)$, $j \geq 2$.

Theorem 54.2. *Let G be a nonabelian 2-group with $c_n(G) = 4$, $n > 2$, and suppose that G has no normal elementary abelian subgroups of order 8. Let $\{U_1, U_2, U_3, U_4\}$ be the set of four cyclic subgroups of order 2^n . Then the subgroup $X = \langle U_1, U_2, U_3, U_4 \rangle$ is of order 2^{n+2} and for the structure of X we have the following possibilities:*

- (a) $n > 2$, $X = WU_1$ with $W \cap U_1 \cong C_4$, where W is an abelian normal subgroup of type $(4, 4)$. We have $\Omega_2(X) = W$ and X is metacyclic.
- (b) $n > 2$, $X = QU_1$, where $Q \cong Q_8$ is a normal quaternion subgroup of X , $Q \cap U_1 = Z(Q)$, $U_1 = \langle b \rangle \cong C_{2^n}$, and b either centralizes Q or b induces on Q an involutory outer automorphism in which case $n > 3$.
- (c) $n = 3$, $|X| = 2^5$, and X has a self-centralizing (in X) abelian normal subgroup A of type $(4, 2)$. Furthermore, $\Omega_2(X) \cong Q_8 \times C_2$ or $\Omega_2(X) \cong D_8 \times C_2$ and so (according to §52) the group X is uniquely determined in each of the two possibilities for $\Omega_2(X)$.

Proof. By Proposition 50.6, G has a normal abelian subgroup W of exponent 4 such that either W is of type $(4, 4)$ or of type $(4, 2)$ and such that $\Omega_2(C_G(W)) = W$; in the first case $C_G(W)$ is metacyclic and in the second case $C_G(W)$ is abelian and has a cyclic subgroup of index 2.

(i) We examine first the possibility that G has a normal subgroup $W \cong C_4 \times C_4$, where $C_G(W)$ is metacyclic. Set $W_0 = \Omega_1(W)$, $H = WU_1$, where $U_1 = \langle a \rangle$ is a cyclic subgroup of order 2^n , $n > 2$. The structure of $\text{Aut}(W)$ is described in

Proposition 50.5. In particular, $\exp(\text{Aut}(W)_2) = 4$, where $\text{Aut}(W)_2 \in \text{Syl}_2(\text{Aut}(W))$ (moreover, $\text{Aut}(W)_2$ is special) and if $\alpha \neq \beta$ are two involutions in $\text{Aut}(W)_2$ which do not stabilize the chain $W > W_0 > 1$, then $\langle \alpha, \beta \rangle$ is a four-group.

We want to show that $W \cap U_1 \cong C_4$. So suppose that $|W \cap U_1| \leq 2$. If $|W \cap U_1| = 1$, then $C_H(W)$ contains the involution $z = a^{2^{n-1}}$ since $|U_1| > 4 = \exp(\text{Aut}(W))_2$ and $W_0 \times \langle z \rangle \cong E_8$, contrary to the fact that $C_H(W)$ is metacyclic. Hence we have $W \cap U_1 = \langle z \rangle$ is of order 2. Set $v = a^{2^{n-2}}$ so that $v^2 = z$. Since $\Omega_2(C_G(W)) = W$, v does not centralize W . Hence in this case $U_1/\langle z \rangle$ acts faithfully on W , where $U_1 = \langle v \rangle$. This gives $o(a) = 8, n = 3, a^2 = v, H/W \cong C_4$ and $|H| = 2^6$. We shall determine the structure of $H = WU_1$, where $U_1 = \langle a \rangle$. Since a induces an automorphism of order 4 on W , a cannot stabilize the chain $W > W_0 > \{1\}$ (Remark 50.2). Set $W = \langle x \rangle \times \langle y \rangle, x^2 = z, y^2 = u$; then $W_0 = \langle z \rangle \times \langle u \rangle$. Assume that a stabilizes the chain $W_0 > \{1\}$. Then x^a is an element containing z so $x^a \in xW_0$. Similarly, $y^a \in yW_0$. We conclude that a stabilizes the chain $W > W_0 > \{1\}$, which is not the case. Thus, we have $u^a = uz$. If $w \in W$ is such that $w^2 = u$, then setting $w^a = y$, we get $y^2 = (w^a)^2 = (w^2)^a = (u^a) = uz$ and $W = \langle w \rangle \times \langle y \rangle$ with $(wy)^2 = z$. Since $W_0\langle a \rangle \cong M_{24}$, we get $c_3(W_0\langle a \rangle) = 2$. It remains to determine the element $y^a = ws$, where $s \in W_0$. We compute

$$w^v = w^{a^2} = y^a = ws, \quad y^v = y^{a^2} = (ws)^a = w^a s^a = ys^a,$$

and so $s \neq 1$ since $a^2 = v$ induces an involutory automorphism on W . Computing again $(a(wy))^2 = awyawy = a^2(wy)^a wy = vywswy = vzs$, we see that $o(awy) = 8$ since $o(vzs) = 4$ noting that $W_0\langle v \rangle$ is abelian of type $(4, 2)$. Since $(wy)^a = (wy)s$, we conclude that $W_0\langle wy \rangle \langle a \rangle$ contains exactly four cyclic subgroups of order 8. Therefore all other elements in aW must be of orders 2 or 4. We compute

$$(aw)^2 = awaw = a^2 w^a w = vyw,$$

$$(vyw)^2 = v^2(yw)^v(yw) = zys^a ws(yw) = s^a s.$$

It follows that $s^a s = 1$, and so $s^a = s$ (otherwise aw would be of order 8). Since $s \in Z(\langle a, W_0 \rangle)^\# = \{z\}$ (recall, that $\langle a, W_0 \rangle \cong M_{24}$), we get $s = z$, and so $y^a = wz$ and $(wy)^a = wyz = (wy)^{-1}$ since $z = (wy)^2$. The structure of H is uniquely determined and $X = \langle U_1, U_2, U_3, U_4 \rangle = W_0\langle wy \rangle \langle a \rangle$ is a normal subgroup of G . The group X is an extension of the normal abelian subgroup $W_0\langle wy \rangle$ of type $(4, 2)$ by C_4 and $(W_0\langle wy \rangle) \cap \langle a \rangle = \langle z \rangle$. We have $u^a = uz$ and $(wy)^a = (wy)^{-1}$ and so $v = a^2$ centralizes $W_0\langle wy \rangle$. Therefore $A = \langle u, wy, v \rangle$ is abelian of type $(4, 2, 2)$ and $\Omega_1(X) = \Omega_1(A) = \langle u, z, wyv \rangle \cong E_8$ is normal in G . This is a contradiction.

We have proved that for each cyclic subgroup U of order 2^n we have $W \cap U \cong C_4$. Set again $H = WU_1$ so that we have $H/W \cong C_{2^{n-2}}$. Set $U_1 = \langle a \rangle, y = a^{2^{n-3}}, y^2 = v$, and $y^4 = z$.

Assume that $C_H(W) > W$. Then $W\langle y \rangle$ is abelian of type $(8, 4)$ and so all elements in $(W\langle y \rangle) - W$ are of order 8; in particular, all elements in the coset Wy are of

order 8. For each $x \in H - (W\langle a^2 \rangle)$, we have $x^{2^{n-3}} \in Wy$ since all elements in $(H/W) - (W\langle a^2 \rangle/W)$ have order 2^{n-2} , and so $o(x^{2^{n-3}}) = 8$ and $o(x) = 2^n$. We get $c_n(H) \geq \frac{|H|-|W\langle a \rangle|}{\varphi(2^n)} = \frac{2^{n+1}}{2^{n-1}} = 4 = c_n(G)$ and so $X = H = WU_1$ as stated in part (a) of our theorem. We have in this case $\Omega_2(X) = W$.

Until the end of part (i), we may assume that $C_H(W) = W$. Since $\exp(\text{Aut}(W)_2) = 4$, where $\text{Aut}(W)_2$ is a Sylow 2-subgroup of $\text{Aut}(W)$, $|H/W| \leq 4$, and so $n = 3$ or 4. Set $W_0 = \Omega_1(W)$ and assume that the involutory automorphism of W induced by y stabilizes the chain $W > W_0 > \{1\}$. (This will certainly happen if $n = 4$ because in that case $y = a^2$.) Let $w \in W$ be such that $W = \langle w \rangle \times \langle v \rangle$. We have $w^y = ws$, where $s \in W_0$ and we compute

$$\begin{aligned} (y(w^i v^j))^2 &= yw^i v^j yw^i v^j = y^2(w^i v^j)^y w^i v^j = v(ws)^i v^j w^i v^j \\ &= vs^i w^{2i} v^{2j}, \end{aligned}$$

where i, j are any integers. Since $o(vs^i w^{2i} v^{2j}) = 4$, all elements in yW are of order 8. If $n = 4$, then for each $x \in H - (\langle y \rangle W)$, $x^2 \in yW$ and so $c_4(H) = 32 : 8 = 4$. If $n = 3$, then $H = \langle y \rangle W$ and so $c_3(H) = 4$. Hence we get again $X = H = WU_1$ and $\Omega_2(X) = W$, as stated in part (a).

It remains to consider the case $C_H(W) = W$, where the involutory automorphism of W induced by y does not stabilize the chain $W > W_0 > \{1\}$. By the above, $n = 3$, $H = \langle y \rangle W$, and if we set $W_0 = \langle u, z \rangle$, then $u^y = uz$ and $z \in Z(G)$. If $w \in W$ is such that $w^2 = u$, then setting $w' = w^y$, we get $(w')^2 = uz$ and $W = \langle w \rangle \times \langle w' \rangle$. Note that $C_W(y) = \langle v \rangle$ and so $(ww)^y = ww'$ implies $ww' = v^{\pm 1}$. But replacing w with w^{-1} (if necessary), we may assume from the start that $ww' = v$ and so $w' = w^{-1}v$.

Since $W_0\langle y \rangle \cong M_{24}$, we get $c_3(W_0\langle y \rangle) = 2$ and we claim that $c_3(H) = 2$. We compute (for any $s \in W_0$)

$$\begin{aligned} (yws)^2 &= y^2(ws)^y ws = vw's^y ws = v^2s^y s = zs^y s, \\ (yw's)^2 &= y^2(w's)^y w's = vws^y w's = v^2s^y s = zs^y s. \end{aligned}$$

Since $o(zs^y s) \leq 2$, the above claim is proved. Hence there exists an element y' of order 8 in $G - H$ such that $v' = (y')^2 \in W$ and y' induces on W an involutory automorphism which does not stabilize the chain $W > W_0 > \{1\}$. Otherwise, we get (as above) $c_3((y')W) = 4$, which is a contradiction (since $c_3(H) = 2$). Since $z \in Z(G)$, we get $u^{y'} = uz$ and therefore $(y')^4 = z$ and $v' = (y')^2 \in W_0\langle v \rangle$. Hence both y and y' normalize the abelian subgroup $A = W_0\langle v \rangle$ of type $(4, 2)$. Since $W_0\langle y' \rangle \cong M_{24}$, we get $c_3(W_0\langle y' \rangle) = 2$.

It is easy to see that $C_G(W) = W$. Indeed, if $W < S \leq C_G(W)$ and $|S : W| = 2$, then S is abelian metacyclic and so S is of type $(8, 4)$ and $c_3(S) = 4$, a contradiction. Hence y and y' induce on W two distinct involutory automorphisms which do not stabilize the chain $W > W_0 > \{1\}$. By our remark about $\text{Aut}(W)$ at the beginning of the proof, yy' induces an involutory automorphism on W which

obviously stabilizes the chain $W > W_0 > \{1\}$. Since the coset $W(yy')$ cannot contain elements of order 8, we get $(yy')^2 \in W_0 \leq A$. The subgroup $A\langle y, y' \rangle$ is of order 2^5 and since $c_3(A\langle y, y' \rangle) = 4$, we get $X = A\langle y, y' \rangle$.

Suppose that $B = A\langle yy' \rangle$ is abelian. Then $\exp(B) = 4$ and all 16 elements in $X - B$ are of order 8. Since $X = \langle U_1, U_2, U_3, U_4 \rangle$ is normal in G , B is normal in G , and so (by assumption) $\Omega_1(B) = \Omega_1(A) = W_0 \cong E_4$ and B is of type $(4, 4)$. (If $\Omega_1(B) \cong E_8$, then G would possess a normal elementary abelian subgroup of order 8.) But $u^y = uz$ and so y does not stabilize the chain $B > W_0 > \{1\}$. By the above, $c_2(B\langle y \rangle) = 2$ which is a contradiction since $B\langle y \rangle = X = \langle U_1, U_2, U_3, U_4 \rangle$. Hence $C_X(A) = A$ and we have obtained a group stated in part (c) with $X/A \cong E_4$.

(ii) It remains to examine the second possibility, where G has a normal abelian subgroup W_1 of type $(4, 2)$ such that $N = C_G(W_1)$ is abelian of type $(2^j, 2)$, $j \geq 2$, and G/N is isomorphic to a subgroup of D_8 . If $j > 2$, then G/N is elementary abelian of order ≤ 4 . Indeed, if $j > 2$, then N contains a characteristic subgroup $Z \cong C_4$. Since $Z < W_1$ and Z is normal in G , it is easy to see that the nontrivial elements in G/N induce on W_1 only involutory automorphisms. We set $W_0 = \Omega_1(W_1) \cong E_4$ and $\langle z \rangle = \Omega_1(W_1) \leq Z(G)$.

Suppose that G/N is not elementary abelian. Then $j = 2$, $W_1 = N = C_G(W_1)$, and $G/N \cong C_4$ or $G/N \cong D_8$. In that case $n \leq 4$. Suppose that $U \leq G$ and $U \cong C_{24}$. Then $U/(U \cap W_1) \cong C_4$ acts faithfully on W_1 . But U centralizes the cyclic subgroup $U \cap W_1 \cong C_4$, a contradiction. It follows $n = 3$. If $L > W_1$ is such that $L/W_1 \cong C_4$, then (by the structure of $\text{Aut}(C_4 \times C_2)$) $\Omega_1(L/W_1) = L_0/W_1$ inverts W_1 . In particular, L_0 does not contain a cyclic subgroup of order 8.

Suppose first that L contains a cyclic subgroup $U_1 = \langle a \rangle$ of order 8. Then U_1 covers L/W_1 and $U_1 \cap W_1 = \langle z \rangle$ is of order 2, where $z = a^4$ and $L_0 = W_1\langle v \rangle$ with $v = a^2$ inverting W_1 . For each $w \in W_1$ we compute $(vw)^2 = v^2w^v w = v^2w^{-1}w = v^2 = z$, and so all elements in $L_0 - W_1 = vW_1$ are of order 4. For each $x \in L - L_0$, $x^2 \in L_0 - W_1$ and so all 16 elements in $L - L_0$ are of order 8. Hence $c_3(L) = 4$ and so $X = L$ is a group of order 2^5 as stated in part (c) of our theorem with $X/W_1 \cong C_4$.

We may assume that $\exp(L) < 8$. In that case $G/W_1 \cong D_8$. Let $U_1 \leq G$ and $U_1 = \langle a_1 \rangle \cong C_8$. Then $U_1 \cap W_1 = \langle v \rangle \cong C_4$, where $v = a_1^2$. We may set $W_1 = \langle v, u \mid v^4 = u^2 = [v, u] = 1, v^2 = z \rangle$, and then $v^{a_1} = v, u^{a_1} = uz$ (since a_1 does not centralize W_1). Obviously, $M = W_1U_1 = \langle a_1, u \rangle \cong M_{24}$ and so $c_3(M) = 2$. Hence there is another cyclic subgroup $U_2 = \langle a_2 \rangle$ in G which is not contained in M and $U_2 \cap W_1 \cong C_4$. Then a_2 must induce on W_1 an involutory automorphism which is distinct from that one induced by a_1 . The only possibility is $(vu)^{a_2} = vu, u^{a_2} = uz$, and so $v^{a_2} = vz = v^{-1}$, with $U_2 \cap W_1 = \langle vu \rangle$. Again, $P = W_1U_2 = \langle a_2, u \rangle \cong M_{24}$ and so $c_3(P) = 2$. Since a_1a_2 inverts W_1 , $\langle a_1, a_2 \rangle$ induces a four-group of automorphisms on W_1 and therefore $(MPW_1)/W_1 \cong E_4$, where $MPW_1 = \langle a_1, a_2 \rangle W_1$. Note that $c_3(\langle a_1a_2 \rangle W_1) = 0$ (by a remark above). We get $X = MPW_1$ and so we have obtained a group of order 2^5 stated in part (c) of our theorem with $X/W_1 \cong E_4$.

It remains to consider the case where G/N is elementary abelian (of order ≤ 4) with N abelian of type $(2^j, 2)$, $j \geq 2$. Assume first $j = 2$. In that case we have again $N = C_G(W_1) = W_1 \cong C_4 \times C_2$. Let $U_1 \leq G$ with $U_1 \cong C_8$. Then $U_1 \cap W_1 \cong C_4$ and (as before) $W_1 U_1 \cong M_{24}$ which gives $c_2(W_1 U_1) = 2$. Hence there is $U_2 \leq G$ with $U_2 \cong C_8$ and $U_2 \not\leq W_1 U_1$. Then again $W_1 U_2 \cong M_{24}$ and $c_2(W_1 U_2) = 2$. We have $G/W_1 \cong E_4$ and we have obtained again a group $X = G$ of order 2^5 as stated in part (c).

We assume now $j \geq 3$ and set $N = \langle u, a \mid u^2 = a^{2^j} = [u, a] = 1 \rangle$. Then put $v = a^{2^{j-2}}$ and $z = v^2$. We see that $W_1 = \langle u, v \rangle$, $z \in Z(G)$, $\langle v \rangle$ is a characteristic subgroup of N , and so $\langle v \rangle$ is normal in G . Obviously, $n \leq j + 1$. Assume first that $n = j + 1$. Let $x \in G - N$ be such that $o(x) = 2^n = 2^{j+1}$. Then x centralizes $x^2 \in N$ and $o(x^2) = 2^j$. In particular, x centralizes $\langle v \rangle$ and so $u^x = uz$ (since x does not centralize W_1). We get $\langle x \rangle N = \langle x, u \rangle \cong M_{2n+1}$ and so $c_2(\langle x \rangle N) = 2$. It follows that $G/N \cong E_4$ and there is another element $y \in G - (\langle x \rangle N)$ with $o(y) = 2^n$. We get again that y centralizes $\langle v \rangle$ and $u^y = uz$. But then xy centralizes W_1 and $xy \in G - N$, a contradiction.

We have proved that $n \leq j$. Then $c_n(N) = 2$. Take $a_0 \in \langle a \rangle \leq N$ with $o(a_0) = 2^n$. Then $A = \langle u \rangle \times \langle a_0 \rangle$ is an abelian normal subgroup of type $(2^n, 2)$ and $c_n(A) = c_n(N) = 2$. There is $b_0 \in G - N$ with $o(b_0) = 2^n$. Since $o(b_0^2) = 2^{n-1}$, it follows that $b_0^2 \in A$, b_0 centralizes a cyclic subgroup of order 4 in W_1 and so $u^{b_0} = uz$. Also, $\langle u, b_0 \rangle \cong M_{2n+1}$ and so $c_n(\langle u, b_0 \rangle) = 2$. We get $X = A\langle b_0 \rangle$.

We see that $\langle b_0^2 \rangle$ (of order 2^{n-1}) is contained in $Z(X)$. Set $Z = Z(X)$ and assume first that $Z > \langle b_0^2 \rangle$. Then Z is a cyclic subgroup of order 2^n contained in A and $\langle b_0 \rangle Z$ is abelian of order 2^{n+1} . Since $\langle b_0 \rangle Z$ is not cyclic (because it contains two distinct cyclic subgroups $Z \leq A$ and $\langle b_0 \rangle \not\leq A$ of order 2^n), there is an involution $t' \in (\langle b_0 \rangle Z) - A$. Since t' acts faithfully on W_0 , it follows that $W_0\langle t' \rangle = D^* \cong D_8$ and $X = D^* * Z$. There is a subgroup $Q^* \cong Q_8$ contained in X (Appendix 16) so that $X = Q^* * Z$ with $Q^* \cap Z = Z(Q^*) = \langle z \rangle$ and $Z \cong C_{2n}$. We have obtained a group X of order 2^{n+2} as stated in part (b) of our theorem.

Assume now that $Z(X) = \langle b_0^2 \rangle$ is cyclic of order 2^{n-1} . Suppose at the moment that $\Omega_2(X) = W_1$. In that case we can apply the classification result of (Lemma 42.1) in which all 2-groups X with $|X| > 2^3$ and $|\Omega_2(X)| \leq 2^3$ are determined. Since $|X : Z(X)| = 2^3$, X is not isomorphic to M_{2n+2} . Hence X is isomorphic to the metacyclic group G^* from part (c) of the above lemma. Since $Z(G^*) \cong C_4$, it follows that $n = 3$ and $|X| = |G^*| = 2^5$. But in that case $c_3(G^*) = 6$, which is a contradiction. We have proved that $\Omega_2(X) > W_1$. Hence there is an element $x_0 \in X - A$ with $o(x_0) \leq 4$. Since $o(x_0^2) \leq 2$, it follows that $x_0^2 \in W_0$ and $D = \langle W_0, x_0 \rangle \cong D_8$ because $u^{x_0} = uz$. Thus $X_0 = D * \langle b_0^2 \rangle$ is the central product of $D \cong D_8$ and $Z(X) = \langle b_0^2 \rangle$, where $D \cap \langle b_0^2 \rangle = Z(D) = \langle z \rangle$. Since $|X_0| = 2^{n+1}$, X_0 is a maximal subgroup of X and obviously $\exp(X_0) = 2^{n-1}$. All 2^{n+1} elements in $X - X_0$ must be of order 2^n (since $c_n(X) = 4$). There exists (as above) a quaternion subgroup $Q \leq X_0$ so that $X_0 = Q * \langle b_0^2 \rangle$. Since Q is a characteristic subgroup in X_0

(because it is a unique quaternion subgroup of X_0), Q is normal in X and $X = Q\langle b_0 \rangle$. From $Z(X) = \langle b_0^2 \rangle$ follows that $C_X(Q) = \langle b_0^2 \rangle$ and so b_0 induces on $Q = \langle x, y \rangle$ an outer involutory automorphism with $x^{b_0} = y$ and $(xy)^{b_0} = (xy)^{-1}$. We compute $(b_0x)^2 = b_0^2x^{b_0}x = b_0^2(yx)$. If $n = 3$, then $b_0^2(yx)$ is an involution. In that case $o(b_0x) = 4$, which is a contradiction (since all elements in $X - X_0$ must be of order 2^3). Hence we must have $n > 3$. In that case $o(b_0x) = 2^n$, as required. We have obtained a group stated in part (b) of our theorem.

It remains to determine $\Omega_2(X)$, where X is a group (of order 2^5) given in part (c) of our theorem with A being a self-centralizing (in X) abelian normal subgroup of type $(4, 2)$. We know that $\text{Aut}(A) \cong D_8$ and $Z(\text{Aut}(A))$ inverts A . Since $|X/A| = 4$ and X/A acts faithfully on A , there is a subgroup $B (> A)$ of order 2^4 such that B/A inverts A . Then $B - A$ cannot contain elements of order 8 and so $\exp(B) = 4$. Since $c_3(X) = 4$, all 16 elements in $X - B$ must be of order 8 and so $B = \Omega_2(X)$. But B is nonabelian and so using the results in §52, we see that B is isomorphic to one of the following groups: $Q_8 \times C_2$, $D_8 \times C_2$, and $Q_8 * C_4$. It is easy to see that the last case cannot occur. Indeed, if $B \cong Q_8 * C_4$, then, by §52, $X \cong Q_8 * C_8$. But in that case A is not self-centralizing. Using again the results in §52, we see that in each of the first two cases the group X is uniquely determined. \square

Proposition 54.3 (see §18). *Let G be a 2-group possessing exactly one L_s -subgroup H of order 2^{s+m} with a fixed integer $m \geq 2$. Then G is either an L_s -group or a U_s -group with respect to the kernel $R = \Omega_1(H)$.*

Proof. Set $R = \Omega_1(H)$ so that $R \cong E_{2^s}$, $s \geq 2$, H/R is cyclic of order 2^m , $m \geq 2$, and R is normal in G . Set $S/R = \Omega_1(H/R)$. Then we have $S/R \leq \Phi(H/R) \leq \Phi(G/R)$ and $\Omega_1(S) = R$.

We use induction on $|G|$. If $H = G$, we are done. In the sequel let $H < G$. Let $H \leq M < G$, where M is maximal in G . By induction, M is either an L_s -group or a U_s -group with respect to the kernel $R = \Omega_1(H)$.

Note that the Frattini subgroup of an arbitrary p -group is not of maximal class. Since $\Phi(G/R) \leq M/R$, $\Phi(G/R)$ is cyclic (of order ≥ 2) or abelian of type $(2, 2)$, where the last case is possible only if $M/R \cong D_8$. However, if $\Phi(G/R)$ is abelian of type $(2, 2)$, then a result of Nekrasov (see Proposition 4.9) implies $\Phi(G/R) \leq Z(G/R)$, and then M/R is abelian, a contradiction. Thus $\Phi(G/R)$ is cyclic and so $S/R = \Omega_1(\Phi(G/R))$.

Let $F/R < G/R$ be cyclic of order 2^m . Now, $\Omega_1(F/R) \leq \Phi(F/R) \leq \Phi(G/R)$ and so $\Omega_1(F/R) = S/R$ which gives $\Omega_1(F) = \Omega_1(S) = R$. It follows that F is an L_s -group of order 2^{s+m} . By assumption, $F = H$ and so G/R has exactly one cyclic subgroup of order 2^m . By Exercise 1.104, G/R is either cyclic or of maximal class.

If G/R is cyclic, $\Omega_1(G) = \Omega_1(S) = R$ and G is an L_s -group. Suppose that G/R is of maximal class and let T/R be a cyclic subgroup of index 2 in G/R . Since $S/R \leq \Phi(G/R) < T/R$, it follows $S/R = \Omega_1(T/R)$ and $\Omega_1(T) = \Omega_1(S) = R$. This means that G is a U_s -group with the kernel R and we are done. \square

Proposition 54.4. *Let G be a 2-group with $c_n(G) = 2$, $n > 2$. Then G is an L_2 -group or a U_2 -group.*

Proof. Since G is neither cyclic nor of maximal class, it has a normal abelian subgroup R of type $(2, 2)$. Let U_1 be a cyclic subgroup of order 2^n . Set $H = U_1 R$ and assume that $R \cap U_1 = \{1\}$. Let K/R be the subgroup of index 2 in H/R and let Z/R be the subgroup of order 2 in K/R . Then $Z \cong E_8$ and for each $x \in H - K$, $x^{2^{n-1}} \in Z - R$ which gives $o(x) = 2^n$. But then $c_n(H) \geq 2^{n+1} : \varphi(2^n) = 2^{n+1} : 2^{n-1} = 4$, a contradiction.

Hence $|U_1 \cap R| = 2$ and so H is an L_2 -group of order 2^{n+1} , i.e., H is either abelian of type $(2^n, 2)$ or $H \cong M_{2^{n+1}}$. In any case H is generated by its two cyclic subgroups of order 2^n and so H is the unique L_2 -subgroup of G of order 2^{n+1} . By Proposition 54.3, G is either an L_2 -group or a U_2 -group with the kernel R . \square

Theorem 54.5. *Let X be a 2-group of order $> 2^4$ with $\Omega_2(X) \cong D_8 \times C_2$ or $\Omega_2(X) \cong Q_8 \times C_2$. Then $|X| = 2^5$ and for each of the two possibilities for $\Omega_2(X)$, X is uniquely determined and is given explicitly in Theorems 52.2(a) and 52.1(d). In both cases $\Phi(X)$ is abelian of type $(4, 2)$, $X' = \Omega_1(\Phi(X)) \cong E_4$, $Z(X) = \mathcal{V}_1(\Phi(X))$ is of order 2, and $c_3(X) = 4$. Also, each maximal subgroup of X is nonabelian and therefore $A = \Phi(X)$ is self-centralizing in X .*

Suppose that G is a 2-group with $G > X$ and $c_3(G) = 4$. Then we have the following possibilities:

- (a) $C_G(A) = A$, $G/A \cong D_8$, and G has a normal elementary abelian group of order 8.
- (b) $C_G(A) = C \cong C_4 \times C_4$, C is self-centralizing in G , and $G/C \cong E_4$ or D_8 .

Proof. The first part of this proposition is a direct consequence of the results in §52. Suppose that X has an abelian maximal subgroup. Then the formula $|X| = 2|Z(X)||X'|$ (see Lemma 1.1) gives a contradiction (since $|X| = 2^5$).

We have to determine the structure of G , where $G > X$ and $c_3(G) = 4 = c_3(X)$. This implies that X is normal in G . If $C_G(A) = A$, then $G > X$ and $\text{Aut}(A) \cong D_8$ imply $G/A \cong D_8$. We have $\Omega_2(X) > A$, $|\Omega_2(X) : A| = 2$, and $\Omega_2(X)/A = Z(G/A)$. Since $X/A \cong E_4$, there is an element $x \in G - X$ such that $x^2 \in \Omega_2(X) - A$. But $o(x^2) \leq 4$ and x is not of order 8. Hence $x^2 = t$ is an involution which gives $\Omega_2(X) \cong D_8 \times C_2$ and $Z(\Omega_2(X)) = \Omega_1(A) = X'$. Thus $E = \langle t \rangle \times \Omega_1(A)$ is an elementary abelian normal subgroup (of order 8) of X . Since x centralizes t and normalizes $\Omega_1(A) = X'$, it follows that $E \triangleleft G$, as required.

We have to study the case $C = C_G(A) > A$ so that we get $C \cap X = A$, C is normal in G , $(XC)/C \cong X/A \cong E_4$, and $G/C \cong E_4$ or D_8 . It remains to determine the structure of C . Since C has no elements of order 8, we get $\exp(C) = 4$. Let s be an element of order 8 in X . Then $s^2 \in A = \Phi(X)$, $D = A\langle s \rangle$ is of order 2^4 , and $\Omega_1(A) = \Omega_1(D)$ is a normal 4-subgroup of D . Since every maximal subgroup of X is nonabelian, it follows that $D \cong M_{2^4}$ and $c_3(D) = 2$. Set $K = C\langle s \rangle = CD$.

Because $K \cap X = D$, we have $c_3(K) = 2$ and D is the unique L_2 -subgroup of K of order 2^4 . By Proposition 54.3, K (of order $\geq 2^5$) is an L_2 -group or a U_2 -group with the kernel $R = \Omega_1(A) = \Omega_1(D)$. If K is an L_2 -group, then $K \cong M_{2^m}$, $m > 4$, a contradiction. Indeed, M_{2^m} is minimal nonabelian contrary to the fact that K contains the nonabelian proper subgroup D .

We have proved that K is a U_2 -group with the kernel $R = \Omega_1(A)$, where K/R is of maximal class. Let T/R be a cyclic subgroup of index 2 in K/R . Then $|T/R| \geq 4$ and $\Omega_1(T) = R$. Let T_1/R be the cyclic subgroup of order 4 in T/R . Then T_1 is an L_2 -subgroup of K of order 2^4 and so $T_1 = D$. If $T_1 \neq T$, then $C_T(R) \geq T_1$ and so $T_1 = D$ would be abelian, a contradiction. Hence $T_1 = T = D$ and so $|K| = 2^5$. Since $|K : C| = 2$, C is of order 2^4 . But $A \leq Z(C)$ and so C is abelian.

Assume that $E_0 = \Omega_1(C) > \Omega_1(A)$ so that E_0 is a normal elementary abelian subgroup of order 8 in G . Consider the subgroup $X_0 = E_0\langle s \rangle$, where $E_0 \cap \langle s \rangle = \langle s^4 \rangle$ is of order 2. We see (as in the proof of Theorem 54.1) that $c_3(X_0) = 4$. This implies $X_0 \leq X$, a contradiction. We have proved that C is of rank 2 and so $C \cong C_4 \times C_4$ (since $\exp(C) = 4$). Our proposition is proved. \square

Next we shall classify 2-groups G appearing in Theorems 54.1 and 54.2.

Theorem 54.6. *Let G be a 2-group with $c_n(G) = 4, n > 2$, and suppose that G has a normal elementary abelian subgroup E of order 8. Let $\{U_1, U_2, U_3, U_4\}$ be the set of four cyclic subgroups of order 2^n . Then $X = \langle U_1, U_2, U_3, U_4 \rangle = EU_1$, where $E \cap U_1 \neq 1$ and we have the following possibilities.*

- (a) $\Omega_2(X) \cong C_4 \times C_2 \times C_2$ and G/E is either cyclic (of order $\geq 2^{n-1}$) or G/E is of maximal class (and order $\geq 2^n$) and for $n = 3$ the last group must be dihedral.
- (b) $n = 3$, $\Omega_2(X) \cong D_8 \times C_2$, and one of the following holds:
 - (b1) $G = X$, which is a uniquely determined group of order 2^5 ;
 - (b2) G has a self-centralizing abelian normal subgroup A of type $(4, 2)$ such that $G/A \cong D_8$;
 - (b3) G has a self-centralizing abelian normal subgroup W of type $(4, 4)$ such that $G/W \cong E_4$ or D_8 .

Proof. Theorem 54.1 implies that $X = EU_1$ with $E \cap U_1 \neq 1$ and $\Omega_2(X) \cong C_4 \times C_2 \times C_2$ or $\Omega_2(X) \cong D_8 \times C_2$, where in the second case $n = 3$.

Suppose that $\Omega_2(X) \cong C_4 \times C_2 \times C_2$. Then $\Omega_1(X) = E \cong E_{2^3}$ and $X/E \cong C_{2^{n-1}}$ with $|X/E| \geq 4$. Hence X is an L_3 -group of order 2^{n+2} . Since X is generated by its cyclic subgroups of order 2^n , it follows that X is the unique L_3 -subgroup of order 2^{n+2} in G . By Proposition 54.3, G is either an L_3 -group or a U_3 -group with respect to the kernel $R = \Omega_1(X) = E$. In particular, G/E is either cyclic (of order $\geq 2^{n-1}$) or G/E is of maximal class (and order $\geq 2^n$). If in the second case $n = 3$, then G/E must be dihedral. Indeed, if $n = 3$ and G/E is of maximal class but not dihedral, then there

is an element $x \in G - X$ such that $x^2 \in \Omega_2(X) - E$, where $\Omega_2(X)/E = Z(G/E)$. But then $o(x) = 8$, a contradiction.

Assume now that $\Omega_2(X) \cong D_8 \times C_2$ in which case $n = 3$. Our result follows at once from Theorem 54.5. \square

Theorem 54.7. *Let G be a 2-group with $c_n(G) = 4$, $n > 2$, and suppose that G does not have a normal elementary abelian subgroup of order 8. Let $\{U_1, U_2, U_3, U_4\}$ be the set of four cyclic subgroups of order 2^n . Then the subgroup $X = \langle U_1, U_2, U_3, U_4 \rangle$ is of order 2^{n+2} and we have the following possibilities.*

- (a) $X = WU_1$ with $W \cap U_1 \cong C_4$, where W is an abelian normal subgroup of type $(4, 4)$, $\Omega_2(X) = W$, X is metacyclic, $C_G(W)$ is metacyclic and one of the following holds:
 - (a1) $n > 3$, and G/W is either cyclic (of order $\geq 2^{n-2}$) or G/W is of maximal class (and order $\geq 2^{n-1}$) and for $n = 4$ the last group must be dihedral;
 - (a2) $n = 3$, G has a normal metacyclic subgroup N such that $C_G(W) \leq N$, $X \leq N$, and G/N is isomorphic to a subgroup of D_8 . Moreover, $C_G(W)/W$ is cyclic, N/W is either cyclic or generalized quaternion, and in the second case G/N is elementary abelian of order ≤ 4 .
- (b) $n > 2$, $X = QU_1$, where $Q \cong Q_8$ is a normal quaternion subgroup of G , $G = QP$ with $Q \cap P = Z(Q)$, $U_1 \leq P$, $C_G(Q) \leq P$, $|P : C_G(Q)| \leq 2$, and P is either cyclic or of maximal class.
- (c) $n = 3$, $|X| = 2^5$, $\Omega_2(X) \cong Q_8 \times C_2$ or $\Omega_2(X) \cong D_8 \times C_2$ and if $G > X$, then G has a self-centralizing normal abelian subgroup W of type $(4, 4)$ with $G/W \cong E_4$ or D_8 .

Proof. We may assume that G is nonabelian.

(i) We consider first the groups G from Theorem 54.2(a). In this case $X = WU_1$ with $U_1 \cong C_{2^n}$, $W \cap U_1 \cong C_4$, where W is an abelian normal subgroup of type $(4, 4)$ and $\Omega_2(X) = W$. Also, X and $C_G(W)$ are metacyclic.

Assume that $n > 3$. Then X/W is cyclic of order $2^{n-2} \geq 4$. Set $S/W = \Omega_1(X/W)$ so that $S/W \leq \Phi(X/W) \leq \Phi(G/W)$. Since S/W stabilizes the chain $W > \Omega_1(W) > \{1\}$, it follows (as in the proof of Theorem 54.2) that all elements in $S - W$ are of order 8. Indeed, set $U_1 \cap S = \langle d \rangle$, where d is an element of order 8. For each $w \in W$, $w^d = wl$ with $l \in \Omega_1(W)$. Then $(dw)^2 = dwdw = d^2w^d w = d^2wlw = d^2w^2l$, where $w^2l \in \Omega_1(W)$ and so $o(dw) = 8$. Also, X is generated by its elements of order 2^n .

We want to show that G/W is either cyclic or of maximal class and we use an induction on $|G|$. If $X = G$, we are done. In the sequel let $X < G$. Let $X \leq M < G$, where M is maximal in G . By induction, M/W is either cyclic or of maximal class. We have $\Phi(G/W) \leq M/W$ and since $\Phi(G/W)$ cannot be of maximal class

(Burnside), $\Phi(G/W)$ is either cyclic (of order ≥ 2) or abelian of type $(2, 2)$ (the last case being possible only if $M/W \cong D_8$). However, if $\Phi(G/W) \cong E_4$, then $\Phi(G/W) \leq Z(G/W)$ (see Proposition 4.9). But then M/W is abelian, a contradiction. Thus $\Phi(G/W)$ is cyclic and so $S/W = \Omega_1(\Phi(G/W))$.

Let F/W be a cyclic subgroup of order 2^{n-2} in G/W . Now, $\Omega_1(F/W) \leq \Phi(F/W) \leq \Phi(G/W)$ and so $\Omega_1(F/W) = S/W$. But all elements in $S - W$ are of order 8 and so $c_n(F) = 4$ and F is generated by its elements of order 2^n . Indeed, let $F_0/W = \Phi(F/W)$ and $x \in F - F_0$. Then $x^{2^{n-3}} \in S - W$ and so $o(x) = 2^n$. This gives $F = X$ and so X/W is the unique cyclic subgroup of order 2^{n-2} in G/W . As in the proof of Proposition 54.3, G/W is either cyclic (of order $\geq 2^{n-2}$) or G/W is of maximal class (and order $\geq 2^{n-1}$) and for $n = 4$ the last group (obviously) must be dihedral.

It remains to consider the case $n = 3$. In this case $|X| = 2^5$ and all 16 elements in $X - W$ are of order 8. Suppose first that X is nonabelian. Then $C_G(W) \cap X = W$ and $C_G(W)$ is metacyclic. If $C_G(W) > W$, then $C_G(W)$ (being metacyclic) has elements of order 8 (which are not contained in X), a contradiction. We have proved that $C_G(W) = W$. By Theorem 50.1, the group G has a normal metacyclic subgroup N such that $W \leq N$, $\Omega_2(N) = W$, and G/N is isomorphic to a subgroup of D_8 and we assume that N is maximal subject to these conditions. In that case $N > W$. Indeed, if $N = W$, then G/W is isomorphic to a subgroup of D_8 . But X is a normal metacyclic subgroup of G , $W \leq X$, $\Omega_2(X) = W$, and G/X (being a factor-group of D_8) is also isomorphic to a subgroup of D_8 . This contradicts the maximality of N and so $N > W$. In that case there are elements of order 8 in N and so $X \leq N$. Suppose that Y/W is a subgroup of order 2 in N/W . Since $\Omega_2(Y) = W$, all elements in $Y - W$ are of order 8. Hence $Y = X$ and so N/W has exactly one subgroup of order 2. By the structure of $\text{Aut}(W)$ (Proposition 50.5), we see that $\text{Aut}(W)$ has no quaternion subgroups. Thus N/W is cyclic (of order ≤ 4). We have obtained all properties stated in part (a2) of our theorem.

We consider now the remaining case, where $X = WU_1$ is abelian of order 2^5 (and of type $(8, 4)$). According to Theorem 50.1, G has a normal metacyclic subgroup N such that $\Omega_2(N) = W$, $C = C_G(W) \leq N$, and G/N is isomorphic to a subgroup of D_8 . Obviously, $X \leq C$. Suppose that Y/W is a subgroup of order 2 in N/W . Since $\Omega_2(Y) = W$, all elements in $Y - W$ are of order 8. Hence $Y = X$ and so N/W has exactly one subgroup of order 2. It follows that N/W is either cyclic or generalized quaternion.

We claim that C/W is cyclic. Suppose false. Then C/W is generalized quaternion. Let $C_0/W \cong Q_8$ be a quaternion subgroup in C/W , where $X < C_0$ (because X/W is the unique subgroup of order 2 in N/W). Let Z_1/W and Z_2/W be two distinct cyclic subgroups of order 4 in C_0/W . Then Z_1 and Z_2 are both abelian, $\langle Z_1, Z_2 \rangle = C_0$, and $Z_1 \cap Z_2 = X$. This implies that $X \leq Z(C_0)$ and so $X = Z(C_0)$. Since C_0 is metacyclic, C'_0 is cyclic and C'_0 covers X/W . All elements in $X - W$ are of order 8, so $|C'_0| = 8$. But then the formula (see Lemma 1.1) $|C_0| = 2^7 = 2|Z(C_0)||C'_0|$ gives

a contradiction. We have proved that $C_G(W)/W$ is cyclic. Thus $C_G(W) = C_G(X)$ is abelian.

We have to consider the case, where N/W is generalized quaternion. We set $K/W = (N/W)' = \Phi(N/W)$ so that K/W is cyclic and $Z(N/W) = X/W$. We have $N/K \cong E_4$ and since N is metacyclic (and therefore $d(N) = 2$), we get $K = \Phi(N)$ and N' is cyclic. On the other hand, N' covers K/W and all elements in $X - W$ are of order 8. Hence $N' \cap X \cong C_8$, $N' \cap W \cong C_4$, and $|K : N'| = 4$. Again, since N is metacyclic, there is a cyclic normal subgroup S of N such that $N' < S$ and $|S : N'| = 2$. If $S \leq K$, then $|S \cap W| = 8$. But a maximal subgroup $S \cap W$ of W is not cyclic since $S \cap W \geq \Phi(W) = \Omega_1(W) \cong E_4$. This contradiction shows that $S \cap K = N'$. Set $T = WS = KS$ so that T/W is a cyclic subgroup of index 2 in N/W . For each $x \in N - T$, we have $x^2 \in X - W$ and so all elements in $N - T$ are of order 16. Also, $T/S \cong W/(S \cap W) \cong C_4$. Now, $\Phi(T) \leq K$ and $\Phi(T) \geq \langle N', \Omega_1(W) \rangle$ since $N' = \Omega_1(S)$ and $\Omega_1(W) = \Phi(W)$. Since $|K : (N'\Omega_1(W))| = 2$ and T is not cyclic, we get $\Phi(T) = N'\Omega_1(W)$, $F = \Phi(T) \cap X$ is abelian of type $(8, 2)$, and $F_1 = \Phi(T) \cap W$ is abelian of type $(4, 2)$.

Set $S = \langle a \rangle$, where $o(a) = 2^m$, $m \geq 4$. Also set $s = a^{2^{m-3}}$, $v = a^{2^{m-2}}$, and $z = a^{2^{m-1}}$, so that $z \in Z(G)$, $\langle s \rangle = S \cap X$, $\langle v \rangle = S \cap W$, and $\langle z \rangle = S \cap \Omega_1(W)$. Obviously, $\langle s \rangle$ and $\langle v \rangle$ are normal subgroups of G . Since $\Phi(N) = K$, there is an element $b \in N - T$ (of order 16) such that $b^2 \in X - W$ and $b^2 \notin F$. Then $b^2 = ws$, where $w \in W - F_1$ and $W = \langle w \rangle \times \langle v \rangle$. We set $w^2 = u$ and so $\Omega_1(W) = \langle u, z \rangle$. We compute $b^4 = w^2s^2 = uv$ and $b^8 = z$. Hence $N = \langle a \rangle \langle b \rangle$, where $\langle a \rangle$ is a cyclic normal subgroup of order 2^m ($m \geq 4$) of N and $\langle b \rangle$ is cyclic of order 16 with $\langle a \rangle \cap \langle b \rangle = \langle z \rangle$ (of order 2). It remains to determine the action of $\langle b \rangle$ on $\langle a \rangle$. Now, $\langle b \rangle$ induces a cyclic automorphism group on $\langle a \rangle$ so that b inverts $\langle a \rangle / \langle v \rangle$ (since N/W is generalized quaternion). Thus $a^b = a^{-1}v_0$ with $v_0 \in \langle v \rangle$ and so $(a^4)^b = (a^b)^4 = (a^{-1}v_0)^4 = a^{-4}$. In particular, b inverts $\langle v \rangle$. On the other hand, b centralizes $b^4 = uv$. We compute $uv = (uv)^b = u^b v^b = u^b v^{-1}$, and so $u^b = uz$. The last relation is crucial and shows that b does not stabilize the chain $W > \Omega_1(W) > \{1\}$.

If A (of order 2^5) is a Sylow 2-subgroup of $\text{Aut}(W)$ and B is the full stabilizer group of the chain $W > \Omega_1(W) > \{1\}$, then B is elementary abelian of order 2^4 and $|A/B| = 2$ (see Proposition 50.5). We note that $C_G(W) \leq N$ and $C_G(W)/W$ is a cyclic normal subgroup of N/W and so $C_G(W) \leq T$. Hence, if L is the set of all $y \in G$ which stabilize the chain $W > \Omega_1(W) > \{1\}$, then the subgroup L covers G/N (since $b \notin L$) and so G/N (being isomorphic to a subgroup of D_8) is elementary abelian of order ≤ 4 . We have obtained all properties stated in part (a2) of our theorem.

(ii) We consider now the groups G from Theorem 54.2(b). In this case $n > 2$, $X = QU_1$, where $Q \cong Q_8$ is a normal quaternion subgroup of X , $Q \cap U_1 = Z(Q)$, $U_1 = \langle b \rangle \cong C_{2^n}$, and b either centralizes Q or b induces on Q an involutory outer automorphism in which case $n > 3$.

Assume first that b centralizes Q . In that case $X = Q * \langle b \rangle$ with $Q \cap \langle b \rangle = Z(Q) = \langle z \rangle$. Set $v = b^{2^{n-2}}$ so that $\Omega_2(X) = Q * \langle v \rangle$. Since Q is the unique quaternion subgroup in $\Omega_2(X)$, it follows that Q is characteristic in X and so Q is a normal subgroup in G . Set $C = C_G(Q)$ so that $X \cap C = U_1 = \langle b \rangle$, C is normal in G , and $|G : (Q * C)| \leq 2$. Since U_1 is the unique cyclic subgroup of order 2^n in C , it follows that C is either cyclic or of maximal class. If $G = Q * C$, we are done.

Suppose that $|G : (Q * C)| = 2$. Since $G/C \cong D_8$ (a Sylow 2-subgroup of $\text{Aut}(Q_8)$), there is an element $d \in G - (QC)$ with $d^2 \in C$. Set $P = C\langle d \rangle$ so that $G = QP$ and $P \cap X = U_1$. Since U_1 is the unique cyclic subgroup of order 2^n in P , we get again that P is either cyclic or of maximal class.

It remains to consider the case, where b induces on Q an outer involutory automorphism (and in that case $n > 3$). Obviously, Q is the unique quaternion subgroup of $Q\langle b^2 \rangle = Q * \langle b^2 \rangle$, where $Q \cap \langle b^2 \rangle = \langle z \rangle$. We have $\exp(Q\langle b^2 \rangle) = 2^{n-1}$ and all elements in $X - (Q\langle b^2 \rangle)$ are of order 2^n . Hence Q is also the unique quaternion subgroup of X and so Q is normal in G . Again set $C = C_G(Q)$ so that C is normal in G and $X \cap C = \langle b^2 \rangle$. Also, $|G : (QC)| = 2$ and so $G = XC$. Set $P = C\langle b \rangle$. We have $|P : C| = 2$, $P \cap X = \langle b \rangle = U_1$, and $G = QP$ with $Q \cap P = \langle z \rangle$. Since U_1 is the unique cyclic subgroup of order 2^n in P , it follows that P is either cyclic or of maximal class and we are done.

(iii) Finally, we consider the groups G from Theorem 54.2(c). In this case $n = 3$, $|X| = 2^5$, and $\Omega_2(X) \cong Q_8 \times C_2$ or $\Omega_2(X) \cong D_8 \times C_2$. Since G has no normal subgroups isomorphic to E_8 , Proposition 54.5 gives at once the result stated in part (c) of our theorem. \square

2-groups G with small subgroup $\langle x \in G \mid o(x) = 2^n \rangle$

In §52, 2-groups G with $|\Omega_2(G)| = 16$ are classified. In this section we consider essentially more difficult problem to classify the 2-groups in which all elements of order 4 generate the subgroup of order 16.

In what follows we suppose that G is a 2-group of order $> 2^4$ all of whose elements of order 4 generate a subgroup H of order 2^4 . In that case, obviously, H is not of maximal class so it has no cyclic subgroups of index 2 (see Theorem 1.2). It is obvious that, in the case under consideration, $c_2(G) \geq 4$. Indeed, if the above assertion is false, then $c_2(G) = 2$, by Theorem 1.17(b). In that case, by §52, the elements of order 4 generate the abelian subgroup of type $(4, 2)$, contrary to our hypothesis (this also follows from §43). If $c_2(G) = 4$, then $H \cong Q_8 * C_4$ or $H \cong C_4 \times C_2 \times C_2$ and the group G was completely determined in §52. If $c_2(G) = 5$, then G is of maximal class (Theorem 1.17(b)) and so $H \cong Q_{16}$ and (since $|G| > 2^4$) $G \cong SD_{32}$. It remains to examine the case $c_2(G) = 6$ since there is no 2-group G with $c_2(G) = 7$ (Theorem 1.17(b)). The 2-groups G with $|\Omega_2(G)| = 2^4$ have been determined in §52, and so we may also assume $|\Omega_2(G)| > 2^4$.

Exercise 1. Let G be a 2-group, $H = \langle x \in G \mid o(x) = 4 \rangle$. If $\exp(Z(H)) = 2$, then $C_G(H) = Z(H)$.

Solution. Assume that $C_G(H) > Z(H)$. Let $x \in C_G(H) - Z(H)$ be such that $x^2 \in Z(H)$. Then $o(x) \leq 4$ so x is an involution since $x \notin H$. If $a \in H$ is of order 4, then $o(ax) = 4$ and $ax \notin H$, a contradiction.

Let G be a 2-group and let $\Omega_2^*(G) = \langle x \in G \mid o(x) = 2^2 \rangle$. Suppose that $|\Omega_2^*(G)| = 2^4$ and $c_2(G) > 4$; then $c_2(G) \geq 6$ (Theorem 1.17(b)) so G contains at least twelve elements of order 4. Then $c_2(G) = 6$ since $c_1(G) \geq 3$.

Theorem 55.1 ([Jan8]). *Let G be a 2-group of order $> 2^4$ all of whose elements of order 4 generate a subgroup H of order 2^4 , i.e., $H = \Omega_2^*(G)$. Assume, in addition, that $c_2(G) = 6$ and $|\Omega_2(G)| > 2^4$. Then we have the following possibilities:*

- (a) $H \cong Q_8 \times C_2$ and $G \cong SD_{16} \times C_2$.
- (b) $H \cong \langle a, b \mid a^4 = b^4 = 1, a^b = a^{-1} \rangle$ is metacyclic and $G = \langle b, t \mid b^4 = t^2 = 1, b^t = ab, a^4 = 1, a^b = a^{-1}, a^t = a^{-1} \rangle$. Here $|G| = 2^5$, $H = \langle a, b \rangle$, $\Phi(G) = \langle a, b^2 \rangle \cong C_4 \times C_2$, $\Omega_2(G) = G$, $Z(G) = \langle a^2, b^2 \rangle \cong E_4$.

- (c) $H \cong C_4 \times C_4$ and G has a metacyclic maximal subgroup M such that $\Omega_2(M) = H$, $G = M\langle t \rangle$, where t is an involution with $C_M(t) = \Omega_1(M) \cong E_4$.

Proof. Since H is neither cyclic nor of maximal class, H has a normal four-subgroup H_0 (Lemma 1.4) and so all twelve elements in $H - H_0$ are of order 4. If H is abelian, then $H_0 = \Omega_1(H)$ implies that $H = C_4 \times C_4$. Suppose that H is nonabelian. Then H/H_0 is elementary abelian and so $\Phi(H) \leq H_0$.

Suppose, in addition, that H is not minimal nonabelian and let Q be a nonabelian subgroup of order 8. Since H has only three involutions, we have $Q \cong Q_8$. If $C_H(Q) \leq Q$, then H is of maximal class (Proposition 10.17), a contradiction. Hence $H = Q * Z$, where $|Z| = 4$ and $Q \cap Z = Z(Q)$. If Z is cyclic, then $c_2(H) = 4$, a contradiction. Hence $Z \cong E_4$ and $H \cong Q_8 \times C_2$.

Now suppose that H is minimal nonabelian. Then $d(H) = 2$ so $\Phi(H) = H_0$ and $|H'| = 2$. In that case, H/H' is abelian of type (4, 2). Let Z/H' be a direct factor of H/H' of order 2. Since H/Z is cyclic of order 4, we get $Z \neq \Phi(H) = \Omega_1(H)$ so Z is cyclic. Let $Z = \langle a \rangle$ and $H/Z = \langle bZ \rangle$; then $\langle b \rangle \cap \langle a \rangle = \{1\}$. Since $\text{Aut}(Z) \cong C_2$, we get $H = \langle a, b \mid a^4 = b^4 = 1, a^b = a^{-1} \rangle$.

We have to determine the structure of G for each of the above three possibilities for the structure of H .

(i) Assume that $H = Q \times \langle u \rangle$, where $Q \cong Q_8$ and u is an involution. Set $\langle z \rangle = Z(Q)$ so that $Z(H) = \langle u, z \rangle$. There are exactly three maximal subgroups of H containing $Z(H)$ and they are abelian of type (4, 2). One of them, say $\langle u, a \rangle$ ($a \in Q - Z(Q)$), is normal in G (consider the action of G by conjugation on the set of above three maximal subgroups of H). If $b \in Q - \langle a \rangle$, then the other two such abelian subgroups of type (4, 2) are $\langle u, b \rangle = \langle u \rangle \times \langle b \rangle$ and $\langle u, ab \rangle = \langle u \rangle \times \langle ab \rangle$.

Since $\Omega_2(G) > H$, there is an involution $t \in G - H$ since H contains all elements of order 4 in G . Let $\langle u, x \rangle$, where $x \in Q - Z(Q)$, be any t -invariant abelian subgroup of type (4, 2) in H . If t acts nontrivially on $Z(H)$, then $\langle t, Z(H) \rangle \cong D_8$ has a cyclic subgroup of order 4 that is not contained in H , a contradiction. Thus t centralizes $Z(H)$. Since $C_H(t)$ must be elementary abelian (otherwise, $(\langle t \rangle \times C_H(t)) - C_H(t)$ has an element of order 4), we get $C_H(t) = Z(H)$ and so t acts fixed-point-free on $\langle u, x \rangle - Z(H)$. If $x^t = xs$ with $s \in Z(H) - \langle z \rangle$, then $(tx)^2 = (txt)x = x^t x = xsx = sx^2 = sz \in Z(H)^\#$, and so $o(tx) = 4$, a contradiction since $tx \notin H$. Hence $x^t = x^{-1}$ and so t inverts the subgroup $\langle u, x \rangle$. In particular, t inverts $\langle u, a \rangle$. If t normalizes $\langle u, b \rangle$, then t also normalizes $\langle u, ab \rangle$. But in that case t inverts $\langle u, b \rangle$ and $\langle u, ab \rangle$ and so t inverts $H = \langle u, a \rangle \cup \langle u, b \rangle \cup \langle u, ab \rangle$. This implies that H is abelian (Burnside) which is not the case. Hence we must have $\langle u, b \rangle^t = \langle u, ab \rangle$.

Let $M = N_G(\langle u, b \rangle)$ so that $H \leq M$, $|G : M| = 2$ and $G = M\langle t \rangle$ (see the last sentence of the previous paragraph). By the previous paragraph, the set $M - H$ has no involutions so $\Omega_2(M) = H$ since $\exp(H) = 4$ and H contains all elements of order 4 from G . Assume that $M > H$ so that we can apply the results of §52 (see Theorem 52.1(d)). It follows that M is a uniquely determined group of order 2^5

which is given explicitly in Theorem 49.1, (A2)(a)). There is an element $y \in M - H$ of order 8 (indeed, $\exp(M) = 8$ and $H = \Omega_2(M)$) such that $y^2 = ua$, $u^y = uz$, $a^y = a^{-1}$, $b^y = bu$. Hence y acts nontrivially on $Z(H)$ and y normalizes all three abelian subgroups of type $(4, 2)$ in H .

We have $G/H \cong E_4$ since M/H and $H\langle t \rangle/H$ are two distinct subgroups of order 2 in G/H . Hence $(yt)^2 \in H$ and we consider the subgroup $N = H\langle yt \rangle$ of order 2^5 . Since yt acts nontrivially on $Z(H)$ (t centralizes $Z(H)$), it follows that there are no involutions in $N - H$ (indeed, if w is an involution in $N - H$, then $\langle w, Z(H) \rangle \cong D_8$ contains an element of order 4 which is not contained in H , a contradiction). Thus $H = \Omega_2(N)$ and so, by the above, N is uniquely determined and therefore $N \cong M$. In particular, N normalizes all three abelian subgroups of type $(4, 2)$ in H . Since $M \neq N$, we get that $G = \langle M, N \rangle$ normalizes all three abelian subgroups of type $(4, 2)$ in H (see the last sentence of the previous paragraph), a contradiction.

We have proved that $H = M$ and so $G = H\langle t \rangle$. Since $\langle u, b \rangle^t = \langle u, ab \rangle$, we have $b^t = abs_0$ with $s_0 \in Z(H)$. Hence t normalizes $Q^* = \langle b, b^t \rangle \cong Q_8$ and $H = \langle u \rangle \times Q^*$. Replacing Q with Q^* , we may assume from the start that t normalizes Q and so t induces on Q an outer automorphism (indeed, $\langle b \rangle$ is not t -invariant). We get $Q\langle t \rangle = D \cong SD_{24}$ (if $D \not\cong SD_{24}$, then $\text{cl}(D) = 2$; in that case, $\langle b \rangle \triangleleft D$ so t -invariant, which is not the case) and $G = \langle u \rangle \times D$. We have obtained the possibility (a).

(ii) Now suppose that $H = \langle a, b \mid a^4 = b^4 = 1, a^b = a^{-1} \rangle$ is metacyclic of order 16. Here $\Phi(H) = Z(H) = \langle a^2, b^2 \rangle = \Omega_1(H) \cong E_4$, $H' = \langle a^2 \rangle$, all elements in $H - Z(H)$ are of order 4 and H/H' is abelian of type $(4, 2)$. It follows that H is minimal nonabelian. Therefore all three maximal subgroups W_i , $i = 1, 2, 3$, of H are abelian of type $(4, 2)$: $W_1 = \langle Z(H), a \rangle$ with $\mathcal{V}_1(W_1) = \langle a^2 \rangle$; $W_2 = \langle Z(H), b \rangle$ with $\mathcal{V}_1(W_2) = \langle b^2 \rangle$; $W_3 = \langle Z(H), ab \rangle$ with $\mathcal{V}_1(W_3) = \langle b^2 \rangle$ since $(ab)^2 = ab^2a^b = ab^2a^{-1} = b^2$. It follows that a^2b^2 is not a square in $H (= W_1 \cup W_2 \cup W_3)$ and W_1 is normal in G . (Note, however, that all involutions in a homocyclic 2-group of composite exponent are squares; see, for example, Theorem 6.1.) Hence $\langle a^2 \rangle = H'$, $\langle b^2 \rangle$, and $\langle a^2b^2 \rangle$ are characteristic subgroups in H and therefore they are normal in G . This gives $Z(H) \leq Z(G)$. In fact we have $Z(H) = Z(G)$, by Exercise 1.

Since $\Omega_2(G) > H$, there is an involution $t \in G - H$. By Exercise 1, $C_H(t) = Z(H) = Z(G)$. If t normalizes a maximal subgroup W_i of H , then t inverts W_i , by Exercise 1. We know that t normalizes W_1 and so t inverts W_1 and therefore $a^t = a^{-1}$. If t normalizes W_2 , then t also normalizes W_3 and consequently t inverts H (see the previous paragraph). But then H is abelian, which is not the case. We have proved that $W_2^t = W_3$.

Let $K = N_G(W_2)$ ($= N_G(W_3)$) so that $H \leq K$, $|G : K| = 2$, and $G = K\langle t \rangle$ (see the last sentence of the previous paragraph). But then the set $K - H$ has no involutions (otherwise, that involution inverts H so H is abelian, which is not the case) and so $\Omega_2(K) = H$. Since H is metacyclic, it follows from Theorem 41.1 and Remark 41.2 that K is also metacyclic. If $K > H$, then [Ber25, Remark R48.2]

implies that $H \cong C_4 \times C_4$, which is not the case. Hence we have $K = H$ and so $G = H\langle t \rangle$ is of order 2^5 .

Since $W_2^t = W_3$, we have $b^t \in \{ab, (ab)^{-1}, (ab)a^2, (ab)^{-1}a^2\}$. Note that $b^a = a^2b$ and so

$$(ab)^a = a(a^2b) = (ab)a^2, \quad ((ab)^{-1})^a = ((ab)^a)^{-1} = ((ab)a^2)^{-1} = (ab)^{-1}a^2.$$

Hence, replacing t with the involution ta (if necessary), we see that we may assume that $b^t \in \{ab, (ab)^{-1} = (ab)b^2 = ab^{-1}\}$. If $b^t = ab^{-1}$, then we replace a with $a' = ab^2$. We get $b^t = ab^{-1} = ab^3 = (ab^2)b = a'b, (a')^b = (a')^{-1}, (a')^t = (a')^{-1}$, and see that one may assume from the start (writing again a instead of a') that $b^t = ab$. The structure of G is uniquely determined as stated in part (b).

(iii) Finally, assume that $H = \langle a \rangle \times \langle b \rangle \cong C_4 \times C_4$. Set $C = C_G(H)$. By Exercise 1, $\Omega_2(C) = H$ and therefore C is metacyclic. Since, by assumption, $\Omega_2(G) > H$, there is an involution $t \in G - C$. Suppose that the coset Ct contains an element y which is not an involution. Then $o(y) \geq 8$ and $o(y^2) \geq 4$. In particular, $y^{o(y)/4} = d$ is an element of order 4 in H . We have $y = ct$ with $c \in C$. But then $d = d^y = d^{ct} = d^t$, contrary to Exercise 1. Hence, all elements in Ct are involutions. This implies that t inverts C and C is abelian (Burnside). Since $\Omega_2(C) = H$, we conclude that C is of rank 2.

Suppose that t' is an involution in $G - (C\langle t \rangle)$. Then, by the above, t' inverts C . But then $tt' \in G - C$ and tt' centralizes C , a contradiction. Thus $C\langle t \rangle = \Omega_2(G)$. Set $D = \Omega_2(G)$. We have $C_G(t) = \langle t \rangle \times H_0 = C_D(t)$, where $H_0 = \Omega_1(H) = \langle a^2, b^2 \rangle$. Indeed, if $C_G(t) \not\leq \Omega_2(G)$, then there is an element $y' \in C_G(t) - C_D(t)$ such that $(y')^2 \in C_D(t) = \Omega_1(H)$ so $o(y') \leq 4$ and $y' \in H$, which is a contradiction.

The last result gives an upper bound for the order of G/C . The conjugacy class of t in G is locked in $D - C$ and so there are at most $|D - C| = |C|$ conjugates of t in G . This gives $\frac{1}{8}|G| = |G : C_G(t)| \leq |C|$ and so $|G/C| \leq 8$. Also note that D/C is a normal subgroup of order 2 in G/C .

Suppose that the involution in D/C is a square in G/C . Then there is an element $k \in G - D$ such that $k^2 \in D - C$. But all elements in $D - C$ are involutions and so k is an element of order 4, a contradiction. It follows that G/C is abelian and $D/C \not\leq \Phi(G/C)$. There is a maximal subgroup M of G such that $D \cap M = C$. Since $\Omega_2(M) = H$, it follows that M is metacyclic. We have $G = M\langle t \rangle$, where $C_M(t) = \Omega_1(M) = \Omega_1(H) \cong E_4$. We have obtained a group stated in part (c) of our theorem which is now completely proved. \square

Let $n > 1$ and let G be a p -group. Denote $\Omega_n^*(G) = \langle x \in G \mid o(x) = p^n \rangle$. We have $\Omega_n^*(G) = \{1\}$ if $\exp(G) < p^n$.

Proposition 55.2 (Berkovich). *Let G be an irregular p -group. Suppose that we have $|\Omega_2^*(G)| = p^{p+1} < p^m = |G|$. Then the following assertions hold:*

- (a) *If $p = 2$, then $G \cong SD_{2^4}$ and $H \cong Q_8$ (see Theorems 43.4 and 52.8). In the sequel we assume that $p > 2$.*

- (b) If $\Omega_2(G) = \Omega_2^*(G)$, then G is not of maximal class and $\Omega_2^*(G)$ is regular (see Lemma 42.1). Moreover, G is a group of Lemma 42.1.
- (c) If G is of maximal class and $p > 3$, then $\Omega_2^*(G) = G_1$, where G_1 is the fundamental subgroup of G . In this case every irregular maximal subgroup of G contains exactly p subgroups of order p^p and exponent p , and G contains exactly p^2 such subgroups. Next, $m = p + 2$.
- (d) If $p = 3$ and G is of maximal class, then $\Omega_2^*(G) = \Omega_2(G_1)$ is metacyclic, all nonmetacyclic subgroups of order 3^3 are nonabelian and their number equals 3^{m-3} . In the sequel we assume that G is not of maximal class.
- (e) If $\Omega_2(G)$ is regular, then $\Omega_2^*(G) = \Omega_2(G)$ (see (b)). In the sequel we assume that $\Omega_2^*(G) < \Omega_2(G)$.
- (f) Suppose that $p > 3$. Let t be an element of order p in $G - \Omega_2^*(G)$ and set $D = \langle t, \Omega_2^*(G) \rangle$. Then $d(D) = 3$, exactly p^2 maximal subgroups of D are of maximal class; other maximal subgroups of D are of exponent p .
- (g) All $p+1$ maximal subgroups of $\Omega_2^*(G)$ are normal in G . $\Phi(\Omega_2^*(G))$ is contained in a G -invariant subgroup L of order p^p and exponent p such that $L \not\leq \Omega_2^*(G)$.

Proof. (a) Let $p = 2$. Then $c_2(G) = c_2(\Omega_2^*(G)) \in \{2, 3\}$. If $c_2(G) = 3$, then G is of maximal class by Theorem 1.17(b). In that case, $G \cong \text{SD}_{24}$. If $c_2(G) = 2$, then such G are described in Theorems 43.4 and 52.8. In what follows we assume that $p > 2$.

(b) The p -groups with $|\Omega_2(G)| = p^{p+1}$ are classified in Lemma 42.1. In all cases, $\Omega_2(G)$ is regular.

(c) Let G be of maximal class and $p > 3$. In this case, $|\Omega_2(G_1)| \geq p^{p+1}$ since $|\Omega_1(G_1)| \geq p^{p-1}$ and $G/\Omega_1(G_1)$ has no cyclic subgroups of index p (see Theorems 9.5 and 9.6). It follows that $\Omega_2^*(G) = \Omega_2(G_1)$ and $|\Omega_2(G_1)| = p^{p+1} < p^{2p-2}$ since $p > 3$. In that case, $G_1 = \Omega_2(G_1) = \Omega_2^*(G)$. If M is an irregular maximal subgroup of G , then $\Omega_2^*(M) = M \cap \Omega_2^*(G) < M$ and $\Omega_2^*(M)$ is the unique absolutely regular maximal subgroup of M . We conclude that M has exactly p distinct maximal subgroups of exponent p . Since $\Phi(G)$, the intersection of any two distinct maximal subgroups of G , is absolutely regular, all remaining assertions of (c) are true.

(d) Now let G be a 3-group of maximal class and order $\geq 3^5$. Since, $\Omega_2(G_1) = \Omega_2^*(G)$ is of order 3^4 , we get $\Omega_2^*(G) = \Omega_2(G_1)$. The remaining assertions in (d) are trivial since the number of irregular subgroups of order 3^4 in G equals 3^{m-4} (Exercise 9.27) and every such subgroup contains exactly three subgroups of order 3^3 and exponent 3 (see the proof of (c)). All subgroups of order 3^3 and exponent 3 are nonabelian since $m > 4$ (this is an easy consequence of Theorems 9.5 and 9.6).

(e) follows from Theorem 7.2. In what follows we assume that $\Omega_2^*(G) < \Omega_2(G)$.

(f, g) By hypothesis, $G - \Omega_2^*(G)$ has an element t of order p . Set $D = \langle t, \Omega_2^*(G) \rangle$. Assume that D is of maximal class. Let D_1 be the fundamental subgroup of D (see §9, Theorems 9.5 and 9.6). Since $p > 3$ and D_1 is absolutely regular of width $p - 1$ and

order $\geq p^{p+1}$, we get $\Omega_2^*(D_1) = \Omega_2(D_1) = D$. It follows that $c_2(G) = c_2(\Omega_2^*(G))$ is not divisible by p^{p-1} so G is of maximal class (Theorem 13.2(b)), contrary to the assumption. Thus, D is not of maximal class. By Theorem 12.12, D contains exactly p^2 subgroups $M_1 = \Omega_2^*(G), \dots, M_{p^2}$ of maximal class and index p . We have $|M_i| = p^{p+1}$ for all i . All other $p+1$ maximal subgroups of D are not generated by two elements so they are regular (Theorem 12.12). Let M be one of regular maximal subgroups of D . Supposing that $\exp(M) = p^2$, we get $\Omega_2^*(M) = M \not\leq \Omega_2^*(G)$, a contradiction. Thus, all regular maximal subgroups of D have exponent p . We see that $N = M \cap \Omega_2^*(G)$ is a maximal subgroup of exponent p in $\Omega_2^*(G)$. If M_1 is another maximal subgroup of exponent p in D , then $N_1 = M_1 \cap \Omega_2^*(G)$ is a maximal subgroup of exponent p in $\Omega_2^*(G)$. By Theorem 12.12(c), $M \cap M_1 = \eta(D)$ and $\eta(D) \not\leq \Omega_2^*(G)$. It follows that $N \neq N_1$. We see that the numbers of subgroups of order p^p and exponent p is not divisible by p . By hypothesis, $\Omega_2^*(G)$ has at least two absolutely regular subgroups of index p . It follows that the number of absolutely regular subgroups of index p in $\Omega_2^*(G)$ is not divisible by p . Therefore, all maximal subgroups of $\Omega_2^*(G)$ are normal in G . Since the number of normal subgroups of order p^p and exponent p in G is $\equiv 1 \pmod{p}$ (Theorem 13.5), the last assertion in (h) follows. \square

Exercise 2. Study the irregular p -groups $G = \Omega_n^*(G)$ of order p^{p+n} , generated by elements of order p^n , $n > 3$, $p > 2$. Is it true that $\exp(G) = p^n$?

Exercise 3. Classify the metacyclic 2-groups G such that $\Omega_2^*(G) = G$.

Exercise 4. Classify the nonmetacyclic 2-groups G with metacyclic $\Omega_2^*(G)$.

Theorem 55.3 ([Jan8, Theorem 4.2]). *Let G be a 2-group with $|\Omega_n^*(G)| = 2^{n+2}$, $n > 2$. Then $c_n(G) = 4$ or 6 . If $c_n(G) = 4$, then such groups G are classified in §54. If $c_n(G) = 6$, then $n = 3$ and the structure of $H = \Omega_3^*(G)$ is uniquely determined. We have $H = \langle a, b \mid a^8 = b^8 = 1, a^b = a^{-1}, a^4 = b^4 = z \rangle$, where $|H| = 2^5$ and $E = \Omega_1(H) = \langle z, a^2b^2 = u \rangle \cong E_4$. If $G > H$, then $|G| = 2^6$ and we have for the structure of G one of the following possibilities:*

- (a) G is the “splitting” metacyclic group $G = \langle w, c \mid w^{16} = c^4 = 1, w^c = w^{11} \rangle$, where $H = \langle wc^{-1}, w^2 \rangle$ and $Z(G) = \langle w^8 \rangle$ is of order 2.
- (b) $G = \langle H, c \rangle$ with $c^2 = z^\epsilon$ ($\epsilon = 0, 1$), $(bc)^2 = a$, and $a^c = a^{-1}$. Here $C_G(E) = \langle u \rangle \times \langle a, c \rangle$, where $\langle a, c \rangle \cong D_{16}$ or Q_{16} for $\epsilon = 0$ or 1, respectively. Also, $Z(G) = \langle z \rangle$ is of order 2.
- (c) G is a non-metacyclic U_2 -group with the kernel $E \cong E_4$ and $G/E \cong SD_{16}$. More precisely, $G = \langle d, s \mid d^{16} = s^2 = 1, d^4 = v, d^8 = z, d^s = d^{-1}vu, u^2 = 1, ud = du, u^s = uz \rangle$, where $E = \langle u, z \rangle$ and $H = \langle sd, d^2 \rangle$ with $Z(H) = Z(G) = \langle vu \rangle \cong C_4$. (This is the group (c) with $n = 4$ of Theorem 67.3.)

All above groups are determined up to isomorphism and they exist.

Proof. Let G be a 2-group with $|\Omega_n^*(G)| = 2^{n+2}$, $n > 2$. This implies that G is neither cyclic nor of maximal class. By Theorem 1.17(b), $c_n(G)$ is even. If $c_n(G) = 2$, then Proposition 54.4 gives that $|\Omega_n^*(G)| = 2^{n+1}$, a contradiction. If $c_n(G) = 4$, then such groups G have been classified in §54. Hence, we may assume that $c_n(G) \geq 6$. However, if $c_n(G) \geq 8$, then the number of elements of order 2^n is $\geq 8\varphi(2^n) = 8 \cdot 2^{n-1} = 2^{n+2}$, a contradiction.

We assume in the sequel that $c_n(G) = 6$ and set $\Omega_n^*(G) = H$. We shall determine the structure of H . The number of elements of order 2^n in H equals $l = 6\varphi(2^n) = 6 \cdot 2^{n-1} = 3 \cdot 2^n = 2^{n+1} + 2^n$. Let E be a normal four-subgroup of H and let Z be a cyclic subgroup of order 2^{n-1} in H . It is easy to see that $H_0 = ZE$ is of exponent 2^{n-1} . Indeed, $H'_0 < E$ and so H_0 is of class ≤ 2 with $|H'_0| \leq 2$. Also, H_0 is generated with elements of orders $\leq 2^{n-1}$ and $2^{n-1} \geq 4$. If $x, y \in H_0$ and $o(x) \leq 2^{n-1}$, $o(y) \leq 2^{n-1}$, then $(xy)^{2^{n-1}} = x^{2^{n-1}}y^{2^{n-1}} = 1$. This shows that $\exp(H_0) = 2^{n-1}$. Since $|H| - l = 2^{n+2} - 2^{n+1} - 2^n = 2^n$, it follows that $|H_0| \leq 2^n$ and so $|H_0| = 2^n$ and $Z \cap E \neq \{1\}$. All elements in $H - H_0$ are of order 2^n . This implies that $\Omega_2(H) = \Omega_2(H_0)$ is of order ≤ 8 and so we may use Lemma 42.1. It follows that H must be isomorphic to a group (c) of that proposition. In particular, H is a U_2 -group with the kernel E , H/E is generalized quaternion, $\Omega_2(H)$ is abelian of type $(4, 2)$, and $\Omega_2(H)/E = Z(H/E)$. If $n > 3$, then $c_n(G) = c_n(H) = 2$, a contradiction. Hence $n = 3$, $H/E \cong Q_8$, $\Omega_2(H) = H_0$, and all 24 elements in $H - H_0$ are of order 8. More precisely, $H = \langle a, b \mid a^8 = b^8 = 1, a^b = a^{-1}, a^4 = b^4 = z \rangle$, and so $|H| = 2^5$, $Z(H) = \langle b^2 \rangle \cong C_4$, $H' = \langle a^2 \rangle \cong C_4$, $H_0 = \Omega_2(H) = \langle a^2, b^2 \rangle$, $E = \Omega_1(H) = \langle z, a^2b^2 = u \rangle \cong E_4$, and $C_H(E) = C_H(H_0) = H_1 = \langle b^2, a \rangle$ is abelian of type $(8, 2)$. The following subgroups E , $\langle z \rangle = \Omega_1(H_0)$, H_0 , $\langle a^2 \rangle$, $\langle b^2 \rangle$, and H_1 are characteristic in H and so they are normal in G . We assume $G > H$ and we intend to determine the structure of G up to isomorphism.

Set $C = C_G(E)$ so that C is a maximal subgroup of G , $C > H_1$, $G = CH = C\langle b \rangle$, $C \cap H = H_1$, and $c_3(C) = 2$. By Proposition 54.4, C is an L_2 -group or a U_2 -group with kernel E . Note that U_2 -groups contain a unique normal four-subgroup. If C is a U_2 -group, then H_0/E is a normal subgroup of order 2 in C/E and therefore $H_0/E = Z(C/E)$. If C/E in this case is not dihedral, then there is an element $y \in C - H_1$ such that $y^2 \in H_0 - E$. But then $o(y) = 8$, which is a contradiction (since $\Omega_3^*(G) = H$). Here we have also used the fact that H_1/E is a normal cyclic subgroup of order 4 in C/E and so H_1/E is contained in a cyclic subgroup of index 2 in C/E . We have proved that C is either an L_2 -group (in which case C is abelian of type $(2^i, 2)$, $i \geq 4$) or C is a U_2 -group with C/E dihedral. In any case, C/E has the unique maximal cyclic subgroup T/E of index ≤ 2 . Then T is normal in G , T is abelian of type $(2^j, 2)$, $j \geq 3$, and $T \geq H_1$ (since H_1/E is the unique cyclic normal subgroup of order 4 in C/E). Since $b^2 \in H_1 \leq T$, it follows that in case $|G/T| = 4$, C/T and $\langle b \rangle T/T$ are two distinct subgroups of order 2 in G/T and so $G/T \cong E_4$. In any case, G/T is elementary abelian of order ≤ 4 . We have $C_{H_1}(b) = \langle b^2 \rangle \cong C_4$ and so $C_T(b) = \langle b^2 \rangle$. Indeed, if b centralizes an element

$y \in T - H_1$, then $o(y) \geq 16$ and so b centralizes an element of order 8 and this one must lie in H_1 , a contradiction.

Set $K = \langle b \rangle T$ and assume $K > H$ or equivalently $T > H_1$. We shall determine the structure of K . Suppose that there is an element k of order 16 in $K - T$. Then $k^2 \in T$ and $o(k^2) = 8$. But $C_T(b) = C_T(k)$ and so b centralizes an element of order 8 in T , which contradicts our last result in the previous paragraph. Hence $c_4(K) = c_4(T) = 2$. Proposition 54.4 implies that K is either an L_2 -group or a U_2 -group with the kernel E . But H is a U_2 -group with $H/E \cong Q_8$ and so K is a U_2 -group. We have $H_0/E = Z(K/E)$ and K/E is of maximal class containing the proper subgroup H/E isomorphic to Q_8 . We know that T/E is the cyclic subgroup of index 2 in K/E . If $x \in K - T$ is such that $x^2 \in H_0 - E$, then $o(x) = 8$ and so $x \in H$. Hence, if $s \in K - (H \cup T)$, then $s^2 \in E$ and $C_T(s) = \langle b^2 \rangle$ implies $s^2 \in E \cap \langle b^2 \rangle = \langle z \rangle$. This forces $K/E \cong SD_{16}$ and $|T/E| = 8$. Note that SD_{16} is the unique 2-group of maximal class and order > 8 containing Q_8 as its maximal generalized quaternion subgroup. Since $s \notin C$, it follows $u^s = uz$, where $E = \langle z, u = a^2b^2 \rangle$. Thus $E\langle s \rangle \cong D_8$ and so (since D_8 has five involutions) we may assume that s is an involution. We may set $T = \langle u \rangle \times \langle d \rangle$, where $o(d) = 16$ and $d^8 = z$. Also set $d^4 = v$ so that $o(v) = 4$ and $v^2 = z$. Note that $E \leq \Phi(H) \leq \Phi(K)$ and so the involution s does not normalize $\langle d \rangle$ (otherwise $\langle d, s \rangle$ would be a maximal subgroup of K not containing E). On the other hand, $K/E \cong SD_{16}$ and so $d^s = d^{-1}ve$, where $e \in E - \langle z \rangle$. Replacing b with b^{-1} leads to the replacement of $u = a^2b^2$ with $a^2b^{-2} = a^2b^2z = uz$ and so we may assume from the start that $e = u$ and $d^s = d^{-1}vu$. It is easy to see that K is not metacyclic. We have $\mathfrak{U}_1(T) = \langle d^2 \rangle$ and so s normalizes $\langle d^2 \rangle$. Indeed, $(d^2)^s = (d^s)^2 = (d^{-1}vu)^2 = d^{-2}v^2u^2 = d^{-2}z$, and so $\langle s, d^2 \rangle \cong SD_{16}$ and $E\langle s, d^2 \rangle$ is a non-metacyclic maximal subgroup of K . We locate H as the subgroup of K generated by elements of order 8 in K . We set $b_0 = sd$ and compute $b_0^2 = (sds)d = d^{-1}vud = vu$. Hence b_0 and d^2 are elements of order 8, $\langle d^2 \rangle$ is normal in K , $\langle b_0 \rangle \cap \langle d^2 \rangle = \langle z \rangle$, and so $H = \langle sd, d^2 \rangle$ with $Z(H) = Z(K) = \langle vu \rangle \cong C_4$.

Suppose in addition that $C > T$ so that C is a U_2 -group with $C/E \cong D_{16}$, $G = KC$, and $G/T \cong E_4$. Let $c \in C - T$. Then $c^2 \in E$, c inverts T/E , c centralizes E (since $C = C_G(E)$), and $d^c = d^{-1}f$ with $f \in E$. We compute $(d^2)^c = (d^{-1}f)^2 = d^{-2}$, and so $v^c = v^{-1}$ because $v = d^4 \in \langle d^2 \rangle$. Hence $d^{sc} = (d^{-1}vu)^c = dfv^{-1}u = dvuzf$ and so $(T\langle sc \rangle)/E \cong M_{24}$. On the other hand, $(T\langle sc \rangle) \cap H = H_1$ and therefore $c_3(T\langle sc \rangle) = c_3(H_1) = 2$. By Proposition 54.4, $T\langle sc \rangle$ is either an L_2 -group or a U_2 -group with the kernel E . But $(T\langle sc \rangle)/E \cong M_{24}$, a contradiction.

We have proved that in this case $G = K$ and so it remains to prove the existence of K . We set:

$$d = (1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16)$$

$$(17, 21, 24, 25, 28, 20, 23, 26, 27, 29, 31, 32, 30, 18, 19, 22),$$

and

$$\begin{aligned} s = & (2, 17)(3, 7)(4, 23)(5, 13)(6, 30)(8, 24)(10, 27) \\ & (11, 15)(12, 19)(14, 28)(16, 31)(18, 20)(22, 32)(25, 26). \end{aligned}$$

Then we see that the even permutations d and s (of degree 32) satisfy the defining relations for $G = K = \langle d, s \rangle$:

$$\begin{aligned} d^{16} = s^2 = 1, \quad d^4 = v, \quad d^8 = z, \quad d^s = d^{-1}vu, \\ u^2 = 1, \quad ud = du, \quad u^s = uz. \end{aligned}$$

Since the permutation $z = d^8$ is non-trivial, $z \in Z(K)$, and $Z(K) \cong C_4$, it follows that the induced permutation representation of G is faithful and so G is realized as a subgroup of the alternating group A_{32} . Thus, G is the group from (c).

It remains to analyze the case $K = H$ or equivalently $T = H_1$. Since $G > H$, we have $C > T$ and so $C/E \cong D_8$. We know that $H/E \cong Q_8$, $G/T = G/H_1 \cong E_4$, and $|G| = 2^6$. Let $c \in C - T$. Since $C/E \cong D_8$ and T/E is the unique cyclic subgroup of order 4 in C/E , it follows $c^2 \in E$. Both elements b and c invert T/E and therefore bc centralizes T/E . Set $N = T\langle bc \rangle$, where $(bc)^2 \in T$. Then $N \cap H = T$ and so $c_3(N) = c_3(T) = 2$. Proposition 54.4 implies that N is either an L_2 -group or a U_2 -group. But bc centralizes T/E and therefore N/E is abelian. This shows that N is an L_2 -group and so $N/E \cong C_{2^3}$ with $\Omega_1(N) = E$. Since $bc \notin C$, $u^{bc} = uz$ and so $N \cong M_{25}$ and $(bc)^2$ is an element of order 8 in $T = H_1$. Hence $(bc)^2 = a^i$ or $(bc)^2 = a^i u$, where i is an odd integer. Set $a' = a^i$ and we see that (replacing a with a') the relations for H remain unchanged:

$$b^8 = (a')^8 = 1, \quad b^4 = (a')^4 = z, \quad \text{and} \quad (a')^b = (a')^{-1},$$

except possibly $(a')^2b^2 = uz$, where $u = a^2b^2$. But in that case we replace b with $b' = b^{-1}$ and obtain the old relations for H : $(b')^8 = (a')^8 = 1$, $(b')^4 = (a')^4 = z$, $(a')^{b'} = (a')^{-1}$ and $(a')^2(b')^2 = (a')^2b'^{-2} = (a')^2b^2z = u$. Hence we may write again a and b instead of a' and b' and so we may assume from the start that: $(bc)^2 = a$ or $(bc)^2 = au$, where $u = a^2b^2$, and the relations for $H = \langle a, b \rangle$ remain unchanged.

Assume first $(bc)^2 = au$. Then bc centralizes au and so we get $au = (au)^{bc} = (a^{-1}uz)^c = (a^{-1})^cuz$, which gives $a^c = a^{-1}z$ and $(a^2)^c = a^{-2}$. Note that $c \in C = C_G(E)$, where $E = \langle u, z \rangle$ and so c centralizes $u = a^2b^2$. We get $u = u^c = (a^2b^2)^c = a^{-2}(b^2)^c = a^2b^2$, and so $(b^2)^c = z b^2 = b^{-2}$. From $(bc)^2 = au$ follows (since $c^2 \in E$ and $c^4 = 1$)

$$bcbc = au, \quad cbc = b^{-1}au, \quad c^2(c^{-1}bc) = b^{-1}au, \quad b^c = c^2b^{-1}au,$$

and so noting that $b^2 \in Z(H)$ we get

$$\begin{aligned} (b^2)^c &= c^2b^{-1}auc^2b^{-1}au = b^{-2}, \quad c^2(b^{-1}auc^2b)au = 1, \\ c^2a^{-1}uz(c^2)^b &au = 1, \quad c^2z(c^2)^b = 1, \quad (c^2)^b = c^2z, \end{aligned}$$

and so $c^2 \in E - \langle z \rangle$ and therefore we may set $c^2 = uz^\eta$ ($\eta = 0, 1$) and $b^c = uz^\eta b^{-1} au$. Conjugating the last relation with c^{-1} we get

$$\begin{aligned} b &= uz^\eta(b^{c^{-1}})^{-1}a^{-1}zu, & b^{c^{-1}} &= uz^{\eta+1}a^{-1}b^{-1}u, \\ b^{c^{-1}} &= uz^{\eta+1}b^{-1}au, & b^{c^{-1}} &= b^cz. \end{aligned}$$

We compute

$$\begin{aligned} uz b^{-1} au &= uz(b^{-1}aub)b^{-1} = uza^{-1}uzb^{-1} = ua^{-1}ub^{-1} \\ &= ua^{-1}(a^2b^2)b^{-1} = (ua)b = (au)b = (bc)^2b, \end{aligned}$$

and noting that $(bc)^8 = (au)^4 = a^4 = z$ we get

$$\begin{aligned} (bc)^c &= b^c c = uz^\eta b^{-1} auc = z^{\eta+1}(uz b^{-1} au)c = z^{\eta+1}(bc)^2 bc \\ &= (bc)^{8(\eta+1)}(bc)^3 = (bc)^{11+8\eta}. \end{aligned}$$

Since $\langle bc \rangle \cap \langle c \rangle = \{1\}$ (which follows from $(bc)^8 = (au)^4 = a^4 = z$ and $c^2 = uz^\eta$), we see that $G = \langle bc, c \rangle$ is a “splitting” metacyclic group with the cyclic normal subgroup $\langle bc \rangle$ of order 16 and a complement $\langle c \rangle \cong C_4$. Since $b^{c^{-1}} = b^cz$, we get

$$(bc)^{c^{-1}} = b^{c^{-1}}c = b^czc = (bc)^cz = (bc)^{11+8\eta}(bc)^8 = (bc)^{3+8\eta}.$$

If $\eta = 0$, then $(bc)^c = (bc)^{11}$ and $(bc)^{c^{-1}} = (bc)^3$. If $\eta = 1$, then $(bc)^c = (bc)^3$ and $(bc)^{c^{-1}} = (bc)^{11}$. Hence, replacing c with c^{-1} (if necessary), we may assume from the start that $(bc)^c = (bc)^{11}$. We set $bc = w$ and so we have obtained the unique metacyclic group $G = \langle w, c \mid w^{16} = c^4 = 1, w^c = w^{11} \rangle$, which was stated in part (a) of our theorem. This group obviously exists because $w \rightarrow w^{11}$ induces an automorphism of order 4 of the cyclic group $\langle w \rangle$ of order 16.

Assume now $(bc)^2 = a$. Then bc centralizes a and so we get $a = a^{bc} = (a^{-1})^c$ which implies $a^c = a^{-1}$ and $(a^2)^c = a^{-2}$. Note that $c \in C = C_G(E)$, where $E = \langle u, z \rangle$ and so c centralizes $u = a^2b^2$. We get

$$u = u^c = (a^2b^2)^c = a^{-2}(b^2)^c = a^2b^2 \quad \text{and so} \quad (b^2)^c = zb^2 = b^{-2}.$$

From $(bc)^2 = a$ follows (since $c^2 \in E$ and $c^4 = 1$)

$$bcbc = a, \quad cbc = b^{-1}a, \quad c^2(c^{-1}bc) = b^{-1}a, \quad b^c = c^2b^{-1}a,$$

and so noting that $b^2 \in Z(H)$ we get

$$\begin{aligned} (b^2)^c &= c^2b^{-1}ac^2b^{-1}a = b^{-2}, & c^2(b^{-1}ac^2b)a &= 1, \\ c^2a^{-1}(c^2)^ba &= 1, & (c^2)^b &= c^2, \end{aligned}$$

and so $c^2 \in \langle z \rangle$. We set $c^2 = z^\epsilon$ ($\epsilon = 0, 1$) and have $C = C_G(E) = \langle u \rangle \times \langle a, c \rangle$. If $\epsilon = 0$, then $\langle a, c \rangle \cong D_{16}$. If $\epsilon = 1$, then $\langle a, c \rangle \cong Q_{16}$. Also, $Z(G) = \langle z \rangle$ since $Z(H) = \langle b^2 \rangle$ and $(b^2)^c = b^{-2}$.

If $\epsilon = 0$, then we set (identify):

$$\begin{aligned} b &= (1, 9, 7, 10, 5, 11, 3, 12)(2, 13, 8, 14, 6, 15, 4, 16), \\ c &= (2, 8)(3, 7)(4, 6)(9, 13)(10, 16)(11, 15)(12, 14). \end{aligned}$$

Since $b^4 = z$ is a nontrivial permutation, we have realized the group $G = \langle b, c \rangle$ as a subgroup of S_{16} .

If $\epsilon = 1$, then we set

$$\begin{aligned} b &= (1, 9, 7, 10, 5, 11, 3, 12)(2, 13, 8, 17, 6, 18, 4, 19) \\ &\quad (14, 15, 23, 24, 28, 22, 31, 27)(16, 30, 25, 32, 29, 20, 21, 26), \\ c &= (1, 16, 5, 29)(2, 22, 6, 15)(3, 25, 7, 21)(4, 27, 8, 24) \\ &\quad (9, 14, 11, 28)(10, 31, 12, 23)(13, 20, 18, 30)(17, 32, 19, 26). \end{aligned}$$

Since $b^4 = z$ is a nontrivial permutation, we have obtained our group $G = \langle b, c \rangle$ as a subgroup of A_{32} .

We have obtained two groups stated in part (b) of our theorem which is now completely proved. \square

In conclusion we prove the following

Theorem 55.4. *Let G be a p -group such that $\Omega_2(G)$ is extraspecial. Then $\Omega_2(G) = G$.*

Proof. Suppose the theorem is false, i.e., $\Omega_2(G) < G$. We consider cases $p = 2$ and $p > 2$ separately.

Case 1. Let $p = 2$. Set $E = \Omega_2(G)$ and $\langle z \rangle = Z(E)$ so that $|E| = 2^{2n+1}$, $n \geq 1$, where n is the width of E . Let F be a subgroup of G containing E such that $|F : E| = 2$. To get a contradiction, one may assume, without loss of generality, that $G = F$. We use induction on n . Suppose that $n = 1$. Then $E \cong D_8$ or Q_8 . If $C_G(E) \not\leq E$, then $C_G(E) - \langle z \rangle$ contains elements of order ≤ 4 , a contradiction. Hence $C_G(E) \leq E$ and then G is of maximal class. But then $\Omega_2(G) = G$, a contradiction.

We assume now $n > 1$. Since $|E| \geq 2^5$ and $\exp(E) = 4$, G has no cyclic subgroups of index 2 and so G is not of maximal class. It follows that G has a normal four-subgroup R . We have $R < E$ since $\Omega_2(G) = E$. In particular, $z \in R$ and we may set $R = \langle z, u \rangle$ for some involution $u \in (E - \langle z \rangle)$ so that $C_G(R) = C_G(u)$. Since $|E : C_E(R)| = 2$, it follows that $C_G(R)$ covers G/E . By the structure of E , $C_E(u) = \langle u \rangle \times E_0$, where E_0 is extraspecial of order $2^{2(n-1)+1}$. Set $F_0 = C_G(u)$ so that $|F_0 : (\langle u \rangle \times E_0)| = 2$ and consider the factor-group $F_0/\langle u \rangle = \bar{F}_0$ (bar convention), where $|\bar{F}_0 : \bar{E}_0| = 2$ and \bar{E}_0 is extraspecial of width $n - 1$.

By induction, there is an element $x \in F_0 - (\langle u \rangle \times E_0)$ such that $o(\bar{x}) \leq 4$. If $o(\bar{x}) = 2$, then $x^2 \in \langle u \rangle$ and so $o(x) \leq 4$, a contradiction. Hence $o(\bar{x}) = 4$ and so $x^4 \in \langle u \rangle$ but $x^2 \notin \langle u \rangle$. We have $x^2 \in C_E(u)$. If x^2 is an involution, then $o(x) = 4$, a contradiction. Hence x^2 is an element of order 4 in $C_E(u)$ and so $x^4 = z$, contrary to $x^4 \in \langle u \rangle$. This completes Case 1.

Case 2. Now let $p > 2$ and let $E = \Omega_2(G)$ be extraspecial. Since $G > E$, we have $\exp(E) = p^2$. We have $E = E_1 * \dots * E_{m-1} * E_m$, where, in case $m > 1$, E_1, \dots, E_{m-1} are nonabelian of order p^3 and exponent p and $E_m \cong M_{p^3}$ (see §4). Then we have $S = \Omega_1(E) = \Omega_1(G) = E_1 \dots E_{m-1} \Omega_1(E_m)$, where $\exp(S) = p$ and $|E : S| = p$ (here we use the fact that E is regular; see Theorems 7.1 and 7.2). Set $\Omega_1(E_m) = R$. We have $C_S(R) = E_1 * \dots * E_{m-1} R = S$ so $R = Z(S)$. It follows that R is normal in G . Set $C = C_G(R)$; then $|G : C| = p$, $S < C$ and $G = EC$. Since $S = \Omega_1(G)$ and $\Omega_1(G/S) = E/S$ is of order p so G/S is cyclic since $p > 2$ and E/C is the unique subgroup of order p in G/S , we must have $E/S \leq C/S$. This is a contradiction since $R \not\leq Z(E)$. The proof is complete. \square

§56

Theorem of Ward on quaternion-free 2-groups

In this section we present the proof of the following important result of Ward [War]:

Theorem 56.1 (H. N. Ward [War]). *Let G be a nonabelian quaternion-free 2-group. Then G has a characteristic subgroup of index 2.*

Recall that a 2-group is quaternion-free if it has no sections isomorphic to Q_8 ; that property is inherited by sections. Note that the original proof of that theorem is based essentially on properties of the Burnside group $B(4, 2)$ (this is a finite two-generator group of exponent 4 of maximal order; by Burnside, $|B(4, 2)| = 2^{12}$). The offered proof is shorter and elementary. However, we use ideas of [War]. The offered proof is due to the second author.

Let $P \in \text{Syl}_2(G)$ be the kernel of a Frobenius group G . If P is nonabelian, it has a section isomorphic to Q_8 . Indeed, P has no characteristic subgroups of index 2 so the result follows from Theorem 56.1. Let $P \in \text{Syl}_2(G)$, where $G = \text{Sz}(2^{2m+1})$ is the Suzuki simple group. Since $N_G(P)$ is a Frobenius group, P has a section isomorphic to Q_8 , by what has been said.

Let G be a nonabelian quaternion-free 2-group and let $A \leq \text{Aut}(G)$ be of odd order. Then A has a fixed point on $G/\Phi(G)$ (use Maschke's theorem).

First we prove the following two auxiliary results.

Lemma 56.2. *In a Q_8 -free 2-group X there are no elements x, y with $o(x) = 2^k > 2$ and $o(y) = 4$ so that $x^y = x^{-1}$. If $D \leq X$ and $D \cong D_8$, then $C_X(D)$ is elementary abelian.*

Proof. If $y^2 = x^{2^{k-1}}$, then we have $\langle x, y \rangle \cong Q_{2^k+1}$. If $\langle x \rangle \cap \langle y \rangle = \{1\}$, then we have $\langle x, y \rangle / \langle x^{2^{k-1}} y^2 \rangle \cong Q_{2^k+1}$. In both cases $\langle x, y \rangle$ is not Q_8 -free, a contradiction. Suppose that $D \leq X$, where $D = \langle a, t \mid a^4 = t^2 = 1, a^t = a^{-1} \rangle$. If v is an element of order 4 in $C_X(D)$, then $o(tv) = 4$ and tv inverts a , contrary to what has just been proved. Thus, $C_X(D)$ must be elementary abelian. \square

Lemma 56.3. *Let X be a Q_8 -free 2-group with $\Phi(X) \leq Z(X)$. If $a, b \in X$, $o(a) = o(b) = 4$, and $[a, b] \neq 1$, then $(ab)^2 = 1$.*

Proof. Set $c = [a, b]$ so that $c^2 = [a, b]^2 = [a^2, b] = 1$ and therefore c is a central involution in X . Also, a^2 and b^2 are central involutions in X . Set $W = \langle a^2c, b^2c \rangle$

and so $W \leq Z(\langle a, b \rangle)$ is of order ≤ 4 and exponent 2. In particular, $a, b \notin W$. We compute $a^b = a[a, b] = ac = a^{-1}(a^2c)$, $b^a = b[b, a] = bc = b^{-1}(b^2c)$.

It follows from the above equalities that $(aW)^b = (aW)^{-1}$ and $(bW)^a = (bW)^{-1}$. Since $\langle a, b \rangle / W$ is Q_8 -free, Lemma 56.2 implies that at least one of aW or bW is an involution. Hence $a^2 = b^2c$ or $b^2 = a^2c$ (indeed, W contains exactly three involutions a^2c, b^2c, a^2b^2 and $a^2 \neq a^2b^2 \neq b^2$). In any case $a^2b^2 = c$. But then $(ab)^2 = a^2b^2[b, a] = c^2 = 1$. and we are done. \square

Proof of Theorem 56.1. We proceed by induction on $|G|$. Let $K > \{1\}$ be a minimal characteristic subgroup of G . If G/K is nonabelian, it has a characteristic subgroup H/K of index 2, by induction; then H is characteristic of index 2 in G . Therefore, we may assume that $K = G'$, i.e., G' is the unique minimal characteristic subgroup of G ; then G' is elementary abelian. Since $G' \cap Z(G)$ is a nonidentity characteristic subgroup of G , we get $G' \leq Z(G)$. Thus, the group G is of class 2 and so for all $x, y \in G$, we have $[x^2, y] = [x, y]^2 = 1$, which gives $\Phi(G) = \Omega_1(G) \leq Z(G)$; in particular, $G/Z(G)$ is elementary abelian. The map $x \mapsto x^{2^m}$ is an endomorphism of G if $m \geq 2$ since

$$(1) \quad (xy)^{2^m} = x^{2^m}y^{2^m}[y, x]^{(2^m(2^m-1))/2} = x^{2^m}y^{2^m},$$

where $x, y \in G$. Let $\exp(G) = 2^{n+1}$ ($n \geq 1$). If $n \geq 2$, G is generated by the elements of order 2^{n+1} . For, if $x^{2^n} = 1$ and $o(y) = 2^{n+1}$, then, taking $m = n$ in (1), we get $o(xy) = 2^{n+1}$ and $x = (xy)y^{-1}$ is a product of two elements of order 2^{n+1} . If $n = 1$, we may also assume that G is generated by the elements of order 4. Indeed, let $H = H_2(G)$ be the subgroup generated by all elements of G of order 4. Since $H > \{1\}$, then $H < G$ implies $|G : H| = 2$ (Straus–Szekeres). As H is characteristic, this is a contradiction. Thus, we may assume that $H = G$, i.e., G is generated by elements of order $4 = 2^{n+1}$ again. We prove our theorem in six steps.

Step 1. Suppose that $n = 1$, i.e., $\exp(G) = 4$. Denote $Z_0 = \Omega_1(Z(G))$. We claim that if a_1, a_2, \dots, a_m are elements of G of order 4 such that $a_1a_2 \dots a_m \in Z_0$, then $a_1^2a_2^2 \dots a_m^2 = 1$.

Indeed, let m be the smallest integer for which a_1, \dots, a_m exist satisfying the hypothesis but not the conclusion of the above statement. Then $m > 1$. In fact $m \geq 3$, for if $a_1a_2 = z \in Z_0$, then $a_1 = a_2^{-1}z$ so $a_1^2 = a_2^{-2}z^2 = a_2^{-2}$ and $a_1^2a_2^2 = 1 \in Z_0$.

Since $[a_i, a_j] \in G' \leq \Phi(G) \leq \Omega_1(Z(G)) = Z_0$, elements a_i and a_j commute modulo Z_0 so the hypothesis $a_1a_2 \dots a_m \in Z_0$ is independent of the ordering of a_i 's.

We have for any $i \neq j$, $(a_i a_j)^2 = a_i^2 a_j^2 [a_j, a_i]$ and so $[a_i, a_j] = a_i^2 a_j^2 (a_i a_j)^2$. Suppose that $[a_i, a_j] = 1$. If, in addition, $(a_i a_j)^2 \neq 1$, then $o(a_i a_j) = 4$ and $(a_i a_j)^2 = a_i^2 a_j^2$. Then the two terms a_i and a_j could be combined to $(a_i a_j)$ and m lowered by one, contrary to the assumption. Thus if $[a_i, a_j] = 1$, then $a_i^2 a_j^2 = (a_i a_j)^2 = 1$. If $[a_i, a_j] \neq 1$, then Lemma 56.3 implies $(a_i a_j)^2 = 1$. So in any event, $[a_i, a_j] = a_i^2 a_j^2$.

Now let i, j, k be distinct. Then, by the last result, using the collecting process, we obtain, since $\mathfrak{U}_1(G) \leq Z(G)$,

$$\begin{aligned} (a_i a_j a_k)^2 &= a_i^2 a_j^2 a_k^2 [a_i, a_j] [a_i, a_k] [a_j, a_k] = a_i^2 a_j^2 a_k^2 \cdot a_i^2 a_j^2 \cdot a_i^2 a_k^2 \cdot a_j^2 a_k^2 \\ &= a_i^2 a_j^2 a_k^2. \end{aligned}$$

If then $(a_i a_j a_k)^2 \neq 1$, a_i, a_j, a_k can be combined to $(a_i a_j a_k)$ and m lowered by 2. Therefore $a_i^2 a_j^2 a_k^2 = 1$ for all triples i, j, k . In particular, $m > 3$, so all the squares a_i^2 coincide (for example, it follows from $a_1^2 a_2^2 a_3^2 = 1 = a_2^2 a_3^2 a_4^2$ that $a_1^2 = a_4^2$). But then $[a_i, a_j] = a_i^2 a_j^2 = a_i^4 = 1$ so the elements a_i 's commute, and, since $a_1 a_2 \dots a_m \in Z_0$, we get $1 = (a_1 a_2 \dots a_m)^2 = a_1^2 a_2^2 \dots a_m^2$ after all.

Step 2. Suppose, as in Step 1, that $n = 1$, i.e., $\exp(G) = 4$. Denote again $Z_0 = \Omega_1(Z(G))$. We claim that there is the unique homomorphism $s : g \mapsto g^s$ of G into Z_0 such that if $o(a) = 4$, then $a^s = a^2$. In addition, $x^s = 1$ for every $x \in Z_0$. (g^s is called the “artificial square” of g .) It remains to define s on involutions from $G - Z_0$.

For $g \in G$, write $g = a_1 a_2 \dots a_m$, where $o(a_i) = 4$ (recall that G is generated by elements of order 4, by the paragraph preceding Step 1). By Step 1, $a_1^2 a_2^2 \dots a_m^2$ depends only on g , not of choice of a_1, \dots, a_m . Indeed, if, in addition, $g = b_1 \dots b_t$, then $a_1 \dots a_m b_t^{-1} \dots b_1^{-1} = 1 \in Z_0$ so, by Step 1, $a_1^2 \dots a_m^2 b_t^{-2} \dots b_1^{-2} = 1$ and $a_1^2 \dots a_m^2 = b_1^2 \dots b_t^2$, justifying our claim. If one defines $g^s = a_1^2 a_2^2 \dots a_m^2$, the results stated in the previous paragraph are direct consequences of Step 1. This definition also works in the case $o(g) = 4$: since g^s depends only on g we must have $g^s = g^2$. It follows that $\text{im}(s) = \bar{G}$ is characteristic in G .

Step 3. We define the endomorphism $\bar{}$ of G by $\bar{x} = x^{2^n}$ if $n > 1$ and $\bar{x} = x^s$ (the artificial square, defined in Step 2) if $n = 1$; recall that $\exp(G) = 2^{n+1}$. It is easy to check, using (1) with $m = n$ if $n > 1$ and Step 1 if $n = 1$ that $\bar{}$ is a homomorphism. We observe that, if $n > 1$, then the kernel of $\bar{}$ equals $\Omega_n(G)$, which is $\langle G \rangle$, by (1) with $m = n$; in that case, $\exp(\bar{G}) = 2$. We claim that in any case $[a, b] \in \langle \bar{a}, \bar{b} \rangle$ for all $a, b \in G$. e have $\text{im}(s) \leq \mathfrak{U}_1(G) \cap \Omega_1(Z(G))$.

Let $n = 1$. We have $(ab)^2 = a^2 b^2 [b, a]$. Then, if $o(a) = o(b) = o(ab) = 4$, we get $[a, b] = a^2 b^2 (ab)^2 = \bar{a} \bar{b} ab = \bar{a}^2 \bar{b}^2 = 1 \in \langle \bar{a}, \bar{b} \rangle$. If $o(ab) < 4$, then, independent of the orders of a and b , $[a, b] = a^2 b^2 \in \langle \bar{a}, \bar{b} \rangle$. If $o(a) < 4$, then $[a, b] = b^2 (ab)^2 \in \langle \bar{a}, \bar{b} \rangle$. Similarly, the same inclusion is true, if $o(b) < 4$. Thus, our claim is true for $n = 1$.

Now let $n > 1$. Suppose first that $\bar{a} \neq 1, \bar{b} \neq 1$, and $\bar{a} \bar{b} \neq 1$ (or, what is the same, elements a, b, ab have the same order $2^{n+1} = \exp(G)$). Then $\langle a^4, b^4 \rangle \leq \mathfrak{U}_2(G) < \Phi(G) \leq Z(G)$, exponent of $\langle a, b \rangle / \langle a^4, b^4 \rangle$ is 4, and the orders of a and b equal 4 modulo $\langle a^4, b^4 \rangle$. If $[a, b] \notin \langle a^4, b^4 \rangle$, then Lemma 56.3 implies $(ab)^2 \in \langle a^4, b^4 \rangle$. But taking 2^{n-1} -th powers of the last inclusion and using (1), one obtains $(ab)^{2^n} \in \langle a^{2^{n+1}}, b^{2^{n+1}} \rangle = \{1\}$ since $\exp(G) = 2^{n+1}$, or, what is the same, $\bar{a} \bar{b} = 1$, contrary to the assumption. Therefore, $[a, b] \in \langle a^4, b^4 \rangle$ and since $\Omega_1(\langle a^4, b^4 \rangle) = \langle \bar{a}, \bar{b} \rangle$ (recall that $\exp(\bar{G}) = 2$) and G' is elementary abelian, $[a, b] \in \langle \bar{a}, \bar{b} \rangle$.

Next let a be an involution and $\bar{b} \neq 1$ (this means that $o(b) = 2^{n+1}$). We may assume that $|\bar{G}| \geq 4$ (otherwise the kernel $\Omega_n(G)$ of $\bar{\cdot}$ is a characteristic subgroup of G of index 2). Hence, for some element $c \in G$, we have $\bar{c} \notin \langle \bar{b} \rangle$ (otherwise, $\bar{G} = \langle \bar{b} \rangle$ were of order 2); it follows that $o(c) = 2^{n+1}$. In $G/\langle b^2 \rangle$ ($b^2 \in Z(G)$), then, some power of c leads to a central element of order 4. By the second part of Lemma 56.2, $G/\langle b^2 \rangle$ has no subgroups isomorphic to D_8 . Hence, a and b commute modulo $\langle b^2 \rangle$, and we have $[a, b] \in \langle b^2 \rangle$ and since $o([a, b]) \leq 2$ (recall that $\exp(G') = 2$), $[a, b] \in \langle \bar{b} \rangle$.

Now let $\bar{a} = 1$, $\bar{b} \neq 1$ (this means that $o(a) \leq 2^n$, $o(b) = 2^{n+1}$), and let a have the minimal order 2^m ($2 \leq m \leq n$) among such elements for which $\bar{a} = 1$ but $[a, b] \notin \langle \bar{a}, \bar{b} \rangle = \langle \bar{b} \rangle$ (case $m = 1$ was considered in the previous paragraph). Then $\langle a^{2^{m-1}}, \bar{b} \rangle \geq \Omega_1(\langle a^4, b^4 \rangle)$, where $\langle a^4, b^4 \rangle \leq Z(G)$. If $[a, b] \notin \langle a^4, b^4 \rangle$, then by Lemma 56.3, $(ab)^2 \in \langle a^4, b^4 \rangle$ and so (taking again 2^{n-1} -th powers) we get $\bar{b} = \bar{1}\bar{b} = \bar{a}\bar{b} = \overline{ab} = 1$, contrary to the assumption of this paragraph. Hence, since $o([a, b]) \leq 2$, we get $[a, b] \in \Omega_1(\langle a^4, b^4 \rangle)$ and so $[a, b] \in \langle a^{2^{m-1}}, \bar{b} \rangle$. Again let $c \in G$ be such that $\bar{c} \notin \langle \bar{b} \rangle$. Since $\overline{ac} = \bar{c} \neq 1$ and $\overline{cb} = \bar{c}\bar{b} \neq 1$, we have, by the above, $[ac, b] \in \langle \bar{c}, \bar{b} \rangle$ and $[c, b] \in \langle \bar{c}, \bar{b} \rangle$. Then $[ac, b] = [a, b][c, b]$ implies $[a, b] \in \langle \bar{c}, \bar{b} \rangle$. Combining this with $[a, b] \in \langle a^{2^{m-1}}, \bar{b} \rangle$, we get $[a, b] \in \langle \bar{b} \rangle$, which is a contradiction, unless $a^{2^{m-1}} \in \langle \bar{c}, \bar{b} \rangle$. But in this case $a^{2^{m-1}} = z^{-2^{m-1}}$ for some $z \in \langle b^2, c^2 \rangle \leq Z(G)$. Then $(az)^{2^{m-1}} = 1$ and so $o(az) < 2^m$ and $[a, b] = [az, b] \in \langle \bar{b} \rangle$, by minimality of m . This contradiction proves that for any $a, b \in G$ with $\bar{a} = 1$ and $\bar{b} \neq 1$, we have $[a, b] \in \langle \bar{b} \rangle$.

If $\bar{a} = \bar{b} \neq 1$, then $[a, b] = [ab, b]$ with $\overline{ab} = \bar{a}^2 = (a^2)^{2^n} = a^{2^{n+1}} = 1$, so that $[a, b] = [ab, b] \in \langle \bar{b} \rangle$, by the previous paragraph.

Finally, suppose that $\bar{a} = \bar{b} = 1$. Let $c \in G$ be any element with $\bar{c} \neq 1$. Then $[a, bc] \in \langle \bar{a}, \overline{bc} \rangle = \langle \bar{c} \rangle$ and $[a, c] \in \langle \bar{a}, \bar{c} \rangle = \langle \bar{c} \rangle$, by the above. Hence $[a, bc] = [a, b][a, c]$ gives $[a, b] \in \langle \bar{c} \rangle$. Since $|\bar{G}| \geq 4$, there is $d \in G$ with $\bar{d} \notin \langle \bar{c} \rangle$. Then, again, $[a, b] \in \langle \bar{d} \rangle$ and so $[a, b] \in \langle \bar{d} \rangle \cap \langle \bar{c} \rangle = \{1\}$ (recall that $\exp(\bar{G}) = 2$), as needed. All possibilities have been considered and so $[a, b] \in \langle \bar{a}, \bar{b} \rangle$ for all $a, b \in G$.

Step 4. We claim now that $G' = \bar{G}$. Obviously, $G' \leq \bar{G}$ since G' is the unique minimal characteristic subgroup of G and \bar{G} is a nonidentity characteristic subgroup of G (this follows from the definition of \bar{G} ; see Step 2). Note that if $G' \neq \bar{G}$, then $|\bar{G} : G'| \geq 4$. Assume that this is false; then $|\bar{G} : G'| = 2$. We have $\bar{G} \cong G/K$ with characteristic subgroup $K < G$, the kernel of $\bar{\cdot}$. Since $G'K < G$ is characteristic in G , we get $|G : G'K| \geq 4$. It follows $|\bar{G} : \bar{G}'| = |G/K : (G'K/K)| = |G : G'K| \geq 4$, as claimed.

Suppose that $G' < \bar{G}$. Then if $\bar{a} \in \bar{G} - G'$, we have $[a, b] = 1$ for all $b \in G$. To see this, note first that if $\bar{a}, \bar{b}, \overline{ab}$, all involutions in $\langle \bar{a}, \bar{b} \rangle$, are not contained in G' , then $[a, b] \in G' \cap \langle \bar{a}, \bar{b} \rangle$ (using Step 3), and that intersection equals $\{1\}$ since $\langle \bar{a}, \bar{b} \rangle = \{1, \bar{a}, \bar{b}, \overline{ab}\}$. Now suppose that $\bar{a} \notin G'$ but $\bar{b} \in G'$. Find $c \in G$ with $\bar{c} \notin \langle G', \bar{a} \rangle$ (c exists since $|\bar{G} : G'| \geq 4$ and $\exp(\bar{G}) = 2$). Then $\overline{ac} \notin G'$, so that

$[a, c] = 1$ by what has just been proved. And, $[a, b] = [a, b][a, c] = [a, bc] \in \langle \bar{a}, \bar{bc} \rangle$, by Step 3. But $\langle \bar{a}, \bar{bc} \rangle \cap G' = \{1\}$. Indeed, $\bar{a}, \bar{bc} \notin G'$, by the choice. It remains to show, that the third involution $\bar{abc} = \bar{ab}\bar{c}$ of $\langle \bar{a}, \bar{bc} \rangle$ is not contained in G' . If this is false, then, since $\bar{b} \in G'$, we get $\bar{ac} = \bar{a}\bar{c} = \bar{ab}\bar{c} \cdot \bar{b} \in G'$, contrary to what has been proved. Hence $[a, b] = 1$. Finally, if $\bar{a} \notin G'$, $\bar{b} \notin G'$, and $\bar{ab} \in G'$, then $[a, b] = [a, ab] = 1$ (the second equality follows, by the previous case). Thus, $[a, b] = 1$ for all $b \in G$. But G is generated by the elements $a \in G$ with $\bar{a} \notin G'$, and G would be abelian, a contradiction. Set $T = \langle x \in G \mid \bar{x} \notin G' \rangle$. To justify our claim, we must to prove that $G = \langle T \rangle$. Indeed, G is generated by all elements of order $2^{n+1} = \exp(G)$. Let $\bar{g} \in G'$ with $\bar{g} \neq 1$ and let $\bar{a} \in \bar{G} - G'$. Then also $\bar{ga} = \bar{g}\bar{a} \in \bar{G} - G'$ and $\bar{g} = \bar{ga}\bar{a}$ so that $g = gaat$ with $\bar{t} = 1$. But then $g = (ga)(at)$ and $\bar{ga} \notin G'$ and $\bar{at} = \bar{a} \notin G'$, i.e., $ga, at \in T$. Thus, $G = \langle T \rangle$, as claimed.

Thus $\bar{G} = G'$. Let K be the kernel of $\bar{}$. Then $\bar{G} = G/K$ is isomorphic to G' and so $|G'| = |G : K| > 2$; the last inequality holds in view of G is nonabelian and K is characteristic in G .

Step 5. Suppose that $|G'| \geq 8$. Then we obtain a characteristic subgroup of index 2 in G as follows.

(i) There exist $a, b \in G$ with $|\langle \bar{a}, \bar{b} \rangle| = 4$ and $[a, b] = 1$ (since $\exp(\bar{G}) = 2$, if such a, b exist, then $\langle \bar{a}, \bar{b} \rangle$ is a four-group).

For, let a and b be such that $|\langle \bar{a}, \bar{b} \rangle| = 4$ but $[a, b] \neq 1$ (we may assume that \bar{G} is noncyclic). By Step 3, $1 \neq [a, b] \in \langle \bar{a}, \bar{b} \rangle$ and so without loss of generality we may take $[a, b] = \bar{a}$. (If $[a, b] = \bar{b}$, then replace $[a, b]$ with $[b, a] = [a, b]^{-1} = \bar{b}^{-1} = \bar{b}$. If $[a, b] = \bar{ab}$, then replace $[a, b]$ with $[ab, b] = [a, b] = \bar{ab}$.) Now take c with $\bar{c} \notin \langle \bar{a}, \bar{b} \rangle$ (such c exists in view of $|\bar{G}| = |G'| \geq 8$). Then $[a, bc] = [a, b][a, c] = \bar{a}[a, c] \in \langle \bar{a}, \bar{bc} \rangle \cap \bar{a}\langle \bar{a}, \bar{c} \rangle = \{1, \bar{a}\}$. If $[a, bc] = 1$, then a and bc are the desired elements. If $[a, bc] = \bar{a}$ ($= [a, b]$), then $[a, c] = 1$ so a and c are the desired elements.

(ii) Suppose that $\bar{a} \neq 1, \bar{b} \neq \bar{a}$, and $[a, b] = 1$. Then $[b, x] \in \langle \bar{b} \rangle$ for all $x \in G$.

For, (by Step 3) $[ax, b] = [x, b] \in \langle \bar{ax}, \bar{b} \rangle \cap \langle \bar{x}, \bar{b} \rangle$. Assume that this intersection is not $\langle \bar{b} \rangle$. Then $\langle \bar{ax}, \bar{b} \rangle = \langle \bar{x}, \bar{b} \rangle$ is a four-group. Since $\bar{a} \neq 1$, we get $\bar{ax} = \bar{b}\bar{x}$ so $\bar{a} = \bar{b}$, contrary to the assumption. Thus, our intersection is $\langle \bar{b} \rangle$, as claimed.

(iii) Now let H be the set of elements $a \in G$ for which $[a, x] \in \langle \bar{a} \rangle$ for all $x \in G$. We show that H is a subgroup of G of index 2; it will clearly be characteristic.

If $a_1, a_2 \in H$, then we have to show that $a_1a_2 \in H$. Suppose that $\bar{b} \notin \langle \bar{a}_1, \bar{a}_2 \rangle$. Then $[a_1a_2, b] = [a_1, b][a_2, b] \in \langle \bar{a}_1\bar{a}_2, \bar{b} \rangle \cap \langle \bar{a}_1 \rangle \langle \bar{a}_2 \rangle = \langle \bar{a}_1\bar{a}_2 \rangle$, as needed. Since G is generated by the set of all such b 's (noting that $\bar{G} = G/K$ is elementary abelian of order $|G'| \geq 8$), we have $[a_1a_2, b] \in \langle \bar{a}_1\bar{a}_2 \rangle$ for all $b \in G$. Thus $a_1a_2 \in H$ so H is a characteristic subgroup of G . Obviously, $G' \leq Z(G) \leq H$.

By (i) and (ii), there is an element $a \in H$ with $\bar{a} \neq 1$. Indeed, by (i), there exist $a, b \in G$ such that $\bar{a} \neq 1, \bar{b} \neq 1, \bar{b} \neq \bar{a}$ and $[a, b] = 1$. Then, by (ii), $b \in H^\#$, proving our claim. Suppose for such an a that $[a, b] = 1$ for some $b \in G$. If $\bar{b} \neq \bar{a}$,

then $b \in H$ by (ii); but if $\bar{b} = \bar{a}$, then $\overline{ba} = \bar{a}\bar{a} = 1 \neq \bar{a}$ and $[a, ba] = [a, b] = 1$ and so by (ii) again, $ba \in H$. Since $a \in H$, so $b \in H$ in any event. We have proved that $C_G(a) \leq H$. So if $b \in G - H$, then $[a, b] \neq 1$. But then $[a, b] = \bar{a}$ (as $a \in H$ and $o(\bar{a}) = 2$). Hence if $H \neq G$, then $|G : H| = 2$. (Suppose there are $b_1, b_2 \in G - H$ such that $b_1b_2 \in G - H$. Then $\bar{a} = [a, b_1b_2] = [a, b_1][a, b_2] = \bar{a}\bar{a} = 1$, a contradiction.)

Assume that $H = G$. Then G is Dedekindian so abelian since it is Q_8 -free (see Theorem 1.19).

Step 6. Finally suppose that $|G'| = 4$ (by the last paragraph of Step 4. $|G'| > 2$). It cannot be that K , the kernel of $\bar{}$, is central, for $|G : K| = 4$ would then imply $|G'| = 2$, by Lemma 1.1. Thus there is $c \in K$ (or, what is the same, $\bar{c} = 1$) and $a \in G$ with $[a, c] \neq 1$. By Step 3, $[a, c] \in \langle \bar{a}, \bar{c} \rangle = \langle \bar{a}, 1 \rangle = \langle \bar{a} \rangle$ and so $[a, c] = \bar{a}$. Suppose that $\bar{b} \notin \langle \bar{a} \rangle$. Then $[ab, c] = [a, c][b, c] = \bar{a}[b, c] \in \langle \overline{ab} \rangle \cap \langle \bar{b} \rangle$, by Step 3, and so $[ab, c] = \overline{ab}$. Thus $[b, c] = \overline{ab}[a, c]^{-1} = \overline{ab}\bar{a}^{-1} = \bar{b}$. Since G is generated by all $b \in G$ with $\bar{b} \notin \langle \bar{a} \rangle$, this implies $[g, c] = \bar{g}$ for all $g \in G$. It follows that $|K : (K \cap Z(G))| = 2$. Indeed, assume that there are $c_1, c_2 \in K - Z(G)$ such that $c_1c_2 \in K - Z(G)$ and $\bar{a} \neq 1$. Then $\bar{a} = [a, c_1c_2] = [a, c_1][a, c_2] = \bar{a}\bar{a} = 1$, which is a contradiction.

Let $a, b \in G$ be such that $\langle \bar{a}, \bar{b} \rangle = G'$. If $[a, b] \neq 1$, we may assume that $[a, b] = \bar{a}$. (If $[a, b] = \bar{a}\bar{b}$, then take the elements ab, b so that $[ab, b] = [a, b] = \overline{ab}$. If $[a, b] = b$, then take the elements b, a so that $[b, a] = [a, b]^{-1} = \bar{b}^{-1} = \bar{b}$.) Then $[a, bc] = [a, b][a, c] = \bar{a}\bar{a} = 1$ and $|\langle \bar{a}, \overline{bc} \rangle| = 4$ (with $c \in K - Z(G)$ as in the previous paragraph). Thus we may assume from the start that $[a, b] = 1$. Now, $G = \langle a, b \rangle K = \langle a, b, c \rangle Z(G)$. By the previous paragraph, $|K : (K \cap Z(G))| = 2$. Therefore, $Z(G) < K$ because otherwise $|G : Z(G)| = 4$ and then $|G| = 2|Z(G)||G'|$ (Lemma 1.1) would imply $|G'| = 2$, a contradiction (see the last paragraph of Step 4). Hence we have $Z(G) < K$ and since $|K : Z(G)| = 2$, it follows that $|G : Z(G)| = 8$. The fact $[a, b] = 1$ implies that $Z(G)\langle a, b \rangle$ is an abelian maximal subgroup of G . Since $|G : Z(G)| = 8$, we see that $Z(G)\langle a, b \rangle$ is the unique abelian maximal subgroup of G and therefore it is a characteristic subgroup of index 2. The proof is complete. \square

Nonabelian 2-groups all of whose minimal nonabelian subgroups are isomorphic and have exponent 4

By Proposition 10.28, a nonabelian p -group is generated by its minimal nonabelian subgroups. Therefore it is natural to try to determine the structure of a p -group if the structure of its minimal nonabelian subgroups is known. Here we classify the title groups and note that there are exactly five minimal nonabelian 2-groups of exponent 4 (see Lemma 65.1). All results of this section are due to the second author.

Recall that there are exactly five minimal nonabelian 2-groups of exponent 4: D_8 , Q_8 , $\mathcal{H}_2 = \langle a, b \mid a^4 = b^4 = 1, a^b = a^{-1} \rangle$, $\mathcal{H}_{16} = \langle a, t \mid a^4 = t^2 = 1, [a, t] = z, z^2 = [a, z] = [t, z] = 1 \rangle$ and $\mathcal{H}_{32} = \langle a, b \mid a^4 = b^4 = 1, [a, b] = z, z^2 = [a, z] = [b, z] = 1 \rangle$.

It is proved in Appendix 17 (Corollary A.17.3) that, if G is a nonabelian 2-group all of whose minimal nonabelian subgroups are isomorphic to Q_8 , then $G = Q \times V$, where $Q \cong Q_{2^n}$, $n \geq 3$, and $\exp(V) \leq 2$. In Theorem 10.33 was proved that if G is a nonabelian 2-group all of whose minimal nonabelian subgroups are isomorphic to D_8 , then G is generalized dihedral. Here we consider the other three minimal nonabelian 2-groups of exponent 4 and first prove the following two key lemmas.

Lemma 57.1. *Let G be a nonabelian p -group and let A be a maximal abelian normal subgroup of G . Then for any $x \in G - A$, there is $a \in A$ such that $[a, x] \neq 1$, $[a, x]^p = 1$, and $[a, x, x] = 1$ which implies that $\langle a, x \rangle$ is minimal nonabelian. Therefore, G is generated by its minimal nonabelian subgroups.*

Proof. Since $C_G(A) = A$, we have $C_A(x) \neq A$ and therefore $\langle x \rangle C_A(x)$ is a proper abelian subgroup of $\langle x \rangle A$. Let B be a subgroup of $\langle x \rangle A$ containing $\langle x \rangle C_A(x)$ as a subgroup of index p . Then $|(A \cap B) : C_A(x)| = p$, $C_A(x) \leq Z(B)$ and $B' \leq C_A(x)$. Let $a \in (A \cap B) - C_A(x)$ so that $a^p \in C_A(x)$. We get $1 = [a^p, x] = [a, x]^p$. On the other hand, $[a, x] \in C_A(x)$ and so $[a, x, x] = 1$. We get $\langle a, x \rangle' = \langle [a, x] \rangle$ and so, by Lemma 65.2(a), $\langle a, x \rangle$ is minimal nonabelian. \square

Lemma 57.2. *Let G be a nonabelian 2-group all of whose minimal nonabelian subgroups are of exponent 4 and let A be a maximal normal abelian subgroup of G . Then all elements in $G - A$ are of order ≤ 4 and so either $\exp(A) = 2$ or $\exp(A) = \exp(G)$.*

If $x \in G - A$ with $x^2 \in A$, then x inverts each element in $\Omega_1(A)$ and in $A/\Omega_1(A)$. If $\exp(G) > 4$, then either G/A is cyclic of order ≤ 4 or $G/A \cong Q_8$.

Proof. By Lemma 57.1, all elements in $G - A$ are of order ≤ 4 . Thus, $\exp(A) = 2$ or $\exp(A) = \exp(G)$. Let $x \in G - A$ with $x^2 \in A$. Then for each $a \in A$ we have $(aa^x)^x = a^x a^{x^2} = a^x a = aa^x$ and so $aa^x = w$ with $w \in C_A(x)$ and $a^x = a^{-1}w$. We compute $(xa)^2 = xaxa = x^2 a^x a = x^2 w$, where $o(x^2) \leq 2$. Since $o(xa) \leq 4$, we have $o(w) \leq 2$ and so x inverts each element of $A/\Omega_1(A)$. Finally, $(a^2)^x = (a^x)^2 = (a^{-1}w)^2 = a^{-2}$ and so x inverts each element of $\Omega_1(A)$. If $\exp(A) > 4$, then G/A does not possess a four-subgroup and so G/A is either cyclic of order at most 4 or $G/A \cong Q_8$. \square

Theorem 57.3. *Let G be a nonabelian 2-group all of whose minimal nonabelian subgroups are isomorphic to $\mathcal{H}_2 = \langle a, b \mid a^4 = b^4 = 1, a^b = a^{-1} \rangle$. Then the following holds:*

- (a) *If G is of exponent ≥ 8 , then G has a unique abelian maximal subgroup A . We have $\exp(A) \geq 8$ and $E = \Omega_1(A) = \Omega_1(G) = Z(G)$ is of order ≥ 4 . All elements in $G - A$ are of order 4 and if v is one of them, then $C_A(v) = E$ and v inverts $\Phi(A)$ and A/E .*
- (b) *If G is of exponent 4, then $G = K \times V$, where $\exp(V) \leq 2$ and for the group K we have one of the following possibilities:*
 - (b1) *$K \cong \mathcal{H}_2$ is of order 2^4 ;*
 - (b2) *K is the minimal nonmetacyclic group of order 2^5 (see Theorem 66.1(d));*
 - (b3) *K is a unique special group of order 2^6 with $Z(K) \cong E_4$ in which every maximal subgroup is minimal nonmetacyclic of order 2^5 (from (b2));*

$$\begin{aligned} K = \langle a, b, c, d \mid a^4 = b^4 = 1, c^2 = a^2 b^2, [a, b] = 1, \\ a^c = a^{-1}, b^c = a^2 b^{-1}, d^2 = a^2, \\ a^d = a^{-1} b^2, b^d = b^{-1}, [c, d] = 1 \rangle; \end{aligned}$$

- (b4) *K is a splitting extension of $B = B_1 \times \cdots \times B_m$, $m \geq 2$, with a cyclic group $\langle b \rangle$ of order 4, where $B_i \cong C_4$, $i = 1, 2, \dots, m$, and b inverts each element of B (and b^2 centralizes B).*

Proof. Since D_8 is not a subgroup of G , $\Omega_1(G)$ is elementary abelian of order > 2 (because G is not generalized quaternion). Let $x \in G - \Omega_1(G)$ with $o(x) = 4$ and assume that there is $a \in \Omega_1(G)$ such that $[a, x] \neq 1$. Then $[a, x]$ is an involution and we have $1 = [a, x^2] = [a, x][a, x]^x$ so that $[a, x]^x = [a, x]$ and $\langle a, x \rangle$ is minimal nonabelian, a contradiction. Here we have used the fact that $\Omega_1(B) \leq Z(B)$ for each minimal nonabelian subgroup $B \leq G$, where $B \cong \mathcal{H}_2$. Since $\Omega_2^*(G) = G$, we have proved that $\Omega_1(G) \leq Z(G)$. Hence, if A is a maximal normal abelian subgroup of G , then $\Omega_1(G) = \Omega_1(A) \leq Z(G)$, G/A is elementary abelian, $\Omega_1(A) < A$, and $G - A$ consists of elements of order 4.

Suppose that there is an element v of order 4 such that $C_G(v)$ is nonabelian and let $H = \langle a, b \mid a^4 = b^4 = 1, a^b = a^{-1} \rangle$ be a minimal nonabelian subgroup of $C_G(v)$, where we set $a^2 = z, b^2 = u$. First suppose that $\langle v \rangle \cap H = \{1\}$. Then $(av)^2 = a^2v^2 = zv^2 \notin H, (av)^b = a^b v = a^{-1}v = (av)z$, so that $\langle av, b \rangle$ is the nonmetacyclic minimal nonabelian group of order 2^5 and exponent 4, a contradiction. Hence, $v \notin H$ but $v^2 \in Z(H)$ and so $v^2 \in \{z, u, uz\}$. If $v^2 = z$, then $i = va$ is an involution, $i \notin H$ and $i^b = iz$ and so $i \notin Z(G)$, a contradiction. If $v^2 = u$, then $j = vb$ is an involution, $j \notin H$ and $a^j = a^{vb} = a^b = a^{-1}$ so that $j \notin Z(G)$, a contradiction. If $v^2 = uz$, then $(vb)^2 = v^2b^2 = (uz)u = z, vb \notin H$, and $a^{vb} = a^b = a^{-1}$ so that $\langle vb, a \rangle \cong Q_8$, a contradiction. We have proved that the centralizer of each element of order 4 is abelian. In particular, for each $x \in G - A$, $C_A(x) = \Omega_1(A)$ and $\Omega_1(A) = Z(G)$.

If $\exp(A) > 4$, then Lemma 57.2 implies that $|G : A| = 2$ and we have obtained groups in part (a) of our theorem. Indeed, since $x \in G - A$ inverts $A/\Omega_1(A)$ and $\exp(A) \geq 8$, we have $|G'| > 2$ and so, using Lemma 1.1, we see that A is a unique abelian maximal subgroup of G (otherwise, $|G : Z(G)| = 4$).

From now on we assume that $\exp(G) = 4$. In that case $\Phi(G) \leq \Omega_1(A) = Z(G)$ and $|\Phi(G)| \geq 4$ (since $|\Phi(\mathcal{H}_2)| = 4$). If x, y are elements of order 4 in G with $[x, y] \neq 1$, then $[x, y]$ is an involution in $Z(G)$ and so $\langle x, y \rangle$ is minimal nonabelian and $\langle x, y \rangle \cong \mathcal{H}_2$ implies that in case $x^2 \neq y^2$ we have $y^x \in \{y^{-1}, yx^2\}$.

Considering $G/\Phi(G)$, we get $G = K \times V$, where $\exp(V) \leq 2$ and $\Omega_1(K) = Z(K) = \Phi(K) = \Phi(G)$. It is easy to determine the structure of G in case $|\Phi(G)| = 4$. Our group K has exactly three involutions and $Z(K) \cong E_4$ is noncyclic. By the results stated in the introduction to §82, K has a metacyclic normal subgroup M such that K/M is elementary abelian of order ≤ 4 . Since in our case K is of exponent 4, we have $|M| \leq 2^4$ and so $|K| \leq 2^6$. If $|K| \leq 2^4$, then $K \cong H_2$. Suppose that $|K| = 2^5$. In this case K is nonmetacyclic (since $\exp(K) = 4$). If K is not minimal nonmetacyclic, then Theorem 66.1 implies that K must possess a subgroup which is isomorphic to E_8 or Q_8 . This is not the case and so K is minimal nonmetacyclic of order 2^5 . Finally, assume that $|K| = 2^6$. Each maximal subgroup of K is minimal nonmetacyclic of order 2^5 and such a group K is unique according to [CIS, Theorem 2 and Remarks] so K is special with $Z(K) \cong E_4$. We have obtained the groups stated in parts (b1), (b2) and (b3).

It remains to treat the case $|\Phi(G)| > 4$. We note that $|A : \Omega_1(A)| = |\mathfrak{O}_1(A)|$ and let $x \in G - A$. Consider any element $y \in A$ with $y^2 \notin \langle x^2 \rangle$ and suppose that $y^x \neq y^{-1}$ so that $y^x = yx^2$. Assume that there is $v \in A$ with $v^2 \notin \langle x^2, y^2 \rangle$. Since $y^x = y^{vx}$ (and $(vx)^2 \in \{v^2, x^2\}$ and so $(vx)^2 \neq y^2$), we get $x^2 = (vx)^2$ which gives $v^x = v^{-1}$. Since $(vy)^2 \notin \langle x^2, y^2 \rangle$, we also get $(vy)^x = (vy)^{-1}$. Hence, $y^x = y^{-1}$ for all $y \in A$ with $y^2 \notin \langle x^2 \rangle$ and so x inverts A . (If $z \in A$ with $z^2 = x^2$, then x inverts zy and so x also inverts z . But in that case $\langle z, x \rangle \cong Q_8$ which cannot happen.) We have proved that in case $|A : \Omega_1(A)| \geq 8$, each element $x \in G - A$ inverts A and so $|G : A| = 2$ and G is as in (b4).

Assume $|A : \Omega_1(A)| = |\mathfrak{V}_1(A)| = 4$ so that $A = \langle y, z \rangle \Omega_1(A)$ and $\mathfrak{V}_1(A) = \langle y^2, z^2 \rangle$. Since $|\Phi(G)| > 4$, there is $u \in G - A$ such that $u^2 \notin \langle y^2, z^2 \rangle$. By the arguments in the previous paragraph, u inverts A , and so $A\langle u \rangle$ is as in (b4). Suppose that $A\langle u \rangle \neq G$. Then there is $x \in G - (A\langle u \rangle)$ such that $\mathfrak{V}_1(A\langle x \rangle) = \mathfrak{V}_1(A)$ and we may assume that $x^2 = z^2$. If $y^x = y^{-1}$, then $xu \in G - A$ and xu centralizes y , a contradiction. It follows that $y^x = yx^2$. From $y^x = y^{zx}$ and $x^2 \neq (zx)^2$ (noting that $\langle z, x \rangle \cong H_2$) follows that $y^2 = (zx)^2 = [z, x]$. We compute $(yz)^x = yx^2z[z, x] = yx^2zy^2 = y^{-1}z^{-1} = (yz)^{-1}$. But then xu centralizes yz , a contradiction. Hence, we must have $G = A\langle u \rangle$.

Finally, suppose $|A : \Omega_1(A)| = 2$ so that $A = \langle y \rangle \Omega_1(A)$. Let $x \in G - A$, where we may assume that $x^2 \neq y^2$. (Indeed, we have $\langle x, y \rangle \cong \mathcal{H}_2$ and so if $x^2 = y^2$, then we replace x with $x' = xy$, where $(x')^2 \neq y^2$. We may assume that $y^x = yx^2$ (otherwise, if each element in $G - A$ inverts A , then $|G : A| = 2$ and G would be as in (b1)). Let $u \in G - \langle A, x \rangle$ with $u^2 \notin \langle x^2, y^2 \rangle$. Then we have $y^u \in \{y^{-1}, yu^2\}$. First suppose that $y^u = y^{-1}$. Then $y^{xu} = (yx^2)^u = y(y^2x^2)$. But $(xu)^2$ is equal either x^2u^2 (if $[u, x] = 1$) or u^2 or x^2 (if $[u, x] \neq 1$ and so $\langle u, x \rangle \cong H_2$) and therefore in any case $(xu)^2 \neq y^2$. Since $\langle y, xu \rangle \cong H_2$, we get $y^{xu} = yy^2$ or $y^{xu} = y(xu)^2$. Since $y^{xu} = y(y^2x^2)$, the only possibility is $(xu)^2 = y^2x^2$ which is a contradiction. Hence, we must have the second possibility $y^u = yu^2$ and we get $y^{xu} = (yx^2)^u = y(u^2x^2)$ and therefore (because $u^2x^2 = y^2$ is excluded) $x^2u^2 = (xu)^2$ which implies $[u, x] = 1$. In that case $A_1 = \langle x, u \rangle \Omega_1(A)$ is an abelian normal subgroup of G with $|A_1 : \Omega_1(A)| = 4$ which leads to one of the former cases, when we consider a maximal normal abelian subgroup A^* (instead of A) containing A_1 . Our theorem is proved. \square

Theorem 57.4. *Let G be a nonabelian 2-group all of whose minimal nonabelian subgroups are isomorphic to $\mathcal{H}_{16} = \langle a, t \mid a^4 = t^2 = 1, [a, t] = z, z^2 = [a, z] = [t, z] = 1 \rangle$. Then $\Omega_1(G)$ is a self-centralizing elementary abelian subgroup and G is of exponent 4. Moreover, the centralizer of any element of order 4 is abelian of type $(4, 2, \dots, 2)$.*

Proof. Since D_8 is not a subgroup of G , $\Omega_1(G)$ is elementary abelian (of order > 2). We choose a maximal normal abelian subgroup A of G so that $\Omega_1(G) \leq A$. Using Lemma 57.2, we see that all elements in $G - A$ are of order 4 which implies $\Phi(G) \leq A$. By Lemma 57.1, we have also $C_G(\Omega_1(A)) = A$.

Let v be an element of order 4 such that $C_G(v)$ is nonabelian and let $H = \langle a, t \mid a^4 = t^2 = 1, [a, t] = z, z^2 = [a, z] = [t, z] = 1 \rangle$ be a minimal nonabelian subgroup of $C_G(v)$. Assume that $\langle v \rangle \cap H = \{1\}$ so that $\langle H, v \rangle = H \times \langle v \rangle$ is of order 2^6 . Since $(vt)^2 = v^2$, it follows that $\langle vt \rangle \cap H = \{1\}$ and $\langle vt \rangle$ normalizes H . Consider the subgroup $\langle a, vt \rangle$. Since $[a, vt] = [a, t] = z$ and z commutes with a and vt , we have $\langle a, vt \rangle' = \langle z \rangle$ and so $S = \langle a, vt \rangle$ is minimal nonabelian of order 2^5 (since $S \cap H = \langle a, z \rangle \cong C_4 \times C_2$ and S covers $\langle H, v \rangle / H$), a contradiction. Hence we must have $\langle v \rangle \cap H = \langle v^2 \rangle$, where $v^2 \in Z(H)$ and so $v^2 \in \{z, a^2, a^2z\}$. Suppose

that $v^2 = z$ so that $(vt)^2 = z$ and $[a, vt] = z$ which implies that $\langle a, vt \rangle$ is metacyclic minimal nonabelian of order 2^4 , a contradiction. Suppose that $v^2 = a^2$ so that va is an involution and $[va, t] = z \neq 1$, a contradiction. Similarly, if $v^2 = a^2z$, then atv is an involution and $[atv, t] = z \neq 1$, a contradiction. We have proved that for each element v of order 4, $C_G(v)$ is abelian.

Let $x, y \in G$ be such that $x \in G - A$, $[x, y^2] = 1 = [x^2, y]$ and $[x, y] \neq 1$. Then $\langle x, y \rangle \cong \mathcal{H}_{16}$ and so either y or xy is an involution. Indeed, $c = [x, y] \in A$ since G/A is abelian. We get $1 = [x, y^2] = [x, y][x, y]^y$, $1 = [x^2, y] = [x, y]^x[x, y]$, and so $c^x = c^{-1}$, $c^y = c^{-1}$. Suppose $o(c) > 2$ and let c_0 be an element of order 4 in $\langle c \rangle$ so that $c_0^x = (c_0)^{-1} = c_0c_0^2$, $\langle c_0, x \rangle' = \langle c_0^2 \rangle$ and therefore $\langle c_0, x \rangle$ is a metacyclic minimal nonabelian subgroup, a contradiction. Hence, $c = [x, y]$ is an involution commuting with x and y so that $\langle x, y \rangle$ is a minimal nonabelian subgroup isomorphic to \mathcal{H}_{16} .

Suppose that $A \neq \Omega_1(A)$. Take an element $x \in G - A$ and an element y of order 4 in A . Since $C_G(y)$ is abelian, $[x, y] \neq 1$. By Lemma 57.2, x inverts each element in $A/\Omega_1(A)$ and so $[x, y] \in \Omega_1(A)$. We have $[x^2, y] = 1$ and $[x, y^2] = [x, y][x, y]^y = [x, y]^2 = 1$. By the above, $\langle x, y \rangle \cong \mathcal{H}_{16}$ and so xy must be an involution, a contradiction. We have proved that $A = \Omega_1(A)$ and so $\exp(G) = 4$.

For each $a \in G - A$, we have $C_G(a) = \langle a, C_A(a) \rangle$. Suppose that this is false. Let $b \in C_G(a) - (A\langle a \rangle)$ so that $\langle a, b \rangle \cong C_4 \times C_4$ and $\langle a, b \rangle \cap A = \langle a^2, b^2 \rangle \cong E_4$. Indeed, if $a^2 = b^2$, then $ab \in G - A$ and ab is an involution, a contradiction. Set $A_0 = C_A(a)$ so that $A_0 \neq A$ and $A_0 = C_A(b)$ (since $C_G(a)$ and $C_G(b)$ are abelian). Let $t \in A - A_0$ and consider the subgroup $\langle a, bt \rangle$. We have $[a, bt] \neq 1$, $o(bt) = 4$ and since $C_A(bt) = C_A(b) = C_A(a) = A_0$, we have $a^2, (bt)^2 \in A_0$ and therefore $[a, (bt)^2] = [a^2, bt] = 1$. By the above, $\langle a, bt \rangle \cong H_{16}$ which implies that abt ($\in G - A$) is an involution, a contradiction. \square

Theorem 57.5. *Let G be a nonabelian 2-group all of whose minimal nonabelian subgroups are isomorphic to $\mathcal{H}_{32} = \langle a, b \mid a^4 = b^4 = 1, [a, b] = z, z^2 = [a, z] = [b, z] = 1 \rangle$. Then $\Omega_1(G) \leq Z(G)$ and G is of exponent 4 and class 2.*

Proof. In exactly the same way as in the first paragraph of the proof of Theorem 57.3, we show that if A is a maximal normal abelian subgroup of G , then $\Omega_1(G) = \Omega_1(A) \leq Z(G)$, $\Omega_1(A) < A$ and $G - A$ consists of elements of order 4. Suppose that $\exp(A) > 4$. By Lemma 57.2, $|G : A| = 2$ and if $x \in G - A$, then $o(x) = 4$ and x inverts each element in $\Omega_1(A)$. Let $y \in \Omega_1(A)$ with $o(y) = 4$. Then $y^x = y^{-1}$ so that $\langle x, y \rangle$ is metacyclic minimal nonabelian (of order 8 or 16), a contradiction. Hence $\exp(A) = 4$ and so $\Phi(G) \leq \Omega_1(G) \leq Z(G)$. \square

In conclusion we classify the nonabelian 2-groups all of whose A_1 -subgroups are isomorphic to M_{16} .

Theorem 57.6. *Let G be a nonabelian 2-group all of whose minimal nonabelian subgroups are isomorphic to $M_{16} = \langle a, t \mid a^8 = t^2 = 1, a^t = a^5 \rangle$. Then $E = \Omega_1(G)$*

is elementary abelian and if A is a maximal normal abelian subgroup of G containing E , then A is of type $(2^s, 2, \dots, 2)$, $s \geq 2$, $|G : A| \leq 4$, each element x in $G - A$ is of order 8, $|E : C_E(x)| = 2$, x inverts each element in A/E and in $\mathfrak{V}_1(A)$ and we have the following possibilities:

- (a) $s > 2$ in which case $|G : A| = 2$ and $G/E \cong Q_{2^s}$ is generalized quaternion of order 2^s ;
- (b) $s = 2$ in which case either $G \cong M_{16} \times V$ with $\exp(V) \leq 2$ or $G/E \cong Q_8$ and $|G : A| = 4$.

Proof. Let G be a nonabelian 2-group all of whose minimal nonabelian subgroups are isomorphic to M_{16} . Since G does not possess dihedral subgroups, $E = \Omega_1(G)$ is elementary abelian. Let A be a maximal normal abelian subgroup of G containing E so that $E = \Omega_1(A)$. By Lemma 57.1, each element in $G - A$ is of order 4 or 8.

Suppose that $x \in G - A$ and $\exp(x) = 4$. Then $x^2 \in E$ and $\exp(E\langle x \rangle) = 4$. It follows that $E\langle x \rangle$ is abelian. But then $A\langle x \rangle$ is nonabelian and $E \leq Z(A\langle x \rangle)$. This is a contradiction since in this case M_{16} cannot be a subgroup of $A\langle x \rangle$. We have proved that all elements in $G - A$ are of order 8 and so G/A is elementary abelian (G is metabelian) and $\exp(A) \geq 4$.

We want to determine the structure of A . Let x be a fixed element in $G - A$ so that $\exp(x) = 8$, $x^2 \in \Omega_2(A) - E$ and we set $z = x^4$. By Lemma 57.1, there is a subgroup $M \cong M_{16}$ in $A\langle x \rangle$ which contains $\langle x \rangle$ as a subgroup of index 2. Since all eight elements in $M - A$ are of order 8, we have $M \cap A = M \cap \Omega_2(A) \cong C_4 \times C_2$ and $M \cap E \cong E_4$. Let t be an involution $(M \cap E) - \langle z \rangle$ so that $t^x = tz$ and $M' = \langle z \rangle$. Set $b = x^2t$ so that $b^2 = z$ and $b^x = (x^2t)^x = (x^2t)z = bz = b^{-1}$. It follows that each element xs with $s \in A$ is of order 8 and inverts the cyclic subgroup $\langle b \rangle$ of order 4. This forces $\langle xs \rangle \cap \langle b \rangle = \langle z \rangle$. Indeed, if $\langle xs \rangle \cap \langle b \rangle = \{1\}$ ($\langle xs \rangle$ cannot contain $\langle b \rangle$ since xs inverts b), then $\langle b, xs \rangle$ is metacyclic minimal nonabelian of order 2^5 , a contradiction. We compute $(xs)^2 = xsxs = x^2s^x s$ and $z = (xs)^4 = x^4(s^x s)^2 = z(s^x s)^2$ and so $(s^x s)^2 = 1$ and therefore $s^x s = w \in E$. Thus, $s^x = s^{-1}w$ with $w \in E$ which shows that x inverts each element of A/E . Further, $(s^2)^x = (s^x)^2 = (s^{-1}w)^2 = s^{-2}$ which shows that x also inverts each element in $\mathfrak{V}_1(A)$.

Assume that there is an element $a \in \Omega_2(A) - E$ such that $a^2 \neq z$. First suppose that x centralizes a . In that case, $(ab)^x = ab^x = ab^{-1} = (ab)z$ and $(ab)^2 = a^2b^2 = a^2z \neq z$. Hence $\langle ab, x \rangle$ with $\langle ab \rangle \cap \langle x \rangle = \{1\}$ is minimal nonabelian of order 2^5 , a contradiction. Now, suppose that $a^x = a\xi$ with $1 \neq \xi \in E$ so that $[a, x] = \xi$. But $a = a^{x^2} = (a\xi)^x = a^x\xi^x = a\xi\xi^x$ and so $\xi^x = \xi$ which gives $\langle \xi \rangle = \langle a, x \rangle'$. It follows that $\langle a, x \rangle$ is minimal nonabelian of order $\geq 2^5$ because $\langle a \rangle \cap \langle x \rangle = \{1\}$. We have proved that $\Omega_2(A)$ is of type $(4, 2, \dots, 2)$ which forces that A is of type $(2^s, 2, \dots, 2)$, $s \geq 2$.

It is easy to see that $|E : C_E(x)| = 2$. Indeed, set $E_0 = C_E(x)$ and suppose $|E : E_0| \geq 4$. Since x induces on E an involutory automorphism, we know that x centralizes E/E_0 and so $[E, x] \leq E_0$ and $[[E, x]] = |E/E_0|$, where $E_0 \geq \langle z \rangle$. In

that case, there is $e \in E - E_0$ such that $[e, x] \in E_0 - \langle z \rangle$. Then $\langle x, e \rangle' = \langle [e, x] \rangle$ and therefore $\langle x, e \rangle$ is nonmetacyclic minimal nonabelian of order 2^5 , a contradiction. We have proved that $C_E(x)$ is a hyperplane of E for each $x \in G - A$.

First suppose that $s > 2$ or equivalently, $\exp(A) > 4$. We know that each element $x \in G - A$ inverts $\mathfrak{U}_1(A)$ and here $\exp(\mathfrak{U}_1(A)) \geq 4$. This forces $|G : A| = 2$ noting that G/A is elementary abelian. Since $A/E \cong C_{2^{s-1}}$ and $|G/E| = 2^s$, $s \geq 3$, G/E cannot be cyclic (otherwise, an element $y \in G - A$ would be of order 2^{s+1} , contrary to the fact that all elements in $G - A$ are of order 8). On the other hand, $\Omega_2(A)/E$ is a unique subgroup of order 2 in G/E because $\Omega_2(A) = \Omega_2(G)$. We have proved that $G/E \cong Q_{2^s}$.

It remains to consider the case $s = 2$ so that $A = \Omega_2(A) = \Omega_2(G)$ and $|A : E| = 2$ since A is of type $(4, 2, \dots, 2)$. For any $x \in G - A$, $\langle x \rangle$ covers A/E and $\langle x^4 \rangle = \mathfrak{U}_1(A)$. Let $M \cong M_{16}$ be a minimal nonabelian subgroup in $A\langle x \rangle$ containing $\langle x \rangle$, where we have again used Lemma 57.1. Since $|E : C_E(x)| = 2$, we get $A\langle x \rangle = M \times V$ with $V \leq E$. If $A\langle x \rangle = G$, we are done. Suppose that $|G : A| \geq 4$ and we note that G/A is elementary abelian. Hence G/E is not cyclic and the fact that $\Omega_2(G) = A$ shows that A/E is a unique subgroup of order 2 in G/E . It follows that G/E is generalized quaternion. But then $d(G/E) = 2$ and so G/A must be elementary abelian of order 4 which forces that $G/E \cong Q_8$ and $|G : A| = 4$. \square

§58

Non-Dedekindian p -groups all of whose nonnormal subgroups of the same order are conjugate

A non-Dedekindian p -group in which all nonnormal subgroups of the same order are conjugate is termed a *CO-group*. The second author classified CO-groups (see Theorem 58.3); this solves Problem 1261. Below we offer another proof of that nice result which is due to the first author. A p -group G is termed a *CCO-group* if it is not Dedekindian and all its nonnormal cyclic subgroups of the same order are conjugate. Obviously, a CO-group is a CCO-group.

Lemma 58.1. *Let $G = \langle a, b \rangle$ be a minimal nonabelian p -group as in Lemma 65.1 (see also Exercise 1.8a). If all nonnormal cyclic subgroups of G of the same order are conjugate, then $G \cong M_{p^t}$.*

Proof. Write $A = \langle a \rangle$ and $B = \langle b \rangle$. Let $H \not\trianglelefteq G$; then $H \cap G' = \{1\}$ and $H^G = H \times G'$.

Let $G = \langle a, b \mid a^{p^m} = b^{p^n} = c^p = 1, [a, b] = c, [a, c] = [b, c] = 1 \rangle$ and assume that $m \geq n$. Let $\Omega_n(A) = \langle x \rangle$. Then B and $\langle bx \rangle$ of the same order are neither G -invariant nor conjugate since $\Omega_1(B_G) \neq \Omega_1(\langle bx \rangle_G)$ so G is not a CCO-group.

Let $G = \langle a, b \mid a^{p^m} = b^{p^n} = 1, a^b = a^{1+p^{m-1}} \rangle$. If $n = 1$, then $G \cong M_{p^{m+1}}$ satisfies the condition. Now let $n > 1$. If $n \leq m$, set $\Omega_n(A) = \langle x \rangle$; then B and $\langle bx \rangle$ of the same order p^n are neither G -invariant nor conjugate. Now assume that $n > m$. Then B and $\langle ab \rangle$ of the same order p^n are neither G -invariant nor conjugate. Indeed, $(ab)^{p^m} = b^{p^m}$ so $o(ab) = p^n$, $\langle ab \rangle \cap A = \{1\}$, and we conclude that $\langle ab \rangle$ is not normal in G (otherwise, $G = \langle a, ab \rangle$ is abelian). Since $\Omega_1(\langle ab \rangle_G) \neq \Omega_1(B_G)$, $\langle ab \rangle$ and B are not conjugate in G so G is not a CCO-group. \square

Lemma 58.2. *If a p -group G is a CCO-group and $|G'| = p$, then $G \cong M_{p^t}$.*

Proof. In view of Lemma 58.1, one may assume that G has a proper minimal nonabelian subgroup, say B ; then $B \triangleleft G$ since $B' = G'$. In that case, $G = B * C$ where $C = C_G(B)$ (Lemma 4.2) and we conclude that B is either Dedekindian or CCO-group; in the first case $B \cong Q_8$, in the second case $B \cong M_{p^t}$ (Lemma 58.1). The size of every conjugate class of non- G -invariant cyclic subgroups equals p .

(i) Let $B = \langle x, y \mid x^4 = 1, y^2 = x^2, x^y = x^3 \rangle \cong Q_8$. We get $\exp(C) > 2$ since G is not Dedekindian. Let $L = \langle l \rangle \leq C$ be cyclic of order 4. Write $H = B * L$; then $H \triangleleft G$. If $B \cap L = Z(B)$, then H has exactly $6 > 2$ nonnormal subgroups of order 2 so they are not conjugate in G , a contradiction. Thus, $B \cap L = \{1\}$; then $H = B \times L$ has $3 > 2$ distinct nonnormal cyclic subgroups $\langle xl \rangle, \langle yl \rangle, \langle xyl \rangle$ of the same order 4 so they are not conjugate, a contradiction. Thus, B has no subgroups isomorphic to Q_8 .

(ii) Now let $B = \langle u, v \mid u^{p^{t-1}} = v^p = 1, u^v = u^{1+p^{t-2}} \rangle \cong M_{p^t}$. Assume that $X = \langle x \rangle < G$ of order p is such that $X \not\leq B$; then X is not conjugate with $\langle v \rangle$ so $X \triangleleft G$ and $F = B \times X$ has exactly $p^2 > p$ noncentral so non- G -invariant subgroups of order p ; then G is not a CO-group, a contradiction. Thus, $\Omega_1(G) = \Omega_1(B) \cong E_{p^2}$ so C has exactly one subgroup of order p ; in that case C is cyclic, by (i). Then there is a cyclic $W = \langle w \rangle \leq C$ such that $W \not\leq B$ and $w^p \in Z(B)$. Let $A < B$ be cyclic of index p . Then AW is noncyclic abelian with cyclic subgroup A of index p so, by basic theorem on abelian groups, $AW = A \times Y$, where $|Y| = p$ and $Y \not\leq B$ has order p , contrary to what has just been proved. \square

Theorem 58.3 (Janko). *If a p -group G is a CO-group, then $G \cong M_{p^t}$.*

Proof (Berkovich). We use induction on $|G|$. In view of Lemma 58.2, one may assume that $|G'| > p$. By Theorem 1.23, there is $K = G' \cap Z(G)$ of order p such that G/K is non-Dedekindian. Since G/K is a CO-group, we get $G/K \cong M_{p^t}$, by induction. Since $K < G' \leq \Phi(G)$, we get $d(G) = d(G/K) = 2$. Let A/K and B/K be two distinct cyclic subgroups of index p in G/K ; then A and B are abelian maximal subgroups of G . It follows that $A \cap B = Z(G)$ so $|G'| = p$ (Lemma 1.1), contrary to the assumption. \square

Corollary 58.4. *Suppose that all nonnormal subgroups of the same order of a nilpotent non-Dedekindian group G are conjugate. Then $G = P \times C$, where $P \in \text{Syl}_p(G)$ is non-Dedekindian and $P \cong M_{p^n}$, C is cyclic.*

Theorem 58.5 (Berkovich). *If G is a non-Dedekindian p -group all of whose nonnormal cyclic subgroups of the same order belong to the same conjugate class of size p , then $G \cong M_{p^t}$.*

Proof. We use induction on $|G|$. In view of Lemma 58.1, one may assume that $|G'| > p$.

Assume that G is a 2-group of maximal class. Then $|G| > 8$. If $G \cong Q_{2^n}$ $n > 3$, then G has > 2 nonnormal cyclic subgroups of order 4. If $G \not\cong Q_{2^n}$, then G has > 2 nonnormal subgroups of order 2. Thus, G is not a 2-group of maximal class.

By Theorem 1.23, there is in $G' \cap Z(G)$ a subgroup R of order p such that G/R is non-Dedekindian. Let $X/R < G/R$ be nonnormal cyclic. Assume that X is noncyclic. Then $X = X_i \times R$, where X_i is cyclic of index p in X , $i = 1, \dots, p$. The subgroup X_i is nonnormal in G (otherwise, $X = X_i R \triangleleft G$). By hypothesis, the

subgroups X_1, \dots, X_p form the conjugate class in G so $X = X_1 \dots X_p \triangleleft G$, a contradiction. Thus, X must be cyclic. By hypothesis, there are in G exactly p nonnormal cyclic subgroups of order $|X|$. Therefore, there are exactly p nonnormal cyclic subgroups of order $|X/R|$ in G/R so G/R satisfies the hypothesis. By induction, the non-Dedekindian group $G/R \cong M_{p^n}$. Then G/R has two distinct cyclic subgroups A/R and B/R of index p . In that case, A and B are two distinct abelian maximal subgroups of G so $A \cap B = Z(G)$. Then $|G'| = \frac{1}{p}|G : Z(G)| = p$ (Lemma 1.1), contrary to the assumption. \square

p -groups with few nonnormal subgroups

By Lemma 58.1, if all nonnormal subgroups of a minimal nonabelian p -group G are conjugate, then $G \cong M_{p^t}$. Of course, Theorem 59.1 follows from Theorem 58.3.

Theorem 59.1 ([Sch3]). *If all nonnormal subgroups of a p -group G are conjugate, then $G \cong M_{p^{n+1}}$.*

Proof (compare with [Sch3]). Let $H < G$ be nonnormal; then H is cyclic since it is not generated by their (G -invariant) maximal subgroups. Set $|H| = p^s$. If $s = 1$, then $G \cong M_{p^{n+1}}$ (Theorem 1.23). Now we assume that $s > 1$. We use induction on $|G|$. We have $R = \Omega_1(H) \triangleleft G$. By induction, $G/R \cong M_{p^n}$; then $|H/R| = p$. Since $R \leq \Phi(H) < \Phi(G)$, we get $d(G) = d(G/R) = 2$. Let U/R and V/R be distinct cyclic subgroups of index p in G/R ; then U and V are abelian subgroups of index p in G so $\Phi(G) = U \cap V = Z(G)$ and G is minimal nonabelian. Then, by the remark preceding the theorem, $G \cong M_{p^{n+1}}$. \square

Given $m > 1$, let $\mathcal{H}_{2,m} = \langle a, b \mid a^{p^2} = b^{p^m} = 1, a^b = a^{1+p} \rangle$ be a metacyclic minimal nonabelian group of order p^{2+m} .

We suggest to the reader, using the above approach, to prove the following fairly deep

Theorem 59.2 ([Sch4]). *If a group G is nilpotent and has exactly two conjugate classes of non-invariant subgroups, then one of the following holds:*

- (a) $G \cong D_8$.
- (b) $G \cong Q_{16}$.
- (c) $p = 2$ and $G \cong \mathcal{H}_{2,m}$.
- (d) $G \cong M_{p^n} \times C_q$, where a prime $q \neq p$.

Note that the proof presented in [Sch4], is not full. For the proof of this theorem, see [Ber26].

§60

The structure of the Burnside group of order 2^{12}

I. N. Sanov [Sano] has proved that each finitely generated group of exponent 4 is finite. W. Burnside [Bur4] has shown that each two-generated group of exponent 4 is a homomorphic image of a certain group $G = B(4, 2)$ of order at most 2^{12} which we call the Burnside group.

In this section, written by the second author, we determine completely the structure of the Burnside group G by presenting this group in a very convenient form from which each structural question about that group can be easily answered which is important for applications (Theorem D). For example, we show that $\Phi(G) = \Omega_1(G)$ is a special 2-group of order 2^{10} with $Z(\Phi(G)) \cong E_{25}$. The group G has exactly 12 maximal elementary abelian subgroups. Each of them is of order 2^6 and the intersection of any two of them is equal $Z(\Phi(G))$. If M, N, K are the maximal subgroups of G , then $d(M) = d(N) = d(K) = 3$, $cl(M) = cl(N) = cl(K) = 4$ and $M' = N' = K'$ is abelian of order 2^7 and type $(4, 4, 2, 2, 2)$. The subgroup G' is of order 2^8 and class 2, $d(G') = 5$, $\Omega_1(G') = Z(\Phi(G)) = Z(G')$, $G'' \cong E_4$, $G'' \leq Z(G)$ and $Z(G) \cong E_8$. Next, $|\text{Aut}(G)| = 2^{21} \cdot 3$ (Theorem C).

Theorem A (see [Hup, p. 300]). *Let G be a group of exponent 4 generated with an element v of order 4 and an involution t . Then $G' = \langle [v^{-1}, t], [v, t] \rangle$ is abelian of order ≤ 8 and so $|G| \leq 2^6$.*

Proof. We have $(tv)^3 = (tv)^{-1} = v^{-1}t$ and $(tv^{-1})^3 = (tv^{-1})^{-1} = vt$ hence

$$\begin{aligned}[v, t][v^{-1}, t] &= (v^{-1}tv)(vtv^{-1}t) = v^{-1}(tv)^3v^2t \\ &= v^{-1}(v^{-1}t)v^2t = (v^2t)^2 = [v^2, t], \\ [v^{-1}, t][v, t] &= (vtv^{-1}t)(v^{-1}tv) = v(tv^{-1})^3v^2t \\ &= v(vt)v^2t = (v^2t)^2 = [v^2, t],\end{aligned}$$

and so:

$$(1) \quad [v, t][v^{-1}, t] = [v^{-1}, t][v, t] = [v^2, t] = (v^2t)^2.$$

Hence the subgroup $P = \langle [v^{-1}, t], [v, t] \rangle$ is abelian of exponent ≤ 4 and order ≤ 8 since $[v^{-1}, t][v, t]$ is of order ≤ 2 and so P cannot be isomorphic to $C_4 \times C_4$. Also, $P \leq G'$ and it is easy to see that P is normal in G . Indeed, from $1 = [v^i, t^2] =$

$[v^i, t][v^i, t]^t$ follows $[v^i, t]^t = [v^i, t]^{-1}$ for each integer $i \pmod{4}$. From $1 = [v^{-1}v, t] = [v^{-1}, t]^v[v, t]$ follows $[v^{-1}, t]^v = [v, t]^{-1}$ and from $[v^2, t] = [v, t]^v[v, t]$ follows (using (1)) $[v, t]^v = [v^2, t][v, t]^{-1} = [v^{-1}, t]$. Since G/P is abelian, we get $G' = \langle [v^{-1}, t], [v, t] \rangle$ and so $|G| \leq 2^6$. \square

Theorem B (see [Hup, p. 300]). Let $G = \langle a, b \rangle$ be a group of exponent 4 such that $[a^2, b^2] = 1$. Then $|G| \leq 2^9$ and $\langle a^2 \rangle^G = \langle a^2, (a^2)^{b^{-1}}, (a^2)^{b^{-1}a^{-1}} \rangle$ is elementary abelian of order ≤ 8 (where $(a^2)^{b^{-1}a^{-1}b^{-1}} = a^2(a^2)^{b^{-1}}(a^2)^{b^{-1}a^{-1}}$). Similarly, $\langle b^2 \rangle^G = \langle b^2, (b^2)^{a^{-1}}, (b^2)^{a^{-1}b^{-1}} \rangle$ is elementary abelian of order ≤ 8 (where $(b^2)^{a^{-1}b^{-1}a^{-1}} = b^2(b^2)^{a^{-1}}(b^2)^{a^{-1}b^{-1}}$).

Proof. Since $[a^2, b^2] = (a^2b^2)^2 = 1$, we get $a^2b^2a^2b^2 = 1$ and $a^2 = b^2a^2b^2$ and so

$$(*) \quad ba^2b^3 = b(b^2a^2b^2)b^3 = b^3a^2b.$$

Now,

$$\begin{aligned} (a^2(a^2)^{b^{-1}})^2 &= (a^2ba^2b^3)^2 = a^2(ba^2b^3) \cdot (a^2ba^2b^3) \\ &= a^2b^3a^2b \cdot a^2ba^2b \cdot b^2 = a^2b^3(a^3b)^3b^2 = a^2b^3(a^2b)^{-1}b^2 \\ &= a^2b^3b^{-1}a^2b^2 = (a^2b^2)^2 = 1, \end{aligned}$$

which implies $[a^2, (a^2)^{b^{-1}}] = 1$ and so also $[a^2, (a^2)^{b^{-1}a^{-1}}] = 1$.

Further, using (*), $baba = a^3b^3a^3b^3$ (which is a consequence of $(ba)^4 = 1$) and $(a^3b)^3 = (a^3b)^{-1} = b^3a$, we get:

$$\begin{aligned} (a^2)^{b^{-1}a^{-1}b^{-1}} &= baba \cdot ab^3a^3b^3 = a^3b^3a^3b^3ab^3a^3b^3 = a^2(ab^3a^3b^3)^2 \\ &= a^2((bab)^3)^{-1})^2 = a^2(baba^3)^2 = a^2 \cdot baba^3 \cdot baba^3 \\ &= a^2b(a^2a^3)ba^3b(a^3a^2)ba^3 = a^2ba^2(a^3b)^3b^3a^2ba^3 \\ &= a^2ba^2(b^3a)b^3a^2ba^3 = a^2ba^2b^3a(b^3a^2b)a^3 \\ &= a^2(a^2)^{b^{-1}} \cdot a(ba^2b^3)a^3 = a^2(a^2)^{b^{-1}}(a^2)^{b^{-1}a^{-1}}. \end{aligned}$$

We have obtained $(a^2)^{b^{-1}a^{-1}b^{-1}} = a^2(a^2)^{b^{-1}}(a^2)^{b^{-1}a^{-1}}$ and so each element conjugate to a^2 is contained in $\langle a^2, (a^2)^{b^{-1}}, (a^2)^{b^{-1}a^{-1}} \rangle$ which gives $\langle a^2 \rangle^G = \langle a^2, (a^2)^{b^{-1}}, (a^2)^{b^{-1}a^{-1}} \rangle$. Further, a^2 commutes with $(a^2)^{b^{-1}}$ and $(a^2)^{b^{-1}a^{-1}}$ and so $a^2 \in Z(\langle a^2 \rangle^G)$. But then $(a^2)^{b^{-1}}$ and $(a^2)^{b^{-1}a^{-1}}$ are also contained in $Z(\langle a^2 \rangle^G)$ and so $\langle a^2 \rangle^G$ is elementary abelian of order ≤ 8 . By Theorem A, $G/\langle a^2 \rangle^G$ is of order $\leq 2^6$ and so $|G| \leq 2^9$. The second half of the theorem is obtained by interchanging a and b . \square

Theorem C. Let G be the group given with: $G = \langle a, b \mid a^4 = b^4 = (ab)^4 = (a^2b)^4 = (ab^2)^4 = (a^{-1}b)^4 = (a^2b^2)^4 = (b^a b)^4 = (a^b a)^4 = 1 \rangle$. Then G is of

order 2^{12} and exponent 4 and so G is the Burnside group. The group G has exactly $k(G) = 88$ conjugate classes. The automorphism group of G is of order $2^{21} \cdot 3$.

Proof. This theorem (apart from the last statement) is proved by using a computer (W. Lempken at the University of Essen).

We may define our group G also in the form: $G = \langle a, b \mid x^4 = 1 \text{ for all } x \in G \rangle$. Then each map α of $\{a, b\}$ into G such that $\langle a^\alpha, b^\alpha \rangle = G$ induces an automorphism of G . Hence $|\text{Aut}(G)| = |\text{Aut}(G/\Phi(G))||\Phi(G)|^2 = 6 \cdot 2^{20}$. \square

The Burnside group G is given in Theorem C in terms of generators a, b and 9 relations. However, from this presentation it is extremely difficult to pin down the structure of all subgroups and factor-groups of G . Therefore we give in the next theorem the group G in terms of 12 generators and 78 relations which will be very convenient to answer any structural question about that group. We shall also deduce many important properties of the Burnside group G by using this new presentation. In the sequel, we use from Theorem C only the fact that the Burnside group G is of order 2^{12} .

Theorem D (Complete determination of the structure of the Burnside group). *Let $G = \langle a, b \rangle$ be the Burnside group of order 2^{12} as defined in Theorem C. Then G has the following properties:*

- (a) $\Phi(G) = \Omega_1(G)$ is a special group of order 2^{10} with $Z(\Phi(G)) = (\Phi(G))' = \Phi(\Phi(G)) \cong E_{25}$.
- (b) If M, N, K are maximal subgroups of G , then they are of class 4 and they are generated by three elements but not by two elements. In addition, $M' = N' = K'$ is abelian of order 2^7 and type $(4, 4, 2, 2, 2)$, $Z(G) \cong E_8$, $Z(G) = Z(M) < Z(\Phi(G))$, $K_3(M) \cong E_{24}$, $K_3(M) < Z(\Phi(G))$, $K_4(M) \cong E_4$, $K_4(M) < Z(G)$, and an automorphism of order 3 of G acts transitively on $\{M, N, K\}$.
- (c) The commutator group G' is of order 2^8 and class 2, $G/G' \cong C_4 \times C_4$, $\Omega_1(G') = Z(\Phi(G)) = Z(G')$, $\Phi(G') = Z(G)$, $G'' \leq Z(G)$, $G'' \cong E_4$, and $M' = K_3(G)$ is an abelian maximal subgroup of G' . In addition, $K_4(G) = Z(\Phi(G))$, $E_4 \cong K_5(G) = K_4(M) \leq Z(G)$, where M is maximal in G , and so G is of class 5. Finally, $Z_2(G) = Z(\Phi(G)) \cong E_{25}$, $Z_3(G) = K_3(G) = M'$ (abelian of type $(4, 4, 2, 2, 2)$), and $Z_4(G) = \Phi(G)$.
- (d) The group G has exactly 12 maximal elementary abelian subgroups. Each of them is of order 2^6 and the intersection of any two of them is equal $Z(\Phi(G)) \cong E_{25}$. Hence the number of involutions in G is $31 + 12 \cdot 32 = 415$ and each abelian subgroup of G is of rank ≤ 6 .
- (e) The special group $\Phi(G) = \Omega_1(G)$ is generated with five involutions d, e, m, n, y and we may set $Z(\Phi(G)) = \langle c, g, h, i, j \rangle \cong E_{25}$ so that:

$$\begin{aligned} [d, e] &= ch, & [d, m] &= c, & [d, n] &= g, & [d, y] &= icgh, & [e, m] &= h, \\ [e, n] &= cgh, & [e, y] &= ig, & [m, n] &= cg, & [m, y] &= jc, & [n, y] &= jg. \end{aligned}$$

We have $G = \langle a, b \rangle$ with $a^2 = d, b^2 = m, (a^{-1}b^{-1})^2 = y$, where the action of a^{-1} and b^{-1} on $\Phi(G)$ is given with:

$$\begin{aligned} c^{a^{-1}} &= g, & g^{a^{-1}} &= c, & h^{a^{-1}} &= cgh, & i^{a^{-1}} &= ich, & j^{a^{-1}} &= jgh, \\ d^{a^{-1}} &= d, & e^{a^{-1}} &= ei, & m^{a^{-1}} &= n, & n^{a^{-1}} &= mc, & y^{a^{-1}} &= demnychij, \\ c^{b^{-1}} &= h, & g^{b^{-1}} &= cgh, & h^{b^{-1}} &= c, & i^{b^{-1}} &= igh, & j^{b^{-1}} &= jcg, \\ a^{b^{-1}} &= e, & e^{b^{-1}} &= dc, & m^{b^{-1}} &= m, & n^{b^{-1}} &= nj, & y^{b^{-1}} &= demnygi. \end{aligned}$$

We have determined completely the structure of our group G . We have here $M = \Phi(G)\langle a \rangle$, $N = \Phi(G)\langle b \rangle$, $K = \Phi(G)\langle a^{-1}b^{-1} \rangle$, where $M' = N' = K' = K_3(G) = Z(\Phi(G))\langle de, mn \rangle$, $K_3(M) = \langle c, g, h, i \rangle$, $K_5(G) = K_4(M) = \langle cg, ch \rangle$, $G' = M'\langle emy \rangle$, $G'' = \langle cg, ch \rangle$, and $Z(G) = Z(M) = \langle cg, ch, cij \rangle \cong E_8$. Also, $\langle c \rangle^G = \langle c, g, h \rangle \cong E_8$, $\langle a^2 \rangle^G = \langle d, e, i, g, h \rangle$ and $\langle b^2 \rangle^G = \langle m, n, j, g, h \rangle$ are subgroups of orders 2^6 which have its commutator subgroup of order 2.

(f) The factor-group $H = G/Z(\Phi(G))$ (of order 2^7) is the group of maximal possible order having the exponent 4, being generated with two elements, and having the property that the squares of any two elements commute. We have $\Phi(H) = \Omega_1(H) \cong E_{25}$, $Z(H) \cong E_4$, $Z(H) < H' \cong E_{23}$, and $[H, H'] = Z(H)$ so that H is of class 3. The class number $k(H)$ of H is 26.

Proof. Let $G = \langle a, b \rangle$ be the Burnside group (as defined in Theorem C) so that G is the free group of exponent 4 generated with two elements. We have $|G| = 2^{12}$ and we want to determine the exact structure of G .

If $[a^2, b^2] = 1$, then by Theorem B we get $|G| \leq 2^9$, a contradiction. Hence $[a^2, b^2] = (a^2b^2)^2 = c$ is an involution and $\langle a^2, b^2 \rangle \cong D_8$ with $Z(\langle a^2, b^2 \rangle) = \langle c \rangle$ so that a and b are elements of order 4 and c commutes with a^2 and b^2 .

We first determine the structure of $\langle c \rangle^G$. We set $h = c^{b^{-1}}$ and claim that $[c, h] = 1$. Indeed, since $b^2 = b^3b^3$ and $(b^3a^2)^3 = (b^3a^2)^{-1} = a^2b$, we get:

$$\begin{aligned} s_1 &= ch = cc^{b^{-1}} = (a^2b^2)^2b(a^2b^2)^2b^3 = a^2b^2a^2b^2 \cdot ba^2b^2a^2b^2b^3 \\ &= a^2(b^3b^3)a^2b^3a^2(b^3b^3)a^2b = a^2b^3(b^3a^2)(b^3a^2)(b^3a^2)a^2b^3a^2b \\ &= a^2b^3 \cdot a^2b \cdot a^2b^3a^2b = (a^2b^3a^2b)^2 \end{aligned}$$

and so

$$(2) \quad s_1 = ch = (a^2b^3a^2b)^2 = (a^2(a^2)^b)^2.$$

Hence $(ch)^2 = 1$ and so $[c, h] = 1$. Also, $s_1^{b^{-1}} = (cc^{b^{-1}})^{b^{-1}} = c^{b^{-1}}c^{b^2} = c^{b^{-1}}c = hc = ch = s_1$, and so s_1 commutes with b .

It is possible to show that s_1 also commutes with a . Using (2),

$$\begin{aligned} a^2b^3ab^3a^2 &= a(ab^3 \cdot ab^3 \cdot ab^3)ba = a(ab^3)^3ba = a(ab^3)^{-1}ba = aba^3ba, \\ (a^3bab)^2 &= (b^3a^3b^3a)^{-2} = (b^3a^3b^3a)^2, \\ b^3a^3b^3a^3b^3 &= (b^3a^3)^3a = (b^3a^3)^{-1}a = aba. \end{aligned}$$

we get (noting that $a^2 = a^3a^3$):

$$\begin{aligned} s_1s_1^{a^{-1}b} &= a^2b^3a^2b \cdot a^2b^3(a^2b \cdot b^3a \cdot a^2)b^3a^2b \cdot a^2b^3a^2b \cdot a^3b \\ &= a^2b^3a^2b(a^2b^3ab^3a^2)ba^2b^3a^2ba^3b \\ &= a^2b^3(a^2b \cdot aba^3ba \cdot b)a^2b^3a^2ba^3b \\ &= a^2b^3a^3(a^3bab)^2a^2b^3a^2ba^3b \\ &= a^2b^3a^3(b^3a^3b^3a \cdot b^3a^3b^3a)a^2b^3a^2ba^3b \\ &= a^2(b^3a^3b^3a^3b^3 \cdot a \cdot b^3a^3b^3a^3b^3)a^2ba^3b \\ &= a^2 \cdot aba \cdot a \cdot aba \cdot a^2ba^3b = (a^3b)^4 = 1. \end{aligned}$$

Hence s_1 also commutes with $a^{-1}b$ which implies that $s_1 = ch = cc^{b^{-1}}$ is contained in $Z(G)$. Applying the automorphism α which interchanges a and b (noting that $c^\alpha = [b^2, a^2] = [a^2, b^2] = c$), we get $[c, c^{a^{-1}}] = 1$ and $s_2 = cc^{a^{-1}} \in Z(G)$. We set $c^{a^{-1}} = g$ so that $\langle ch, cg \rangle \leq Z(G)$, where $\langle cg, ch \rangle$ is elementary abelian of order ≤ 4 . Since c commutes with h and g , we get $ch \cdot cg = hg$ and so $(hg)^2 = 1$ and therefore h also commutes with g and $\langle c, g, h \rangle$ is elementary abelian of order ≤ 8 .

We have

$$\begin{aligned} h^{b^{-1}} &= c^{b^2} = c, & g^{a^{-1}} &= c^{a^2} = c, \\ h^{a^{-1}} &= (c \cdot ch)^{a^{-1}} = c^{a^{-1}}ch = gch = cgh, \\ g^{b^{-1}} &= (c \cdot cg)^{b^{-1}} = c^{b^{-1}}cg = hcg = cgh, \end{aligned}$$

which implies that $\langle c, g, h \rangle$ is a normal subgroup of G and so $\langle c, g, h \rangle = \langle c \rangle^G$. By Theorem B, $G/\langle c \rangle^G$ is of order $\leq 2^9$. Since $|G| = 2^{12}$, we have $\langle c \rangle^G \cong E_8$ and $G/\langle c \rangle^G$ is of order 2^9 . Also, $\langle cg, ch \rangle \cong E_4$ and $\langle cg, ch \rangle \leq Z(G)$. We have also determined the action of a and b on $\langle c, g, h \rangle \cong E_8$.

We determine now the structure of $\langle a^2 \rangle^G$. Set $a^2 = d$, $e = (a^2)^{b^{-1}} = d^{b^{-1}}$, $f = (a^2)^{b^{-1}a^{-1}} = e^{a^{-1}}$ and $S = \langle c, g, h \rangle \langle d, e, f \rangle$. By Theorem B, $S/\langle c, g, h \rangle$ is a normal elementary abelian subgroup of order ≤ 8 of $G/\langle c, g, h \rangle$ with $\langle a^2 \rangle^G \leq S$. By Theorem A, $|G/S| \leq 2^6$. Since $G/\langle c, g, h \rangle$ is of order 2^9 , we have $S/\langle c, g, h \rangle \cong E_8$ and $|G/S| = 2^6$. We note that $\langle s_1, s_2 \rangle$ is a maximal subgroup of $\langle c, g, h \rangle$ and $\langle s_1, s_2 \rangle \cong Z(G)$.

We know that $a^2 = d$ centralizes c and so d centralizes $\langle c, s_1, s_2 \rangle = \langle c \rangle^G$. From $[c, a^2] = 1$ follows $[c^{b^{-1}}, (a^2)^{b^{-1}}] = 1$ and so $[h, e] = 1$ which gives that e centralizes $\langle h, s_1, s_2 \rangle = \langle c \rangle^G$. From $[c, e] = 1$ follows $[c^{a^{-1}}, e^{a^{-1}}] = 1$ and so $[g, f] = 1$ which gives that f centralizes $\langle g, s_1, s_2 \rangle = \langle c \rangle^G$. We have proved that $\langle c, g, h \rangle \leq Z(S)$ and so S is of class ≤ 2 .

From (2) follows $s_1 = [a^2, (a^2)^b]$ and conjugating this relation with b^{-1} gives $s_1 = [(a^2)^{b^{-1}}, a^2]$ so that (since $s_1 = ch$ is an involution) $[e, d] = [d, e] = s_1 = ch$. Conjugating the last relation with a^{-1} we get $[e^{a^{-1}}, d] = s_1$ and so $[f, d] = [d, f] = ch$. By Theorem B, $f^{b^{-1}} = defl$ for some $l \in \langle c, g, h \rangle$. From $[d, f] = s_1$ follows conjugating with b^{-1} :

$$[d^{b^{-1}}, f^{b^{-1}}] = s_1 \quad \text{and so} \quad [e, defl] = [e, d][e, f] = s_1,$$

which implies $s_1[e, f] = s_1$ and $[e, f] = 1$. We get $[d, ef] = [d, e][d, f] = s_1s_1 = 1$ and so $ef \in Z(\langle d, e, f \rangle)$ which gives:

$$\begin{aligned} \langle d, e, f \rangle &= \langle ef \rangle \times \langle d, e \rangle \cong C_2 \times D_8 && \text{with} && \langle d, e, f \rangle' = \langle s_1 \rangle, \\ S &= \langle c, g, h \rangle * \langle d, e, f \rangle, && \text{where} && \langle c, g, h \rangle \cap \langle d, e, f \rangle = \langle s_1 \rangle, \end{aligned}$$

so that $S' = \langle s_1 \rangle$ and $Z(S) = \langle c, g, h, ef \rangle \cong E_{24}$.

It remains to show that $\langle a^2 \rangle^G = S$. For that purpose we have to determine exactly the element $f^{b^{-1}}$. First we note that c commutes with a^2 and b^2 . From $[a^2, b^2] = c$ follows $a^2b^2a^2b^2 = c$ and $a^2 = cb^2a^2b^2$ and so

$$ba^2b^3 = b \cdot cb^2a^2b^2 \cdot b^3 = (bcm)(b \cdot b^2a^2b^2 \cdot b^3) = c^{b^{-1}}(b^3a^2b),$$

which gives:

$$(**) \quad ba^2b^3 = h(b^3a^2b).$$

We compute:

$$f^{b^{-1}} = (a^2)^{b^{-1}a^{-1}b^{-1}} = babab^3a^3b^3$$

(using $baba = a^3b^3a^3b^3$ which follows from $(bab)(bab) = 1$)

$$\begin{aligned} &= a^3b^3a^3b^3 \cdot a \cdot b^3a^3b^3 = a^2(ab^3a^3b^3)(ab^3a^3b^3) \\ &= a^2(ab^3a^3b^3)^2 = a^2(baba^3)^{-2} = a^2(baba^3)^2 \\ &= a^2baba^3baba^3 = a^2b(a^2a^3)ba^3b(a^3a^2)ba^3 \\ &= a^2ba^2(a^3b)(a^3b)b^3a^2ba^3 \end{aligned}$$

(since $(a^3b)^3 = (a^3b)^{-1} = b^3a$ and using (**))

$$\begin{aligned} &= a^2ba^2 \cdot b^3a \cdot (b^3a^2b)a^3 = a^2(ba^2b^3)a \cdot hba^2b^3a^3 \\ &= a^2(ba^2b^3)(aha^3)(ab \cdot a^2 \cdot b^3a^3) \\ &= a^2(a^2)^{b^{-1}}h^{a^{-1}}(a^2)^{b^{-1}a^{-1}} = deh^{a^{-1}}f = def \cdot cgh, \end{aligned}$$

where we have used $h^{a^{-1}} = cgh$ (which was proved before) and $cgh \in Z(S)$.

We have obtained the desired relation $f^{b^{-1}} = defcgh$. We compute $f^{a^{-1}} = e^{a^2} = e^d = e[e, d] = ech$ and so

$$f^{b^{-1}a^{-1}} = (defcgh)^{a^{-1}} = df(ech)gc(cgh) = dfec = defc.$$

Now, $\langle d = a^2, e, f \rangle \leq \langle a^2 \rangle^G$ and so $[d, e] = ch \in \langle a^2 \rangle^G$. From $f^{b^{-1}} = def \cdot cgh$ follows that $cgh \in \langle a^2 \rangle^G$ and from $f^{b^{-1}a^{-1}} = def \cdot c$ follows that $c \in \langle a^2 \rangle^G$. Hence $\langle c, g, h \rangle \leq \langle a^2 \rangle^G$ and so $S = \langle d, e, f \rangle \langle c, g, h \rangle = \langle a^2 \rangle^G$.

Let α be the automorphism of order 2 of G such that $a^\alpha = b$ and $b^\alpha = a$. Note that $c^\alpha = [b^2, a^2] = [a^2, b^2] = c$ and $g^\alpha = h$, $h^\alpha = g$ so that $(\langle c \rangle^G)^\alpha = \langle c \rangle^G = \langle c, g, h \rangle$. Set $\langle b^2 \rangle^G = T$ so that $T = S^\alpha$, $|T| = 2^6$, $T > \langle c, g, h \rangle$, $T/\langle c, g, h \rangle \cong E_8$. We have $U = ST = \langle a^2, b^2 \rangle^G$ and G/U is generated with two involutions and so $|G/U| \leq 2^3$. Since $|U| \leq 2^9$, we must have $|G/U| = 2^3$ and then $|U| = 2^9$, $S \cap T = \langle c, g, h \rangle$, and $G/U \cong D_8$. Set $b^2 = m$, $(b^2)^{a^{-1}} = n$, $(b^2)^{a^{-1}b^{-1}} = p$ so that $m = d^\alpha$, $n = e^\alpha$, $p = f^\alpha$ and α transports the relations for S into the relations for T . We get $\langle m, n, p \rangle = \langle np \rangle \times \langle m, n \rangle \cong C_2 \times D_8$, where $[n, p] = 1$, $[m, n] = [m, p] = s_2 = cg$ and $T = \langle m, n, p \rangle * \langle c, g, h \rangle$ with $\langle m, n, p \rangle \cap \langle c, g, h \rangle = \langle s_2 \rangle$, $Z(T) = \langle c, g, h, np \rangle \cong Z_{24}$, $T' = \langle s_2 \rangle$. Also, from $f^{b^{-1}} = defcgh$ follows $p^{a^{-1}} = mnpcgh$.

Since $\langle c, g, h \rangle \leq Z(S)$ and $\langle c, g, h \rangle \leq Z(T)$, we have $\langle c, g, h \rangle \leq Z(U)$. But $\Phi(U) \leq S \cap T = \langle c, g, h \rangle$ (noting that $U/S \cong U/T \cong E_8$) and so U is of class 2. We shall determine completely the structure of $U = ST = \langle a^2, b^2 \rangle^G$. This is done by the following computation (using all the previous relations):

$$f^{a^{-1}} = (a^2)^{b^{-1}a^2} = e^{a^2} = e^d = e[e, d] = ech,$$

$$d^m = (a^2)^{b^2} = a^2c = dc,$$

$$f^m = f^{b^2} = (f^{b^{-1}})^{b^{-1}} = (defcgh)^{b^{-1}} = e \cdot dc \cdot defcgh \cdot h \cdot cgh \cdot c = fh,$$

$$\begin{aligned} e^n &= e^{ab^2a^{-1}} = (e^{a^{-1}})^{a^2b^2a^{-1}} = (f^d)^{ma^{-1}} = (fch)^{ma^{-1}} \\ &= (fh \cdot c \cdot h)^{a^{-1}} = (fc)^{a^{-1}} = echg, \end{aligned}$$

$$d^n = d^{m^{a^{-1}}} = d^{ama^{-1}} = (a^2)^{ma^{-1}} = d^{ma^{-1}} = (dc)^{a^{-1}} = dc^{a^{-1}} = dg,$$

and

$$\begin{aligned}
d^p &= d^{n^{b^{-1}}} = d^{bnb^{-1}} = (d^{b^2})^{b^{-1}nb^{-1}} = (dc)^{b^{-1}nb^{-1}} = (eh)^{nb^{-1}} \\
&= (echg \cdot h)^{b^{-1}} = (ecg)^{b^{-1}} = dc \cdot h \cdot cgh = dg, \\
e^m &= e^{b^2} = (e^{b^{-1}})^{b^{-1}} = (dc)^{b^{-1}} = eh, \\
e^p &= e^{bnb^{-1}} = (e^{b^2})^{b^{-1}nb^{-1}} = (e^m)^{b^{-1}nb^{-1}} = (eh)^{b^{-1}nb^{-1}} \\
&= (dc \cdot c)^{nb^{-1}} = d^{nb^{-1}} = (dg)^{b^{-1}} = ecgh, \\
f^n &= f^{ama^{-1}} = (f^{a^{-1}})^{a^2ma^{-1}} = (ech)^{dma^{-1}} = (ech \cdot c \cdot h)^{ma^{-1}} \\
&= e^{ma^{-1}} = (eh)^{a^{-1}} = f \cdot cgh, \\
f^p &= f^{bnb^{-1}} = (f^{b^2})^{b^{-1}nb^{-1}} = (f^m)^{b^{-1}nb^{-1}} = (fh)^{b^{-1}nb^{-1}} \\
&= (defcgh \cdot c)^{nb^{-1}} = (defgh)^{nb^{-1}} = (dg \cdot echg \cdot fcgh \cdot g \cdot h)^{b^{-1}} \\
&= (defh)^{b^{-1}} = e \cdot dc \cdot defcgh \cdot c = fcgh.
\end{aligned}$$

From the above relations we get at once the desired commutators which determine completely the structure of $U = ST$:

$$\begin{aligned}
[d, m] &= c, & [d, n] &= g, & [d, p] &= g, & [e, m] &= h, & [e, n] &= cgh, \\
[e, p] &= cgh, & [f, m] &= h, & [f, n] &= cgh, & [f, p] &= cgh.
\end{aligned}$$

In particular, we see that $U' = \Phi(U) = \langle c, g, h \rangle$. We know that $\langle c, g, h \rangle \leq Z(U)$, $ef \in Z(S)$ and $np \in Z(T)$. In addition, we compute (noting that U is of class 2):

$$\begin{aligned}
[ef, m] &= [e, m][f, m] = h \cdot h = 1, & [ef, n] &= 1, & [ef, p] &= 1, \\
[d, np] &= 1, & [e, np] &= 1, & [f, np] &= 1,
\end{aligned}$$

and so $ef, np \in Z(U)$. Therefore $Z(U) \geq \langle c, g, h, ef, np \rangle$.

We show that we have in fact $Z(U) = \langle c, g, h, ef, np \rangle \cong E_{25}$. Indeed, we set $U_1 = \langle c, g, h \rangle \langle d, e, m, n \rangle$, $U_2 = \langle ef, np \rangle \cong E_4$ so that $U = U_1 \times U_2$, where $U'_1 = \Phi(U_1) = \langle c, g, h \rangle \leq Z(U_1)$ and we claim that $\langle c, g, h \rangle = Z(U_1)$. Suppose that $w = d^\alpha e^\beta m^\gamma n^\delta \in Z(U_1)$ ($\alpha, \beta, \gamma, \delta = 0, 1$) which implies

$$1 = [w, d] = [e, d]^\beta [m, d]^\gamma [n, d]^\delta = (ch)^\beta c^\gamma g^\delta = c^{\beta+\gamma} g^\delta h^\beta$$

and so $\beta = \gamma = \delta = 0$ and $w = d^\alpha$. From $1 = [w, e] = [d, e]^\alpha = c^\alpha h^\alpha$ follows $\alpha = 0$ and so $w = 1$. We have proved that $Z(U_1) = \langle c, g, h \rangle$ and so $Z(U) = \langle c, g, h, ef, np \rangle$.

The factor-group $G/U \cong D_8$ is generated with involutions $a^{-1}U$ and $b^{-1}U$ so that $x = a^{-1}b^{-1}$ must be an element of order 4 with $\langle x \rangle \cap U = \{1\}$. Set $y = x^2$ so

that $U\langle y \rangle / U = Z(G/U) = \Phi(G/U)$. It follows that $\Phi(G) = U\langle y \rangle$. By Theorem A, the set $G - \Phi(G)$ cannot contain involutions and so (since $\Omega_1(U) = U$) we have $\Omega_1(G) = \Phi(G)$.

We have $\langle c \rangle^G = \langle c, g, h \rangle = \langle c, s_1, s_2 \rangle$, where $\langle s_1, s_2 \rangle \leq Z(G)$, and so $C_G(c) = C_G(\langle c, g, h \rangle)$ which shows that $C_G(c)$ is a normal subgroup of G . On the other hand, $C_G(c) \geq U$ and $|G : C_G(c)| = 4$ (since the four conjugates of c are contained in $\langle c, g, h \rangle - \langle s_1, s_2 \rangle$), which implies that $C_G(c) = U\langle y \rangle = \Phi(G)$ and so $c^y = c$ and $\langle c, g, h \rangle \leq Z(\Phi(G))$.

We determine now the action of G/U on U by giving the actions of the elements a^{-1} and b^{-1} (we use a^{-1} and b^{-1} rather than a and b because of some technical reasons) on the elements $c, g, h, d, e, f, m, n, p$ of U . We get (by using all previous relations):

$$\begin{aligned} c^{a^{-1}} &= g, & g^{a^{-1}} &= c^{a^2} = c, \\ h^{a^{-1}} &= cgh, & d^{a^{-1}} &= d, \\ e^{a^{-1}} &= f, & f^{a^{-1}} &= ((a^2)^{b^{-1}})^{a^2} = e^d = e[e, d] = ech, \\ m^{a^{-1}} &= n, & n^{a^{-1}} &= (b^2)^{a^2} = b^2[b^2, a^2] = mc, \\ p^{a^{-1}} &= mnpcgh, & c^{b^{-1}} &= h, \\ g^{b^{-1}} &= cgh, & h^{b^{-1}} &= c^{b^2} = c, \\ d^{b^{-1}} &= e, & e^{b^{-1}} &= d^{b^2} = d^m = d[d, m] = dc, \\ f^{b^{-1}} &= defcgh, & m^{b^{-1}} &= m, \\ n^{b^{-1}} &= p, & p^{b^{-1}} &= ((b^2)^{a^{-1}})^{b^2} = (m^{a^{-1}})^m = n^m = n[n, m] = ncg. \end{aligned}$$

Since $y = x^2 = (a^{-1}b^{-1})^2$, we get from the above relations the action of y on U . We know that y centralizes $\langle c, g, h \rangle$ and we get:

$$d^y = defcgh, \quad e^y = fg, \quad f^y = eg, \quad m^y = mnpc, \quad n^y = pg, \quad p^y = ng.$$

Since $(ef)^y = ef$ and $(np)^y = np$, we get that $Z(U) = \langle c, g, h, ef, np \rangle \leq Z(\Phi(G))$. From the above relations we also get:

$$\begin{aligned} [d, y] &= (ef)cgh, & [e, y] &= (ef)g, & [f, y] &= (ef)g, \\ [m, y] &= (np)c, & [n, y] &= (np)g, & [p, y] &= (np)g. \end{aligned}$$

Our relations also show that $\Phi(G)/Z(U)$ is abelian and so elementary abelian. On the other hand, we see that $ef, np \in (\Phi(G))'$ and so $(\Phi(G))' = Z(U)$. If $Z(\Phi(G)) > Z(U)$, then $\Phi(G) = U * Z(\Phi(G))$ which implies that $(\Phi(G))' = U' = \langle c, g, h \rangle$, a

contradiction. Thus $Z(\Phi(G)) = Z(U) \cong E_{2^5}$ and so $\Phi(G)$ is a special group of order 2^{10} , as claimed in part (a) of our theorem.

It remains to determine the elements $y^{a^{-1}}$ and $y^{b^{-1}}$. This will complete the determination of the action of a^{-1} and b^{-1} on the special group $\Phi(G)$.

Since $x = a^{-1}b^{-1}$ and $y = x^2$, we get

$$\begin{aligned} y^{a^{-1}} &= (x^2)^{a^{-1}} = (x^{a^{-1}})^2 = (b^{-1}a^{-1})^2 = b^{-1}a^{-1}b^{-1}a^{-1} \\ &= b^{-1}(a^{-1}b^{-1}a^{-1}b^{-1})b = b^{-1}yb = y^b = (y^{b^2})^{b^{-1}} = (y^m)^{b^{-1}} \\ &= ([m, y]y)^{b^{-1}} = ((np)cy)^{b^{-1}} = (y(np)c)^{b^{-1}} = y^{b^{-1}} \cdot p \cdot ncg \cdot h \\ &= y^{b^{-1}}(np)cgh, \end{aligned}$$

and so $y^{a^{-1}} = y^{b^{-1}}(np)cgh$. On the other hand, $x^a = a^{-1}(a^{-1}b^{-1})a = a^2b^{-1}a = a^2b^2(ba) = a^2b^2(a^{-1}b^{-1})^{-1} = dm x^{-1}$, and so

$$y^a = (x^2)^a = (x^a)^2 = dm x^{-1} dm x^{-1} = dm(dm)^x x^2 = dm(dm)^x y.$$

Conjugating the last relation with a^{-1} , we get $d^{a^{-1}} m^{a^{-1}} (dm)^{a^{-1}b^{-1}a^{-1}} y^{a^{-1}} = y$, and so using our previous relations we get:

$$d \cdot n \cdot (fmnp cgh) \cdot y^{a^{-1}} = y, \quad y^{a^{-1}} = (pnmfnd)y cgh.$$

Using our commutator relations in $\Phi(G)$, we get $pnmfnd = demng(ef)(np)$, and so $y^{a^{-1}} = demnycg(ef)(np)$. Putting the last relation in (3), we get also $y^{b^{-1}} = demnyg(ef)$.

We have determined completely the structure of the Burnside group $G = \langle a, b \rangle$. We set $ef = i$ and $np = j$ so that $Z(\Phi(G)) = \langle c, g, h, i, j \rangle \cong E_{2^5}$ and the special group $\Phi(G)$ is generated with five involutions d, e, m, n, y with $a^2 = d$, $b^2 = m$, $(a^{-1}b^{-1})^2 = y$ and the commutator relations and the action of a^{-1} and b^{-1} on $\Phi(G)$ as given in part (e) of our theorem.

In the rest of the proof we shall use only this presentation of the group G as given in part (e) of our theorem. We show now that $Z(G) = \langle cg, ch, cij \rangle \cong E_8$. Indeed, $G/U \cong D_8$ and $Z(G/U) = U\langle y \rangle / U$ and so $Z(G) \leq U\langle y \rangle = \Phi(G)$. It follows that $Z(G) \leq Z(\Phi(G))$. On the other hand, $\langle cg, ch \rangle \leq Z(G)$. We compute:

$$(cij)^{a^{-1}} = g \cdot ich \cdot jgh = cij, \quad (cij)^{b^{-1}} = h \cdot igh \cdot jcg = cij,$$

and so $cij \in Z(G)$. But $\langle i, j \rangle$ is a complement of $\langle cg, ch, cij \rangle$ in $Z(\Phi(G))$ and

$$i^{a^{-1}} = ich, \quad j^{a^{-1}} = jgh, \quad (ij)^{a^{-1}} = ijcg,$$

which shows that $\langle i, j \rangle \cap Z(G) = \{1\}$ and therefore $Z(G) = \langle cg, ch, cij \rangle \cong E_8$.

We examine now the non-trivial cosets of $Z(\Phi(G))$ in $\Phi(G)$. Each such coset consists either of involutions or only of elements of order 4. Using the defining relations for $\Phi(G)$, we find out that there are exactly 12 such cosets which consist of involutions and they are the cosets with representatives from the set:

$$V = \{d, e, m, n, y, dem, den, dey, dm, emn, mny, demny\}.$$

Also we see that if $v, w \in V$, $v \neq w$, then $o(vw) = 4$. This shows that G has exactly 12 maximal elementary abelian subgroups. Each of them is of order 2^6 and the intersection of any two of them is equal $Z(\Phi(G))$.

In order to determine the structure of various subgroups of G which contain the subgroup $Z(\Phi(G))$, it is convenient first to determine the structure of $H = G/Z(\Phi(G))$ of order 2^7 . Since $Z(\Phi(G)) = (\Phi(G))'$, H is obviously the group of maximal possible order having the exponent 4, being generated with two elements, and having the property that the squares of any two elements commute. The images of elements a, b, d, e, m, n, y of G in $H = G/Z(\Phi(G))$ we denote again with the same symbols. Then we have $E = \Omega_1(H) = \Phi(H) = \langle d, e, m, n, y \rangle \cong E_{25}$, $H = \langle a, b \rangle$ with $a^2 = d, b^2 = m, (a^3b^3)^2 = y$, and the action of a and b on E is given with:

$$\begin{aligned} d^a &= d, & e^a &= e, & m^a &= n, & n^a &= m, & y^a &= demny, \\ d^b &= e, & e^b &= d, & m^b &= m, & n^b &= n, & y^b &= demny. \end{aligned}$$

We have $C_E(a) = \langle d, e, mn \rangle$, $C_E(b) = \langle de, m, n \rangle$, $C_E(ab) = \langle de, mn, y \rangle$, $Z(H) = \langle de, mn \rangle \cong E_4$, $(E\langle a \rangle)' = (E\langle b \rangle)' = (E\langle ab \rangle)' = \langle de, mn \rangle = Z(H)$, $E\langle a \rangle/Z(H)$, $E\langle b \rangle/Z(H)$, $E\langle ab \rangle/Z(H)$ are abelian groups of type $(4, 2, 2)$. It follows that the maximal subgroups of H are of rank 3. Also, it is easy to see from these information that the number of conjugate classes in H is $k(H) = 26$. Indeed, 4 elements in $Z(H)$ give 4 classes of size 1, 12 elements in $dZ(H) \cup mZ(H) \cup yZ(H)$ give 6 classes of size 2, the remaining 16 elements in E give 4 classes of size 4, and $96 = 2^7 - 2^5$ elements in $H - E$ give 12 classes of size 8 each. We compute:

$$\begin{aligned} y &= (a^{-1}b^{-1})^2 = a^{-1}b^{-1}a^{-1}b^{-1} = (a^{-1}b^{-1}ab) \cdot b^{-1}a^{-1}a^{-1}b^{-1} \\ &= [a, b]b^{-1}a^2b^{-1} = [a, b] \cdot d^b \cdot b^2 = [a, b]em, \end{aligned}$$

so that $[a, b] = emy$. This gives $H' = \langle de, mn, emy \rangle \cong E_8$ and $H/H' \cong C_4 \times C_4$. Since

$$(emy)^a = e \cdot n \cdot demny = dmy = (emy)de,$$

$$(emy)^b = d \cdot m \cdot demny = eny = (emy)mn,$$

it follows that $[H, H'] = Z(H) = \langle de, mn \rangle$, H is of class 3, and $H/[H, H']$ is the non-metacyclic minimal nonabelian group of order 2^5 and exponent 4. We have obtained the results stated in part (f) of our theorem.

We return now to our group G and consider the structure of maximal subgroups $M = \Phi(G)\langle a \rangle$, $N = \Phi(G)\langle b \rangle$, $K = \Phi(G)\langle a^{-1}b^{-1} \rangle$. By the preceding paragraph, $M' = N' = K' = Z(\Phi(G))\langle de, mn \rangle$ and M/M' is an abelian group of type $(4, 2, 2)$ so that $d(M) = 3$. Let μ be the automorphism of G of order 3 induced with $a^\mu = b$, $b^\mu = a^{-1}b^{-1}$. Then μ acts transitively on $\{M, N, K\}$ and therefore it is enough to determine the structure of M . By the preceding paragraph, $G' = Z(\Phi(G))\langle de, mn, emy \rangle = M'\langle emy \rangle$, $G/G' \cong C_4 \times C_4$, and $M'/Z(\Phi(G)) = Z(H) = K_3(H)$, $H = G/Z(\Phi(G))$ and therefore $M' = Z(\Phi(G))\langle de, mn \rangle$ is a characteristic subgroup of G . It follows from $d(G) = 2$ that $G'/K_3(G)$ is cyclic and $G' = K_3(G)\langle [a, b] \rangle$. But $1 = (ab)^4 \equiv a^4b^4[b, a]^6 \pmod{K_3(G)}$ so that $[b, a]^2 \in K_3(G)$ and $|G'/K_3(G)| = 2$. This gives that $K_3(G) = Z(\Phi(G))\langle de, mn \rangle = M'$.

We compute:

$$\begin{aligned}[de, mn] &= [d, m][d, n][e, m][e, n] = c \cdot g \cdot h \cdot cgh = 1, \\ (de)^2 &= d^2e^2[e, d] = ch, \quad (mn)^2 = cg, \quad (demn)^2 = gh,\end{aligned}$$

which shows that $M' = K_3(G)$ is abelian of type $(4, 4, 2, 2, 2)$ with $\Phi(M') = \langle cg, ch \rangle \cong E_4$. Since $C_G(c) = \Phi(G)$, we have $Z(M) \leq Z(\Phi(G))$. But $C_{\langle i, j \rangle}(a^{-1}) = \{1\}$ and so $Z(M) = Z(G) = \langle cg, ch, cij \rangle$, where we have used the fact that $\langle i, j \rangle$ is a complement of $Z(G)$ in $Z(\Phi(G))$. Since

$$\begin{aligned}(de)^{a^{-1}} &= (de)i, \quad (de)^y = (de)ch, \quad (de)^n = (de)ch, \quad (mn)^{a^{-1}} = (mn)g, \\ (mn)^y &= (mn)cg, \quad (mn)^n = (mn)cg, \quad i^{a^{-1}} = ich, \quad j^{a^{-1}} = jgh,\end{aligned}$$

we get that $\langle c, g, h, i \rangle \cong E_{24}$ is normal in M , $M'/\langle c, g, h, i \rangle \leq Z(M/\langle c, g, h, i \rangle)$ and $K_3(M) = \langle c, g, h, i \rangle$. Finally, $\langle c, g, h, i \rangle \leq Z(\Phi(G))$, $c^{a^{-1}} = c(cg)$, $g^{a^{-1}} = g(cg)$, $h^{a^{-1}} = h(cg)$, $i^{a^{-1}} = i(ch)$ so that $K_4(M) = \langle cg, ch \rangle \leq Z(G)$ and M is of class 4.

We determine now the structure of $G' = Z(\Phi(G))\langle de, mn, emy \rangle$, where $G/G' \cong C_4 \times C_4$. We know that $K_3(G) = Z(\Phi(G))\langle de, mn \rangle$ is an abelian maximal subgroup of G' , where $\Omega_1(K_3(G)) = Z(\Phi(G))$. But we see that the elements:

$$emy, de \cdot emy = dmy, mn \cdot emy \equiv eny, de \cdot mn \cdot emy \equiv dny \pmod{Z(\Phi(G))}$$

are all of order 4 and so $\Omega_1(G') = Z(\Phi(G))$. We compute $[de, emy] = ch$ and $[mn, emy] = cg$ and so $G'' = \langle cg, ch \rangle \leq Z(G)$. From $|G'| = 2|Z(G')||G''|$ follows $|Z(G')| = 2^5$ and so $Z(G') = Z(\Phi(G))$. Also, $(de)^2 = ch$, $(mn)^2 = cg$ and $(emy)^2 = cghij$, which gives $\Phi(G') = \langle cg, ch, cghij \rangle = \langle cg, ch, cij \rangle = Z(G)$.

We have $M' = K_3(G)$ and $K_3(M) = [M, M'] = [M, K_3(G)] = \langle c, g, h, i \rangle$, $(mn)^{b^{-1}} = (mn)j$, and so $K_4(G) \geq \langle c, g, h, i, j \rangle = Z(\Phi(G))$. On the other hand, we know that $K_3(G)/Z(\Phi(G)) = Z(G/Z(\Phi(G))) = Z(H)$ and so $K_4(G) = Z(\Phi(G))$. We have $i^{b^{-1}} = i(gh)$, $j^{a^{-1}} = j(gh)$, $j^{b^{-1}} = j(cg)$, and so we see that $K_5(G) = \langle cg, ch \rangle \leq Z(G)$, $K_6(G) = \{1\}$, and G is of class 5.

Finally, we see that $Z_2(G) = Z(\Phi(G)) \cong E_{25}$, $Z_3(G) = K_3(G) = M'$ (abelian of type $(4, 4, 2, 2, 2)$), and $Z_4(G) = \Phi(G)$. Our theorem is proved. \square

§61

Groups of exponent 4 generated by three involutions

It is known that a group generated with two non-commuting involutions is dihedral. But the problem to determine groups generated with three involutions is already very difficult. In this section we classify groups of exponent 4 which are generated with three involutions.

Theorem 61.1. *Let G be a group of exponent 4 with $d(G) = 3$ so that G is generated with involutions a, b, c and at least one of ab, ac, bc is an involution. Then $|G| \leq 2^6$ and one of the following holds:*

- (a) $G \cong C_2 \times D_8$, where $|G| = 2^4$.
- (b) G is a splitting extension of the abelian group $H = \langle v, w \mid v^4 = w^4 = [v, w] = 1, v^2 = w^2 \rangle$ of type $(4, 2)$ with the four-group $\langle a, b \rangle$, where $v^a = w, v^b = v^{-1}, w^b = w^{-1}$. We have $|G| = 2^5$ and $G = \langle a, b, c \rangle$ with $c = bv$.
- (c) G is a splitting extension of the nonmetacyclic minimal nonabelian group $H = \langle v, w \mid v^4 = w^4 = (wv)^2 = [w^2, v] = 1 \rangle$ of order 2^4 with the four-group $\langle a, b \rangle$, where $v^a = w, v^b = v^{-1}, w^b = w^{-1}$. We have $|G| = 2^6$ and $G = \langle a, b, c \rangle$ with $c = bv$. The group G is isomorphic to a Sylow 2-subgroup of the alternating group A_8 .

Proof. Let G be a group of exponent 4 with $d(G) = 3$ so that G is generated with three involutions a, b, c . If a, b, c pairwise commute, then $G \cong E_8$, a contradiction. If a commutes with b and c but $[b, c] \neq 1$, then $G = \langle a \rangle \times \langle b, c \rangle \cong C_2 \times D_8$.

Assume now that $[a, b] = (ab)^2 = 1$ but G is not isomorphic to $C_2 \times D_8$. This implies $[b, c] \neq 1$ and $[a, c] \neq 1$. Set $v = bc$ so that $o(v) = 4$ and $D = \langle b, c \rangle = \langle b, v \rangle \cong D_8$ with $\langle v^2 \rangle = Z(D)$. Also, $\langle a, c \rangle \cong D_8$ and so $o(ac) = 4$.

Set $w = v^a$. Since b inverts v and a centralizes b , it follows that b inverts $\langle w \rangle$. Also, $w^a = v$ and so the four-group $\langle a, b \rangle$ normalizes the subgroup $H = \langle v, w \rangle$. Hence $G = H\langle a, b \rangle$. We compute

$$(ac)^2 = (aca)c = c^a c = (bv)^a bv = (bwv)v = w^{-1}v$$

and so $o(w^{-1}v) = 2$. From $(av)^4 = 1$ follows $(av)^2 = (ava)v = v^a v = wv$ and

$(wv)^2 = 1$. The last relation gives

$$\begin{aligned} 1 &= wvwv = w^2(w^{-1}vw^{-1})w^2v = w^2(w^{-1}vw^{-1}v)v^{-1}w^2v \\ &= w^2(w^{-1}v)^2v^{-1}w^2v = [w^2, v]. \end{aligned}$$

If $\langle w \rangle = \langle v \rangle$, then $H = \langle v \rangle$ and $G = D\langle a \rangle$. There is an involution $i \in \langle a, b \rangle - \langle b \rangle$ which centralizes $\langle v \rangle$ and so $G = \langle i \rangle \times D$, contrary to our assumption.

We have $\langle v \rangle \neq \langle w \rangle$ and since $[w^2, v] = 1$, we get $w^2 \in Z(H)$. Consider $\bar{H} = H/\langle w^2 \rangle$ (bar convention) so that $\bar{H} = \langle \bar{w}, \bar{v} \rangle$. Suppose $v^2 = w^2$ which implies that \bar{H} is generated with two distinct involutions \bar{v} and \bar{w} . We know that $(wv)^2 = 1$ and so $\bar{w}\bar{v} = \bar{v}\bar{w}$ is also an involution. Hence $\bar{H} \cong E_4$. Suppose that H is nonabelian. Since $\langle v \rangle$ and $\langle w \rangle$ are two distinct cyclic subgroups of order 4 in H , we get $H \cong Q_8$. But we know that $(wv)^2 = 1$, a contradiction. Hence H is abelian of type $(4, 2)$. We have $G = H\langle a, b \rangle$ and so the group G is a splitting extension of the abelian group $H = \langle v, w \mid v^4 = w^4 = [v, w] = 1, v^2 = w^2 \rangle$ of type $(4, 2)$ with the four-group $\langle a, b \rangle$, where $v^a = w, v^b = v^{-1}, w^b = w^{-1}$. We get $|G| = 2^5$ and $G = \langle a, b, c \rangle$ with $c = bv$.

Assume now that $v^2 \neq w^2$ so that $\langle v \rangle \cap \langle w \rangle = \{1\}$. We have $o(\bar{w}) = 2, o(\bar{v}) = 4$ and $o(\bar{w}\bar{v}) = 2$ (since $(wv)^2 = 1$). Hence $\bar{H} \cong D_8$ and so $|H| = 2^4$. The group H is not of maximal class since H possesses the abelian subgroup $\langle w^2 \rangle \times \langle v \rangle$ of type $(4, 2)$. Hence H is of class 2 and therefore $1 = [w^2, v] = [w, v]^2 = [w, v^2]$, so that $[w, v]$ is an involution. Since $[w, v] \in Z(H)$, we get that $H/\langle [w, v] \rangle$ is abelian. Consequently, $H' = \langle [w, v] \rangle$ and so H is minimal nonabelian with $Z(H) = \langle w^2, v^2 \rangle \cong E_4$. Also, $1 = (wv)^2 = w^2v^2[v, w]$, and so $[v, w] = [w, v] = w^2v^2$. Since $wv \notin Z(H) = \langle w^2, v^2 \rangle$, we get $\langle w^2, v^2, wv \rangle \cong E_8$ and so H is non-metacyclic. The group G is a splitting extension of the non-metacyclic minimal nonabelian group $H = \langle v, w \mid v^4 = w^4 = (wv)^2 = [w^2, v] = 1 \rangle$ of order 2^4 with the four-group $\langle a, b \rangle$, where $v^a = w, v^b = v^{-1}, w^b = w^{-1}$. We have $\langle a, b \rangle \cap H = \{1\}$ and so $|G| = 2^6$ and $G = \langle a, b, c \rangle$ with $c = bv$ and $Z(G) = \langle v^2w^2 \rangle = \langle (bc)^2((bc)^2)^a \rangle$. Indeed, it is easy to see that the involutions in $\langle a, b \rangle \cong E_4$ induces on H only outer automorphisms. No element $x \in H$ could invert an element y of order 4 in H since $[w, v] = w^2v^2$ is not a square in H . Also, $\langle y^x \rangle \cap \langle y \rangle \geq \langle y^2 \rangle$ since $y^2 \in \Phi(H) = Z(H)$.

The group G is isomorphic to a Sylow 2-subgroup of the alternating group A_8 . Set $D = \langle v, b \rangle \cong D_8$ so that $(v^2)^a = w^2$ and therefore $v^2 \notin D_G$. No subgroup of order 2 in $D - \langle v \rangle$ is normal in D . Hence $D_G = \{1\}$ and so G has a faithful transitive permutation representation of degree 8. If we set:

$$a = (1, 2)(3, 4)(5, 6)(7, 8), \quad b = (4, 5)(3, 6), \quad c = (2, 3)(6, 7),$$

then we see that the permutations a, b, c satisfy all the above relations for G and

$$(bc)^2((bc)^2)^a = (1, 8)(2, 7)(3, 6)(4, 5) \neq 1$$

and so the obtained permutation representation is faithful. Since these permutations are even, we are done. \square

Theorem 61.2. Let G be the group given with

$$\begin{aligned} G = \langle a, b, c \mid a^2 = b^2 = c^2 = (ab)^4 = (bc)^4 = (ca)^4 = 1, \\ (abc)^4 = (c(ab)^2)^4 = (b(ac)^2)^4 = (acab)^4 = 1 \rangle. \end{aligned}$$

Then G is of order 2^{10} and exponent 4. Hence each group of exponent 4 which is generated with three involutions is a epimorphic image of the above group of order 2^{10} .

Proof. This theorem is proved by using a computer (W. Lempken of the University of Essen). \square

In what follows we shall determine the structure of the group $G = \langle a, b, c \rangle$ of order 2^{10} as defined in Theorem 61.2 so that G is the free group of exponent 4 generated with three involutions a, b, c .

We set $(ab)^2 = d$, $d^c = e$, $e^a = f$, and $f^b = g$. We shall determine the structure of the normal subgroup $S = \langle d \rangle^G \geq \langle d, e, f, g \rangle$, where d, e, f, g are some involutions in $\Phi(G)$. Since $\langle a, b \rangle \cong D_8$, the involution $d = [a, b]$ commutes with a and b . From the above follows $e^c = d$, $f^a = e$ and $g^b = f$. We compute

$$(de)^2 = (abab \cdot cababc)^2 = (ababc \cdot ababc)^2 = (ababc)^4 = 1,$$

and so $[d, e] = 1$. From the last relation we obtain (conjugating with the element a and then with the element b): $[d, e^a] = [d, f] = 1$, $[d, f^b] = [d, g] = 1$. Further computation gives (noting that $(ab)^2 = (ba)^2$ and $(bac)^3 = (bac)^{-1} = cab$):

$$\begin{aligned} (ef)^2 &= (e \cdot aea)^2 = (ea)^4 = 1, \\ (fg)^2 &= (f \cdot bfb)^2 = (fb)^4 = 1, \\ (eg)^2 &= (cbabac \cdot bacbabacab)^2 = (cba(bac \cdot bac \cdot bac)cbacab)^2 \\ &= (cba \cdot cab \cdot cba \cdot cab)^2 = (cbacab)^4 = 1, \end{aligned}$$

and so $[e, f] = 1$, $[f, g] = 1$ and $[e, g] = 1$. We have proved that the subgroup $\langle d, e, f, g \rangle$ is elementary abelian of order $\leq 2^4$.

It is possible to show that the subgroup $\langle d, e, f, g \rangle$ is normal in G and so we get $S = \langle d \rangle^G = \langle d, e, f, g \rangle$. Indeed, we compute (noting that $(ca)^3 = (ca)^{-1} = ac$, $(ab)^3 = ba$, $(cab)^3 = (cab)^{-1} = babc$):

$$\begin{aligned} ff^c &= acababca \cdot cacababcac = acabab(ca)^3babcac = acabab \cdot ac \cdot babcac \\ &= ac(ababab)bcbabcac = ac \cdot ba \cdot bcbabcac \\ &= a(cbab)(cbab)(cbab)babac = a \cdot babc \cdot babac \\ &= (ab)^2c(ba)^2c = dd^c = de, \end{aligned}$$

and so $ff^c = de$ which gives $f^c = def$. Also we get:

$$g^a = (d^c)^{aba} = e^{aba} = e^{abab \cdot b} = (e^{(ab)^2})^b = (e^d)^b = e^b,$$

and so $g^a = e^b$.

We compute (noting that $(ab)^2 = (ba)^2$ and $bcbcb = (bc)^3c = (bc)^{-1}c = cbc$):

$$ee^b = caba(bc \cdot bcb)abacb = caba(cbc)abacb = (cabacb)^2,$$

and similarly (noting that $baca \cdot baca \cdot ba = (baca)^3ac = (baca)^{-1}ac = acabac$),

$$\begin{aligned} fg &= acba(baca \cdot bacaba)bcab = acba \cdot acabac \cdot bcab = (acbcab)^2 \\ &= (acbcab)^{-2} = (bacbca)^2. \end{aligned}$$

Using the above relations we get (noting that $(ac)^2 = (ca)^2$, $(bca)^2 = (bca)^{-2} = (acb)^2$, $(cab)^2 = (bac)^2$, and $(b(ac)^2)^3 = (b(ac)^2)^{-1} = (ac)^2b$):

$$\begin{aligned} ee^b fg &= (cabacb \cdot cabacb)(bacbca \cdot bacbca) \\ &= cabac(bca \cdot bca \cdot cab \cdot cab)acbca = cabac(acb)^2(bac)^2acbca \\ &= cabacacbba bacbacbca = ca \cdot (b(ac)^2 \cdot b(ac)^2 \cdot b(ac)^2)bca \\ &= ca \cdot (ac)^2b \cdot bca = ca(ca)^2ca = (ca)^4 = 1, \end{aligned}$$

and so $e^b = efg = g^a$.

Finally, we get (using $(ab)^3 = ba$):

$$\begin{aligned} g^c e &= cbacbabac(abc \cdot cabab)c = cba \cdot cba \cdot bac(ab)^3c = (cba)^2(bac)^2 \\ &= (cba)^{-2}(bac)^{-2} = (abc)^2(cab)^2 = abcabccabcb \\ &= abc(ab)^2cab = (ab)^2 \cdot bac(ab)^2cab = dg, \end{aligned}$$

and so $g^c = deg$. We have proved by now:

$$\begin{array}{llll} d^a = d, & e^a = f, & f^a = e, & g^a = efg, \\ d^b = d, & e^b = efg, & f^b = g, & g^b = f, \\ d^c = e, & e^c = d, & f^c = def, & g^c = deg. \end{array}$$

This shows that $\langle d, e, f, g \rangle$ is normal in G and so $S = \langle d, e, f, g \rangle = \langle d \rangle^G$ is elementary abelian of order $\leq 2^4$. By Theorem 61.1, G/S is of order $\leq 2^6$. Since $|G| = 2^{10}$ (Theorem 61.2), we have $S \cong E_{2^4}$ and $|G/S| = 2^6$.

From the above results we get at once that $\langle ef, eg \rangle \leq Z(G)$. The subgroup $\langle d, e \rangle$ is a complement of $\langle ef, eg \rangle$ in S and $Z(G) \cap \langle d, e \rangle = \{1\}$. This gives $Z(G) \cap S = \langle ef, eg \rangle$.

Define the automorphism μ of G induced with $a^\mu = b, b^\mu = c, c^\mu = a$. Set

$$\begin{aligned} d^\mu &= h = (bc)^2, & e^\mu &= i = ((bc)^2)^a, \\ f^\mu &= j = ((bc)^2)^{ab}, & g^\mu &= k = ((bc)^2)^{abc} \end{aligned}$$

so that $T = \langle h \rangle^G = \langle h, i, j, k \rangle \cong E_{24}$ and μ transports the above relations for the elements in S into the relations for the elements in T . In particular, $h^a = i, i^a = h, h^b = h, i^b = j, h^c = h, i^c = ijk$.

We want to determine $S \cap T$. For that purpose we compute (noting that $(bc)^3 = cb, (cba)^2 = (abc)^2, (ca)^3 = ac, (bc)^3 = cb$):

$$\begin{aligned} efik &= cababc \cdot acaba(bca \cdot abcabc)a \cdot cbabcbcab \\ &= cababacacaba(cb \cdot acba)bcabcabc = cababacacaba \cdot abcabc \cdot bcabcabc \\ &= cabab(ca)^3(bc)^3abc = cabab \cdot ac \cdot cb \cdot abc = c(ab)^4c = 1, \end{aligned}$$

and similarly (noting that we have $(bc)^2 = (cb)^2, (cbab)^2 = (bab)^2, (ab)^3 = ba, (bac)^3 = cab$):

$$\begin{aligned} egjk &= cababc \cdot bacababcbab \cdot bacbcbab \cdot cbabcbcab \\ &= cababcbacaba(cbabcbab)cabcabc \\ &= cababcbac(aba \cdot bab)cbabc \cdot cbcabc = cababc(bac \cdot ba \cdot cbac)abc \\ &= cababc \cdot cab \cdot abc = c(ab)^4c = 1, \end{aligned}$$

which gives $ef = ik, eg = jk$ and so $S \cap T \geq \langle ef, eg \rangle \cong E_4$ and $i^b = j = i(ij) = i(fg), i^c = i(jk) = i(eg)$. We have $|ST| \leq 2^6$. By Theorem 61.1, $|G/ST| \leq 2^4$ and so the fact that $|G| = 2^{10}$ gives $U = ST$ is of order 2^6 and $G/U \cong C_2 \times D_8$. This implies that $y = (ca)^2 \notin U$ and $S \cap T = \langle ef, eg \rangle = \langle ik, jk \rangle \leq Z(G)$. Note that $\langle h, i \rangle$ is a complement of $S \cap T$ in T and we compute:

$$\begin{aligned} d^h &= d^{bcbc} = d(fg), & d^i &= d^{abcbca} = d(fg), \\ e^h &= e^{bcbc} = e(fg), & e^i &= e^{abcbca} = e(fg), \end{aligned}$$

and so $[d, h] = [d, i] = [e, h] = [e, i] = fg$.

We have $U' \leq S \cap T \leq Z(G)$ and so U' is of class 2 and, by the above, $U' = \langle fg \rangle$ and $U = \langle d, e, f, g \rangle \langle h, i \rangle \leq \Phi(G)$. Since $y = (ca)^2 \notin U$ and G/G' is generated with involutions, we have $\Phi(G) = G' = \Omega_1(\Phi(G)) = U\langle y \rangle$.

We note that $fg, eg, ef \in Z(G)$,

$$hg = gh[h, g] = gh[h, e(eg)] = gh[h, e] = ghfg$$

and $[d, hi] = [d, h][d, i] = (fg)^2 = 1$ so

$$\begin{aligned} y^b &= (caca)^b = ch \cdot ad \cdot ch \cdot ad = cah^a dchad = caidchad = caci^c d^c had \\ &= caci(eg)ehad = cacighad = (caca)i^a g^a h^a d = y \cdot h(ef)gi \cdot d \\ &= y(ef)(hg)id = y(ef)gh(fg)id = y(ef)(fg)g(hi)d = yedhi, \end{aligned}$$

and hence we have $y^b = ydehi$, $y^a = y$ and $y^c = y$.

Set $fg = z_1$, $eg = z_2$ so that $E_4 \cong \langle z_1, z_2 \rangle \leq Z(G)$,

$$d^y = d^{caca} = dz_1z_2, \quad e^y = ez_1z_2, \quad h^y = hz_2, \quad i^y = iz_2,$$

$$Z(U) = \langle z_1, z_2, de, hi \rangle \cong E_{2^4}, \quad U' = \langle z_1 \rangle.$$

Obviously we have $Z(\Phi(G)) \leq Z(U)$ and since $(de)^y = de$, $(hi)^y = hi$, we get $\langle de, hi \rangle \leq Z(\Phi(G))$ and so $Z(\Phi(G)) = Z(U)$. By the above, $z_1, z_2 \in (\Phi(G))'$ and since the factor-group $\Phi(G)/\langle z_1, z_2 \rangle$ is abelian, we get $G'' = (\Phi(G))' = \langle z_1, z_2 \rangle$. Also, $\langle de, hi \rangle$ is a complement of $\langle z_1, z_2 \rangle$ in $Z(\Phi(G))$, $Z(G) \leq \Phi(G)$ and $(de)^a = df$, $(hi)^b = hj$, $(dehi)^a = dfhi$ which all imply that $\langle z_1, z_2 \rangle = Z(G)$.

Our relations give at once that $K_3(G) = Z(\Phi(G)) = \langle z_1, z_2, de, hi \rangle \cong E_{2^4}$ and $K_4(G) = \langle z_1, z_2 \rangle = Z(G)$ so that G is of class 4. We have proved the following

Theorem 61.3. *Let G be the free group of exponent 4 which is generated with three involutions a, b, c . Then G is of order 2^{10} and has the following properties:*

- (a) $\Phi(G) = G' = \Omega_1(G')$ is of order 2^7 and class 2 with $Z(\Phi(G)) \cong E_{2^4}$ and $(\Phi(G))' = G'' = \Phi(\Phi(G)) \cong E_4$.
- (b) We have $K_3(G) = [G, G'] = Z(\Phi(G))$ and $K_4(G) = (\Phi(G))' = Z(G)$ so that G is of class 4.
- (c) The group $\Phi(G)$ is generated with five involutions d, e, h, i, y so that $(\Phi(G))' = \langle z_1, z_2 \rangle \cong E_4$ and $[d, e] = [h, i] = 1$, $[d, h] = [d, i] = [e, h] = [e, i] = z_1$, $[d, y] = [e, y] = z_1z_2$, $[h, y] = [i, y] = z_2$, where $\langle z_1, z_2 \rangle = Z(G)$ and $Z(\Phi(G)) = \langle z_1, z_2, de, hi \rangle \cong E_{2^4}$. We have $G = \langle a, b, c \rangle$ with $(ab)^2 = d$, $(bc)^2 = h$, $(ca)^2 = y$, where the action of a, b, c on $\Phi(G)$ is given with:

$$\begin{aligned} d^a &= d, & e^a &= ez_1z_2, & h^a &= i, & i^a &= h, & y^a &= y, \\ d^b &= d, & e^b &= ez_1, & h^b &= h, \\ d^c &= e, & e^c &= d, & h^c &= h, & i^c &= iz_2, & y^c &= y. \end{aligned}$$

Groups with large normal closures of nonnormal cyclic subgroups

Let H be a nonnormal subgroup of a p -group; then $|G : H^G| \geq p$, where H^G is a normal closure of H in G . Therefore, it is natural to classify the p -groups G such that $|G : H^G| = p$ for all nonnormal subgroups $H < G$. Such G are classified by the second author but all proofs in this section are due to the first author.

Theorem 62.1 (Z. Janko). *Let G be a non-Dedekindian p -group. Suppose that $|G : H^G| = p$ for all nonnormal cyclic subgroups H of G . Then one and only one of the following holds:*

- (a) $|G| = p^3$.
- (b) $G = \langle a, b \mid a^{p^2} = b^{p^2} = 1, a^b = a^{1+p} \rangle$ is the unique nonabelian metacyclic group of order p^4 and exponent p^2 .
- (c) G is a 2-group of maximal class.
- (d) $p = 2$, $G = H \cdot Z$ is a semidirect product with cyclic kernel Z of order > 4 and a cyclic complement H of order 4. Write $R = \Omega_1(H)$. We have $Z(G) = R \times \Omega_1(Z) \cong E_4$, G/R is of maximal class not isomorphic with generalized quaternion group, and G/G' is abelian of type $(4, 2)$. We have $G = \langle h, z \mid h^4 = z^{2^n} = 1, n > 2, z^h = z^{-1+\epsilon 2^{n-1}}, \epsilon = 0, 1 \rangle$.

It is trivial that groups (a), (b) and (c) of Theorem 62.1 satisfy the hypothesis. For example, if $N \triangleleft G$ is of index > 2 , where G is 2-group of maximal class, then $N \leq \Phi(G)$, and this implies that groups of (c) satisfy the hypothesis.

Now let G be as in Theorem 62.1(d) and let $X < G$ be nonnormal cyclic. Let us prove that $|G : X^G| = 2$. It follows from $\Omega_1(G) = Z(G)$ that $|X| > 2$. The group G has no proper subgroups which are generalized quaternion (Proposition 10.19(a)) hence $\Omega_1(G) < X^G$ (otherwise, X^G is cyclic so $X \triangleleft G$). If $\Omega_1(H) = R < X$, then X/R is a nonnormal cyclic subgroup of the 2-group of maximal class G/R (since $|(G/R) : (R'/R)| = 4$) so $|G : X^G| = 2$, by (c). Now we assume that $R \not\leq X$. Suppose that $XR = X \times R \not\trianglelefteq G$; then $XR/R \not\trianglelefteq G/R$ so $|G : (XR)^G| = 2$. We have $(XR)^G = X^G R = X^G$ since $R < \Omega_1(G) < X^G$, so $|G : X^G| = 2$. Now assume that $XR \triangleleft G$. Then $XR/R \leq T/R$, where T/R is a cyclic subgroup of index 2 in G/R . We have $T = V \times R$ and $\Phi(V) = \Phi(T) \triangleleft G$ so all cyclic subgroups of T of

order 2^k for all $k < n$, where $|V| = 2^n$ ($n > 2$), are G -invariant, so $|X| = 2^n$; then $|G : X| = 4$. In that case, $X^G = T$ so $|G : X^G| = 2$, as required.

Lemma 62.2. *Let G be a non-Dedekindian minimal nonabelian p -group of order $> p^3$. If $|G : H^G| = p$ for all nonnormal $H < G$, then G is the unique nonabelian metacyclic group of order p^4 and exponent p^2 which we denote $\mathcal{H}_{p,2}$.*

Proof. Let $H < G$ be nonnormal cyclic; then $H^G = H \times G'$ so $|G : H| = p^2$. If the nonmetacyclic G is as in Lemma 65.1(a), then $o(a) = o(b) = p$ so $|G| = p^3$, contrary to the hypothesis. Thus, G is metacyclic as in Lemma 65.1(b) so $G = B \cdot A$, where $A = \langle a \rangle \triangleleft G$, $B = \langle b \rangle$ and $|A| = p^2$, by the above. Assume that $n > 2$. Write $\Omega_2(B) = \langle x \rangle$, $F = \langle xa \rangle$; then $|F| = p^2$. We have $(xa)^b = xa^{1+p} \notin F$ so F is not G -invariant; then $F^G = F \times G'$ has index $p^{n-1} > p$ in G , a final contradiction. \square

Proof of Theorem 62.1. Let $H < G$ be nonnormal cyclic. Since $H^G \leq H\Phi(G) < G$, we get $|G : H\Phi(G)| = p$ so $H \not\leq \Phi(G)$ and $d(G) = 2$. Hence all cyclic subgroups of $\Phi(G)$ are G -invariant so $\Phi(G)$ is Dedekindian. Since $\Phi(G)$ has no G -invariant subgroups isomorphic to Q_8 (Lemma 1.4), it is abelian. If $|G'| = p$, then G is minimal nonabelian (Lemma 65.2(a)) so G is as in Theorem 62.1(b), by Lemma 62.2. Now suppose that $|G'| > p$ so G is not minimal nonabelian.

(i) Let $\Phi(G)$ be cyclic. If $p > 2$, then $\Phi(G) = Z(G)$ and $|G'| = p$ (Theorem 4.4), a contradiction. Thus, $p = 2$; then $\Phi(G) = \mathfrak{V}_1(G)$ so G has a cyclic subgroup of index 2 hence G is of maximal class. Now suppose that $\Phi(G)$ is noncyclic.

(ii) Let $p > 2$. Suppose that $\Phi(G) = U \times V$ and $U > \{1\}$ is cyclic (by (i), $V > \{1\}$ and, by the above, U, V are G -invariant). Take $x \in G$. By induction, $[x, \Phi(G)] \leq U \cap V = \{1\}$ so $\Phi(G) \leq Z(G)$. Then G is minimal nonabelian, a contradiction.

(iii) Thus, $p = 2$ and $\Phi(G)$ is noncyclic abelian. Assume that G is not metacyclic. Then, by Schreier inequality (see Appendix 25) and Corollary 36.6, there is $M \in \Gamma_1$ such that $d(M) = 3$. Write $\bar{G} = G/\Phi(M)$; then \bar{G} of order 2^4 is neither abelian (in view of $d(G) = 2 < d(M)$) nor of maximal class so there is $\bar{L} < \bar{M}$ of order 2 such that $\bar{L} \not\leq Z(\bar{G})$. Since \bar{G} is not of maximal class, we get $|\bar{G}'| = 2$, by Taussky, so $\bar{L}\bar{G} = \bar{L} \times \bar{G}'$ has index 4 in \bar{G} , a contradiction (our hypothesis is inherited by non-Dedekindian epimorphic images of G). Thus, G is metacyclic so G/Z is cyclic for a cyclic $Z \triangleleft G$. Since G is not of maximal class, we get $\Omega_1(G) \cong E_4$ so $\Omega_1(G) \leq Z(G)$ in view of $G/\Omega_1(G) > 2$. Since G is not of maximal class, we get $|G/G'| \geq 8$ (Taussky). Let $R < G'$ be of index 2; then G/R is minimal nonabelian and non-Dedekindian since $d(G/R) = 2$ and $|G/R| > 8$ (Lemma 62.2). Therefore, by Lemma 62.2, $G/R \cong \mathcal{H}_{2,2}$ so G/G' is abelian of type $(4, 2)$. It follows that $|G : Z| = 4$ since $Z < G'$.

Let $M < G$ be minimal nonabelian; then $|M| > 8$ (Proposition 10.19) so M is as in Lemma 65.1(b); then $M = H_1 \cdot Z_1$ is a semidirect product with cyclic factors Z_1

and H_1 and H_1 is not normal in M so in G . However, $M' = \Omega_1(Z_1) < G'$ and G' is cyclic so $H_1 \cap G' = \{1\}$. Since $2 = |G : H_1^G|$, we get $H_1^G = H_1 \cdot G'$; then $|H_1| = 4$ since $\Omega_1(G) \leq Z(G)$, and G/G' is abelian of type $(4, 2)$, $H_1 \cap Z = \{1\}$ since $G' < Z$ and Z is cyclic. It follows that $G = H_1 \cdot Z$, a semidirect product. Since $\mathfrak{U}_1(H_1) \triangleleft G$ as a subgroup of $\Phi(G)$, then $A = \mathfrak{U}_1(H_1) \times Z$ is abelian of index 2 in G so $4 = \frac{1}{2}|G : G'| = |Z(G)|$ (Lemma 1.1). Since $|G/\mathfrak{U}_1(H_1) : (G/\mathfrak{U}_1(H_1))'| = 4$, the group $G/\mathfrak{U}_1(H)$ is of maximal class (Taussky); moreover, it is not generalized quaternion since $G/\Omega_1(G) = (H_1\Omega_1(G)/\Omega_1(G)) \cdot (Z\Omega_1(G)/\Omega_1(G))$ is a semidirect product. Next, $|Z| > 4$ (otherwise, G is as in (b)). If $G/\Omega_1(G)$ is generalized quaternion, then $|\Omega_2(G)| = 8$ so G is a group of Lemma 42.1(c); then $Z(G)$ is cyclic, a contradiction. Thus, G is as stated in (d). \square

Groups all of whose cyclic subgroups of composite orders are normal

Definition 1. If all cyclic subgroups of a p -group G of composite orders are normal, then G is said to be a \mathfrak{K}_p -group.

The property \mathfrak{K}_p is inherited by sections. Below we classify \mathfrak{K}_p -groups and prove that the property (\mathfrak{K}_p) is equivalent to the following condition: Whenever $\{1\} < B < A \leq G$, where A is cyclic, then $N_G(B) = N_G(A)$ [Kaz1]. All proofs, apart of the proof of Supplement to Theorems 63.1 and 63.3, are due to the first author.

Proposition 63.1. *If G is a nonabelian \mathfrak{K}_p -group, $p > 2$, and $\exp(G) > p$, then $|G'| = p$.*

Proof. Let $Z < G$ be cyclic of order p^2 and $C_0 = \Omega_1(Z)$; then $C_0 \triangleleft G$. Assume that $K/C_0 < G/C_0$ is nonnormal of order p ; then K is abelian of type (p, p) . Set $H = KZ$; then $|H| = p^3$. Since $p > 2$, H has exactly p cyclic subgroups of order p^2 and they generate H so $H \trianglelefteq G$. Then $\Omega_1(H) = K \triangleleft G$, a contradiction. \square

Lemma 63.2. *Let a 2-group G be a \mathfrak{K}_2 -group. Then:*

- (a) *If $L \triangleleft G$ is of order 2 and $G/L \cong Q_8$, then L is a direct factor of G .*
- (b) *If $T < G$ is cyclic of order 2^e , $e > 1$, then $G/T \not\cong Q_8$.*

Proof. (a) By Theorem 1.2, G has no cyclic subgroups of index 2 so $L \not\leq G'$, by Taussky's theorem. Then, if $Z/L < G/L$ is cyclic of order 4, then Z is abelian of type $(4, 2)$ and $\Omega_1(Z) = Z(G)$ so all subgroups of order 2 are normal in G , and we conclude that G is Dedekindian. Then, by Theorem 1.20, L is a direct factor of G .

(b) Assume that $G/T \cong Q_8$. We use induction on $|G|$. Let $L < T$ be of order 2; then $|T/L| = 2$, by induction, so, by (a), $G/L = (T/L) \times (Q/L)$, where $Q/L \cong Q_8$. By (a), $Q = L \times Q_1$, where $Q_1 \cong Q_8$. Since $Q_1 \cong Q_8$ is generated by cyclic subgroups of order 4, it is normal in G so $G = T \times Q_1$. Since all subgroups of order 2 are normal in G , G is Dedekindian, contrary to Theorem 1.20. \square

Recall that the H_p -subgroup $H_p(G)$ of a group G is defined as $\langle x \in G \mid o(x) \neq p \rangle$. By Burnside, a nontrivial H_2 -subgroup has index 2 in G . If G is a (\mathfrak{K}_p) -group, then $H_p(G)$ centralizes G' . Note that if $|G : H_2(G)| = 2$, then $\exp(Z(G)) = 2$.

Theorem 63.3 ([Kaz1]). *If G is a nonabelian \mathfrak{K}_2 -group, then either (a) $|G'| = 2$ or (b) $H_2(G)$ has index 2 in G .*

Proof. Suppose that G is a counterexample of minimal order. As we noticed, $H_2(G)$ centralizes G' . Since $|G : H_2(G)| \leq 2$, $G' < H_2(G)$. If $|G : H_2(G)| = 2$, we have case (b). Now we assume that $G = H_2(G)$. Then, by what has just been said, $\text{cl}(G) = 2$.

(i) Let $|G'| > 4$. If $C < G'$ is of order 2, then, by induction, G/C has an abelian subgroup A/C of index 2 such that all elements in $(G/C) - (A/C)$ are involutions since $|(G/C)'| = |G'/C| > 2$. Let $x \in G - A$; then $x^2 \in A$. Assume that $o(x) > 2$; then $X = \langle x \rangle \triangleleft G$. In that case, $|XC/C| = 2$ so $x^2 \in C$ and $G/C = (A/C) \times (X/C)$ is abelian so $C = G'$ is of order 2, which is not the case. Thus, if $|G'| > 4$, we obtain case (b). It remains to consider the case where G' is either cyclic of order 4 or abelian of type $(2, 2)$.

(ii) Let $G' = \langle c \rangle \cong C_4$. We have $c = [x, y]$ for some $x, y \in G$. Set $H = \langle x, y \rangle$; then $H' = G' = \langle c \rangle$ is a central subgroup of order 4. We see that (a nonabelian \mathfrak{K}_2 -group) H of composite exponent is not a group from the conclusion (indeed, since $\exp(Z(H)) > 2$, H coincides with its H_2 -subgroup; in addition, $|H'| = 4 > 2$); therefore, $H = G$, by induction. If x, y are involutions, then G is dihedral of class 2 so $|G'| = 2$, a contradiction. Therefore, one may assume that $o(x) > 2$; in that case, $G = \langle x \rangle \langle y \rangle$ is metacyclic. Next, G has no cyclic subgroups of index 2 (otherwise, since G is of class 2, $|G'| = 2$). Then $\Omega_1(G)$ is of type $(2, 2)$ and G has no nonabelian subgroups of order 8 (this follows from Proposition 10.19). Therefore, if $K/\Omega_1(G)$ is a subgroup of order 2 in $G/\Omega_1(G)$ then K is abelian of type $(4, 2)$ so it is normal in G since $K = \langle y \mid o(y) = 4 \rangle$. It follows that $G/\Omega_1(G)$ is nonabelian Dedekindian (nonabelian since G' is cyclic of order $4 > 2$). Then $G/\Omega_1(G) \cong Q_8$ since it is metacyclic (Theorem 1.20). By Taussky's theorem, G/G' is abelian of type $(4, 2)$. Since $G' \leq Z(G)$, G is minimal nonabelian. In that case, $|G'| = 2$, a contradiction.

(iii) It remains to consider the case where $G' \cong E_4$. Let $Z < G$ be cyclic of order $2^e = \exp(G)$; then G/Z is nonabelian since $G' \not\leq Z$. By Lemma 63.2(b), G/Z has no subgroups isomorphic to Q_8 . It follows from Theorem 1.20 that G/Z contains a nonnormal subgroup L/Z of order 2. Since $L \not\trianglelefteq G$, the subgroup L is not generated by cyclic subgroups of composite orders so L is dihedral, by Theorem 1.2 (indeed, $|L : Z| = 2$ and Z is cyclic). Since L' is cyclic and $\exp(G') = 2$, we get $|L'| = 2$ hence $|L| = 8$, $|Z| = 4$ and $e = 2$. Since $G = H_2(G)$ is nonabelian, there are two cyclic subgroups, say U and V , of order 4 that generate a nonabelian subgroup $Q = UV$. In that case, $Q \cong Q_8$ and $Q \triangleleft G$. Since $G' \not\leq Q$, the quotient group G/Q is nonabelian so it contains a cyclic subgroup M/Q of order 4 ($= \exp(G)$). Set $M = \langle x, Q \rangle$; then $X = \langle x \rangle$ is of order 4 and $M = Q \times X$. Since M is not Dedekindian (Theorem 1.20) and all subgroups of order 2 are normal in M , it contains a nonnormal cyclic subgroup of order 4, a final contradiction. \square

Supplement to Theorems 63.1 and 63.3 ([Kaz1]). Let G be a (\mathbb{K}_p) -group. If there holds $\exp(G) > p$ and $|G'| = p$, then $\Phi(G)$ is cyclic.

Proof (Kazarin, personal communication). Assume that $\Phi(G)$ is noncyclic; then we have $|G| > p^3$ and $\exp(G) \geq \exp(G/G') > p$.

(i) If $x, y \in G$, then $1 = [x, y]^p = [x, y^p]$ so $y^p \in Z(G)$ and $\Phi(G) = G'\mathfrak{U}_1(G) \leq Z(G)$.

(ii) Let $C < G$ be cyclic of order $> p$. Assume that $G' \not\leq C$; then G/C is nonabelian, $C \cap G' = \{1\}$ so $[C, G] \leq C \cap G' = \{1\}$ and hence $C \leq Z(G)$. By Lemma 63.2(b), G/C has no subgroups isomorphic to Q_8 so it is not Dedekindian. Therefore, there is a nonnormal $B/C < G/C$ of order p ; B is abelian of type $(|C|, p)$ since $C \leq Z(G)$. Then $B \triangleleft G$ since $B = \langle x \in B \mid o(x) > p \rangle$, contrary to the choice of B . Thus, every cyclic subgroup of G of composite order contains G' .

(iii) Let G be minimal nonabelian. Then $G/G' = \langle aG' \rangle \times \langle bG' \rangle$ is abelian of type (p^m, p^n) with $m \geq n$; then $m > 1$. Let $o(aG') = p^m$, $o(bG') = p^n$. By (ii), $G' \leq \langle a \rangle$ so G' is not a maximal cyclic subgroup of G so G is metacyclic and $G = \langle b \rangle \cdot \langle a \rangle$ (Lemma 65.1). By (ii), $n = 1$ so $\Phi(G)$ is cyclic.

(iv) If $x, y \in G$ are elements of composite orders, then $H = \langle x, y \rangle$ is either abelian or minimal nonabelian and in both cases it contains a cyclic subgroup of index p . Indeed, suppose that H is abelian. Let $o(x) \geq o(y)$. Then $H = \langle x \rangle \times \langle z \rangle$ so, by (ii), $o(z) = p$, i.e., H has a cyclic subgroup $\langle x \rangle$ of index p . Now suppose that H is nonabelian. Since $\langle x \rangle \triangleleft G$, H is metacyclic. Since $\Phi(H) \leq Z(H)$, by (i), and $H/\Phi(H) \cong E_{p^2}$, H is minimal nonabelian. By (iii), H has a cyclic subgroup of index p so $\Phi(H)$ is cyclic. Thus, in any case, $\langle x^p, y^p \rangle$ is cyclic for all $x, y \in G$.

Let $x \in G$ be of maximal order. Then, by (iv), $\mathfrak{U}_1(G) \leq \langle x \rangle$ so, by (ii), $\Phi(G) = \mathfrak{U}_1(G)G' \leq \langle x \rangle$ whence $\Phi(G)$ is cyclic. \square

Thus, Theorems 63.1 and 63.3 can be formulated as follows.

Theorem 63.4 ([Kaz1]). If G is a (\mathbb{K}_p) -group, then one of the following holds:

- (a) G is abelian,
- (b) $\exp(G) = p$,
- (c) $|G'| = p$ and $\Phi(G)$ is cyclic,
- (d) $p = 2$ and $|G : H_2(G)| = 2$.

The above four groups satisfy the hypothesis.

Definition 2. A p -group G is said to be an \mathfrak{N}_p -group if every cyclic subgroup A of composite order satisfies the following condition: Whenever $\{1\} < B < A$, then $N_G(B) = N_G(A)$. (Clearly, subgroups of \mathfrak{N}_p -groups are \mathfrak{N}_p -groups.)

Theorem 63.5 ([Kaz]). Let G be a nonabelian p -group, $\exp(G) > p > 2$. Then the following assertions are equivalent:

- (a) G is an \mathfrak{N}_p -group,
- (b) G is a \mathfrak{K}_p -group.

Proof. Obviously, (b) implies (a). Now suppose that an \mathfrak{N}_p -group G is not a \mathfrak{K}_p -group. Then G has a nonnormal cyclic subgroup A of composite order so, in view of Theorem 1.2, G has no cyclic subgroups of index p . By hypothesis,

(i) Every nonidentity subgroup of A is not normal in G , i.e., $A_G = \{1\}$.

Suppose that G is a counterexample of minimal order. In that case, every proper subgroup of G of composite exponent is a \mathfrak{K}_p -group so the normalizer of every non-normal cyclic subgroup of G of composite order is maximal in G since this normalizer is an \mathfrak{K}_p -group; thus $N = N_G(A) \in \Gamma_1$. Then, by Proposition 63.1, $|N'| \leq p$. Let $M \in \Gamma_1 - \{N\}$; then $A \not\subseteq M$ (otherwise, A is normal in M so in G). If $|A \cap M| > p$, then, by induction, $N_G(M \cap A) \geq MN = G$ so $A_G \geq A \cap M > \{1\}$, contrary to (i). Thus $|M \cap A| = p$ so $|A| = p^2$. Thus

(ii) Let A be a nonnormal cyclic subgroup of G of composite order. Then $|A| = p^2$ and A is contained in exactly one maximal subgroup of G .

Suppose that $|G'| = p$. Then $G' \not\subseteq A$ so $G'A = G' \times A \triangleleft G$. In that case, $\Phi(G' \times A) > \{1\}$ is contained in A and normal in G , contrary to (i). Thus, if $|G'| = p$. the theorem is true. In what follows we assume that

(iii) $|G'| > p$.

(iv) G has at most one abelian subgroup of index p . Indeed, otherwise, we have $|G : Z(G)| = p^2$ so $|G'| = p$, by Lemma 1.1.

Let $R \leq N$ be of composite exponent. Since $|N'| \leq p$ and $p > 2$, R is regular. It follows that R is generated by cyclic subgroups of composite orders so R is normal in N (by induction, N is a \mathfrak{K}_p -group). It follows that N/A is abelian since it is Dedekindian and $p > 2$ so $N' < A$. By (i), $N' = \{1\}$ so N is abelian. Thus, by (iv),

(v) N is the unique abelian maximal subgroup of G . Moreover, the normalizer of any nonnormal cyclic subgroup of composite order is an abelian maximal subgroup of G so coincides with N .

It follows that

(vi) All nonnormal cyclic subgroups of orders $> p$ in G are contained in N .

Let $B \triangleleft G$ be cyclic of order $> p$. Assume that $B \not\subseteq N$, or, what is the same, B does not normalize A ; then $B \triangleleft G$, by (vi). Then, AB is not a \mathfrak{K}_p -group so it is not an \mathfrak{N}_p -group and we get, by induction, $AB = G$. Thus, G is metacyclic. By (i), $A \cap B = \{1\}$, and, obviously, $C_N(B) = Z(G)$ (recall that N is the unique abelian maximal subgroup of G). Note that $|B : (B \cap N)| = p$ and $B \cap N \leq Z(G)$. Since $A_G = \{1\}$, we get $Z(G) < B$ so $B \cap N = Z(G)$. Then $G/Z(G)$ is abelian of type (p^2, p) . We have $Z(G) = \Phi(B) \leq \Phi(G)$. Let $U/Z(G)$ and $V/Z(G)$ be distinct cyclic subgroups of order p^2 in $G/Z(G)$. Then U and V are distinct abelian maximal subgroups of G , contrary to (v). Thus, $B < N$ so all cyclic subgroups of

composite orders are contained in N , i.e., $N = \mathrm{H}_p(G)$. This is a contradiction since $\langle G - N \rangle = \langle G - \mathrm{H}_p(G) \rangle = G$. Thus,

(vii) All cyclic subgroups of G of composite orders are contained in $N = \mathrm{H}_p(G)$.

Let $B \triangleleft G$ be normal cyclic of composite order. Take $x \in G - N$ and set $H = \langle x, B \rangle$; then H is metacyclic. It follows from $p > 2$ that H is generated by its cyclic subgroups of maximal order so $H \leq N$, by (vii), contrary to the choice of x . Thus,

(viii) All cyclic subgroups of composite orders are not normal in G . We see that the normalizer of every cyclic subgroup of composite order is abelian so coincides with N . It follows that N is the unique maximal subgroup of G of composite exponent, by (ii). Moreover, $\Omega_2(N) = N$, by (ii), so $\exp(G) = p^2$.

Let $M \in \Gamma_1 - \{N\}$; then $\exp(M) = p$, by (viii). In that case N contains the elementary abelian subgroup $N \cap M$ of index p . Then $N = A \times E$, where E is elementary abelian. In that case, $\Phi(N) = \Phi(A) > \{1\}$ is characteristic in N so normal in G , contrary to (i). Thus, all cyclic subgroups of composite orders are normal in G so G is a \mathfrak{K}_p -group. \square

Theorem 63.6 ([Kaz1]). *Let G be a nonabelian 2-group, and let $\exp(G) > 2$. Then the following assertions are equivalent:*

(a) G is a \mathfrak{N}_2 -group,

(b) G is a \mathfrak{K}_2 -group.

Proof. Clearly, (b) implies (a). It remains to prove the reverse implication. Suppose that G is a counterexample of minimal order. Then G has a nonnormal cyclic subgroup $B = \langle b \rangle$ of composite order. As above,

(*) $|X| = 4$ and $X_G = \{1\}$, where $X < G$ is nonnormal cyclic of order > 2 .

Let $B < N$, where $|G : N| = 2$. Then N is a \mathfrak{K}_2 -group, by induction, so $N = \mathrm{N}_G(B)$ and N is the unique maximal subgroup of G containing B . Let $a \in G - N$ be such that $o(a)$ is as large as possible; then $B^a \neq B$. If $\Omega_1(B^a) = \Omega_1(B)$, then $\Omega_1(B)^a = \Omega_1(B)$ and $\mathrm{N}_G(\Omega_1(B)) \geq \langle N, a \rangle = G$, contrary to (*). Thus, $\Omega_1(B^a) \neq \Omega_1(B)$ so $B \cap B^a = \{1\}$. Since $B, B^a \leq N$, these two subgroups are normal in N so $H = BB^a = B \times B^a$ is abelian of type $(4, 4)$. Since $B \not\triangleleftharpoonup \langle a, B \rangle$, we get $G = \langle a, B \rangle = \langle a, H \rangle$, by induction. Set $A = \langle a \rangle$; then $H \triangleleft G$ since $a^2 \in N$, $G = AH$, G/H is cyclic. Since H is abelian, $A \cap H \triangleleft G$. If $o(a) = 2$, then G is a \mathfrak{K}_2 -group (indeed, then H is an H_2 -subgroup of G). In what follows we assume that $o(a) > 2$.

If $A \cap H > \{1\}$, then $A \triangleleft G$ since $A \cap H \triangleleft G$ (see (*)), and so, by induction, $G = BA$ is a semidirect product with kernel A since $B \cap A = \{1\}$, by (*). In that case, $G = B \cdot A$ is metacyclic.

Suppose that $A \cap H = \{1\}$. Then A is not normal in G since G is nonabelian so $\mathrm{C}_G(H) = H$, by (*). In that case, the abelian subgroup $\mathrm{N}_G(A) = A \times \mathrm{Z}(G)$ is

maximal in G , by induction, so $Z(G)$ is a subgroup of index 2 in H ; then $B \cap Z(G) > \{1\}$, contrary to (*). Thus, it remains to consider the following two cases.

(i) Let $G = B \cdot A$, a semidirect product with kernel $A = \langle a \rangle \cong C_{2^n}$ ($n > 1$), $B = \langle b \rangle \cong C_4$. As above, $N = N_G(B)$, a maximal subgroup of G , is abelian of type $(2^2, 2^{n-1})$, $C_G(A) = A$ and $N \cap A = Z(G)$ has index 2 in A . Then $G/Z(G)$ is abelian of type $(4, 2)$ so G is minimal nonabelian. In that case, $Z(G) = \Phi(G)$ and $\{1\} < B \cap Z(G) \leq B_G$, contrary to (*).

(ii) Let $G = A \cdot H$, a semidirect product with abelian kernel H of type $(4, 4)$, $A = \langle a \rangle \cong C_4$, $H = B \times B^a$, where $B = \langle b \rangle \cong C_4$. Set $N_G(A) = M$; then $|G : M| = 2$, $M \cap H = Z(G)$ is abelian of type $(4, 2)$ so $B_G \geq B \cap Z(G) > \{1\}$, contrary to (*). \square

It follows from the above that epimorphic images of \mathfrak{N}_p -groups are \mathfrak{N}_p -groups or have exponent $\leq p$.

Let G be a p -group with $\exp(G) > p$. If every subgroup of composite exponent is normal in a p -group G , then either $|G'| \leq p$ or $G \cong D_{2^4}$ [Man18]. Obviously, G is a \mathfrak{K}_p -group. Suppose that $|G'| > p$. Then $p = 2$ and $A = H_2(G)$ has index 2 in G , by Theorem 63.4. If A is cyclic, we are done, by Theorem 1.2. Assume that A is not cyclic. Since $G' > \{1\}$, we get $\exp(A) > 2$. Let Z be a cyclic subgroup of order 4 in A . By hypothesis, all subgroups are normal in G/Z , i.e., G/Z is Dedekindian. By Lemma 63.2(b), G/Z has no subgroups isomorphic to Q_8 so G/Z is abelian. Let $Z_1 \neq Z$ be another cyclic subgroup of order 4 in A (see Theorem 1.17(b)). Then G/Z_1 is abelian, by what has just been proved. It follows that $G' \leq Z \cap Z_1$, so $|G'| \leq 2$.

Proposition 63.7 ([Li3] (compare with Theorem 58.5)). *Suppose that all nonnormal cyclic subgroups of a nonabelian p -group G , $p > 2$, are conjugate. Then $G \cong M_{p^n}$.*

Proof. Let $T < G$ be a nonnormal cyclic subgroup of G . Set $|T| = p^t$. Let \mathcal{K} be the set of all nonnormal cyclic subgroups of G ; then $|\mathcal{K}|$ is a power of p .

(i) Let $t = 1$.

(i1) Assume that $\exp(G) = p$. Set $|G| = p^m$, $|Z(G)| = p^z$. Then $|\mathcal{K}| = \frac{p^m - p^z}{p-1} = p^z(1 + p + \dots + p^{m-z-1})$. Since $m - z - 1 > 0$, $|\mathcal{K}|$ is not a power of p so not all members of the set \mathcal{K} are conjugate in G , a contradiction.

(i2) Thus, $\exp(G) > p$. Then G is a \mathfrak{K}_p -group so, by Theorem 63.1, $|G'| = p$, and G is regular since $p > 2$. Let $|\Omega_1(G)| = p^k$ and $|\Omega_1(Z(G))| = p^\mu$. Then the number of nonnormal subgroups of order p in G equals $\frac{p^k - p^\mu}{p-1} = p^\mu(1 + p + p^{k-\mu-1})$, which is a power of p , so $k = \mu + 1$. Since $|G'| = p$, it follows that there are exactly p subgroups conjugate with T in G . It follows that $\mu = 1$ so $k = 2$. Then $|G/\Omega_1(G)| = |\Omega_1(G)| = p^2$ so G is metacyclic. It follows that G is minimal nonabelian (Lemma 65.2(a)). Then, by Lemma 58.1, $G \cong M_{p^n}$.

(ii) Now let $t > 1$. Set $T_0 = \Omega_1(T)$; then $T_0 \leq T_G \triangleleft G$ so T_0 is contained in all nonnormal cyclic subgroups of G . Set $\bar{G} = G/T_0$. Let $\bar{U} < \bar{G}$ be nonnormal cyclic. If U is noncyclic, then $U = T_0 \times U_0$ and U_0 is not normal in G . Then $T_0 \not\leq U_0$, contrary to what has just been said. Thus, U is cyclic so conjugate with T . It follows that all nonnormal cyclic subgroups of \bar{G} are conjugate, i.e., \bar{G} satisfies the hypothesis. Therefore, by induction, $\bar{G} \cong M_{p^n}$. We also have $T_0 \leq \Phi(T) \leq \Phi(G)$ so $d(G) = d(\bar{G}) = 2$. If $A/T_0, B/T_0 < G/T_0$ be two distinct cyclic subgroups of index p , then $A, B \in \Gamma_1$ are distinct abelian so $A \cap B = Z(G)$, and we conclude that G is minimal nonabelian. By Lemma 58.1, $G \cong M_{p^n}$. However, all nonnormal cyclic subgroups of M_{p^n} have order $p < p^t$, so case $t > 1$ is impossible. \square

Exercise 1. Suppose that all nonnormal cyclic subgroups of a nonabelian 2-group G , are conjugate. Then $G \cong M_{2^n}$, i.e., Theorem 63.1 is also true for $p = 2$.

Exercise 2. Let a group G be nonabelian of exponent p . Then the number of nonnormal subgroups of order p in G is not a power of p .

There are in the book a number of results on cyclic subgroups of p -groups.

Problem. Classify the non-Dedekindian p -groups in which any two nonnormal cyclic subgroups of the same order are conjugate.

p -groups generated by elements of given order

1^o. In what follows, G is a group of order p^m , $\Omega_k^*(G) = \langle x \in G \mid o(x) = p^k \rangle$, where $p^k \leq \exp(G)$. Then $\Omega_k^*(G) \leq \Omega_k(G)$ and $\Omega_k^*(G)$ is the least subgroup H of G subjecting $c_k(H) = c_k(G)$. We have $\sum_{i=0}^{\infty} \varphi(p^i)c_i(G) = |G|$, where $\varphi(*)$ is Euler's totient function. Given $k > 0$, set $\text{sol}_k(G) = |\{x \in G \mid o(x) \leq p^k\}|$. Then $\text{sol}_k(G) = \sum_{i=0}^k \varphi(p^i)c_i(G)$. For definition of L_s- and U₂-groups, see §§17, 18, 67.

A 2-group G is said to be a U_n-group, if there is $E_{2^n} \cong R \triangleleft G$ such that G/R is of maximal class with cyclic subgroup T/R of index 2 and $\Omega_1(T) = R$. It is easy to show that R contains all normal elementary abelian subgroups of G and all elements in the set $G - T$ have orders ≤ 8 . A subgroup R is called the *kernel* of G .

For the sake of completeness, we collected in Lemma 64.1 some known facts. We use this lemma until end of the book.

Lemma 64.1. *Let G be a p -group.*

(a) (Theorems 7.1 and 7.2) *If G is regular of exponent p^e and $k \leq e$, then we have $\exp(\Omega_k(G)) = p^k$. All p -groups of class $< p$ are regular. Groups of exponent p are regular. Regular 2-groups are abelian.*

(b) (Theorem 12.1) *If G has no normal subgroups of order p^p and exponent p , it is either absolutely regular or of maximal class. If an irregular p -group G has an absolutely regular maximal subgroup H , then G is either of maximal class or $G = H\Omega_1(G)$, where $|\Omega_1(G)| = p^p$.*

(c) (Theorems 9.5 and 9.6) *A p -group of maximal class and order $> p^p$ is irregular. A p -group of maximal class and order p^m contains only one normal subgroup of order p^i for $1 \leq i \leq m - 2$.*

(d) (Theorem 9.6, Lemma 12.3) *A p -group of maximal class and order $> p^{p+1}$ has no normal subgroups of order p^p and exponent p . For such G , we have $c_1(G) \equiv 1 + p + \dots + p^{p-2} \pmod{p^p}$ and $c_2(G) \equiv p^{p-2} \pmod{p^{p-1}}$. If $p^2 < p^k \leq \exp(G)$, then $c_k(G) = 1$ if $p = 2$ (see Lemma 64.10, below) and p^{p-1} divides $c_k(G)$ if $p > 2$.*

(e) (Theorem 9.6) *An irregular p -group G of maximal class has an absolutely regular subgroup G_1 of index p such that $|\Omega_n(G_1)| = p^{(p-1)n}$ for $p^n < \exp(G_1) = \exp(G)$. If, in addition, $|G| > p^{p+1}$, then $Z(G_1)$ is noncyclic (G_1 is called the fundamental subgroup of G); all other maximal subgroups of G are of maximal class. If $2 < k \leq \exp(G)$, then $\Omega_k^*(G) \leq G_1$.*

(f) (Theorems 13.2 and 13.5) If G is neither absolutely regular nor of maximal class, then $c_1(G) \equiv 1 + p + \dots + p^{p-1} \pmod{p^p}$ and, for $k > 1$, $c_k(G) \equiv 0 \pmod{p^{p-1}}$. The number of subgroups of order p^p and exponent p in G is $\equiv 1 \pmod{p}$.

(g) (Theorem 13.19) If G is an irregular p -group of maximal class and $H \leq G$ is of order $> p^p$, then H is either absolutely regular or of maximal class.

(h) If $A \triangleleft G$ is of order p^{p-1} and exponent p , G is a p -group of maximal class and $R < G$ is of order p^p and exponent p , then $A < R$. Next, A is contained in every irregular subgroup of G .

(i) (Proposition 10.17) If $B \leq G$ is nonabelian of order p^3 such that $C_G(B) < B$, then G is of maximal class.

(j) (Corollary 18.7) Suppose that an irregular p -group G is not of maximal class, $k > 2$. Then $c_k(G) \equiv 0 \pmod{p^p}$, unless G is an L_p - or U_2 -group. In particular, in that case, $\text{sol}_k(G) \equiv 0 \pmod{p^{p+2}}$.

(k) Let $C < H < G$, where G is a 2-group which is not of maximal class, $|H : C| = 2$, C is cyclic. Then the number of subgroups of G of order $|H|$, that are of maximal class, is even.

(l) (Theorems 41.1 and 66.1) If G is minimal nonmetacyclic, then one of the following holds: (i) G is of order p^3 and exponent p , (ii) G is of order 3^4 and class 3, $|\Omega_1(G)| = 9$, (iii) $G = C_2 \times Q_8$, (iv) $G = Q_8 * C_4 \cong D_8 * C_8$ of order 2^4 , (v) G is special group of order 2^5 with $|\text{Z}(G)| = 2^2$. Thus, if $\Omega_2(G)$ is metacyclic then G is metacyclic.

(m) (Lemma 44.1, Corollary 44.6, Theorem 9.11) A p -group G is metacyclic if one of the following quotient groups is metacyclic: $G/\Phi(G')K_3(G)$, $G/\Phi(G')$, $G/K_3(G)$. If $p > 2$ and $|G/\mathfrak{U}_1(G)| \leq p^2$, then G is metacyclic (Huppert).

(n) (Theorem 44.5) A 2-group G is metacyclic if G and all its maximal subgroups are two-generator.

(o) (Corollary 44.9) If $G/\mathfrak{U}_2(G)$ is metacyclic then G is metacyclic.

(p) ([Bla5, Theorem 4.2]) If a p -group G , $p > 2$, and all its maximal subgroups are two-generator, then G is either metacyclic or $\mathfrak{U}_1(G) = K_3(G)$ is of index p^3 in G (in the last case, $|G : G'| = p^2$).

(q) (Tuan; see Lemma 1.1) If G is nonabelian and $A < G$ is abelian of index p , then $|G| = p|G'||\text{Z}(G)|$.

(r) (Lemma 4.2). If $|G'| = p$, then $G = (A_1 * \dots * A_s)\text{Z}(G)$, where A_1, \dots, A_s are minimal nonabelian; then $G/\text{Z}(G)$ is elementary abelian.

(s) (Taussky; Proposition 1.6) If G is a nonabelian 2-group with $|G : G'| = 4$, then G is of maximal class, i.e., dihedral, semidihedral or generalized quaternion.

(t) If a nonabelian p -group G has a cyclic subgroup of index p , then G is either M_{p^n} or $p = 2$ and G is of maximal class (see (s)).

- (u) (see Exercise 1.69) If $U, V \in \Gamma_1$ are distinct, then $|G' : U'V'| \leq p$.
- (v) (Lemma 1.4) Let M be a G -invariant subgroup of $\Phi(G)$. If $Z(M)$ is cyclic, M is also cyclic. In particular, M cannot be nonabelian of order p^3 .
- (w) (Exercise 9.13) If a p -group G of maximal class, $p > 2$, has a subgroup H with $d(H) > p - 1$, then G is isomorphic to a Sylow p -subgroup of S_{p^2} .
- (x) (§5) $c_1(G) \equiv 1 + p \pmod{p^2}$ and, for $k > 1$, $c_k(G) \equiv 0 \pmod{p}$, unless G is either cyclic or a 2-group of maximal class. Under the last exceptions, G has a normal abelian subgroup of type (p, p) .
- (y) If $\langle U' \mid U \in \Gamma_1 \rangle < G'$, then $d(G) = 2$.

Let us prove parts (g), (h), (y) of Lemma 64.1.

Proof of Lemma 64.1(g). Let $|G| > p^{p+1}$. If $|G| = p^{p+2}$, the result follows from Theorem 9.6. Now let $|G| > p^{p+2}$ and $H \not\leq G_1$, where G_1 is the fundamental subgroup of G . Let $H < M \in \Gamma_1$; then $M (\neq G_1)$ is of maximal class (Lemma J(e)) and $M_1 = M \cap G_1 = \Phi(G)$ is the fundamental subgroup of M since $|M| > p^{p+1}$. Then, by induction on $|G|$, H is of maximal class since $H \not\leq M_1$. \square

Proof of Lemma 64.1(h). We have $A = \Omega_1(\Phi(G))$. One may assume that $|G| > p^{p+1}$ (if $|G| = p^{p+1}$, then $A = \Phi(G)$). Let $R < G$ be either of order p^p and exponent p or irregular. Since $|\Omega_1(R \cap G_1)| = p^{p-1}$, the result follows. \square

Proof of Lemma 64.1(y). Set $D = \langle U' \mid U \in \Gamma_1 \rangle$. Since, by hypothesis, $D < G'$, there exist $x, y \in G$ such that $[x, y] \notin D$. Assume that $H = \langle x, y \rangle \leq M \in \Gamma_1$; then $M' \not\leq D$, a contradiction. Thus, $H = G$. \square

2^o. We begin with the following

Definition 1 (Ito). Let G be a group of order p^m . Then G is called *one-stepped* if there exist m elements x_1, \dots, x_m of order p in G such that $|\langle x_1, \dots, x_i \rangle| = p^i$ for $i = 1, \dots, m$. We consider the identity group $\{1\}$ as one-stepped.

Lemma 64.2. A p -group G is one-stepped if and only if $\Omega_1(G) = G$.

Proof. We have to prove that if $\Omega_1(G) = G$, then G is one-stepped. Let $H \leq G$ be one-stepped of maximal order. Assume that $H < G$. Set $N = N_G(H)$. If $N - H$ has an element x of order p , then $H_1 = \langle x, H \rangle$ is one-stepped of order $> |H|$, a contradiction. Thus, $H = \Omega_1(N)$, i.e., H is characteristic in N . Then $N = G > H = \Omega_1(G) = G$, a contradiction. \square

Lemma 64.3. Suppose that $A < G$ are one-stepped p -groups and $|G : A| = p^n$. Then there are $x_1, \dots, x_n \in G - A$ of order p such that $|A_i : A_{i-1}| = p$, where $A_0 = A$, $A_i = \langle A, x_1, \dots, x_i \rangle$ for $i = 1, \dots, n$.

Proof. Suppose that A_i has constructed. Assuming that $A_i < G$, we have to construct A_{i+1} . Set $N_i = N_G(A_i)$. As in the proof of Lemma 64.2, there is $x_{i+1} \in N_i - A_i$ of order p . Set $A_{i+1} = \langle x_{i+1}, A_i \rangle$. Then $A_n = G$. \square

A series $A = A_0 < A_1 < \dots < A_n = G$, constructed in Lemma 64.3, we call the *Ito series* or (*Ito 1-series*; see below) connecting $A = A_0$ with G .

3°. In this subsection we give some estimates of the order of a p -group $G = \Omega_k^*(G)$ in terms of $c_k(G)$. For p -groups of maximal class and order $> p^{p+1}$ these estimates are best possible.

Set $\sigma(G) = [\frac{1}{p^p} \cdot c_1(G)]$ and, for $k > 1$, set $\tau_k(G) = [\frac{1}{p^{p-1}} \cdot c_k(G)]$.

Theorem 64.4. *Suppose that a one-stepped p -group G is not a group of maximal class. Then $|G| \leq p^{p+1+\sigma(G)}$.*

Proof. We use induction on $|G|$. One may assume that $|G| = p^m > p^{p+1}$ (otherwise, there is nothing to prove). If G is regular, then $\exp(G) = p$ (Lemma 64.1(a)), $c_1(G) = 1 + p + \dots + p^{m-1}$, and we have to check only that

$$m \leq 1 + p + \left[\frac{1}{p^p} \cdot (1 + p + \dots + p^{m-1}) \right] = 1 + p + (1 + p + \dots + p^{m-p-1}).$$

This is true since $1 + p + \dots + p^{m-p-1} \geq 1 + m - p - 1 = m - p$.

Now let G be irregular. Then there is $R \triangleleft G$ of order p^p and exponent p (Lemma 64.1(b)) and $x \in G - R$ of order p . Set $A = A_0 = \langle x, R \rangle$. Let $A = A_0 < A_1 < \dots < A_n = G$ be an Ito series connecting $A = A_0$ with G . Then $|G| = |A_0| \cdot p^n = p^{p+1+n}$ so it suffices to prove that $n \leq \sigma(G)$. For $i = 0, 1, \dots, n-1$ we have $c_1(A_{i+1}) > c_1(A_i)$ and, since A_{i+1} is not of maximal class in view of $R \triangleleft A_i$ and $|A_{i+1}| > p^{p+1}$ (Lemma 64.1(d)), we get $c_1(A_{i+1}) \equiv c_1(A_i) \pmod{p^p}$ (Lemma 64.1(f)), so

$$c_1(G) \geq c_1(A_0) + n \cdot p^p \geq (1 + p + \dots + p^{p-1}) + n \cdot p^p.$$

However, by Lemma 64.1(f), $c_1(G) = 1 + p + \dots + p^{p-1} + \sigma(G) \cdot p^p$ so $n \leq \sigma(G)$. \square

Corollary 64.5. *If a p -group G is not of maximal class, then $|\Omega_1(G)| \leq p^{p+1+\sigma(G)}$ so, if $p = 2$ and $c_1(G) = 4k + 3$, then $|\Omega_1(G)| \leq 2^{3+k}$.*

Let G be one-stepped of maximal class and order $p^m > p^{p+1}$ and let $G_1 < G$ be the fundamental subgroup. Then $R = \Omega_1(G_1) \triangleleft G$ is of order p^{p-1} and exponent p . Let $x \in G - R$ be of order p ; then $H = \langle x, R \rangle$ is of order p^p and exponent p (Lemma 64.1(a)). By Lemma 64.1(g), $N_G(H)$ is of maximal class and order p^{p+1} so there are exactly $|G : N_G(H)| = p^{m-p-1}$ conjugates with H in G . All these conjugates contain exactly

$$c_1(R) + (c_1(H) - c_1(R))p^{m-p-1} = 1 + p + \dots + p^{p-2} + p^{m-2}$$

distinct subgroups of order p and they generate $M \in \Gamma_1$ (take into account the above formula!). Since G is one-stepped, there is $y \in G - M$ of order p . Setting $H_1 = \langle y, R \rangle$, we, as above, obtain at least p^{m-2} new subgroups of order p that together with R generate $M_1 \in \Gamma_1 - \{M\}$. Let λ_G be the number of one-stepped members in the set Γ_1 . Then (see Lemma 12.3) we get

$$1 + p + \cdots + p^{p-2} + \sigma(G) \cdot p^p = c_1(G) \geq \lambda_G \cdot p^{m-2}.$$

It follows that $p^m \leq \frac{p^{p+2}}{\lambda_G} \cdot \sigma(G)$. Since G is one-stepped, $p \geq \lambda_G > 1$ so we obtain

Theorem 64.6. *Let G be a one-stepped p -group of maximal class and order $> p^{p+1}$. Then $|G| \leq p^{p+1} \cdot \sigma(G)$ or, what is the same. $|G| \leq p \cdot c'_1(G)$, where $c'_1(G)$ is the number of subgroups of order p not contained in G_1 .*

Definition 2. A p -group G is said to be *k-stepped* if it has elements x_1, \dots, x_t , all of order p^k , such that $G = \langle x_1, \dots, x_t \rangle$ and $|A_i : A_{i-1}| > 1$, where $A_i = \langle x_1, \dots, x_i \rangle$ and $x_i \in N_G(A_{i-1})$ for $i = 1, \dots, t$. If $\Omega_k^*(A) = A = A_0 < G$ and there are elements x_1, \dots, x_n , all of order p^k , such that, denoting $A_i = \langle A_0, x_1, \dots, x_i \rangle$, we have $x_i \in N_G(A_{i-1})$ and $A_n = G$, then the series $A_0 < A_1 < \cdots < A_n = G$ is said to be an *Ito k-series* connecting A_0 with G .

If $A_0 < A_1 < \cdots < A_n = G$ is an Ito k -series connecting A_0 with G , then $|G : A_0| \leq p^{kn}$. As in Lemma 64.2, G is k -stepped if and only if $\Omega_k^*(G) = G$. If $A = A_0$ is a k -stepped subgroup of a k -stepped p -group G , then there exists an Ito k -series $A_0 < A_1 < \cdots < A_n < G$ connecting A_0 with G .

Lemma 64.7. *Let $R \triangleleft G$ be of order p^p and exponent p and let G/R be cyclic of order $> p$. Then $\exp(\Omega_j(G)) = p^j$ for all j with $p^j \leq p^e = \exp(G)$. Next, $\Omega_e^*(G) = G$, i.e., G is e -stepped. If G/R is of order p^e , then $c_e(G) = p^p$. If G/R is of order p^{e-1} (in that case $\Omega_1(G) = R$), then $c_e(G) = p^{p-1}$.*

Proof. It suffices to show that $\exp(\Omega_1(G)) = p$. However, this follows from Lemma 17.4(c). \square

Let $k > 2$ and suppose that a p -group $G = \Omega_k^*(G)$ is not absolutely regular (by Theorem 13.19, G is not of maximal class); then there is $R \triangleleft G$ of order p^p and exponent p (Lemma 64.1(b)). Take in G an element x_0 of order p^k and set $A_0 = \langle x_0, R \rangle$; then $p^{p+k-1} \leq |A_0| \leq |R|p^k = p^{p+k}$. By Lemma 64.7, A_0 is k -stepped. Let $A_0 < A_1 < \cdots < A_n = G$ be an Ito k -series connecting A_0 with G . Since $c_k(A_0) \geq p^{p-1}$ and $c_k(A_1) > c_k(A_0) \geq p^{p-1}$, A_1 is not an L_p -group. Next, if $p = 2$ and $k > 3$, then A_1 is not a U_2 -group. Then, if $p > 2$, then $c_k(A_1) \geq p^p$ (Lemma 64.1(j)), and this is also true for $p = 2$. It follows that $c_k(A_{i+1}) > c_k(A_i)$, and, by Lemma 64.1(j), $c_k(A_{i+1}) \equiv c_k(A_i) \pmod{p^p}$, $i = 1, \dots, n-1$, so we have $\tau_k(G)p^{p-1} = c_k(G) \geq c_k(A_1) + (n-1)p^p \geq np^p$, hence $\tau_k(G) \geq np$, and we conclude that $|G| \leq |A_0|p^{kn} \leq p^{p+k+k[\frac{1}{p}\tau_k(G)]}$. Thus, we have

Theorem 64.8. Suppose that $k > 2$ and a k -stepped p -group G of order p^m is neither absolutely regular nor of maximal class. Then $m \leq p + k + \frac{k}{p}\tau_k(G)$.

Corollary 64.9. Let $k > 2$ and let a p -group G be neither absolutely regular nor of maximal class. Then $|\Omega_k^*(G)| \leq p^{p+k+k \cdot \lceil \frac{1}{p}\tau_k(G) \rceil}$.

The case $k = 2$ we consider for p -groups of maximal class only.

Let $G = \Omega_2^*(G)$ be a p -group of maximal class, $k > 1$, $|G| = p^m \geq p^{2p}$ and $p > 2$; then $k = 2$ (Lemma 64.1(e)) and $\exp(G) > p^2$. Let $c'_2(G)$ be the number of cyclic subgroups of order p^2 in G not contained in G_1 . Set $R = \Omega_1(G_1)$, where $G_1 < G$ is fundamental; then $|R| = p^{p-1}$. Let $x \in G - G_1$ be of order p^2 . Set $A = \langle x, R \rangle$; then A is absolutely regular of order p^p since $x^p \in Z(G_1)$ (Theorem 13.19). Set $N = N_G(A)$. Since $N \not\leq G_1$ and $|N| > p^p$, N is of maximal class (Lemma 64.1(g)). Since $A \not\leq G$, we get $N < G$ so A is not characteristic in N and hence $\Omega_2^*(N) > A$. Then $|N : A| = p$ (every normal subgroup of index $> p$ in N is characteristic) so there are exactly $|G : N| = p^{m-p-1}$ subgroups conjugate with A in G ; their intersection equals R so their contribution in $c'_2(G)$ is equal to $p^{m-p-1}c_2(A) = p^{m-p-1}p^{p-2} = p^{m-3}$. These G -conjugates of A generate $M \in \Gamma_1$ (every normal subgroup of index $\geq p^2$ in G is contained in $\Phi(G) < G_1$). We have $G_1 \cap M = \Phi(G)$. Since $m \geq 2p$, we get $\Omega_2(G_1) \leq \Phi(G)$. Since G is 2-stepped, there is $y \in G - M$ of order p^2 ; by the above, also $y \in G - G_1$. Set $A_1 = \langle y, R \rangle$; then $A \cap A_1 = R$. As above, the G -conjugates of A_1 generate $M_1 \in \Gamma_1 - \{M\}$; their intersection equals R again. Let μ_G be the number of 2-stepped members in the set Γ_1 . Then $c'_2(G) = \mu_G \cdot p^{m-3}$ so $|G| = p^m = \frac{p^3}{\mu_G} \cdot c'_2(G)$. If $p = 2$, then $G \cong Q_{2^m}$ since $\Omega_2^*(G) = G$, and equality is attained. Thus we have

Supplement to Theorem 64.8. If G is a 2-stepped p -group of maximal class and order $\geq p^{2p}$, then $|G| = \frac{p^3}{\mu_G} \cdot c'_2(G)$, where μ_G is the number of 2-stepped members in the set Γ_1 .

Theorem 64.10. Let a p -group G , $c_1(G) = 1 + p + p^2$ and $\exp(\Omega_1(G)) > p$. Then $p = 2$, $\Omega_1(G) = D_8 * C_2$ is of order 2^4 and one of the following holds:

- (a) $G = D * C$, where $D_8 \cong D$, C is cyclic of order ≥ 4 , $D \cap C = Z(D)$.
- (b) $G = DC$, where $D_8 \cong D \triangleleft G$, C is nonnormal cyclic of index 4 in G , $D \cap C = Z(D)$ and $C_G(D) = Z(G)$ has index 2 in C , $G/C_G(D) \cong D_8$.
- (c) $G = DQ$, where $D_8 \cong D \triangleleft G$, Q is a nonnormal generalized quaternion group of index 4 in G , $D \cap Q = Z(D)$, $C_G(D)$ is a cyclic subgroup of index 2 in Q , $G/C_G(D) \cong D_8$. If L is a cyclic subgroup of order 4 in Q such that $L \not\leq C_G(D)$, then $DL \cong SD_{2^4}$.

Proof. Let $p > 2$. Let $E_{p^2} \cong R \triangleleft G$ and let $x \in G - R$ be of order p in $G - R$; then $H = \langle x, R \rangle$ is of order p^3 and exponent p . Since $c_1(G) = c_1(H)$, $\Omega_1(G) = H$ is of order p^3 and exponent p , a contradiction. For $p = 2$, the assertion coincides with Theorem 43.9. \square

4^o. In this subsection we study p -groups G with small $c_k(G)$.

Proposition 64.11. *Let G be a p -group, $p > 2$, with $\Omega_1(G) = G$, $c_1(G) = 1 + p + \dots + p^p$ and $\exp(G) > p$. Then:*

- (a) *G is irregular of order p^{p+2} ; all members of the set Γ_1 have exponent p^2 .*
- (b) *$d(G) = 3$, $\Phi(G) = G'$ is of order p^{p-1} and exponent p , $cl(G) = p$.*
- (c) *$G/\mathfrak{V}_1(G)$ is of order p^{p+1} and exponent p , $\mathfrak{V}_1(G) = K_p(G)$.*
- (d) *$c_2(G) = p^p$.*
- (e) *$\Gamma_1 = \{M_1, \dots, M_{p^2}, T_1, \dots, T_{p+1}\}$, where M_1, \dots, M_{p^2} are of maximal class, T_1, \dots, T_{p+1} are not generated by two elements so regular and have exponent p^2 . Next, $\eta(G) = \bigcap_{i=1}^{p+1} T_i$ has exponent p^2 and index p^2 in G , where $\eta(G)/K_3(G) = Z(G/K_3(G))$.*
- (f) *G has exactly $p+1$ subgroups of order p^p and exponent p , all those subgroups contain $\Phi(G)$ so normal in G .*
- (g) *Exactly p^2 subgroups of G of order p^p , containing $\Phi(G)$, have exponent p^2 .*
- (h) *If L is a subgroup of order p^p and exponent p in G , then exactly p maximal subgroups of G , containing L , are of maximal class.*
- (i) *Let $S \in \Gamma_2$ be of exponent p^2 . If $S \neq \eta(G)$ (see (e)), then S is contained in exactly p irregular members of the set Γ_1 .*

Proof. By Theorems 12.3 and 7.2(b), G is neither of maximal class nor absolutely regular so there is $R \triangleleft G$ of order p^p and exponent p (Theorem 12.1(a)).

(a) By Theorem 64.1(a), G is irregular. By Theorem 64.4, $|G| \leq p^{p+1+\sigma(G)} = p^{p+2}$, since $\sigma(G) = [\frac{1}{p^p} c_1(G)] = 1$; here $[x]$ is the integer part of $x \in \mathbb{R}$. Since $\Omega_1(G) = G$, we get $G/R \cong E_{p^2}$ so $\exp(G) = p^2$. We also have $|G| = p^{p+2}$. Assume that $\exp(H) = p$ for some $H \in \Gamma_1$. Then $c_1(H) = c_1(G)$ so $(G =) \Omega_1(G) = H$ has exponent p , a contradiction. Thus, all members of the set Γ_1 have exponent p^2 .

(b) If $x \in G - R$ is of order p , then $\exp(\langle x, R \rangle) > p$, by (a), so $M = \langle x, R \rangle \in \Gamma_1$ is of maximal class (Theorem 7.1); then $d(G) = 3$ and $\Phi(G) = G' = \Phi(M) = M'$ has exponent p , by (a) and Theorem 12.12(a), and we conclude that $cl(G) = p$.

(c) follows from Theorem 12.12(b).

(d) follows from (a) and the hypothesis. Indeed, $c_2(G) = \frac{|G|-(p-1)c_1(G)-1}{\varphi(p^2)} = p^p$.

(e) The first assertion follows from Theorem 12.12(c). Now assume $\exp(\eta(G)) = p$. Then $c_2(T_i) = \frac{1}{p(p-1)}(|T_i| - |\eta(G)|) = p^{p-1}$ for $i = 1, \dots, p+1$ so $c_2(G) = \sum_{i=1}^{p+1} c_2(T_i) = (p+1)p^{p-1} > p^p$, contrary to (d). Thus, $\exp(\eta(G)) = p^2$.

(f) Assume that $S < G$ of order p^p and exponent p is not normal in G ; then $\Phi(G) = G' \not\leq S$ so $H = S\Phi(G) \in \Gamma_1$. It follows from Theorem 7.2(b) and (a) that

H is irregular so it is of maximal class; in that case, $\Phi(G) = \Phi(H)$ (compare orders!) so $H = S \not\in \Gamma_1$, a contradiction. If t is the number of subgroups of order p^p and exponent p in G , then

$$1 + p + \cdots + p^{p-1} + p^p = c_1(G) = c_1(\Phi(G)) + tp^{p-1} = 1 + p + \cdots + p^{p-2} + tp^{p-1}$$

so $t = p + 1$.

(g) follows from (a), (b) and (f).

(h,i) By (e), the intersection of two distinct regular maximal subgroups of G coincides with $\eta(G)$. Let $L \neq \eta(G)$ be a normal subgroup of index p^2 in G ; then L is contained in at most one regular maximal subgroup of G and $G/L \cong E_{p^2}$ since $\Omega_1(G) = G$. Let D be a G -invariant subgroup of index p^2 in L . Set $C = C_G(L/D)$. Let $L < H \leq C$, where $H \in \Gamma_1$; then H is regular. It follows that L is contained in exactly one regular member of the set Γ_1 , and the proof is complete. \square

Exercise 1. Suppose that $G = \Omega_1(G)$ is an irregular p -group containing exactly $p+1$ subgroups of order p^p and exponent p . Then $c_1(G) = 1 + p + \cdots + p^p$. If $p = 2$, then $\Omega_1(G) = Q_8 * C_4$.

Exercise 2. Let G be a p -group of maximal class, $p > 2$. Then $\Omega_1(G) = G$ or $\Omega_2^*(G) = G$. (*Hint.* $\Omega_1(G)\Omega_2^*(G) = \Omega_2(G) = G$. Since any two normal subgroups of G of distinct orders are incident, we are done.)

Proposition 64.12. Suppose that a p -group G , $p > 2$, is such that $c_k(G) = p^{p-2}$ for $k > 1$. Then one of the following holds:

- (i) G is regular with cyclic $G/\Omega_{k-1}(G)$ and $|\Omega_{k-1}(G)| = p^{p+k-3}$.
- (ii) $k = 2$ and G is of maximal class and order p^{p+1} having exactly p subgroups of order p^p and exponent p .

Proof. (i) Let G be regular and $|\Omega_k(G)| = p^a$, $|\Omega_{k-1}(G)| = p^b$. Then

$$p^{p-2} = c_k(G) = \frac{|\Omega_k(G)| - |\Omega_{k-1}(G)|}{p^{k-1}(p-1)} = \frac{p^{a-b} - 1}{p-1} p^{b-k+1}.$$

It follows that $a - b = 1$ so $|\Omega_k(G)/\Omega_{k-1}(G)| = p$, and we conclude that the quotient group $G/\Omega_{k-1}(G)$ is cyclic. Then $p-2 = b-k+1$ so $|\Omega_{k-1}(G)| = p^b = p^{p+k-3}$.

(ii) Now let G be irregular. By Lemma 64.1(f), G is of maximal class. Assume that $|G| > p^{p+1}$. Let G_1 be the fundamental subgroup of G ; then $|\Omega_{k-1}(G_1)| = p^{(k-1)(p-1)}$. If $k > 2$, then

$$c_k(G_1) = \frac{|\Omega_k(G_1)| - |\Omega_{k-1}(G_1)|}{\varphi(p^k)} \geq \frac{p^{(k-1)(p-1)+1} - p^{(k-1)(p-1)}}{(p-1)p^{k-1}},$$

$$p^{(k-1)(p-2)} > p^{p-2} = c_k(G),$$

a contradiction. Thus, $k = 2$. Then $|\Omega_2(G_1)| \geq p^{(p-1)+2} = p^{p+1}$ so

$$c_2(G_1) \geq \frac{p^{p+1} - p^{p-1}}{p(p-1)} = p^{p-2}(p+1) > p^{p-2} = c_2(G),$$

again a contradiction. Thus, $|G| = p^{p+1}$. The second assertion in (ii) is checked easily. \square

\mathcal{A}_2 -groups

A p -group G is said to be an \mathcal{A}_n -group if it contains a nonabelian subgroup of index p^{n-1} but all its subgroups of index p^n are abelian.

Lemma 65.1 (= Exercise 1.8a (Redei)). *Let G be a minimal nonabelian p -group (= \mathcal{A}_1 -group). Then $G = \langle a, b \rangle$ and one of the following holds:*

- (a) $a^{p^m} = b^{p^n} = c^p = 1$, $[a, b] = c$, $[a, c] = [b, c] = 1$, $|G| = p^{m+n+1}$,
 $G = \langle b \rangle \cdot (\langle a \rangle \times \langle c \rangle) = \langle a \rangle \cdot (\langle b \rangle \times \langle c \rangle)$ is nonmetacyclic.
- (b) $a^{p^m} = b^{p^n} = 1$, $a^b = a^{1+p^{m-1}}$, $|G| = p^{m+n}$ and $G = \langle b \rangle \cdot \langle a \rangle$ is metacyclic.
- (c) $a^4 = 1$, $a^2 = b^2$, $a^b = a^{-1}$, $G \cong Q_8$.

We have $|G'| = p$ and $H/\Omega_1(H)| \leq p^3$ for $H \leq G$. If $|G| > p^3$ and $|\Omega_1(G)| \leq p^2$, then G is metacyclic. The group G is nonmetacyclic if and only if G' is a maximal cyclic subgroup of G . Next, $|G/\Omega_1(G)| \leq p^3$ with equality if and only if G is from (a) and $p > 2$. If, in (a), $u \in G - \Phi(G)$, then $\langle u \rangle$ is not normal in G .

Suppose that $G' < L < G$, where L is cyclic of order p^2 . By Theorem 6.1, $L/G' \leq C/G'$, where C/G' is a cyclic direct factor of G/G' ; in particular, G/C is cyclic. It remains to show that C is cyclic. We get $G' = \Phi(L) \leq \Phi(C)$. It follows that $C/\Phi(C)$ as an epimorphic image of a cyclic group $C/\Phi(L)$, is cyclic so C is cyclic and G is metacyclic. The last assertion of Lemma 65.1 is a partial case of the following general fact. If a nonmetacyclic $G = \langle u, v \rangle$, then $\langle u \rangle \not\trianglelefteq G$.

The aim of this section is to clear up the subgroup and normal structure of \mathcal{A}_2 -groups. Using comparatively easy arguments, we obtain a lot of information on \mathcal{A}_2 -groups which is difficult to read out from their defining relations. Some results which we shall prove in the sequel, are contained in the thesis of Lev Kazarin (unpublished), however, the proofs presented below, as a rule, are new. The length of [She], also devoted to classification of \mathcal{A}_2 -groups, indicates the degree of the difficulty of this problem.

Every nonabelian group of order p^4 is either an \mathcal{A}_1 - or \mathcal{A}_2 -group. Therefore, in what follows, we assume that $|G| = p^m > p^4$. \mathcal{A}_2 -groups belong to a wider class of p -groups all of whose nonabelian subgroups are normal.

Lemma 65.2. *Let G be a nonabelian p -group. Then:*

- (a) *If $G' \leq \Omega_1(Z(G))$ and $d(G) = 2$, then G is an \mathcal{A}_1 -group.*

- (b) If G is metacyclic with $|G'| = p^2$, then G is an \mathcal{A}_2 -group.
- (c) If G has two distinct abelian maximal subgroups, then $|G'| = p$.
- (d) Suppose that $|H'| \leq p$ for all $H \in \Gamma_1$. Then $|G'| \leq p^3$ and G' is abelian. If $F, H \in \Gamma_1$ are distinct and $F' \leq H'$, then $|G'| \leq p^2$. If $|G'| = p^3$, then G has no abelian maximal subgroups, and if, in addition, $d(G) > 2$, then $d(G) = 3$ and $E_{p^3} \cong G' \leq Z(G)$.
- (e) If $G' \cap Z(G)$ is cyclic and $|H'| \leq p$ for all $H \in \Gamma_1$, then $|G'| \leq p^2$. If, in addition, $G' \not\leq Z(G)$, then $d(G) = 2$ and $G/(G' \cap Z(G))$ is an \mathcal{A}_1 -group.

Proof. (a) If $a, b \in G$, then $1 = [a, b]^p = [a, b^p]$ so $\mathfrak{U}_1(G) \leq Z(G)$. Then $\Phi(G) = G'\mathfrak{U}_1(G) \leq Z(G)$ so $Z(G) = \Phi(G)$ has index p^2 in G . Hence, all members of the set Γ_1 are abelian so G is an \mathcal{A}_1 -group.

(b) By Lemma 65.1, G is not an \mathcal{A}_1 -group. Let $L = \mathfrak{U}_1(G')$ and $H \in \Gamma_1$; then $L < G' < H$. By (a), G/L is an \mathcal{A}_1 -group so H/L is abelian; then, again by (a), H is either abelian or an \mathcal{A}_1 -group. Thus, G is an \mathcal{A}_2 -group.

(c) follows from Lemma 64.1(u).

(d) Let $F, H \in \Gamma_1$ be distinct. Then $|G'| \leq p|F'H'| \leq p^3$ (Lemma 64.1(u)). If, in addition, $F' \leq H'$, then $|G'| \leq p^2$. Now let $|G'| = p^3$. Since $F' \not\leq H'$ and $H' \not\leq F'$, Γ_1 has no abelian members. Let, in addition, $d(G) > 2$. Then $A' \neq B'$ for distinct $A, B \in \Gamma_1$ so $c_1(G') \geq |\Gamma_1| \geq 1 + p + p^2$, and we get $d(G') = 3$, $E_{p^3} \cong G' \leq Z(G)$. Therefore, since $1 + p + p^2 = c_1(G') = |\Gamma_1|$, we get $d(G) = 3$.

(e) We have $D = \langle H' \mid H \in \Gamma_1 \rangle \leq \Omega_1(G' \cap Z(G))$ so $|D| = p$ since $\Omega_1(G' \cap Z(G))$ is cyclic. Then G/D is either abelian or \mathcal{A}_1 -group so $|(G/D)'| \leq p$ (Lemma 65.1), and we get $|G'| \leq p^2$. Let, in addition, $G' \not\leq Z(G)$. Then G/D is nonabelian so it is an \mathcal{A}_1 -group. Since $D < \Phi(G)$, we get $d(G) = d(G/D) = 2$. \square

Corollary 65.3. A metacyclic p -group G is an \mathcal{A}_2 -group if and only if $|G'| = p^2$.

Remarks. 1. Let us prove that if a p -group G has the cyclic derived subgroup G' , then all elements of G' are commutators. We have $G' = \langle [x, y] \rangle$ for some $x, y \in G$. One may assume that $G = \langle x, y \rangle$. By Lemma 64.1(u), there is $H \in \Gamma_1$ such that $H' = \mathfrak{U}_1(G')$. By induction, all elements of H' are commutators. By [BZ, Theorem 3.27], all generators of G' , i.e., members of the set $G' - H'$, are commutators, completing the proof.

2. Let us prove that if G of order p^4 and exponent p has no nontrivial direct factors, it is of class 3. Let H be an \mathcal{A}_1 -subgroup of G ; then $|H| = p^3$. If $Z(G) \not\leq H$, then $G = H \times C$, where $C < Z(G)$ is of order p such that $C \not\leq H$. Thus, $Z(G) < H$ so $Z(G)$ is of order p . Since $C_G(H) = Z(G)$, we get $C_G(H) < H$. Then G is of maximal class (Proposition 10.17).

Lemma 65.4. Let G be an \mathcal{A}_2 -group of order $p^m > p^4$.

(a) If $K \leq G$, then $|K/\mathfrak{U}_1(K)| \leq p^4$, and this estimate is best possible.

(b) If $K < G$ with $|K/\mathfrak{U}_1(K)| = p^4$, then $E_{p^4} \cong \Omega_1(K) \triangleleft G$ and, if $\Omega_1(K) \leq H \in \Gamma_1$, then H is abelian. If, in addition, $|G'| > p$, then $|G'| = p^2$, $|G : Z(G)| = p^3$ and $G/\Omega_1(K)$ is cyclic.

(c) If $K \triangleleft G$ and G/K is generated by subgroups of index p^2 , then $K \leq Z(G)$. In particular, if $d(G) = 3$, then $\Phi(G) \leq Z(G)$.

(d) Let $|G'| = p$. Then either $G = H \times C$, $|C| = p$ or $G = H * Z$, where $H \in \Gamma_1$ is an \mathcal{A}_1 -subgroup and Z is cyclic of order p^2 .

(e) $\mathfrak{U}_2(G) \leq Z(G)$. If $p > 2$ and G is not metacyclic, then $\mathfrak{U}_1(G) \leq Z(G)$ and $|G/Z(G)| \leq p^3$.

(f) Let $|G/\mathfrak{U}_1(G)| = p^4$, $m > 5$ and $G' \not\leq Z(G)$. Then $p > 2$, $G' \cong E_{p^2}$, $\text{cl}(G/\mathfrak{U}_1(G)) = 3$, $\mathfrak{U}_1(G) \leq Z(G)$ is cyclic, $G/G' \cong C_{p^{m-3}} \times C_p$ so $d(G) = 2$. If L/G' is a direct factor of G/G' of order p , then $L \cong E_{p^3}$ and $G = Z \cdot L$ is a semidirect product of L with a cyclic subgroup Z of order p^{m-3} hence $\mathfrak{U}_1(G) = \mathfrak{U}_1(Z)$, $\Omega_1(G) = L \times \Omega_1(\mathfrak{U}_1(G)) \cong E_{p^4}$, $G' \cap \mathfrak{U}_1(G) = \{1\}$ and G is an L_4 -group (see §§I7, I8). Next, $G/(G' \cap Z(G))$ is an \mathcal{A}_1 -group.

(g) If $|G'| = p^3$ and $d(G) = 2$, then $p > 2$ and $|G| = p^5$.

(h) If $G/Z(G)$ is nonabelian, then $G/(G' \cap Z(G))$ is an \mathcal{A}_1 -group.

(i) Let G be metacyclic. Then $G/Z(G)$ is of order $\leq p^4$ and exponent p^2 . If the number $|G/Z(G)| = p^3$, then $p = 2$ and $G/Z(G) \cong D_8$. Now suppose that $|G/Z(G)| = p^4$. If $p = 2$, then $G/Z(G)$ is abelian of type $(4, 4)$. If $p > 2$, then $G/Z(G)$ can be abelian or nonabelian of exponent p^2 (see examples following the lemma).

(j) If G has no normal elementary abelian subgroups of order p^3 , then it is either metacyclic or minimal nonmetacyclic.

Proof. (a) In view of Lemma 65.1, one may assume that $K < G$. Suppose that $|K/\mathfrak{U}_1(K)| > p^3$. Then K is not a subgroup of an \mathcal{A}_1 -group (Lemma 65.1) so it is abelian. Considering $K \cap A$, where $A \in \Gamma_1$ is nonabelian, we get $|\Omega_1(K)| \leq p^4$ (Lemma 65.1), and we are done since $|K/\mathfrak{U}_1(K)| = |\Omega_1(K)|$. If \mathcal{A}_2 -group $G = U \times C$, where U is a nonmetacyclic \mathcal{A}_1 -group of order $> p^3$ and $|C| = p$, then $\Omega_1(G)$ is of order p^4 and exponent p .

(b) Let $|K/\mathfrak{U}_1(K)| = p^4$ for $K < G$. Then every member of the set Γ_1 containing K is abelian (Lemma 65.1) so $E_{p^4} \cong \Omega_1(K) \triangleleft G$. Let, in addition, $|G'| > p$. Then $G/\Omega_1(K)$ is cyclic since the set Γ_1 has exactly one abelian member (Lemma 65.2(c)). By Lemma 65.2(d), $|G'| = p^2$ so $|G : Z(G)| = p^3$ (Lemma 64.1(q)).

(c) Let $R/K < G/K$ be of index p^2 in G/K . Then R is abelian so $R \leq C_G(K)$ and $K \leq Z(G)$ since $G = \langle R < G \mid K < R, |G : R| = p^2 \rangle$. Now the second assertion follows.

(d) This follows from Lemma 64.1(r).

(e) If there is $K \triangleleft G$ such that G/K is of order p^3 and exponent p , then $K \leq Z(G)$, by (c), so we are done since $\mathfrak{U}_2(G) \leq K$. Now assume that such K does not exist. Then $G/\mathfrak{U}_1(G) \cong E_{p^2}$. If $\mathfrak{U}_1(G)$ is cyclic, then $p = 2$, $m = 4$ and so $\mathfrak{U}_2(G) = Z(G)$ (Lemma 64.1(t)). Now let $\mathfrak{U}_1(G)$ be noncyclic. Then $\mathfrak{U}_1(G)$ has a G -invariant subgroup T such that $\mathfrak{U}_1(G)/T \cong E_{p^2}$. In that case, $\mathfrak{U}_2(G) \leq T$ and the result follows from (c).

(f) Since $d(G) \leq 3$, we get $p > 2$. By (c), $\mathfrak{U}_1(G) < Z(G)$. Next, $G/\mathfrak{U}_1(G)$ has an abelian subgroup $A/\mathfrak{U}_1(G)$ of index p ; $d(A) \geq d(A/\mathfrak{U}_1(G)) = 3$ so A is abelian (Lemma 65.1). Then $|G'| = p^2$ (Lemma 64.1(u)) so $|G/Z(G)| = p^3$ (Lemma 64.1(q)). By Corollary 65.3, $G' \cong E_{p^2}$ since G is nonmetacyclic. By the above, $A/\mathfrak{U}_1(G)$ is the unique abelian maximal subgroup of $G/\mathfrak{U}_1(G)$, and we conclude that $d(G/\mathfrak{U}_1(G)) = 2$; then $d(G) = 2$ since $\mathfrak{U}_1(G) < \Phi(G)$. It follows that $\text{cl}(G/\mathfrak{U}_1(G)) = 3$ (Remark 2). Thus, $G/Z(G)$ is nonabelian so $G' \not\leq Z(G)$. Then, by (c), G/G' is not generated by subgroups of index p^2 so it is abelian of type (p^{m-3}, p) . Let L/G' be a direct factor of G/G' of order p ; then L is abelian of order p^3 since $|G : L| = p^{m-3} > p^2$. We have $G/L \cong C_{p^{m-3}}$ so there exists a cyclic $Z < G$ with $G = Z \cdot L$ (semidirect product) since $Z \cap L = \{1\}$ in view of $|G/\mathfrak{U}_1(G)| = p^4$. We also see that $\mathfrak{U}_1(Z) = \mathfrak{U}_1(G)$ (compare indices!) so $\exp(L) = p$, $L \cong E_{p^3}$. Then $G' \cap \mathfrak{U}_1(G) \leq L \cap \mathfrak{U}_1(Z) = \{1\}$. Since a Sylow p -subgroup of $\text{Aut}(L)$ is nonabelian of order p^3 and exponent p , we get $\Omega_1(G) = L \times \Omega_1(\mathfrak{U}_1(G)) \cong E_{p^4}$ (recall that $m > 5$). By remark, preceding the lemma, $\text{cl}(G/\mathfrak{U}_1(G)) = 3$. Next, the last assertion follows from Lemma 65.2(a).

(g) All members of the set Γ_1 are \mathcal{A}_1 -groups (Lemma 65.2(d)) so they are generated by two elements (Lemma 65.1). By Lemma 64.1(n), $p > 2$. In that case, $|G : G'| = p^2$ (Lemma 64.1(p)) so $|G| = |G : G'||G'| = p^2 p^3 = p^5$.

(h) Since $G' \not\leq Z(G)$, we get $|G'| \geq p^2$, and, by (c), $d(G) = 2$. Then $T = G' \cap Z(G)$ has index p in G' . Indeed, this is true, if $|G'| = p^2$. If $|G'| = p^3$, there are nonabelian $F, H \in \Gamma_1$ such that $F' \neq H'$ (Lemma 64.1(u)) so $F'H' = T$ has index p in G' . Then G/T is an \mathcal{A}_1 -group since $|G/T)'| = p$ and $d(G) = 2$ (Lemma 65.2(a,e)).

(i) Since G is not an \mathcal{A}_1 -group, we have $|G : Z(G)| > p^2$. Assume that $|G : Z(G)| = p^3$. Then $G/Z(G)$ has exactly one cyclic subgroup of index p (otherwise, $|G : Z(G)| = p^2$) so $G/Z(G) \cong D_8$. Since $\mathfrak{U}_2(G) \leq Z(G)$, by (e), we get $|G/Z(G)| \leq p^4$. Suppose that $p = 2$ and $\bar{G} = G/Z(G)$ is nonabelian of order 2^4 . Then $\bar{G} = \langle a, b \mid a^4 = b^4 = 1, a^b = a^{-1} \rangle$. Set $\bar{U} = \langle b^2 \rangle$. Then $G/U \cong D_8$, and so $U \leq Z(G)$, by (c), a contradiction. Thus, in that case, $G/Z(G)$ is abelian.

(j) Let $H \in \Gamma_1$. Since $\Omega_1(H) \triangleleft G$, we get $|\Omega_1(H)| \leq p^2$ so H is metacyclic (Lemma 65.1). \square

Not all groups of Lemma 65.4(d) are \mathcal{A}_2 -groups. Indeed, let $G = H * C$, where $H = \langle a, b \mid a^4 = b^4 = 1, a^b = a^{-1} \rangle$, $C = \langle c \mid c^4 = 1 \rangle$, $H \cap C = \Omega_1(C)$. The group G is an \mathcal{A}_2 -group if and only if $c^2 = a^2$.

The group $G = \langle a, b \mid a^8 = b^4 = 1, [a, b] = a^2 \rangle$ is a metacyclic \mathcal{A}_2 -group with $G/Z(G) \cong D_8$.

The group $G = \langle a, b \mid a^{p^n} = b^{p^2} = 1, [a, b] = a^{p^{n-2}} \rangle$, $n > 3$, is metacyclic with $G/Z(G) \cong C_{p^2} \times C_{p^2}$.

Let $p > 2$ and $G = \langle a, b \mid a^{p^3} = b^{p^2} = 1, [a, b] = a^p \rangle$. Then $G' = \langle a^p \rangle$, $Z(G) = \langle a^{p^2} \rangle$, $G/Z(G)$ is nonabelian of order p^4 . The above three groups realize all possibilities of Lemma 65.4(i).

Let G be a metacyclic 2-group with $G/Z(G) \cong D_8$. Then $|G'| = 4$ (Lemma 64.1(u)) so G is an \mathcal{A}_2 -group (Corollary 65.3).

If G is a metacyclic p -group such that $G/Z(G)$ is of order p^4 and exponent p^2 , then G is an \mathcal{A}_2 -group. Indeed, if $H \in \Gamma_1$, then $H/Z(G)$ is abelian of type (p^2, p) so H is either abelian or minimal nonabelian since $d(H) = 2$.

Lemma 65.5. *Let an \mathcal{A}_2 -group G of order $> p^4$ have no abelian maximal subgroups, and $d(G) = 2$. Then:*

- (a) *If $p = 2$, then G is metacyclic.*
- (b) *If $p > 2$ and G is nonmetacyclic, then $|G| = p^5$. $K_3(G) = \mathfrak{U}_1(G) = Z(G)$ is of order p^2 and all subgroups of index p^2 in G contain $Z(G)$.*

Proof. (a) follows from Lemmas 65.1 and 64.1(n).

(b) The quotient group $G/\mathfrak{U}_1(G)$ is nonabelian of order p^3 and exponent p , $\mathfrak{U}_1(G) = K_3(G)$, $|G : G'| = p^2$ (Lemma 64.1(p)) and $\mathfrak{U}_1(G) = Z(G)$ (Lemma 65.4(c)). If $T < G$ is of index p^2 , then $TZ(G)$ is abelian so $Z(G) < T$. Next, we have $|G| = |G : G'||G'| \leq p^5$ so $|G| = p^5$. \square

Lemma 65.6. *Let G be a group of order $p^m > p^4$ and all members of the set Γ_1 are generated by two elements.*

- (a) *If $Z(G) = \Phi(G)$ has index p^3 in G , then G is an \mathcal{A}_2 -group.*
- (b) *If $d(G) = 2$ and $Z(G) = \mathfrak{U}_1(G)$ has index p^3 in G , then G is an \mathcal{A}_2 -group.*

Proof. (a) If $H \in \Gamma_1$, then $d(H) = 2$ hence all maximal subgroups of H are members of the set Γ_2 so abelian, and H is either abelian or minimal nonabelian.

(b) Given $H \in \Gamma_1$, it follows from $d(H) = 2$ that all maximal subgroups of H contain $Z(G)$ (since $Z(G) \leq \Phi(G)$) so abelian. Thus, again H is either abelian or minimal nonabelian. \square

Theorem 65.7. *Suppose that G is an \mathcal{A}_2 -group of order $> p^4$.*

- (a) *If G' is cyclic of order $> p$, then G is metacyclic and $|G'| = p^2$.*
- (b) *Suppose that $|G'| = p^3$. Then every subgroup of index p^2 in G contains $Z(G)$. If $d(G) = 2$, then $p > 2$ and $|G : Z(G)| = p^3$. If $d(G) = 3$, then $\Phi(G) = Z(G)$ and $G' \cong E_{p^3}$. If $p = 2$, then $d(G) = 3$ so $G' \leq Z(G)$ is elementary abelian.*

- (c) If $p = 2$, G is nonmetacyclic and $D \in \Gamma_1$ is abelian, then $G' \leq Z(G)$.
- (d) If G is nonmetacyclic, then G' is elementary abelian.
- (e) If G is nonmetacyclic, then $|G/Z(G)| \leq p^3$.
- (f) If G is nonmetacyclic and $A, B \in \Gamma_1$ are distinct nonabelian, then $Z(A) = Z(B) \leq Z(G)$.
- (g) If $p = 2$ and $G/Z(G) \cong D_8$, then G is metacyclic.
- (h) Suppose that G is nonmetacyclic and the set Γ_1 has exactly one abelian member A ; then $|G'| = p^2$. If $G' \not\leq Z(G)$, then $p > 2$ and $G/Z(G)$ is nonabelian of order p^3 and exponent p . If $G' \leq Z(G)$, then $G/Z(G) \cong E_{p^3}$.

Proof. (a) Since G' is cyclic, all nonabelian maximal subgroups of G have the same derived subgroup $= \Omega_1(G')$. Then, by Lemma 64.1(u), $|G'| = p^2$. Let a nonabelian $F \in \Gamma_1$. Since $F' < G' < F$, then F is metacyclic (Lemma 65.1). If all members of the set Γ_1 are metacyclic, then G is also metacyclic (Theorem 69.1). Suppose that there is a nonmetacyclic $A \in \Gamma_1$; then A is abelian. We have $\Omega_1(A) \cong E_{p^3}$ since $d(A) = 3$: $F \cap A$ is metacyclic of index p in A . Since all members of the set Γ_1 which contain $\Omega_1(A)$, are nonmetacyclic so abelian, $G/\Omega_1(A)$ is cyclic. Then $G' < \Omega_1(A)$ so $G' \cong E_{p^2}$, a contradiction. Thus, A does not exist so, by what has been said before, G is metacyclic.

(b) If $T < G$ is of index p^2 , then $TZ(G) = T$ and $|G : Z(G)| > p^2$ since T is abelian and the set Γ_1 has no abelian members (Lemma 65.2(d)); therefore, if $H \in \Gamma_1$, then $Z(G) \leq \Phi(H) \leq \Phi(G)$. Suppose that $d(G) = 2$. Since G is nonmetacyclic (Corollary 65.3 and (a)), we get $p > 2$ (Lemma 64.1(n) since all members of the set Γ_1 are two-generator) and $|G/\mathfrak{U}_1(G)| \geq p^3$ (Lemma 64.1(m)), $\mathfrak{U}_1(G) \leq Z(G)$ (Lemma 65.4(c)) and $|G : Z(G)| = p^3$. Now let $d(G) = 3$. Then $G' \leq \Phi(G) \leq Z(G)$ (Lemma 65.4(c)) so $\Phi(G) = Z(G)$ (Lemma 64.1(q)), $\exp(G') \leq \exp(G/Z(G)) = p$, and we have $G' \cong E_{p^3}$. Let, in addition, $p = 2$. Then $d(G) = 3$ since all members of the set Γ_1 are two generator (Lemma 64.1(n)), and $[x, y]^2 = [x, y^2] = 1$ for $x, y \in G$, so $\exp(G') = 2$ since G' is abelian (Burnside).

(c) Assuming $G' \not\leq Z(G)$, we get $|G'| = 4$ (Lemma 64.1(u)), $G' \cong E_4$, by (a), and $d(G) = 2$ (Lemma 65.4(c)). By Lemma 65.2(c), D is the unique abelian member of the set Γ_1 . Since $G/Z(G)$ is nonabelian of order 8 (Lemma 64.1(q)), it has exactly one cyclic subgroup of index 2 so $G/Z(G) \cong D_8$. Let $H \in \Gamma_1 - \{D\}$; then $H \cap D = \Phi(G)$. If $a \in H - \Phi(G)$ and $x \in D - \Phi(G)$, then $G = \langle a, x \rangle$. We have $o([a, x]) = 2 (= \exp(G'))$ and $\langle [a, x] \rangle \not\leq G$ (otherwise, $G/\langle [a, x] \rangle$ is abelian so $|G'| = 2$). Next, $a^2 \in D$ so

$$1 = [a^2, x] = a^{-2}(x^{-1}ax)^2 = a^{-2}(a[a, x])^2 = a^{-2}a^2[a, x]^2[[a, x], a] = [[a, x], a]$$

since $\langle a, [a, x] \rangle (\leq H)$ has class at most 2 (Lemma 65.1) and $\exp(G') = 2$. Then a centralizes $G' = \langle G' \cap Z(G), [a, x] \rangle$. It follows from $G' < D$ that $C_G(G') \geq \langle a, D \rangle = G$, contrary to the assumption.

(d) Assume that $\exp(G') > p$; then G' is abelian (Lemma 64.1(v)) of type (p^2, p) since G' is noncyclic, by (a). By Lemma 65.1, $H' \leq \Omega_1(G') < G'$ for all $H \in \Gamma_1$ so $d(G) = 2$ (Lemma 64.1(y)). By Lemma 65.2(d), all members of the set Γ_1 as \mathcal{A}_1 -groups are two-generator so $p > 2$ and $K_3(G) = \mathfrak{U}_1(G)$ has index p^3 in G hence $|G : G'| = p^2$ (Corollary 36.6). Since $\mathfrak{U}_1(G) \leq Z(G)$ (Lemma 65.4(c)), we get $\mathfrak{U}_1(G) = Z(G)$. There is $H \in \Gamma_1$ such that $H' \neq \mathfrak{U}_1(G')$. Then $(G/H')' = G'/H'$ is cyclic of order p^2 so G/H' is metacyclic, by (a). This is a contradiction since $G/Z(G)$ is nonmetacyclic and $H' \leq Z(G)$.

(e) Assume that $|G/Z(G)| > p^3$. Then $p = 2$, $\exp(G/Z(G)) = 4$ (Lemma 65.4(e)), G has no epimorphic images isomorphic to D_8 or E_8 (Lemma 65.4(c)) so $d(G) = 2$. By Lemma 64.1(n), there exists $A \in \Gamma_1$ with $d(A) > 2$; then A is abelian (Lemma 65.1). Let $B \in \Gamma_1$ be nonabelian; then $Z(B) = \Phi(B) < \Phi(G) < A$ so $C_G(Z(B)) \geq AB = G$. It follows that $|G : Z(G)| \leq |G : Z(B)| = |G : B||B : Z(B)| = 8$, a contradiction.

(f) By (e), $G/Z(G)| \leq p^3$. Assume that $Z(A) \neq Z(B)$. Then $Z(A)Z(B)(\leq \Phi(G))$ has index p^2 in G so $d(G) = 2$ and $Z(G) < \Phi(G)$ ($<$ since A is nonabelian); moreover, $|G/Z(G)| = p^3$. It follows that $Z(A) = Z(G)$. Similarly, $Z(B) = Z(G)$. Then $Z(A) = Z(B)$, and G is not a counterexample. (Clearly, (e) follows from (f).)

(g) Assume that $G/Z(G) \cong D_8$ and G is nonmetacyclic. Then $G' \not\leq Z(G)$. If $D/Z(G)$ is the cyclic subgroup of order 4 in $G/Z(G)$, then $D \in \Gamma_1$ is abelian. Then, by (c), $G' \leq Z(G)$, a contradiction.

(h) By Lemma 65.4(d), $|G'| > p$ so $|G'| = p^2$ (Lemma 64.1(u)). First assume that $G' \not\leq Z(G)$. By (c), $p > 2$. By (e) and Lemma 65.4(e), $G/Z(G)$ is nonabelian of order p^3 and exponent p . Now let $G' \leq Z(G)$. By Lemma 64.1(q), $|G : Z(G)| = p|G'| = p^3$ so $G/Z(G) \cong E_{p^3}$. \square

Probably, (a) and (d) are most important parts of Theorem 65.7. We use those parts in the study of \mathcal{A}_3 - and \mathcal{A}_4 -groups in §72.

Theorem 65.8. *Let a two-generator \mathcal{A}_2 -group G be a 2-group. Then G is metacyclic.*

Proof. Assume that an \mathcal{A}_2 -group G is a nonmetacyclic two-generator 2-group. Then there is $A \in \Gamma_1$ with $d(A) > 2$ (Lemma 64.1(n)) so $d(A) = 3$, by Schreier's theorem (Appendix 25). Since A is not an \mathcal{A}_1 -group, it is abelian. Let $\Gamma_1 = \{A, M, N\}$; then M and N are nonabelian (if M is abelian, then G is an \mathcal{A}_1 -group) so \mathcal{A}_1 -subgroups. We have $Z(M) = \Phi(M) < \Phi(G) < A$ so $C_G(Z(M)) \geq AM = G$ whence $Z(M) = Z(G)$ since $Z(G) < \Phi(G)$. Similarly, $Z(N) = Z(G)$. Since a nonelementary abelian group $G/Z(G)$ of order 8 has two four-subgroups, we get $G/Z(G) \cong D_8$. By Lemma 65.4(c), if $U \triangleleft G$ is such that $G/U \cong D_8$, then $U = Z(G)$. Since $|G'| > 2$ (Lemma 65.2(a)), A is the unique abelian member of the set Γ_1 (Lemma 65.2(c)).

Write $\bar{G} = G/\mathfrak{U}_1(A)$. Then \bar{G} is nonabelian of order 16 since $d(A) = 3 > 2 = d(G)$. Since $\exp(\bar{G}) = 4$, \bar{G} is not of maximal class. Then, by Proposition 10.17, \bar{G}

has no nonabelian subgroups of order 8 (otherwise, $d(G) > 2$) so it is an \mathcal{A}_1 -group. It follows that $\Omega_1(\bar{G}) = \bar{A}$ (Lemma 65.3) so $Z(\bar{G}) \cong E_4$. Let $\bar{R} < Z(\bar{G})$ be of order 2 and $\bar{R} \neq \bar{G}'$; then $\bar{G}/\bar{R} \cong D_8$ since a nonabelian group \bar{G}/\bar{R} has a subgroup $\bar{A}/\bar{R} \cong E_4$. By the previous paragraph, $R = Z(G)$. Let $B/R < G/R$ be cyclic of order 4; then $B \in \Gamma_1 - \{A\}$ is abelian, a contradiction. \square

Lemma 65.9. *Let G be a nonmetacyclic p -group and $R < G'$ be G -invariant of order p . If G/R is minimal nonabelian and all nonabelian maximal subgroups of G are two-generator, then G is an \mathcal{A}_2 -group and $p > 2$.*

Proof. By hypothesis, $|G'| > p$ so G is not an \mathcal{A}_1 -group. We also have $d(G) = d(G/R) = 2$. Therefore, in view of Theorem 65.8, we have to prove that G is an \mathcal{A}_2 -group. Let $M \in \Gamma_1$ be nonabelian. Then $d(M) = 2$ and M/R (as a maximal subgroup of G/R) is abelian which implies $M' = R$. Hence M is an \mathcal{A}_1 -group (Lemma 65.2(a)) and so G is an \mathcal{A}_2 -group. \square

Theorem 65.10 ([CP] (for $p = 2$), [ZAX]). *Suppose that a nonabelian p -group G is neither minimal nonabelian nor metacyclic nor minimal nonmetacyclic. If all nonabelian subgroups of G are metacyclic, then one and only one of the following holds:*

- (a) $G = M \times C$, where $M \not\cong Q_8$ is a metacyclic \mathcal{A}_1 -group and $|C| = p$.
- (b) $p > 2$, $d(G) = 2$, $G = \Omega_1(G)C$, where $\Omega_1(G) \cong E_{p^3}$, C is a cyclic subgroup of index p^2 in G , $C_G = \mathfrak{O}_1(C) = Z(G)$ is of index p^3 in G .

Proof. Let us check that groups of (a) and (b) satisfy the hypothesis. This is clear for groups from (a). Now let G be as in (b) and $V \in \Gamma_1$. If $\Omega_1(G) \leq V$, then $V = \Omega_1(G)\mathfrak{O}_1(C)$ so V is abelian since $\Omega_1(G)$ is abelian and $\mathfrak{O}_1(C) = Z(G)$. Now assume that $\Omega_1(G) \not\leq V$. Then $\Omega_1(V) = V \cap \Omega_1(G) \cong E_{p^2}$ and $V/\Omega_1(V)$ is cyclic hence V has a cyclic subgroup of index p and so metacyclic.

Now, assuming that G satisfies the hypothesis, we have to prove that G is either as in (a) or in (b). By hypothesis, there are in G two maximal subgroups M and A such that M is nonabelian so metacyclic and A is nonmetacyclic so abelian; then $d(A) > 2$ and $d(G) \leq d(M) + 1 = 2 + 1 = 3$. Since $M \cap A$ is a metacyclic maximal subgroup of A , we get $d(A) = 3$. Set $E = \Omega_1(A)$; then $E_{p^3} \cong E \triangleleft G$. By the product formula, $G = ME$ so $M \cap E \cong E_{p^2}$. All maximal subgroups of G containing E , are nonmetacyclic so abelian, hence $d(G/E) = d(M/(M \cap E)) \leq 2$ (Exercise 1.6(a) and Lemma 65.1). In what follows, A , M and E are such as defined in this paragraph.

Let $d(G/E) = 2$. Then there is a maximal subgroup $B/E < G/E$ with $B \neq A$ so $E \leq A \cap B = Z(G)$ since B is abelian. If $x \in E - M$, then $G = M \times X$, where $X = \langle x \rangle$. Let a noncyclic $N < M$ be maximal. Then $N \times X$ is abelian (otherwise, $d(N) \geq 2$ so $d(N \times X) \geq 3$). Thus, M is a metacyclic \mathcal{A}_1 -group so G is as in (a).

Now suppose that G/E is cyclic; then $G' < E$.

(i) Let $|G/E| = p$; then $|M| = p^3$. If $C_G(M) < M$, then G is of maximal class (Proposition 1.17) and $p > 2$ since G is not metacyclic, and E is the unique

abelian maximal subgroup of G (Lemma 65.2(c)) so $\exp(G) = p^2$ since $M \in \Gamma_1$ is metacyclic. If $E = Z(G) \times L$, then $L_G = \{1\}$ so G is isomorphic to a subgroup of exponent p^2 of a Sylow p -subgroup of the symmetric group S_{p^2} ; then G has a subgroup $\neq A$ of order p^3 and exponent p which is nonabelian and nonmetacyclic, a contradiction. Thus, $G = MZ(G)$. If $Z(G)$ is noncyclic, then $G = M \times L$ is as in (a) (in that case, $M \not\cong Q_8$ since G is not minimal nonmetacyclic). If $Z(G)$ is cyclic, then, since $|Z(G)| = p^2$, we get $G = EZ(G)$, by the product formula, so G is abelian, a contradiction.

(ii) Now suppose that G/E is cyclic of order $> p$; then $G' < E$ so $|G'| \leq p^2$. We have $\Omega_1(G/\Omega_1(G)) < A/\Omega_1(G)$ so $\Omega_1(G) = \Omega_1(A) = E$. Since $M/(M \cap E) = M/\Omega_1(M) \cong G/E$ is cyclic, we get $M \cong M_{p^n}$, $n > 3$, since M is nonabelian and has a cyclic subgroup of index p (Theorem 1.2). Thus, all nonabelian maximal subgroups of G are isomorphic to M_{p^n} . (It follows that G is an \mathcal{A}_2 -group so one can use the classification of \mathcal{A}_2 -groups, however we prefer to present independent, more elementary, proof.)

Let $d(G) = 2$; then $Z(G) < \Phi(G)$ and, since G is not an \mathcal{A}_1 -group, we get $G' \not\leq Z(G)$ (Lemma 65.2(a)) so $G' \cong E_{p^2}$; then $\text{cl}(G) = 3$, A is the unique abelian maximal subgroup of G and $|G : Z(G)| = p|G'| = p^3$ (Lemma 64.1(q)). Since $G' < M$, we get $G' = \Omega_1(M)$ so M/G' is a cyclic subgroup of index p of the abelian group G/G' . Since $Z(G) < M$, then $Z(G) = Z(M)$ (compare indices!) so $Z(G)$ is cyclic. Assume that there is a cyclic $U/Z(G)$ of index p in $G/Z(G)$. Then U is abelian and metacyclic so $U \neq A$, a contradiction. Thus, $\exp(G/Z(G)) = p$ so $G/Z(G)$ is nonabelian of exponent p ; then $p > 2$. We have $Z(G) < C < M$, where C is cyclic of index p in M . Since $|G : C| = p^2$, we get $G = EC$, and C is not normal in G since G' is noncyclic. Thus, G is as in (b).

Now we assume that $d(G) = 3$. Then G/G' has no cyclic subgroups of index p so $|G'| = p$, and we get $|G : Z(G)| = p|G'| = p^2$ (Lemma 64.1(q)). Since $|A : Z(G)| = p$ and $d(A) = 3$, the subgroup $Z(G)$ is noncyclic. By what has been proved already, $M \cong M_{p^n}$. In that case, $\Omega_1(Z(G)) \not\leq M$ since $Z(M)$ is cyclic. If $L < Z(G)$ of order p is not contained in M , then $G = M \times L$ so G is as in (a). \square

Exercise 1. Let G be a nonabelian p -group and $d(G) > 2$. Prove that all members of the set Γ_2 are abelian if and only if $d(G) = 3$ and $\Phi(G) \leq Z(G)$.

Exercise 2 (Janko). Let $A < G$ be a maximal normal abelian subgroup of a nonabelian p -group G . Prove that, for $x \in G - A$, there exists $a \in A$ such that $\langle x, a \rangle$ is an \mathcal{A}_1 -group.

Exercise 3. Let a p -group G be neither abelian nor minimal nonabelian and let $\mathcal{A}_1(G)$ be the set of all minimal nonabelian subgroups of G . Prove that if G is not generated by any proper subset of the set $\mathcal{A}_1(G)$, then $p = 2$, G is an \mathcal{A}_2 -group and $|\mathcal{A}_1(G)| = 2$. (Hint. Use Lemma 76.5. Try to give an independent proof.)

Problem. Classify the p -groups all of whose nonnormal subgroups are abelian.

A new proof of Blackburn's theorem on minimal nonmetacyclic 2-groups

Here we present a new proof, due to Janko, of Blackburn's theorem on minimal nonmetacyclic 2-groups avoiding his tedious calculations. It is difficult to estimate the crucial role of this theorem in our book. Only case $p = 2$ is considered below since, in case $p > 2$, the original proof is easy but nonelementary.

Theorem 66.1 (Blackburn). *Suppose that G is a minimal nonmetacyclic 2-group. Then G is one of the following groups:*

- (a) E_8 .
- (b) The direct product $C_2 \times Q_8$.
- (c) The central product $Q_8 * C_4 \cong D_8 * C_4$ of order 2^4 .
- (d) The group $G = \langle a, b, c \rangle$ with $a^4 = b^4 = [a, b] = 1$, $c^2 = a^2$, $a^c = ab^2$, $b^c = ba^2$, where G is special of order 2^5 with $\exp(G) = 4$, $\Omega_1(G) = G' = Z(G) = \Phi(G) = \langle a^2, b^2 \rangle \cong E_4$, $M = \langle a \rangle \times \langle b \rangle \cong C_4 \times C_4$ is the unique abelian maximal subgroup of G , and all other six maximal subgroups of G are isomorphic to $X = \langle x, y \mid x^4 = y^4 = 1, x^y = x^{-1} \rangle$ (which is the metacyclic minimal nonabelian group of order 2^4 and exponent 4).

Proof [Jan8]. Suppose that G is a minimal nonmetacyclic 2-group. Then Theorem 44.5 implies $d(G) = 3$. If $|G| \leq 2^3$, then $\Phi(G) = \{1\}$ and so $G \cong E_8$. Clearly, if G is abelian then a consideration of $\Omega_1(G)$ shows that $G = \Omega_1(G) \cong E_8$.

Suppose that $|G| = 2^4$. Since $d(G) = 3$, G is neither abelian nor minimal nonabelian. Let Q be a nonabelian subgroup of order 8 in G . Since G is not of maximal class, Proposition 10.17 implies $G = Q * Z$ with $|Z| = 4$ and $Q \cap Z = Z(Q)$. If $Z \cong E_4$, then $Q \cong Q_8$ (because in case $Q \cong D_8$ the group G would contain a (proper) subgroup isomorphic to E_8 which is nonmetacyclic). Thus, $G \cong C_2 \times Q_8$. If $Z \cong C_4$, then $G \cong Q_8 * C_4 \cong D_8 * C_4$ with $Q_8 \cap C_4 = Z(Q)$.

In what follows we assume that $|G| \geq 2^5$. Assume that G contains a nonabelian subgroup D of order 2^3 . If $C_G(D) \leq D$, then, by Proposition 10.17, G is of maximal class and so G is metacyclic, a contradiction. Hence $C_G(D) \not\leq D$ and take in $C_G(D)$ a subgroup U of order 4 containing $Z(D)$. Then $|D * U| = 2^4$ and $D * U$ is not metacyclic since $d(D * U) = 3$, a contradiction. We have proved that every subgroup of order 8 in G is abelian.

Now suppose that $|G| = 2^5$. Since $d(G) = 3$, it follows that $|\Phi(G)| = 4$. Assume $\Phi(G) \not\leq Z(G)$. Then there exists an element $x \in G - C_G(\Phi(G))$; then $\langle \Phi(G), x \rangle$ is nonabelian of order 8 since $x^2 \in \Phi(G)$, contrary to the result of the previous paragraph. Hence $\Phi(G) \leq Z(G)$. On the other hand, $G' \leq \Phi(G)$ and suppose that $|G'| = 2$. Then G/G' is abelian and minimal nonmetacyclic of order 2^4 , contrary to the result of the first paragraph of the proof. Hence $G' = \Phi(G)$. For any $x, y \in G$, we have $[x, y]^2 = [x^2, y] = 1$ since G is of class 2, and so $\Phi(G) = G' \cong E_4$. In particular, $\exp(G) = 4$ and $\Omega_1(G) = \Phi(G)$. Assume that $Z(G) > \Phi(G)$ so that $|Z(G)| = 2^3$ (recall that $|G| = 2^5$) and G has an abelian subgroup of index 2. But then Lemma 64.1(q) gives $|G| = 2|Z(G)||G'| = 2^6$, a contradiction. We have proved that $\Omega_1(G) = G' = Z(G) = \Phi(G) \cong E_4$, and so G is a special group of order 2^5 . In fact, we shall show that the structure of G is uniquely determined.

There are elements $x_1, x_2 \in G - G'$ such that $[x_1, x_2] = t_1$, where t_1 is an involution in G' . Then $X = \langle x_1, x_2 \rangle$ is a maximal subgroup of G since it is nonabelian so of order 2^4 , and $X' = \langle t_1 \rangle$ since $X/\langle t_1 \rangle$ is abelian. Since $G/\langle t_1 \rangle$ is nonabelian in view of $|G'| = 4$, there is $x_3 \in G - X$ such that (interchanging x_1 and x_2 if necessary) $[x_1, x_3] = t_2 \in G' - \langle t_1 \rangle$. We have $\langle t_1, t_2 \rangle = G'$ and $G = \langle X, x_3 \rangle = \langle x_1, x_2, G', x_3 \rangle = \langle x_1, x_2, x_3 \rangle$.

For $[x_2, x_3]$ we have one of the following possibilities:

- (1) $[x_2, x_3] = 1$. In that case, $\langle x_2, x_3, G' \rangle$ is an abelian maximal subgroup of G .
- (2) $[x_2, x_3] = t_1$ and then $[x_1 x_3, x_2] = [x_1, x_2][x_3, x_2] = t_1 t_1 = 1$. In that case, $\langle x_1 x_3, x_2, G' \rangle$ is an abelian maximal subgroup of G .
- (3) $[x_2, x_3] = t_2$ and then $[x_1 x_2, x_3] = [x_1, x_3][x_2, x_3] = t_2 t_2 = 1$. In that case, $\langle x_1 x_2, x_3, G' \rangle$ is an abelian maximal subgroup of G .
- (4) $[x_2, x_3] = t_1 t_2$ and then $[x_1 x_2, x_2 x_3] = [x_1, x_2 x_3][x_2, x_2 x_3] = t_1 t_2 \cdot t_1 t_2 = 1$. In that case $\langle x_1 x_2, x_2 x_3, G' \rangle$ is an abelian maximal subgroup of G .

We see that at least one maximal subgroup M of G is abelian and so (being metacyclic of exponent 4) $M \cong C_4 \times C_4$. Since $|Z(G)| = 4$, M is also the unique abelian maximal subgroup of G , by Lemma 64.1(q).

Take an element $c \in G - M$ so that c^2 is an involution (in G'). Such element exists (otherwise, $\langle c, G' \rangle \cong E_8$ since $\exp(G) = 4$; this argument shows that $\Omega_1(G) = G'$). Since $Z(G) = G'$, we get $C_M(c) = G'$ and c stabilizes the chain $M > G' > \{1\}$. Let $a \in M - G'$ be an element (of order 4) with $a^2 = c^2$ (recall that every involution in M is a square of an element from M). If c normalizes $\langle a \rangle$, then $\langle a, c \rangle \cong Q_8$ is nonabelian, a contradiction. Hence $a^c = at$, where $t \in G' - \langle a \rangle = G' - \langle a^2 \rangle$. Let $b \in M - G'$ be such that $b^2 = t$. We get $M = \langle a \rangle \times \langle b \rangle$ and $a^c = ab^2$. Since $[b, c] \in G' - \langle b^2 \rangle$ (as above), it follows that either $b^c = ba^2$ or $b^c = b(a^2 b^2)$. However, if $b^c = b(a^2 b^2)$, then $(cb)^2 = cbcb = c^2 b^c b = a^2 b(a^2 b^2)b = 1$. This is a contradiction since $cb \notin G'$ and $\Omega_1(G) = G'$. Hence $b^c = ba^2$ and the structure of G is uniquely determined as stated in the theorem.

It remains to show that $|G| < 2^6$. Assume that G is a minimal counterexample. Then, considering an appropriate quotient group G/N , where N is a subgroup of order 2 in $G' \cap Z(G)$, we get $|G| = 2^6$. Let N be a subgroup of order 2 in $G' \cap Z(G)$. Then G/N is isomorphic to the group (d) of our theorem. Set $W/N = (G/N)' = \Phi(G/N) \cong E_4$ so that $W = G' = \Phi(G)$ is of order 8. Then W is abelian, by Burnside; moreover, W is abelian of type (4, 2) since W is metacyclic and $W/N \cong E_4$. We get $N = \Phi(W) = \Omega_1(W) = \langle z \rangle$ and set $W_0 = \Omega_1(W)$.

It is easily seen that $W_0 \not\leq Z(G)$. Indeed, if $W_0 \leq Z(G)$, then we consider a subgroup N_0 of order 2 in $W_0 \cong E_4$ with $N_0 \cap N = \{1\}$ so that $W/N_0 \cong C_4$. On the other hand, G/N_0 is also isomorphic to the group (d) of our theorem and therefore $(G/N_0)' \cong E_4$ coincides with $W/N_0 \cong C_4$, a contradiction. We have $\exp(G) \leq 2^3$ because $G/W \cong E_8$ and $\exp(W) = 4$. Also, $Z(G) \geq N$ and $Z(G) \leq W$ since $Z(G/N) = W/N$. It follows that either $Z(G) = N$ or $Z(G) \cong C_4$ with $N < Z(G) < W$.

Set $C = C_G(W_0)$ so that $|G : C| = 2$. If $x \in G - C$, then $x^2 \in \Phi(G) = W$. If $x^2 \in W_0$, then $\langle x, W_0 \rangle \cong D_8$ is nonabelian of order 8, a contradiction. Thus $x^2 \in W - W_0$ is an element of order 4 and so all elements in $G - C$ are of order 8. In particular, $\exp(G) = 2^3$. Since $C = C_G(W_0)$ is metacyclic, there are no involutions in $C - W_0$ and so $W_0 = \Omega_1(G)$.

By the structure of G/N , G has exactly six maximal subgroups M_1, M_2, \dots, M_6 such that $M_i/N \cong X$ ($i = 1, 2, \dots, 6$), where $X = \langle x, y \mid x^4 = y^4 = 1, x^y = x^{-1} \rangle$ is the metacyclic minimal nonabelian group of order 2^4 and exponent 4. For the seventh maximal subgroup M_7 of G we have $M_7/N \cong C_4 \times C_4$. Hence M_7 is either abelian of type $(2^3, 2^2)$ or $M'_7 = N$ in which case M_7 is minimal nonabelian (Lemma 65.2(a)) with $\exp(M_7) = 2^3$. In both cases $W_0 \leq Z(M_7)$ and so $M_7 = C = C_G(W_0)$ (indeed, if M_7 is minimal nonabelian, $W_0 = \Omega_1(M_7)$ and M_7/W_0 is noncyclic so $W_0 \leq Z(M_7)$).

We shall determine the structure of M_i , $i \in \{1, 2, \dots, 6\}$. We have $\Phi(M_i) = W$ since $M_i/W \cong E_4$ and M_i is metacyclic. Also, $M'_i \leq W$ and $M'_i > \{1\}$ is cyclic since M_i is metacyclic. Suppose $|M'_i| = 2$. The case $M'_i = N$ is not possible since in that case M_i/N would be abelian. Hence $M'_i \neq N$ and so $W_0 = M'_i \times N$. But then $C_G(W_0) \geq M_i M_7 = G$ hence $W_0 \leq Z(M_i)$, contrary to what has been proved already. Hence M'_i is cyclic of order 4 and $W > M'_i > N$. Since $C_G(W_0) = M_7$, we have $W_0 \not\leq Z(M_i)$ for $i < 7$. Because M_i , $i < 7$, is metacyclic and $\exp(M_i) = 2^3$, M_i possesses a cyclic normal subgroup $Z_i > M'_i$ with $|Z_i| = 2^3$ and $M_i/Z_i \cong C_4$. If M_i splits over Z_i , then $M_i = Z_i U_i$ with $Z_i \cap U_i = \{1\}$ and $U_i \cong C_4$. But then $\Omega_1(U_i) \leq W_0$ and $\Omega_1(U_i)$ centralizes Z_i since $\text{Aut}(Z_i) \cong E_4$. In that case $W_0 \leq Z(M_i)$, a contradiction. Hence M_i does not split over Z_i . Let $a_i \in M_i - Z_i$ be such that $\langle a_i \rangle$ covers M_i/Z_i . Since $\exp(M_i) = 2^3$, we have $\langle a_i \rangle \cap Z_i = N = \langle z \rangle$. Then a_i^2 is of order 4, $a_i^2 \in W - W_0$, and $a_i^2 \notin M'_i$ since $a_i^2 \notin Z_i$, by the choice, and $M'_i < Z_i$. Set $\langle z_i \rangle = Z_i$ so that $z_i^{a_i} = z_i^{-1} z^\epsilon$, $\epsilon = 0, 1$ (recall that $z \in N^\#$). We have $\Omega_2(M_i) = W$ and so M_i is uniquely determined according to Lemma 42.1. In

particular, we may assume $\epsilon = 0$ and we have $Z(M_i) = \langle a_i^2 \rangle < W$. We see that M'_i and $Z(M_i)$ are two distinct cyclic subgroups of order 4 in W .

On the other hand, $c_2(W) = 2$ and let W_1 and W_2 be two cyclic subgroups of order 4 in W . For a given $i < 7$, one of these two subgroups is equal to $Z(M_i)$ and the other one is equal to M'_i . Therefore, we have (interchanging W_1 and W_2 if necessary) $W_1 = Z(M_i) = Z(M_j)$ for certain $i \neq j$, $i, j \in \{1, 2, \dots, 6\}$. We get $C_G(W_1) \geq \langle M_i, M_j \rangle = G$ and so $W_1 = Z(G)$. In that case $W_1 = Z(M_i)$ and $W_2 = M'_i$ for all $i < 7$. It follows that all seven maximal subgroups of G/W_2 are abelian so G/W_2 is abelian. Then $E_4 < G' \leq W_2 \cong C_4$, a final contradiction. \square

For another proof of Theorem 66.1, see Theorem 69.1.

Lemma 66.2 (= Theorem 1.25). *Suppose that all nonnormal subgroups of a non-Dedekindian 2-group G have order 2. Then one of the following holds: (a) $G \cong M_{2^n}$; (b) $G = Z * G_0$, where Z is cyclic and $G_0 = D_8$; (c) $G = D_8 * Q_8$.*

Exercise 1. Classify the p -groups all of whose subgroups of index p^2 are absolutely regular.

Exercise 2 ([Pas]). Let G be a non-Dedekindian 2-group all of whose nonnormal subgroups have the same order $2^n > 2$. Then either G is metacyclic or $n = 2$.

Solution. As in Supplement to Theorem 1.25, $E_4 \cong \Omega_1(G) \leq Z(G)$, unless $Q \cong Q_{16}$, and all nonnormal subgroups of G are cyclic. Suppose that G is nonmetacyclic. It follows from Theorem 66.1 that if M is a minimal nonmetacyclic subgroup of G then M is either the group of Theorem 66.1(d) or $M \cong Q_8 \times C_2$ or is the group of Theorem 66.1(d). In the first case, M has a subgroup $X \cong \langle a, b \mid a^4 = b^4 = 1, a^b = a^{-1} \rangle$. Since X has a nonnormal subgroup $\langle b \rangle$ of order 4, we get $n = 2$. In the second case, G has a subgroup $Q \cong Q_8$, and $Q \triangleleft G$ since Q is noncyclic. Set $C = C_G(Q)$. Assume that C has a cyclic subgroup Z of order 4. If $Q \cap Z > \{1\}$, then $QC = Q * Z \cong D_8 * Z$ has a nonnormal subgroup of order 2 (see Appendix 16, Subsection 1^o), a contradiction, since $n > 1$. If $Q \cap Z = \{1\}$, then $Q \times Z$ has a nonnormal cyclic subgroup of order 4 (Theorem 1.20) since $\Omega_1(Q \times Z) \leq Z(G)$, and we get $n = 2$. Thus, one may assume that C is elementary abelian. Next, G/C is isomorphic to a 2-subgroup of $\text{Aut}(Q) \cong S_4$ that contains a subgroup which is isomorphic to $Q/Z(Q) \cong E_4$. If $G/C \cong E_4$, then $G = Q * C = Q \times E$, where E is a subgroup of index 2 in C ; in that case G is Dedekindian, a contradiction. Thus, $G/C \cong D_8$. If $x \in G - C$ is such that $\langle xC \rangle$ is not normal in G/C , then the subgroup $\langle x \rangle$ is not normal in G . Since $o(x^2) \leq \exp(C) = 2$ and $n > 1$, we get $o(x) = 4$ so $n = 2$.

Exercise 3. Classify the groups of Exercise 2 containing a subgroup $Q \cong Q_8$.

Exercise 4. If a 2-group of Exercise 2 is metacyclic, then either $G \cong Q_{16}$ or $G = \langle a, b \mid a^{2^m} = b^{2^n} = 1, a^b = a^{1+2^{m-1}} \rangle$, $n \geq m$ (in the second case, G is minimal nonabelian).

Exercise 5. Suppose that a nonmetacyclic 2-group G of Exercise 2 has a subgroup such as the group of Theorem 66.1(d). If Z is a nonnormal subgroup of G of order 4 then, all nonnormal subgroups of $G/\Omega_1(Z)$ have the same order 2.

Solution. Clearly, Z is cyclic. Suppose that $H/\Omega_1(Z) \not\leq G/\Omega_1(Z)$; then $H \not\leq G$. Since G is nonmetacyclic, we get $|H| = 4$ (Exercise 2) so $|H/Z| = 2$.

Exercise 6. Suppose that a 2-group G of Exercise 2 has a nonnormal (cyclic) subgroup Z . Then G/Z_G is such as in Lemma 66.2. If $G/Z_G \cong M_{2^t}$, then G is metacyclic.

Hint. It remains prove that if $G/Z_G \cong M_{2^n}$, then G is metacyclic. Assume that this is false. Then $|Z| = 4$, by Exercise 2. The group G/Z_G has two distinct cyclic subgroups A/Z_G and B/Z_G of index 2. The subgroups A and B are abelian so $A \cap B = Z(G)$. Since $Z_G = \Phi(Z) \leq \Phi(G)$, we get $dG) = d(G/Z_G) = 2$, and we conclude that G is minimal nonabelian. As above, $\Omega_1(G) \cong E_4$ so G is metacyclic and G is not a counterexample.

Exercise 7. Study the non-Dedekindian 2-groups G all of whose nonnormal abelian subgroups are cyclic of the same order $2^n > 2$. (The groups Q_{2^n} , $n > 3$, satisfy this condition.)

Hint. We have $\Omega_1(Z(G)) = \Omega_1(G) \cong E_4$, unless G is a generalized quaternion group (indeed, given $U < G$ nonnormal cyclic, let us consider the abelian $U\Omega_1(Z(G))$). All cyclic subgroups of $G/\Omega_1(G)$ are normal so this group is Dedekindian. Assume that $G/\Omega_1(G)$ is nonabelian. Then $G/\Omega_1(G)$ contains a subgroup $L/\Omega_1(G) \cong Q_8$ (Theorem 1.20). Since all subgroups of L containing $\Omega_1(G)$, are abelian, we get $|L : Z(L)| = 4$ so $|L'| = 2$. It follows that $L' < \Omega_1(G)$, a contradiction since $L/\Omega_1(G)$ is nonabelian. Thus, $G/\Omega_1(G)$ is abelian. Now assume that G has a subgroup $Q \cong Q_8$ and set $C = C_G(Q)$. If G is metacyclic, it is generalized quaternion (Proposition 1.19). The subgroup C is elementary abelian of order 4 since G is not of maximal class (Proposition 1.17). It follows that $QC = Q \times L$, where $|L| = 2$. Since all noncyclic abelian subgroups of QC are normal in G and QC is generated by these subgroups, we get $QC \triangleleft G$. It follows that $G/C \cong E_4$ since G/C is isomorphic to a subgroup of $\text{Aut}(Q) \cong S_4$ containing a subgroup $\cong Q/Z(Q) \cong E_4$. In that case, $G = Q \times E$, where E is a subgroup of index 2 in C , so G is Dedekindian, contrary to the hypothesis. Thus, G has no subgroups isomorphic to Q_8 . It follows that if M is a minimal nonmetacyclic subgroup of G , then M is isomorphic to a group of Lemma 66.1(d).

Problem. Classify the nonmetacyclic 2-groups all of whose minimal nonmetacyclic subgroups have order 16.

Determination of U_2 -groups

Recall that a 2-group G is said to be a U_2 -group if it contains a normal four-subgroup R such that G/R is of maximal class and, provided T/R is cyclic of index 2 in G/R , then $\Omega_1(T) = R$ (see §§17, 18). The subgroup R is said to be the *kernel* of G . The kernel R is the unique normal four-subgroup of G .

Theorem 67.1 (Janko [Jan8]). *Let G be a U_2 -group with $d(G) = 3$. Then there is $M \in \Gamma_1$ of maximal class, and one of the following holds:*

- (a) $G = M \times C_2$;
- (b) $G = M * C_4$ with $M \cap C_4 = Z(M)$;
- (c) $G = M\langle u \rangle$, where u is an involution inducing on M an involutory “outer” automorphism such that $C_M(u) = M_1$ is of maximal class, $|M : M_1| = 2$, and for each $x \in M - M_1$, $x^u = xz$ with $\langle z \rangle = Z(M)$ (in particular, $z^2 = 1$).

Proof. Let G be a U_2 -group with the kernel R and $d(G) = 3$. Then G possesses a maximal subgroup M such that $R \not\leq M$ since, by hypothesis, $R \not\leq \Phi(G)$. In that case, $M \cap R = \langle z \rangle$ is of order 2 and $M/\langle z \rangle \cong G/R$ so M is nonabelian. Next, M has no G -invariant abelian subgroups of type $(2, 2)$ since $R \not\leq M$ so M is of maximal class (Lemma 1.4). Since $|M| > 2^3$, $M/\langle z \rangle \cong G/R$ is dihedral.

Let $u \in R - \langle z \rangle$. If $R \leq Z(G)$, then $G = \langle u \rangle \times M$ and we are done. Suppose $R \not\leq Z(G)$ and set $M_1 = C_M(R) = C_M(u)$ so that $|M : M_1| = 2$. If M_1 is cyclic, then take an element v of order 4 in M_1 and $x \in M - M_1$. Since $R^\# = \{u, z, uz\}$ and u and z are not G -conjugate, we have $(uv)^x = u^x v^x = (uz)v^x = (uz)v^{-1} = (uz)(vz) = uv$ and so $C = \langle uv \rangle \cong C_4$ and $C \leq Z(G)$ since $\langle M - M_1 \rangle = M$ and $CM = G$. In this case $G = M * C$ with $C \cap M = \langle z \rangle = Z(M)$ and we have obtained the group from (b). Now suppose that M_1 is of maximal class. Then u induces on M an outer involutory automorphism such that $M_1 = C_M(u)$ is a maximal subgroup of M and for each $x \in M - M_1$, $x^u = xz$. \square

In the rest of this section we assume that G is a U_2 -group with the kernel R and $d(G) = 2$. Then G/R is of maximal class and order 2^n , $n \geq 3$, and $\Phi(G) \geq R$. Let T/R (of order 2^{n-1}) be a cyclic subgroup of index 2 in G/R and let $\langle a \rangle$ be a cyclic subgroup of T which covers T/R . Since $\Omega_1(T) = R$, $\langle a \rangle$ is of order 2^n and $\langle a \rangle \cap R = \langle z \rangle$ is of order 2. Hence T is either abelian of type $(2^n, 2)$ or $T \cong M_{2^{n+1}}$.

In any case, $\Phi(T) = \langle a^2 \rangle$, $z \in \langle a^2 \rangle$, $\langle a^2 \rangle$ is normal in G , and $z \in Z(G)$. Let $v = a^{2^{n-2}}$ so that $o(v) = 4$, $v^2 = z$, $A = R\langle v \rangle = \Omega_2(T)$ is abelian of type $(4, 2)$, and $\langle v \rangle = A \cap \Phi(T)$ is normal in G . Hence $A/R = Z(G/R)$ and so for each $x \in G - T$, $x^2 \in A$ since G/R is of maximal class. Since $\mathfrak{V}_1(G) = \Phi(G) = R\langle a^2 \rangle$ is of exponent 2^{n-1} , we get $\langle a \rangle \not\leq \Phi(G)$ so, if $\langle a \rangle$ is normal in G , G is metacyclic.

If $G/R \cong Q_{2^n}$, then for each $x \in G - T$, $x^2 \in A - R$. All elements in $A - R$ are of order 4 and so $o(x) = 8$. In this case $\Omega_2(G) = \Omega_2(T) = A$ and so G is metacyclic and is isomorphic to a group (c) of Lemma 42.1. Therefore, we may assume in the sequel that $G/R \not\cong Q_{2^n}$. In particular, T/R is the unique cyclic subgroup of index 2 in G/R . Conversely, assume that G is metacyclic. Then G' is cyclic, $G' \leq \Phi(G) = R\langle a^2 \rangle$, $|G' \cap R| = 2$, and G' covers $(R\langle a^2 \rangle)/R$. Thus $|G'| = 2^{n-1}$. Let S be a cyclic normal subgroup of G such that $G' < S$ and $|S : G'| = 2$. But then $|S| = 2^n$ and $(RS)/R$ is a cyclic subgroup of index 2 in G/R . The uniqueness of T/R implies $RS = T$. But $c_n(T) = 2$, and so $\langle a \rangle$ is normal in G .

We have proved that (under our assumptions) G is metacyclic if and only if $\langle a \rangle$ is normal in G . We shall use the above notation in the rest of this section.

Theorem 67.2. *Let G be a metacyclic U₂-group with the kernel R . Then one of the following holds.*

- (a) $G = \langle a, b \mid a^{2^n} = b^4 = 1, a^b = a^{-1}z^\epsilon, \epsilon = 0, 1, z = a^{2^{n-1}}, n \geq 3 \rangle$, where $R = \langle b^2, z \rangle = Z(G)$ and $G/R \cong D_{2^n}$.
- (b) G is isomorphic to a group (c) of Lemma 42.1 and here $G/R \cong Q_{2^n}$ and $Z(G) \cong C_4$.
- (c) $G = \langle a, b \mid a^{2^n} = b^4 = 1, a^b = a^{-1+2^{n-2}}, z = a^{2^{n-1}}, n \geq 4 \rangle$, where $R = \langle b^2, z \rangle$, $G/R \cong SD_{2^n}$, and $Z(G) = \langle z \rangle \cong C_2$.

Proof. Suppose that G is a metacyclic U₂-group with the kernel R , where $G/R \not\cong Q_{2^n}$ (for the case $G/R \cong Q_{2^n}$, see the second paragraph following the proof of Theorem 67.1). Then $\langle a \rangle$ is normal in G , by the paragraph preceding the theorem. Since G is not of maximal class, $R = \Omega_1(G)$.

Assume that G/R is dihedral. Take $x \in G - T$; then $x^2 \in R$ so $H = \langle x, R \rangle$ is of order 8 and abelian (otherwise, G would be of maximal class). It follows that $C_G(R) \geq \langle G - T \rangle = G$. We have obtained the group (a).

Suppose now that $G/R \cong SD_{2^n}$, $n \geq 4$. There is $b \in G - T$ with $b^2 \in R$. If $b^2 \in \langle z \rangle$, then $\langle a, b \rangle$ is a maximal subgroup of G , by the product formula so $R < \Phi(G) < \langle a, b \rangle$. However, this is a contradiction since we must have $\langle a, b \rangle / R = G/R$ so that $\langle a, b \rangle = G$. Thus $b^2 = u \in R - \langle z \rangle$. We have, in view of the structure of G/R that $a^b = a^{-1}vz^\eta$ ($\eta = 0, 1$), where $v = a^{2^{n-2}}$ (recall that $\langle a \rangle$ is normal in G). We have $(a^4)^b = (a^b)^4 = (a^{-1}vz^\eta)^4 = a^{-4}$, and so $v^b = v^{-1}$ since $v \in \langle a^4 \rangle$ (recall that $\langle a \rangle$ is normal in G). We compute further $a^{b^2} = a^u = (a^{-1}vz^\eta)^b = (a^{-1}vz^\eta)^{-1}v^{-1}z^\eta = av^{-2} = az$, so $a^u = az$ and therefore $T \cong M_{2^{n+1}}$. If $\eta = 1$, then we replace b with $b' = bu$; then $(b')^2 = b^2 = u$ and $a^{b'} = a^{bu} = (a^{-1}vz)^u =$

$a^{-1}zvz = a^{-1}v$. Hence, we may assume from the start that $a^b = a^{-1}v$, and we have obtained the group (c). \square

Theorem 67.3. *Let G be a nonmetacyclic U_2 -group with $d(G) = 2$ and the kernel R . Then one of the following holds:*

- (a) $G = \langle a, b \mid a^{2^n} = 1, a^{2^{n-1}} = z, b^2 = z^\epsilon, \epsilon = 0, 1, a^b = a^{-1}u, u^2 = [u, a] = [u, b] = 1, n \geq 3 \rangle$, where $R = \langle u, z \rangle = Z(G)$ and $G/R \cong D_{2^n}$.
- (b) $G = \langle a, t \mid a^{2^n} = t^2 = 1, a^{2^{n-1}} = z, a^t = a^{-1}u, u^2 = 1, [u, a] = [u, t] = z, n \geq 3 \rangle$, where $R = \langle u, z \rangle$ and $G/R \cong D_{2^n}$. If $n = 3$, then $Z(G) = \langle a^2 \rangle \cong C_4$ and if $n > 3$, then $Z(G) = \langle z \rangle \cong C_2$.
- (c) $G = \langle a, t \mid a^{2^n} = t^2 = 1, a^{2^{n-1}} = z, a^{2^{n-2}} = v, a^t = a^{-1}vu, u^2 = [u, a] = 1, u^t = uz, n \geq 4 \rangle$, where $R = \langle u, z \rangle$, $G/R \cong SD_{2^n}$, and $Z(G) = \langle vu \rangle \cong C_4$.
- (d) $G = \langle a, b \mid a^{2^n} = 1, a^{2^{n-1}} = z, a^{2^{n-2}} = v, b^2 = z^\epsilon, \epsilon = 0, 1, a^b = a^{-1}vu, u^2 = [u, b] = 1, u^a = uz, n \geq 4 \rangle$, where $R = \langle u, z \rangle$, $G/R \cong SD_{2^n}$ and $Z(G) = \langle z \rangle \cong C_2$.

Proof. Suppose that G is a nonmetacyclic U_2 -group with the kernel R and $d(G) = 2$. In that case $G/R \not\cong Q_{2^n}$ (see the proof of Theorem 67.2) so G/R has the unique cyclic subgroup T/R of index 2. In that case, T is either abelian of type $(2^n, 2)$ or $T \cong M_{2^{n+1}}$. Let $\langle a \rangle$ be a cyclic subgroup of index 2 in T ; then $\langle a \rangle$ is not normal in G (see the paragraph preceding Theorem 67.2). Let z be an involution in $\langle a \rangle$; then $z \in Z(G)$.

(i) Suppose that $G/R \cong D_{2^n}$ and T is abelian. If $x \in G - T$, then $x^2 \in R$. Since $\Omega_1(G) = \Phi(G) \geq R$ and $\Omega_1(T)$ does not contain R , there is $b_0 \in G - T$ with $b_0^2 = u_0 \in R - \langle z \rangle$ and so $R \leq Z(G)$. But $\langle a \rangle$ is not normal in G and so $a^{b_0} = a^{-1}u_0z^\epsilon$ ($\epsilon = 0, 1$). We have $(b_0a)^2 = b_0ab_0a = b_0^2a^{b_0}a = u_0a^{-1}u_0z^\epsilon a = z^\epsilon$. Hence, setting $b_0a = b$ and $u_0z^\epsilon = u$, we have $b^2 = z^\epsilon$ and $a^b = a^{-1}u$. We have obtained group (a).

(ii) Now suppose that $G/R \cong D_{2^n}$ and $T \cong M_{2^{n+1}}$. In that case, $R \not\leq Z(G)$. Since $\Omega_1(G/R) = G/R$, it follows that there is a subgroup H/R of order 2 such that $H \not\leq T$ and H is nonabelian. Then $H \cong D_8$. Let $t \in H - R$ be an involution. Then $a^t = a^{-1}u$ with $u \in R - \langle z \rangle$, $u^t = uz$, and $u^a = uz$. We have obtained the group (b).

(iii) It remains to consider the case where $G/R \cong SD_{2^n}$, $n \geq 4$. If Q/R is the generalized quaternion subgroup of index 2 in G/R , then $(T \cap Q)/R$ is a cyclic subgroup of index 2 in Q/R and $\Omega_1(T \cap Q) = R$. Thus Q is a U_2 -group with the kernel R . Since Q/R is generalized quaternion, Q is metacyclic in view of $\Omega_2(Q) = \Omega_2(T)$ is of order 8 (see Lemma 42.1), and the same lemma implies that $Z(Q) \cong C_4$. In particular, $R \not\leq Z(G)$.

Suppose, in addition, that T is abelian. Then $C_G(R) = T$. If D/R is the dihedral subgroup of index 2 in G/R , then $\Omega_1(D \cap T) = R$ and so D is a U_2 -group with

$R \not\leq Z(D)$. In particular, there is an element $x \in D - T$ such that $x^2 \in R$ and $R\langle x \rangle \cong D_8$. It follows that there is an involution $t \in D - T$ acting faithfully on R (see (ii)) and, since $\langle a \rangle$ is not normal in G , we get $a^t = a^{-1}vu$ with $u \in R - \langle z \rangle$, $u^t = uz$, $[u, a] = 1$. We have obtained the group (c).

Finally, suppose that T is nonabelian, i.e., $T \cong M_{2n+1}$ so that $\langle a \rangle$ acts non-trivially on R . Then, in view of $R \not\leq Z(G)$, $M = C_G(R)$ is a maximal subgroup of G , where M/R is noncyclic so dihedral, $T \cap M = \langle a^2 \rangle R$, $\Phi(T) = \langle a^2 \rangle$ is normal in G , $\Omega_1(T \cap M) = R$, and so M is a U_2 -group. Since $R \leq Z(M)$, M/R is dihedral. Indeed, if Q/R is the generalized quaternion subgroup of index 2 in G/R , then we know that Q is metacyclic. Since $d(G) = d(T) = d(Q) = 2$ and G is, by assumption, nonmetacyclic, Theorem 44.5 implies that $d(M) = 3$. Hence M is isomorphic to a group (a) of Theorem 67.1. In particular, there is $b \in M - T$ such that $b^2 \in \langle z \rangle$. We set $b^2 = z^\epsilon$, $\epsilon = 0, 1$. Finally, b centralizes R , $\langle a \rangle$ acts non-trivially on R , and $a^b = a^{-1}vu$ with $u \in R - \langle z \rangle$. We have obtained the group (d). \square

Corollary 67.4 (Berkovich). *Suppose that a 2-group G of rank three has order 2^{n+2} and class $n > 2$. Then one of the following holds:*

- (a) $G = H_1 \times C$, where H_1 is of maximal class and $|C| = 2$ (three groups); all four subgroups of maximal class and index 2 are isomorphic.
- (b) $G = H_1 * C$, where H_1 is of maximal class and $C = Z(G)$ is cyclic of order 4, $C \cap H_1 = Z(H_1)$.

In what follows we assume that $Z(G) = Z(H_1)$ so $Z(G)$ is of order 2.

- (c) $G = \langle a, b, x \mid a^{2^n} = b^2 = x^2 = 1, a^b = a^{-1}, a^x = a^{1+2^{n-1}}, b^x = a^{2^{n-1}}b \rangle$. Here $H_1 = \langle a, b \rangle \cong D_{2^{n+1}}$.
- (d) $G = \langle a, b, x \mid a^{2^n} = x^2 = 1, a^{2^{n-1}} = b^2, a^b = a^{-1}, a^x = a^{1+2^{n-1}}, b^x = a^{2^{n-1}}b \rangle$. Here $H_1 = \langle a, b \rangle \cong Q_{2^{n+1}}$.
- (e) $G = \langle a, b, x \mid a^{2^n} = b^2 = x^2 = 1, a^b = a^{-1+2^{n-1}}, a^x = a^{1+2^{n-1}}, b^x = a^{2^{n-1}}b \rangle$. Here $H_1 = \langle a, b \rangle \cong SD_{2^{n+1}}$.

Proof. Let $K = K_3(G)$; then $|G' : K| = 2$. We have $|Z(G/K)| = 4$ and G/K is not minimal nonabelian. Let $H/K < G/K$ be minimal nonabelian; then $G = K\eta(G)$, where $\eta(G)/K = Z(G/K)$. It follows from Theorem 1.40 that $\text{cl}(H) = \text{cl}(G)$ so H is of maximal class. By Lemma 1.4, G has a normal subgroup R of type (2, 2). Since $|H| > 8$, we get $R \not\leq H$ so $G = HR$. Since $G/R \cong H/(H \cap R) \cong D_{2^n}$, we conclude that G is a U_2 -group. Now the result follows from Theorem 67.1. \square

Exercise. Let G be a group of order p^m , $\text{cl}(G) = m - 2$ and $G/G' \cong E_{p^3}$. Let L be a G -invariant subgroup of index p in G' . Let $H/L < G/L$ be nonabelian of index p . Prove that H is of maximal class.

Characterization of groups of prime exponent

Recall that the set $\Sigma = \{A_i\}_1^n$ of subgroups of a group G is a *partition* of G if $G = \bigcup_1^n A_i$ and $A_i \cap A_j = \{1\}$ for $i \neq j$. In what follows we assume that Σ is a nontrivial partition of a group G (this means that $n > 1$ and $A_i > \{1\}$ for all i). Subgroups A_i are called *components* of Σ . If all components of Σ have equal order, then G is said to be *equally partitioned* [Isa8]. It follows from Cauchy's lemma that, for equally partitioned G , we have $\pi(A_1) = \pi(G)$.

In this section we characterize groups of prime exponent as equally partitioned groups proving the following Isaacs' result [Isa8]: a group G is equally partitioned by a nontrivial partition Σ if and only if G is of prime exponent. Note that this theorem is not a consequence of known results on partitioned groups.

Lemma 68.1. *Let Σ be a nontrivial partition of a group G and $x, y \in G^\#$ with $xy = yx$. If x and y lie in different components of Σ , then $o(x) = o(y)$ is a prime.*

Proof. Suppose that $o(x) < o(y)$. Then $(xy)^{o(x)} = y^{o(x)} \neq 1$, and so xy and y lie in the same $H \in \Sigma$. Then $x = (xy)y^{-1} \in H$, which is not the case. Thus, $o(x) = o(y)$. If $n > 1$ is a proper divisor of $o(x)$, the nonidentity commuting elements x^n and y of different orders lie in different components of Σ , contrary to what has just been proved. Thus $o(x) = o(y)$ is a prime. \square

If a component $H \in \Sigma$ does not contain $Z(G)$, then $\exp(H) = p$ for some prime p . Indeed, if $x \in H^\#$ and $z \in Z(G) - H$, then x and xz commute and lie in different components of Σ so $o(x) = o(xz)$ is a prime, say p (Lemma 68.1); then $o(z) = p$. Assume that $y \in H^\#$ is of prime order $q \neq p$. In that case, $o(y) = o(yz) = q$ so $o(z) = q \neq p$, a contradiction. It follows that, if a p -group G of exponent $> p$ admits a nontrivial partition Σ and $Z(G) \leq H \in \Sigma$, then H is the unique component of Σ of composite exponent so H contains the Hedges subgroup $H_p(G)$ of G .

Lemma 68.2 ([Isa8]). *Let Σ be a nontrivial partition of an equally partitioned group G and $\emptyset \neq X \subseteq G^\#$. Then there exists $H \in \Sigma$ such that $X^z \not\subseteq H$ for all $z \in G$.*

Proof. Suppose that the lemma is false and for each $H \in \Sigma$, choose X_H , a G -conjugate of X , with $X_H \subset H$. Let $N_H = N_H(X_H)$ so that H contains at least $|H : N_H|$ conjugates of X . Let $N = N_G(X)$, $g = |G|$, $h = |H|$. We have

$$|G : N| = |G : N_G(X_H)| \leq |G : N_H| = |G : H| \cdot |H : N_H|$$

(the first equality follows since X and X_H are conjugate in G), and hence $|H : N_H| \geq \frac{h}{g}|G : N|$. Since $\frac{g-1}{h-1} - \frac{g}{h} = \frac{g-h}{h(h-1)} > 0$, we get $\frac{g}{h} < \frac{g-1}{h-1} = |\Sigma|$. Now $|G : N|$ is the number of conjugates of X in G and thus, since Σ is a partition, we get

$$|G : N| \geq \sum_{H \in \Sigma} |H : N_H| = |\Sigma| |H : N_H| \geq |\Sigma| \cdot \frac{h}{g} |G : N|,$$

so $\frac{g}{h} \geq |\Sigma| = \frac{g-1}{h-1}$, a contradiction. \square

Lemma 68.3 ([Isa8]). *Let Σ be a nontrivial partition of an equally partitioned group G . Then every element of $G^\#$ has a prime order.*

Proof. Suppose that $x \in G$ has a composite order and let $K = K_x$ be the conjugacy G -class of x . By Lemma 68.2, there exists $H \in \Sigma$ such that $x^z \notin H$ for all $z \in G$ so that $K \cap H = \emptyset$. By Lemma 68.1, no element of $H^\#$ centralizes any element of K . Thus, H acts semi-regularly by conjugation on K and hence $|H|$ divides $|K|$. Since $1 \in H$ and $1 \notin K$ it follows that $|H| < |K|$.

Now pick $F \in \Sigma$ with $x \in F$. Since $|F| = |H| < |K|$, the set $K - F$ is nonempty, and, obviously, this set is F -invariant. By Lemma 68.1, F acts on $K - F$ semi-regularly via conjugation so that $|H| = |F|$ divides $|K - F| > 0$. Since $K = (K - F) \cup (K \cap F)$ is a partition, $|F|$ divides $|K \cap F| < |F|$, which is a contradiction. Thus elements of $G^\#$ have prime orders. \square

Exercise 1. Suppose that U is a nontrivial normal p -subgroup of G , where p is the largest prime divisor of $|G|$. Assume that every element of $G^\#$ has prime order and let $P \in \text{Syl}_p(G)$. Then either $P = G$ or $|G : P|$ is prime (and so $P \triangleleft G$).

Solution. Take $q \in \pi(G) - \{p\}$ and $Q \in \text{Syl}_q(G)$. Then QU is a Frobenius group with kernel U so $|Q| = q$. It follows that $P \triangleleft G$. Indeed, if r is a minimal prime divisor of $|G|$, then $|G|_r = r$ so G is r -nilpotent (Burnside). Applying this to the r -normal complement of G , we at last prove our claim. If $P < G$, then G is a Frobenius group with kernel P and complement of square free order without elements of composite order. It follows that p' -Hall subgroup of G is of prime order [BZ, Chapter 10].

Exercise 2. Suppose that every element of $G^\#$ is of prime order. Let $P \in \text{Syl}_p(G)$, where p is the largest prime divisor of G . Then P is a TI-set, i.e., $P \cap P^x = \{1\}$ for $x \in G - N_G(P)$, unless $P \trianglelefteq G$.

Solution. Assume that $\{1\} < D = P \cap P^x$, where $P \neq P^x$ and $|D|$ is as large as possible. Applying Exercise 1 to $N_G(D)$ whose Sylow p -subgroup is not normal (Burnside), we obtain a contradiction.

Now we are ready to prove the main result of this section.

Theorem 68.4 ([Isa8]). *Let Σ be a nontrivial partition of an equally partitioned group G . Then $\exp(G) = p$ for some prime p .*

Proof. One may assume that $|\pi(G)| > 1$ (Lemma 68.3). Let p be the largest prime divisor of $|G|$ and $P \in \text{Syl}_p(G)$. By Lemma 68.3 and Exercise 2, P is a TI-set since $P \not\leq G$. By Lemma 68.3 and Exercise 1, $\text{N}_G(P) = C \cdot P$, where either $C = \{1\}$ or $|C| = q$, a prime.

In the first case, $G = P \cdot H$ is a Frobenius group with kernel H and complement P . Then $|P| = p$, a prime. In that case, G is not equally partitioned (by Lemma 68.2: take there $X = P^\#$).

Thus, $\text{N}_G(P) = C \cdot P$ is a Frobenius group with kernel P and complement C of prime order $q \neq p$.

Let $|G| = g$, $|P| = p^b$, $|H| = h$ for $H \in \Sigma$ and $p^\alpha = h_p$, the p -part of h . By Lemma 68.2, given $x \in P^\#$, there exists $F \in \Sigma$ such that $x^z \notin F$ for all $z \in G$, so $\alpha < b$ since $|F| = |H| = h$ (Sylow).

Since P is a TI-set, $|P \cap H| = p^\alpha$ for all $H \in \Sigma$ such that $P \cap H \neq \{1\}$ (note that a Sylow p -subgroup of any component H of Σ is also a TI-subset in H).

By Lemma 68.2, one may choose $H \in \Sigma$ with $H \cap C^x = \{1\}$ for all $x \in G$. Take $P_0 \in \text{Syl}_p(H)$. We may assume that $P_0 < P$. Since P is a TI-set, we must have $\text{N}_H(P_0) \leq \text{N}_G(P) = C \cdot P$. It follows that $\text{N}_H(P_0) = P_0 \cdot C_0$, where $p \nmid |C_0|$. Assume that $y \in C_0^\#$. Then $\{1\} < P_0 \leq P \cap P^y$ so $P^y = P$ and so C_0 is conjugate with C in $\text{N}_G(P)$, by Sylow's theorem, contrary to the choice of H . It follows that $C_0 = \{1\}$ so $\text{N}_H(P_0) = P_0$. By assumption, $\pi(g) = \pi(h)$ so, to complete the proof, it suffices to prove that H is a p -group. Assume that this is false. Then $H = P_0 \cdot Q_0$ is a Frobenius group with kernel Q_0 and complement P_0 since P_0 is a TI-subgroup in H (see Frobenius' theorem in [BZ, Chapter 10]). Since P_0 has only one subgroup of order p and its exponent is p , we get $|P_0| = p$, i.e., $\alpha = 1$. Since Q_0 is nilpotent (Thompson), it is a q -group for some prime q , by Lemma 68.3. Then G is a $\{p, q\}$ -group, and so G is solvable, by Burnside's two-prime theorem. We have $\{1\} < Q_1 = \text{O}_q(G)$ since P is a nonnormal TI-subgroup of G (in view of the existence of H). Since $P \cdot Q_1$ is a Frobenius group, we get $|P| = p = |P_0|$, a contradiction since $1 = \alpha < b$. Thus, H is a p -subgroup. \square

For more elementary proof of Theorem 68.4, see [Isa8].

Exercise 3. Suppose that a 2-group G of exponent > 2 admits a nontrivial partition. Then $G = A\langle b \rangle$, where $o(b) = 2$ and b inverts A . (*Hint.* Use Lemma 68.1 and the paragraph following it.)

Problem 1 (Isaacs). Does there exist a group partitioned by proper subgroups of equal order not all of which are abelian?

Problem 2. Let Σ be a nontrivial partition of G . Study the structure of G if orders of components of Σ form a chain under divisibility.

Problem 3. Classify all nontrivial partitions of elementary abelian p -groups.

Elementary proofs of some Blackburn's theorems

In this section we present elementary proofs of some Blackburn's theorems; these proofs are due to the first author.

1^o. Blackburn has classified minimal nonmetacyclic p -groups. For a simpler proof in the case $p = 2$, due to the second author, see Theorem 66.1. Here we offer another elementary proof for all p .

The p -groups, $p > 2$, without normal elementary abelian subgroups of order p^3 were classified by Blackburn (see Theorem 13.7). The proof of Theorem 13.7 was based on the deep theorem 12.1(a). Here we offer another proof based on Theorem 12.12 which is elementary for $p = 3$ (see Remark 1.)

Remark 1. The proof of Theorem 12.12(a) is elementary. Now let $p = 3$. In the proof of part (c) of that theorem we use the following fact: If G is a 3-group of maximal class and order $3^m > 3^3$, then $|G/\mathfrak{U}_1(G)| = 3^3$. It suffices to prove this for $m = 4$. By Lemma 64.1(m), $|G/\mathfrak{U}_1(G)| > 3^2$, since G is nonmetacyclic. It is known that groups of exponent 3 are of class ≤ 2 , so $|G/\mathfrak{U}_1(G)| = 3^3$.

Similarly, using Theorem 9.5. it is easy to show that, if a nonabelian group G of exponent 3 is generated by two elements, then its order is 3^3 .

Theorem 69.1. *If G is a minimal nonmetacyclic p -group, then, one of the following holds: (a) G is of order p^3 and exponent p ; (b) G is a group of maximal class and order 3^4 ; (c) $p = 2$ and $|G| \leq 2^5$; if $|G| = 2^5$, then G is an \mathcal{A}_2 -group.*

Proof. We use induction on $|G|$. One may assume that $|G| > p^3$. Clearly, we have $|G/\mathfrak{U}_1(G)| \leq p^3$ (otherwise, all maximal subgroups of G are nonmetacyclic).

(i) Let $p > 2$. Obviously, G has no subgroups of order p^3 and exponent p . Then G is irregular (otherwise, $|G/\mathfrak{U}_1(G)| = |\Omega_1(G)| = p^2$ and G is metacyclic, by Lemma 64.1(m)). Therefore, if $|G| = p^4$, then $\text{cl}(G) = 3$ so $p = 3$ (Lemma 64.1(a)). Now suppose that $|G| > p^4$. Let $R \leq \mathfrak{U}_1(G) \cap Z(G)$ be of order p . By Lemma 64.1(m), G/R is nonmetacyclic so minimal nonmetacyclic; then $p = 3$ and G/R is of maximal class and order 3^4 , by induction. We get $|G| = 3^5$ and $|G : \mathfrak{U}_1(G)| = 3^3$ (Remark 1). Let H/R be maximal in G/R ; then H/R is either abelian of type $(9, 3)$ or isomorphic to M_{33} . Since H is metacyclic of order 3^4 , $|H'| \leq 3$ so H is either abelian or \mathcal{A}_1 -group (Lemma 65.2(a)). Since $R \leq \Phi(H) \leq \Phi(G)$, we conclude that all members of

the set Γ_1 are either abelian or \mathcal{A}_1 -groups so G is an \mathcal{A}_2 -group. By Lemma 64.1(p), $|G : G'| = 3^2$ hence $G' \cong E_{3^3}$ (Theorem 65.7(d)) so nonmetacyclic, a contradiction.

(ii) Now assume that $p = 2$; then $d(G) = 3$, by Lemma 64.1(n). Since all maximal subgroups of an (abelian) group G/G' are 2-generator and $d(G/G') = 3$, we conclude that $G/G' \cong E_8$ so $G' = \Phi(G)$. Take $H \in \Gamma_1$.

Set $\bar{G} = G/K_3(G)$; then $|\bar{G}| \geq 2^4$. Since $d(\bar{G}) = 3$, \bar{G} is neither metacyclic nor an \mathcal{A}_1 -group. Next, $\bar{G}' \leq Z(\bar{G})$ since $\text{cl}(\bar{G}) = 2$. In view of $|\bar{H} : (\bar{Z}(\bar{G}) \cap \bar{H})| \leq |\bar{H} : \bar{G}'| = 4$ and $d(\bar{H}) = 2$, \bar{H} is either abelian or \mathcal{A}_1 -group (Lemma 65.2(a)). It follows that \bar{G} is a (nonmetacyclic) \mathcal{A}_2 -group. By Theorem 65.7(d), \bar{G}' is elementary abelian; in particular, $|\bar{G}'| \leq 4$ (\bar{G}' is metacyclic!) and $\exp(\bar{G}) = 4$. Therefore, we have $2^2 \geq |\bar{G}'| = \frac{1}{8}|\bar{G}|$ so $|\bar{G}| \leq 2^5$.

Suppose that $|\bar{G}| = 2^5$; then $|\bar{G}'| = 4$. In that case, $Z(\bar{G}) = \bar{G}'$ ($\cong E_4$), by Lemmas 4.9 and 64.1(q) (indeed, if $Z(\bar{G}) > \bar{G}'$, then $|\bar{G}'| = 2$). Then all (noncyclic!) subgroups \bar{A} of \bar{G} of order 8 contain $Z(\bar{G}) = \bar{G}'$ (otherwise, $d(\bar{A}Z(\bar{G})) > 2$, which is not the case since $\bar{A}Z(\bar{G}) < \bar{G}$) so $\bar{A} \triangleleft \bar{G}$. Since $\bar{G}' = \Phi(\bar{G})$, we conclude that \bar{G} is special.

Assume that $K = K_3(G) > \{1\}$. By the above, $\bar{G} = G/K$ is an \mathcal{A}_2 -group of order $\leq 2^5$.

Suppose that $|G| = 2^5$. Assume that G is not an \mathcal{A}_2 -group. Then G contains a nonabelian subgroup H of order 8. By Lemma 64.1(i), $C_G(H)$ contains a subgroup F of order 4 since G is not of maximal class. Taking F so that $H \cap F = Z(H)$, we get $H * F \in \Gamma_1$ and $d(H * F) = 3$, a contradiction. Thus, if $|G| = 2^5$, then G is a special \mathcal{A}_2 -group.

Suppose that $|\bar{G}| = 2^4$. We claim that this is impossible. Let R be a G -invariant subgroup of index 2 in K ; then $\text{cl}(G/R) = 3$. One may assume that $R = \{1\}$: then $|G| = 2^5$, contrary to the previous paragraph.

It remains to consider the case where $K > \{1\}$ and $|G/K| = 2^5$. We claim that this is impossible. Let R be a G -invariant subgroup of index 2 in K . To obtain a contradiction, one may assume that $R = \{1\}$; then $|G| = 2^6$. Since $\text{cl}(G) = 3$ and $d(G) = 3$, G is not an \mathcal{A}_2 -group (Lemma 65.4(c)). It follows that $K = K_3(G)$ is the unique minimal normal subgroup of G . Therefore, there exists a nonabelian subgroup H of index 4 in G . We have $K < H$ (otherwise, $d(K \times H) > 2$). Since $E_4 \cong Z(G/K) < H/K$, H is not of maximal class. There are the following two possibilities for (the metacyclic subgroup) H : either $H \cong M_{24}$ or $H = \langle a, b \mid a^4 = b^4 = 1, a^b = a^{-1} \rangle$. Since $\bar{G}' < \bar{H}$, we conclude that $H \triangleleft G$.

Assume that $H \cong M_{24}$. We have $c_3(H) = 2$ and $H \triangleleft G$ so, if L is a cyclic subgroup of H of index 2, then $|G : N_G(L)| \leq 2$. Let $H < M \leq N_G(L)$ with $|M : H| = 2$. There are two possibilities for M/L : $M/L \in \{C_4, E_4\}$. If $M/L \cong C_4$, then $C_M(L) = L$ since H is the unique subgroup of order 16 in M containing L and H is nonabelian. Then $M/L \cong C_4$ is a subgroup of $\text{Aut}(L) \cong E_4$, a contradiction. Now suppose that $M/L \cong E_4$. Let F/L be a subgroup of order 2 in M/L with

$F/L \neq H/L$. Since $K < L < F$, $F/K \triangleleft G/K$ (see the end of the second paragraph of (ii)). We have $G' = H \cap F = L$ is cyclic. This is a contradiction since $G'/K \cong E_4$.

Now assume that $H = \langle a, b \mid a^4 = b^4 = 1, a^b = a^{-1} \rangle$. Since H has exactly two nonidentity squares ($a^2 \in K$ and b^2) and K is characteristic in H , we see that all subgroups of order 2 are characteristic in H so normal in G . This is a contradiction since K is the unique normal subgroup of G of order 2. The proof is complete. \square

The groups of Theorem 69.1(c) are described in Theorem 66.1.

2^o. Here we offer another proof of Theorem 13.7. As follows from the proof of Theorem 13.7, it suffices to prove Theorem 69.3, below. First we prove the following

Lemma 69.2. *Let G be a p -group, $p > 2$ and $c_1(G) = 1 + p$. Then G is either metacyclic or a 3-group of maximal class.*

Proof. Let G be a counterexample of minimal order. Then every proper subgroup of G is either metacyclic or a 3-group of maximal class, by induction. Let $H \leq G$ be minimal nonmetacyclic; then H is a 3-group of maximal class and order 3^4 (Theorem 69.1) so $H < G$. Let B be a nonabelian subgroup of order 3^3 in H (B exists since H is not minimal nonabelian); then $C_G(B) \not\leq B$ (Lemma 64.1(i)). Let U be a subgroup of order 9 in $C_G(B)$ with $B \cap U = Z(B)$; then $BU < G$ is neither metacyclic nor of maximal class, a contradiction. \square

It follows from Lemma 69.2 the following new

Proof of the last assertion of Lemma 64.1(m) = Theorem 9.11. We have to prove that, if $p > 2$ and $|G/\mathfrak{U}_1(G)| \leq p^2$, then G is metacyclic. Indeed, in that case, G is regular, by Lemma 64.1(a). If $|G/\mathfrak{U}_1(G)| = p$, then G is cyclic. Now let $|G/\mathfrak{U}_1(G)| = p^2$; then $|\Omega_1(G)| = p^2$ (Lemma 64.1(a)) so $c_1(G) = 1 + p$. By Lemma 69.2, G is either metacyclic or an irregular 3-group of maximal class. In the second case, however, $|G/\mathfrak{U}_1(G)| = 3^3$, by Remark 1. \square

Remark 2. If a p -group G has an absolutely regular maximal subgroup A and irregular subgroup M of maximal class, then G is of maximal class. This coincides with Proposition 12.13.

Theorem 69.3. *If a p -group G , $p > 2$, has no normal subgroups of order p^3 and exponent p , then G is either metacyclic or a 3-group of maximal class.*

Proof. Suppose that G is a counterexample of minimal order. Then G is irregular (Lemma 64.1(a,m)). By Theorem 10.4, G has no elementary abelian subgroups of order p^3 so it has no subgroups of order p^4 and exponent p . Let $E_{p^2} \cong R \triangleleft G$ (Lemma 64.1(x)). By Lemma 69.2, $T = C_G(R)$ is metacyclic since $\Omega_1(T) = R$, and so $T \in \Gamma_1$. By Lemma 69.2 again, there exists $x \in G - R$ of order p ; then $B = \langle x, R \rangle$ is of order p^3 and exponent p (Lemma 64.1(a)). Since $B \not\trianglelefteq G$, there

exists $y \in N_G(B) - B$ of order p (see the proof of Lemma 64.2). Set $H = \langle y, B \rangle$; then $\exp(H) > p$ so $p = 3$, H is of maximal class and order 3^4 (Lemma 64.1(a)). Existence of T and H shows: G is of maximal class (Remark 2). \square

We are ready to prove Blackburn's Theorem 13.7.

Theorem 69.4 (Blackburn). *Suppose that a group G of order p^m , $m > 3$, $p > 2$, has no subgroups $\cong E_{p^3}$. If G is neither metacyclic nor a 3-group of maximal class, then $G = UE$, where $E = \Omega_1(G)$ is nonabelian of order p^3 and exponent p , U is cyclic, $Z(G) \leq C$.*

Proof. By Theorem 69.3, G has a normal (nonabelian) subgroup E of order p^3 and exponent p . By Theorem 10.4, G has no elementary abelian subgroups of order p^3 so it has no subgroups of order p^4 and exponent p . Therefore, setting $C = C_G(E)$ we see that subgroups of order p in C lie in $C \cap E = Z(E)$ so C is cyclic. Next, $C \triangleleft G$ and G/C is isomorphic to a p -subgroup of $\text{Aut}(E)$ (which is nonabelian of order p^3 and exponent p) containing a subgroup $EC/C \cong E/(E \cap C) \cong E_{p^2}$. If $G/C \cong E_{p^2}$, then $G = E * C$, and we are done since G is of class 2 so $\Omega_1(G) = E$.

Now let $|G/C| = p^3$; then G/C is nonabelian of order p^3 and exponent p . Let $E_{p^2} \cong R < E$ be normal in G and set $F = C_G(R)$; then $F \in \Gamma_1$ since $E \not\leq C_G(R)$. Since $\Omega_1(F) = R$, F is metacyclic (Lemma 69.2). Assume that there is $x \in G - E$ of order p . Then $H = \langle x, E \rangle$ is of exponent $> p$ so $p = 3$ and H is of maximal class and order 3^4 . Existence of F and H shows that G is of maximal class (Remark 2), a contradiction. Thus, $\Omega_1(G) = E$. Let $U/C < G/C$ be a subgroup of order p such that $U/C \not\leq CE/C$. Since $\Omega_1(U) = U \cap E = Z(E)$, U has only one subgroup of order p , namely $Z(E)$, so U is cyclic; clearly, $G = EU$. Since $C_G(C) \geq EU = G$, the proof is complete. \square

Corollary 69.5. *Let A be a p -group of operators of a nonmetacyclic p -group G , $p > 2$, $|G| > p^3$. If all proper A -invariant subgroups of G of order p^3 are metacyclic, then G is a 3-group of maximal class.*

Indeed, by Theorem 10.4, G has no elementary abelian subgroups of order p^3 . Now the result follows from Theorem 69.4.

Exercise 1. Let G be a noncyclic p -group. Suppose that for each $H \triangleleft G$, there is $h \in H$ such that $\langle h^x \mid x \in G \rangle = H$. Prove that G is of maximal class.

Solution. We use induction on $|G|$. One may assume that G is nonabelian and $|G| > p^3$. Clearly, $|G : G'| = p^2$. Indeed, if this is not true, let $H/G' < G/G'$ be of type (p, p) . Then there is no $h \in H$ such that $\langle h^x \mid x \in G \rangle = H$. Next, the factors of the lower central series of G apart of the first one, are cyclic and the factors of the upper central series of G apart of the last one, are cyclic. One may assume that $|G| > p^3$. Let R be a minimal normal subgroup of G . Then, by induction, G/R is of maximal class. Assuming that G is not of maximal class, we conclude that $Z(G) \cong C_{p^2}$ and,

by Lemma 1.4, G has a normal abelian subgroup L of type (p, p) . We have $R < L$ so $Z(G/R) \cong E_{p^2}$, and G/R is not of maximal class, a contradiction.

Exercise 2. If a 3-group G of order $> 3^4$ is nonmetacyclic but all its minimal nonmetacyclic subgroups have the same order 3^4 , then G is of maximal class with $\Omega_1(G) \cong E_9$. (*Hint.* Use Theorem 69.4.)

Exercise 3. If G is a minimal nonmetacyclic group of order 2^5 , then (a) G is special with $|G'| = 4$, (b) the set Γ_1 has exactly one abelian member.

Solution. (a) By Theorem 69.1, $G/G' \cong E_8$ so $G' = \Phi(G)$. Assume that G has a nonabelian subgroup H of order 8. Since G is not of maximal class, we get $C_G(H) \not\leq H$ (Lemma 64.1(i)). If F is a subgroup of order 4 in $C_G(H)$ with $Z(H) < F$, then $d(HF) = 3$, a contradiction. Thus, G is an \mathcal{A}_2 -group so $G' \cong E_4$ (Lemma 65.7(d)). We have $C_G(G') \geq \langle H \mid H \in \Gamma_2 \rangle$ so $G' \leq Z(G)$. If $G' < Z(G)$, then by Lemma 64.1(q), $|G'| = 2$, a contradiction. It follows that G is special.

(b) Assume that the set Γ_1 has no abelian members. Let Z_i , $i = 1, 2, 3$, be all subgroups of order 2 in G and let $\mathfrak{A}_i = \{T \in \Gamma_1 \mid T' = Z_i\}$. Since G/Z_i has exactly three abelian subgroups of index 2, we have $|\mathfrak{A}_i| = 3$, $i = 1, 2, 3$, and assume that all \mathfrak{A}_i are non-empty. Obviously, the sets $\mathfrak{A}_1, \mathfrak{A}_2, \mathfrak{A}_3$ are pairwise disjoint, a contradiction since $|\mathfrak{A}_1 \cup \mathfrak{A}_2 \cup \mathfrak{A}_3| = 3 + 3 + 3 = 9 > |\Gamma_1|$. Thus, Γ_1 has exactly one abelian member since $|G'| = 4$.

Non-2-generator p -groups all of whose maximal subgroups are 2-generator

We begin with a study of p -groups of the title by proving the following five theorems. We use results on \mathcal{A}_2 -groups from §65. The following theorem is essential in determination of \mathcal{A}_2 -groups (see §71). For $p > 2$, Theorem 70.1 was proved by Blackburn (however, another proof is presented below).

Theorem 70.1. *Let G be a nonabelian p -group with $d(G) = 3$. Suppose that all members of the set Γ_1 are generated by two elements. If G is of class 2, then it is an \mathcal{A}_2 -group of order $\leq p^6$ and one of the following holds:*

- (a) $|G| = p^4$ and either $G = E * C$, where E is nonabelian of order p^3 , $C \cong C_{p^2}$, $E \cap C = Z(E)$ or $G = Q \times Z$ with $Q \cong Q_8$ and $|Z| = 2$.
- (b) $G = \langle a, b, c \mid a^4 = b^4 = [a, b] = 1, c^2 = a^2, a^c = ab^2, b^c = ba^2 \rangle$ is the minimal nonmetacyclic group of order 2^5 , G is special, $\Omega_1(G) = G' = Z(G) = \Phi(G) = \langle a^2, b^2 \rangle \cong E_4$, $\langle a, b \rangle \cong C_4 \times C_4$ is the unique abelian maximal subgroup of G . All subgroups of G of order 8 contain $Z(G) = G'$.
- (c) $|G| = p^5$, $E_{p^2} \cong \Phi(G) = G' = Z(G) < \Omega_1(G) \cong E_{p^3}$ so G is special, Exactly p^2 members of the set Γ_1 , not containing $\Omega_1(G)$, are metacyclic and exactly one of them is abelian and $p + 1$ other members of the set Γ_1 , containing $\Omega_1(G)$, are nonmetacyclic minimal nonabelian. More precisely, $G = \langle a, b, c \rangle$ with

$$\begin{aligned} a^p &= b^{p^2} = c^{p^2} = [b, c] = 1, \quad [a, b] = x, \quad [a, c] = y, \quad b^p = x^\alpha y^\beta, \\ c^p &= x^\gamma y^\delta, \quad x^p = y^p = [a, x] = [a, y] = [b, x] = [b, y] = [c, x] = [c, y] = 1, \end{aligned}$$

where in case $p = 2$ we have $\alpha = 0$, $\beta = \gamma = \delta = 1$, and in case $p > 2$, the number $4\beta\gamma + (\delta - \alpha)^2$ is a quadratic non-residue mod p . Here $G' = \langle x, y \rangle$, $\Omega_1(G) = G' \times \langle a \rangle$, and $\langle b, c \rangle \cong C_{p^2} \times C_{p^2}$ is the unique abelian member of the set Γ_1 . All subgroups of G of order p^3 contain $Z(G) = G'$.

- (d) $p = 2$, $G = \langle a, b, c \rangle$ is of order 2^6 and

$$\begin{aligned} a^4 &= b^4 = c^4 = 1, \quad [a, b] = c^2, \quad [a, c] = b^2 c^2, \quad [b, c] = a^2 b^2, \\ [a^2, b] &= [a^2, c] = [b^2, a] = [b^2, c] = [c^2, a] = [c^2, b] = 1, \end{aligned}$$

where $G' = \langle a^2, b^2, c^2 \rangle = Z(G) = \Phi(G) = \Omega_1(G) \cong E_{2^3}$, so G is special and all members of the set Γ_1 are nonmetacyclic minimal nonabelian. If $H < G$ is of order 2^4 , then $H \geq G'$.

Proof. Let G satisfy the assumptions of the theorem; then G is not an \mathcal{A}_1 -group (Lemma 65.1) so $|G| > p^3$. Since G/G' is of rank 3 and all maximal subgroups of G/G' are two-generator, we get $G/G' \cong E_{p^3}$ and so $G' = \Phi(G)$. For any $a, b \in G$, $[a, b]^p = [a^p, b] = 1$ since G is of class 2, and so G' is elementary abelian. If $|G| = p^4$ and $E < G$ is an \mathcal{A}_1 -subgroup, then $G = EZ(G)$ (Lemma 64.1(i)), so G is from (a).

From now on we assume that $|G| \geq p^5$ and so $|G'| = \frac{1}{p^3}|G| \geq p^2$. If the set Γ_1 has an abelian member, then $|G| = p|Z(G)||G'|$ (Lemma 64.1(q)) implies $|G : Z(G)| \geq p^3$. If the set Γ_1 has no abelian members, then $|G : Z(G)| \geq p^3$ again. Since $|G : G'| = p^3$ and $G' \leq Z(G)$, we get $Z(G) = G' = \Phi(G)$ so G is special and $\exp(G) \leq p^2$. Let $H \in \Gamma_1$. Then $|H : Z(G)| = p^2 = p^{d(H)}$ so $Z(G) = \Phi(H)$ and H is either abelian or an \mathcal{A}_1 -subgroup (Lemma 65.2(a)). Thus G is an \mathcal{A}_2 -group so $|G'| \leq p^3$ (Lemma 65.2(d)) and $|G| = |G : G'||G'| \leq p^6$. Since G has a minimal nonabelian subgroup $H \in \Gamma_1$, then $\exp(H) \geq p^2$ so $\exp(G) = p^2$.

(i) Assume first that $|G| = p^5$; then $G' \cong E_{p^2}$. If each $H \in \Gamma_1$ is metacyclic, then G is minimal nonmetacyclic. By Lemma 64.1(l), $p = 2$ and G is the uniquely determined group of order 2^5 given in (b) (see Theorem 66.1).

In what follows we assume that G is not minimal nonmetacyclic. Let $H \in \Gamma_1$ be nonmetacyclic. Since $d(H) = 2$, H must be an \mathcal{A}_1 -group and so $H = \langle a, b \mid a^{p^2} = b^p = 1, [a, b] = c, c^p = [c, a] = [c, b] = 1 \rangle$; we have $E = \Omega_1(H) = \langle a^p, b, c \rangle \cong E_{p^3}$ (Lemma 65.1). Assume that there is $x \in G - E$ of order p . Then $D = \langle x, E \rangle \in \Gamma_1$ is neither abelian (since $d(D) = 2$) nor an \mathcal{A}_1 -group (Lemma 65.1), a contradiction. Thus, $E = \Omega_1(G) \cong E_{p^3}$. Let $T_1/E, \dots, T_{p+1}/E$ be all maximal subgroups of G/E . Then T_1, \dots, T_{p+1} are nonmetacyclic \mathcal{A}_1 -groups (since $d(T_i) = 2$) isomorphic to H (Lemma 65.1). Suppose that $M \in \Gamma_1$ does not contain E . Then $\Omega_1(M) = E \cap M \cong E_{p^2}$ and so M is metacyclic since it is either abelian or an \mathcal{A}_1 -group (Lemma 65.1).

Let $X < G$ and $|X| = p^3 (> p^2 = \exp(G))$; then X is noncyclic. If $Z(G) \not\leq X$ then $d(XZ(G)) > 2$ and $XZ(G) \in \Gamma_1$, a contradiction. Hence $(G' =)Z(G) < X$ and so X is abelian and normal in G .

Let $G = \langle \bar{a}, \bar{b}, \bar{c} \rangle$; then $G' = \langle [\bar{a}, \bar{b}], [\bar{a}, \bar{c}], [\bar{b}, \bar{c}] \rangle$. Hence $G' (\cong E_{p^2})$ is generated by two of these elements, say $\bar{x} = [\bar{a}, \bar{b}]$ and $\bar{y} = [\bar{a}, \bar{c}]$. If $[\bar{b}, \bar{c}] = \bar{x}^\rho \bar{y}^\sigma$, let $b = \bar{b}\bar{a}^{-\sigma}$, $c = \bar{c}\bar{a}^\rho$. We compute (recall that G is of class 2)

$$[b, c] = [\bar{b}\bar{a}^{-\sigma}, \bar{c}\bar{a}^\rho] = [\bar{b}, \bar{c}][\bar{b}, \bar{a}]^\rho[\bar{a}, \bar{c}]^{-\sigma} = \bar{x}^\rho \bar{y}^\sigma \bar{x}^{-\rho} \bar{y}^{-\sigma} = 1.$$

Then $A = \langle b, c, G' \rangle \in \Gamma_1$ is abelian and so $A \not\leq E = \Omega_1(G)$ (otherwise, $d(A) = 3$). Hence $A = \langle b \rangle \times \langle c \rangle \cong C_{p^2} \times C_{p^2}$ with $\Omega_1(A) = G' = \mathfrak{V}_1(A)$. Take an element

$a \in E - A$ (of order p) so that $G = \langle a, b, c \rangle$. Setting $x = [a, b]$, $y = [a, c]$, we get $G' = \langle x, y \rangle = \langle b^p, c^p \rangle$ since $x \neq 1 \neq y \neq x$. Set $b^p = x^\alpha y^\beta$, $c^p = x^\gamma y^\delta$.

The subgroup $L = \langle a, b^\xi c^\eta, G' \rangle \in \Gamma_1$ for any integers ξ, η , unless $\xi \equiv \eta \equiv 0 \pmod{p}$ since a, b, c independent modulo G' . Since, for such ξ and η , we have $[a, b^\xi c^\eta] = x^\xi y^\eta \neq 1$, L is nonabelian. In that case, $d(L) = 2$ so $\Phi(L) = G' = Z(L)$, and G' is generated by elements $(b^\xi c^\eta)^p = x^{\alpha\xi + \gamma\eta} y^{\beta\xi + \delta\eta}$ and $[a, b^\xi c^\eta] = x^\xi y^\eta$, which are linear independent since $G' \cong E_{p^2}$. Hence $\begin{vmatrix} \alpha\xi + \gamma\eta & \beta\xi + \delta\eta \\ \xi & \eta \end{vmatrix} \equiv 0 \pmod{p}$ only if $\xi \equiv \eta \equiv 0 \pmod{p}$. This gives

$$(1) \quad \beta\xi^2 + (\delta - \alpha)\xi\eta - \gamma\eta^2 \equiv 0 \text{ only if } \xi \equiv \eta \equiv 0 \pmod{p}.$$

From (1) we get $\beta \not\equiv 0 \pmod{p}$ (otherwise, $\xi = 1, \eta = 0$ is a nontrivial solution of (1)) and $\gamma \not\equiv 0 \pmod{p}$ (otherwise, $\xi = 0, \eta = 1$ is a nontrivial solution of (1)).

(i1) Assume that $p > 2$. We compute

$$(2) \quad (2\beta\xi + (\delta - \alpha)\eta)^2 - (4\beta\gamma + (\delta - \alpha)^2)\eta^2 = 4\beta(\beta\xi^2 + (\delta - \alpha)\xi\eta - \gamma\eta^2).$$

Using (1), we see (because $\beta \not\equiv 0 \pmod{p}$) that the right hand side of (2) vanishes \pmod{p} only if $\xi \equiv \eta \equiv 0 \pmod{p}$, and so we have the same for the left hand side of (2):

$$(3) \quad (2\beta\xi + (\delta - \alpha)\eta)^2 \equiv (4\beta\gamma + (\delta - \alpha)^2)\eta^2 \pmod{p}$$

only if $\xi \equiv \eta \equiv 0 \pmod{p}$.

Hence $4\beta\gamma + (\delta - \alpha)^2$ is a quadratic non-residue \pmod{p} . Indeed, if $4\beta\gamma + (\delta - \alpha)^2 \equiv \mu^2 \pmod{p}$, then we set $\eta = 1$ in (3) and solve the congruence $(2\beta\xi + (\delta - \alpha))^2 \equiv \mu^2 \pmod{p}$ for ξ , which gives a contradiction (since for $\eta = 1$ we have obtained a nontrivial solution of (3) in ξ and η).

(i2) Suppose that $p = 2$. Then $\beta \equiv \gamma \equiv 1 \pmod{2}$ and so relation (1) becomes

$$(4) \quad \xi^2 + (\delta + \alpha)\xi\eta + \eta^2 \equiv 0 \pmod{2} \text{ only if } \xi \equiv \eta \equiv 0 \pmod{2}.$$

If $\delta + \alpha \equiv 0 \pmod{2}$, then $\xi \equiv \eta \equiv 1 \pmod{2}$ satisfies (4), a contradiction. Hence $\delta + \alpha \equiv 1 \pmod{2}$ and we get $b^2 = x^\alpha y$, $c^2 = xy^{1+\alpha}$. If $\alpha \equiv 0 \pmod{2}$, then (recall that $o(x) = o(y) = 2$)

$$(5) \quad b^2 = y, \quad c^2 = xy.$$

If $\alpha \equiv 1 \pmod{2}$, then

$$(6) \quad b^2 = xy, \quad c^2 = x.$$

However, interchanging b and c and also x and y , we obtain from (6) the relations (5). Hence we may assume from the start that $\alpha = 0$, $\beta = \gamma = \delta = 1$ and our group G is uniquely determined. We have obtained the groups from (c).

(ii) Now suppose that $|G| = p^6$ so that $\Phi(G) = G' \cong E_{p^3}$. Each $H \in \Gamma_1$ is nonmetacyclic and minimal nonabelian since it is 2-generator, and so one may set $H = \langle b, c \mid b^{p^2} = c^{p^2} = 1, [b, c] = z, z^p = [b, z] = [c, z] = 1 \rangle$, where $\Phi(H) = \langle b^p, c^p, z \rangle = \Phi(G) = G' \cong E_{p^3}$, and $\Omega_1(H) = \Phi(H)$ implies $\Omega_1(G) = G' = \Phi(G) = Z(G)$ and we again conclude that G is special.

(iii) First assume that $p > 2$. Then $\Omega_1(H) = \langle b^p, c^p \rangle$ and $H' = \langle z \rangle$, where $z \notin \Omega_1(H)$. All $p^2 + p + 1$ members of the set Γ_1 are isomorphic to H (Lemma 65.1) and their derived subgroups (of order p) are pairwise distinct (Lemma 65.2(d)). Since G is regular and $|G : \Omega_1(G)| = p^3$ (if $|G/\Omega_1(G)| > p^3$, then $G/\Omega_1(G)$ has a maximal subgroup that is not generated by two elements), we get $\Omega_1(G) = G' = \{x^p \mid x \in G\}$ (Lemma 64.1(a)). In particular, there exists $a \in G - H$ with $a^p = z$. Set $b^p = x$, $c^p = y$. We have $G = \langle a, H \rangle = \langle a, b, c \rangle$ and $G' = \langle x, y, z \rangle$ (by Lemma 65.2(d), all elements of G' are commutators). Set $[a, b] = x^\alpha y^\beta z^\kappa$, $[a, c] = x^\gamma y^\delta z^\lambda$, and recall that $[b, c] = z$. We shall construct a maximal subgroup K of G with $d(K) > 2$. To do this we shall do some purely number-theoretic computations using heavily the oddness of p . First, we solve the equation

$$(*) \quad t^2 \equiv \eta^2(\kappa^2 - 4\beta) + 2\xi\eta(\kappa\lambda - 2(\delta - \alpha)) + \xi^2(\lambda^2 + 4\gamma) \pmod{p}$$

for t, ξ, η with ξ, η not both $\equiv 0 \pmod{p}$. If $r = \lambda^2 + 4\gamma \equiv 0 \pmod{p}$, we set $\xi = 1, \eta = 0$. If $r = \lambda^2 + 4\gamma \not\equiv 0 \pmod{p}$, we put $\eta = 1$ and set $\kappa\lambda - 2(\delta - \alpha) = s$, $\kappa^2 - 4\beta = u$, so that $(*)$ can be rewritten in the simplified form

$$(**) \quad t^2 \equiv r(\xi + r^{-1}s)^2 - r^{-1}s^2 + u \pmod{p},$$

where r, s, u are constant numbers mod p and ξ, t run through all integers mod p . The left hand side of $(**)$ runs through $1 + (p-1)/2 = (p+1)/2$ distinct values (quadratic residues) mod p . Now, $\xi + r^{-1}s$ runs through all numbers mod p , $(\xi + r^{-1}s)^2$ runs through $(p+1)/2$ distinct values (quadratic residues) mod p so that the right hand side of $(**)$ runs through $(p+1)/2$ distinct values (mod p) (take into account that $-r^{-1}s^2 + u$ is a constant number modulo p). Since $(p+1)/2 + (p+1)/2 = p+1 > p$, it follows that there are values for t and ξ which satisfy $(**)$, as required.

Since at least one of the integers ξ, η is not a multiple of p , we can solve $t \equiv 2(\xi\bar{\eta} - \bar{\xi}\eta) + \kappa\eta + \lambda\xi \pmod{p}$ for $\xi, \bar{\eta}$. Substituting this into $(*)$, we obtain (after reforming)

$$(\kappa\eta + \lambda\xi + \bar{\eta}\xi - \eta\bar{\xi})(\xi\bar{\eta} - \bar{\xi}\eta) + \eta(\beta\eta + \delta\xi) - \xi(\alpha\eta + \gamma\xi) \equiv 0 \pmod{p},$$

or in the determinant form:

$$\begin{vmatrix} \kappa\eta + \lambda\xi + \bar{\eta}\xi - \eta\bar{\xi} & \alpha\eta + \gamma\xi & \beta\eta + \delta\xi \\ 1 & \bar{\eta} & \bar{\xi} \\ 0 & \eta & \xi \end{vmatrix} \equiv 0 \pmod{p}.$$

We now define the elements $a^* = ab\bar{\eta}c\bar{\xi}$, $b^* = b^\eta c^\xi$ of G , where p does not divide at least one of the integers ξ, η . Let $K = \langle a^*, b^*, G' \rangle$; then $K \in \Gamma_1$. It follows from $\Phi(K) = \mathfrak{O}_1(K)K'$ that $\Phi(K) = \langle [a^*, b^*], (a^*)^p, (b^*)^p \rangle$. We have

$$[a^*, b^*] = z^{\kappa\eta + \lambda\xi + \bar{\eta}\bar{\xi} - \eta\bar{\xi}} x^{\alpha\eta + \gamma\xi} y^{\beta\eta + \delta\xi}, \quad (a^*)^p = zx\bar{\eta}y\bar{\xi}, \quad (b^*)^p = x^\eta y^\xi,$$

where x, y, z are determined in the first paragraph of this part (ii1). From the vanishing of the above determinant, we see that “linear independent” elements x, y, z cannot be expressed as “linear combinations” of $[a^*, b^*]$, $(a^*)^p$, $(b^*)^p$ and so $\Phi(K) < G' = \langle x, y, z \rangle$ so $|K : \Phi(K)| > p^2$ or, what is the same, $d(K) > 2$, contrary to the hypothesis of the theorem.

(ii2) Now assume that $p = 2$. Let $G'x, G'y$ be two distinct involutions in G/G' . Then $X = \langle x, G' \rangle$ and $Y = \langle y, G' \rangle$ are distinct abelian subgroups of type $(4, 2, 2)$. We have $\Phi(X) = \langle x^2 \rangle$ and $\Phi(Y) = \langle y^2 \rangle$. Assume that $x^2 = y^2$. Then $X/\Phi(X) \cong E_8 \cong Y/\Phi(Y) = Y/\Phi(X)$ and $X/\Phi(X) \neq Y/\Phi(X)$. This is a contradiction since $\Omega_1(G/\Phi(X)) \cong E_8$. Thus, $x^2 \neq y^2$. Hence, the seven nontrivial elements in G/G' produce seven pairwise distinct squares in G' which are the seven involutions in G' . In particular, each involution in G' is a square in G .

Let $H \in \Gamma_1$ be fixed. We may set $H = \langle a, b \mid a^4 = b^4 = 1, [a, b] = z, z^2 = [a, z] = [b, z] = 1 \rangle$ (Lemma 65.1(a)). Set $a^2 = x, b^2 = y$ so that $G' = \langle x \rangle \times \langle y \rangle \times \langle z \rangle$ and $(ab)^2 = a^2b^a b = xbzb = xb^2z = xyz$. There exists $c \in G - H$ such that $c^2 = z$ (see the previous paragraph; note that z is not a square in H). Then $G = \langle H, c \rangle = \langle a, b, c \rangle$. We claim that $ac \neq ca$. Assume that this is false. Then $C_G(c) \geq \langle a, Z(G), c \rangle$, and the subgroup at the right hand side is abelian of index ≤ 2 in G , a contradiction since the set Γ_1 has no abelian members (Lemma 65.2(d)). It follows that $\langle a, c \rangle$ is nonabelian. Since G is an \mathcal{A}_2 -group, we get $\langle a, c \rangle \in \Gamma_1$. Since $\Phi(\langle a, c \rangle) = \langle a^2 = x, c^2 = z, [a, c] \rangle = G'$, we must have $[a, c] \in G' - \langle x, z \rangle$ and so $[a, c] = x^\alpha yz^\beta$. Similarly, considering the maximal subgroup $\langle b, c \rangle$, we get $[b, c] \in G' - \langle y, z \rangle$ and so $[b, c] = xy^\gamma z^\delta$.

Consider the subgroup $K = \langle a, bc \rangle$. Assume that $a \cdot bc = bc \cdot a$. It follows $bca = ab \cdot c = baz \cdot c$ so $c^a = cz = cc^2 = c^{-1}$ and $\langle a, c \rangle$ has order 16 so is not a member of the set Γ_1 , a contradiction. Since G is an \mathcal{A}_2 -group and $d(G) = 3$, we get $K \in \Gamma_1$. We have

$$\Phi(K) = \langle a^2 = x, (bc)^2 = xy^{1+\gamma}z^{1+\delta}, [a, bc] = x^\alpha yz^{1+\beta} \rangle \cong E_{2^3},$$

and since $\Phi(K) = G' = \langle x, y, z \rangle$, we have

$$\begin{vmatrix} 1 & 0 & 0 \\ 1 & 1 + \gamma & 1 + \delta \\ \alpha & 1 & 1 + \beta \end{vmatrix} = 1$$

and so

$$(7) \quad \beta + \gamma + \beta\gamma + \delta = 1.$$

Considering the maximal subgroup $L = \langle ab, c \rangle$, we get

$$\Phi(L) = \langle xyz, z, x^{1+\alpha}y^{1+\gamma}z^{\beta+\delta} \rangle \cong E_{2^3},$$

and so

$$\begin{vmatrix} 1 & 1 & 1 \\ 0 & 0 & 1 \\ 1+\alpha & 1+\gamma & \beta+\delta \end{vmatrix} = 1,$$

which gives

$$(8) \quad \alpha + \gamma = 1.$$

Considering $M = \langle b, ac \rangle \in \Gamma_1$, we get $\Phi(M) = \langle y, x^{1+\alpha}yz^{1+\beta}, xy^\gamma z^{1+\delta} \rangle$ so

$$(9) \quad \alpha + \delta + \alpha\delta + \beta = 1.$$

Finally, consider the maximal subgroup $N = \langle ab, ac \rangle$. We get

$$\Phi(N) = \langle (ab)^2 = xyz, (ac)^2 = x^{1+\alpha}yz^{1+\beta}, [ab, ac] = x^{1+\alpha}y^{1+\gamma}z^{1+\beta+\delta} \rangle,$$

and so

$$(10) \quad \alpha\gamma + \alpha\delta + \beta\gamma = 1.$$

Relations (7–10) have exactly two solutions:

- (A) $\alpha = 0, \beta = 1, \gamma = 1, \delta = 0$, which implies $[a, c] = yz, [b, c] = xy$, and
- (B) $\alpha = 1, \beta = 0, \gamma = 0, \delta = 1$, which implies $[a, c] = xy, [b, c] = xz$.

However, interchanging a and b and also $a^2 = x$ and $b^2 = y$, we obtain from the solution (A) the solution (B). Hence we may assume from the start that we have solution (A) and so the group G of order 2^6 is uniquely determined as stated in part (d).

Assume that F is a subgroup of G of order 2^4 and $F \not\geq G'$. We have $FG' < G$ so $M = FG' \in \Gamma_1$. But then $M/(F \cap G') \cong E_{2^3}$ so $d(M) \geq 3$, a contradiction. Thus, G' is contained in all subgroups of G of order 2^4 . The proof is complete. \square

Theorem 70.2. Suppose that all maximal subgroups of a p -group G are generated by two elements but $d(G) = 3$. If G is of class > 2 , then $p = 2, |G| \geq 2^7$, and $G/K_3(G)$ is isomorphic to the group of order 2^6 of Theorem 70.1(d). If, in addition, $|G| = 2^7$, then the class of G is 3 and G is uniquely determined, namely, $G = \langle a, b, c \rangle$, where

$$\begin{aligned} a^4 = b^4 = c^4 = k^2 &= [a, k] = [b, k] = [c, k] = 1, \\ [a, b] &= c^2, \quad [a, c] = b^2c^2, \quad [b, c] = a^2b^2, \quad [a^2, b] = k, \quad [a^2, c] = k, \\ [b^2, a] &= 1, \quad [b^2, c] = k, \quad [c^2, a] = k, \quad [c^2, b] = 1. \end{aligned}$$

Here $\langle k \rangle = K_3(G) = [G, G'] = Z(G)$ is of order 2, $\langle a^2, b^2, c^2, k \rangle = G' = \Phi(G) = \Omega_1(G) \cong E_{2^4}$, and G exists as a subgroup of the alternating group A_{16} .

Proof. Suppose that G is a p -group of class > 2 , $d(G) > 2$, and all members of the set Γ_1 are generated by two elements. Then $K_3(G) \neq \{1\}$ and $G/K_3(G)$ is isomorphic to a group of Theorem 70.1. In particular, $|G| \geq p^5$. Let $|G| = p^5$ and assume that G has a nonabelian subgroup S of order p^3 . Since $d(G) = 3$, G is neither of maximal class nor an \mathcal{A}_1 -group. Hence $C_G(S) \not\leq S$ (Lemma 64.1(i)) and let $F > Z(S)$ be a subgroup of order p^2 in $C_G(S)$ containing $Z(S)$. Then $SF = S * F \in \Gamma_1$ and $d(SF) = 3$, a contradiction. Thus S does not exist so G is an \mathcal{A}_2 -group. But then $|G/\Phi(G)| = p^3$ and so $\Phi(G) \leq Z(G)$ (Lemma 65.4(c)), so G is of class 2, a contradiction. Thus, $|G| \geq p^6$.

(i) Let $|G| = p^6$. If $|G/K_3(G)| = p^4$, then take in $K_3(G)$ a G -invariant subgroup L of index p . But then $|G/L| = p^5$ and G/L satisfies the hypothesis, contrary to the previous paragraph. Hence $|G/K_3(G)| = p^5$ and so $G/K_3(G)$ is isomorphic to a group (b) or (c) of Theorem 70.1. Also, $K = K_3(G)$ is of order p . We have $G'/K = Z(G/K) \cong E_{p^2}$ and $G/G' \cong E_{p^3}$.

The subgroup K is the unique minimal normal subgroup of G . Indeed, let L be a minimal normal subgroup of G distinct from K . Then $L < Z(G)$ and so $L < G'$. We have $d(G/L) = 3$ and each maximal subgroup of G/L is generated by two elements. By the above, G/L is of class 2 and so $[G, G'] \leq L$. This is a contradiction since $[G, G'] = K$ and $K \cap L = \{1\}$.

The group G is not an \mathcal{A}_2 -group (otherwise, $d(G) = 3$ would imply $G' \leq Z(G)$, by Lemma 65.4(c)). Therefore G has a nonabelian subgroup H of order p^4 . We have $H \geq K$ (otherwise, $KH = K \times H \in \Gamma_1$ and $d(KH) > 2$). By Theorem 70.1, applied to G/K , $H > G'$ and so H is normal in G . Also, G/K is an \mathcal{A}_2 -group and so $H/K \cong E_{p^2} H' = K$.

Assume that H is not minimal nonabelian. Then H (of class 2) contains a nonabelian subgroup B of order p^3 , and we have $d(H) > 2$ since $H = BC_G(B)$ (Lemma 64.1(i)) so $H/H' = H/K \cong E_{p^3}$, G/K is isomorphic to a group (c) of Theorem 70.1 and $H/K = \Omega_1(G/K)$, i.e., H is the uniquely determined subgroup of index p^2 in G . Let $H < M \in \Gamma_1$. Since $d(M) = 2$, we get $\Phi(M) = \Phi(G) = G'$ so all maximal subgroups of M are normal in G . Any nonabelian p -group has exactly 0, 1 or $p + 1$ abelian subgroups of index p (Exercise 1.6(a)) so M has a nonabelian maximal subgroup $F \neq H$. As above, $K < F$. Since H is the unique \mathcal{A}_2 -subgroup of index p^2 in G , by the above, F is an \mathcal{A}_1 -subgroup and F is normal in G . Since $F/K \neq H/K = \Omega_1(G/K)$, the subgroup F/K is abelian of type (p^2, p) . Assume that F is not metacyclic. If $p > 2$, then $\mathcal{V}_1(F)$ is a normal subgroup of G of order p (Theorem 9.11), distinct from K , contrary to what has proved already. Now let $p = 2$. Then $Z(F) \cong E_4$ ($Z(F)$ is noncyclic since $Z(F) = \Phi(G) = \mathcal{V}_1(F)$) and $F' = K$. Let $U = C_G(Z(F))$; then $U \in \Gamma_1$ since $Z(G)$ is cyclic. Let $K_1 \neq K$ be a subgroup of order 2 in $Z(F)$. Then U/K_1 contains a nonabelian subgroup F/K_1 of order 8. Since $d(U/K_1) = 2$, it follows that U/K_1 is of maximal class (Lemma 64.1(i)). By Taussky's theorem, $K_1 \not\leq U'$ so $U' \cong C_4$. We have $F < U$ so $F' < U' < F$ and U' is cyclic of order 4. It follows that F is metacyclic (Lemma 65.1). Thus, all subgroups

of G of index p^2 which are different from H , are either abelian or metacyclic. We conclude that if G has an \mathcal{A}_2 -subgroup of index p^2 , then G has a normal metacyclic minimal nonabelian subgroup F of the same index.

Let $p > 2$. It follows from $G' < F$ that G' is abelian of type (p^2, p) . As we know, $\mathfrak{V}_1(G) = \Phi(G) = G'$. By Theorem 13.7 (or Theorem 69.4), G has a normal subgroup $E \cong E_{p^3}$. It follows from the structure of G/K that $E\Omega_1(H)/K \leq \Omega_1(G/K) = H/K$ so $E \leq \Omega_1(H)$, and we conclude that M/E is cyclic of order p^2 (indeed, M has at most one abelian maximal subgroup so, in view of $p > 2$, it has at least $p - 1 \geq 2$ nonabelian metacyclic maximal subgroups). Then $C_M(E) > E$ since p^2 does not divide $\exp(\text{Aut}(E))$. Since H is the unique maximal subgroup of M containing E , we get $H \leq C_M(E)$ so H is abelian, which is a contradiction. Thus, if $p > 2$, all nonabelian subgroups of G of index p^2 are \mathcal{A}_1 -groups.

Now let $p = 2$. Assume that $\exp(F) = 4$, where $F \neq H$ is metacyclic of order 16. Then all subgroups of order 2 in F are characteristic so normal in G , a contradiction since $Z(G)$ is cyclic. Thus, $F \cong M_{24}$. This case we shall consider in (i1).

(i1) Assume that $p = 2$ and $F \cong M_{24}$. We have $c_3(F) = 2$ and $F \triangleleft G$. Therefore, if L is a cyclic subgroup of F of index 2, then $|G : N_G(L)| \leq 2$. Let $F < M \leq N_G(L)$ with $|M : F| = 2$. If $M/L \cong C_4$, then $C_M(L) = L$ since F/L is the unique subgroup of order 2 in M/L . But in this case M/L is isomorphic to a subgroup of $\text{Aut}(L) \cong E_4$, a contradiction. Hence, we have $M/L \cong E_4$. Let R/L be a subgroup of order 2 in M/L with $R/L \neq F/L$. Since $K < L < R$ and $|R/K| = 2^3$, Theorem 70.1 forces $R > G'$. But then $R \cap F = L \geq G'$ and so G' is cyclic. This is a contradiction since $G'/K \cong E_4$.

Thus, if $p = 2$, then G has no nonabelian metacyclic subgroups of order 2^4 . It follows that then G has no \mathcal{A}_2 -subgroups of index 4 (otherwise, by the above, it has a nonabelian metacyclic subgroup of order 2^4).

(i2) Assume that $p = 2$ and H is a nonmetacyclic \mathcal{A}_1 -group of exponent 4. Then $\Phi(H) = Z(H) = L \times K$, where $|L| = 2$, $Z(H)$ is normal in G and $H/Z(H) \cong E_4$. Set $U = C_G(L) = C_G(Z(H))$. Then $|G : U| = 2$ since $L \not\leq Z(G)$ (recalling that K is the unique minimal normal subgroup of G). In that case H/L is a (proper) nonabelian subgroup of order 8 in U/L which implies that U/L is not an \mathcal{A}_1 -group. By hypothesis, $d(U) = 2$ and so $L < \Phi(U)$ and $C_U(H/L) < H/L$. It follows that U/L is of maximal class (Lemma 64.1(i)), and so $(U/L)' \cong C_4$. By Taussky's theorem, $L \not\leq U'$ so $U' \cong C_4$. However, $H < U$ and $H' < U' < H$ so H is metacyclic (Lemma 65.1), contrary to the assumption.

Thus, if $p = 2$, then $|G| > 2^6$ (otherwise, G is an \mathcal{A}_2 -group so of class 2).

(i3) Now we assume that $p > 2$. Then, as we have been proved already, all nonabelian subgroups of G of order p^4 are either abelian or \mathcal{A}_1 -groups. Let H be a nonabelian subgroup of index p^2 in G .

Assume that H is a nonmetacyclic \mathcal{A}_1 -group. Then H/K is abelian of type (p^2, p) and $\mathfrak{V}_1(H) > \{1\}$ (see Lemma 65.1) is a normal subgroup of G not containing $K = H'$, a contradiction since $K = K_3(G)$ is the unique minimal normal subgroup of G .

Hence, H is metacyclic, H/K is abelian of type (p^2, p) and $\bar{G} = G/K$ is isomorphic to a group of Theorem 70.1(c). Set $\bar{E} = \Omega_1(\bar{G})$ so that $\bar{E} \cong E_{p^3}$ and E (the inverse image of \bar{E} in G) of order p^4 , is abelian since it is not an \mathcal{A}_1 -group in view of $d(E) \geq 3$ (see the paragraph, preceding (i1)). Since $\bar{H} \geq Z(\bar{G})$ and $Z(\bar{G}) < \Omega_1(\bar{G})$, we get $\bar{E} \cap \bar{H} = Z(\bar{G})$ and $|H \cap E| = p^3$. But H is metacyclic and so $H \cap E$ is abelian of type (p^2, p) and therefore E is abelian of type (p^2, p, p) . Set $E_1 = \Omega_1(E)$ so that $E_1 \cong E_{p^3}$, $E_1 \cap H \cong E_{p^2}$, and $E_1 > K$. The quotient group G/E_1 is noncyclic since $\bar{G}/\bar{E} \cong E_{p^2}$ is its epimorphic image. Let A/E_1 and B/E_1 be two distinct subgroups of order p in G/E_1 so that $(AB)/E_1 \cong E_{p^2}$. Note that Theorem 70.1(c) implies that \bar{A}, \bar{B} being order p^3 are normal in \bar{G} . Since A and B are nonmetacyclic of order p^4 , they must be abelian. Therefore $C_G(E_1) = AB \in \Gamma_1$ (note that $E_1 \not\leq Z(G)$ because of $Z(G)$ is cyclic). Since $d(AB) = 2$, AB is nonabelian. But AB has two distinct abelian maximal subgroups and so $|(AB)'| = 2$ (Lemma 65.2(c)), and we get $(AB)' = K$. It follows that AB is a nonmetacyclic \mathcal{A}_1 -group with $Z(AB) = \Phi(AB) = E_1$ (Lemma 65.2(a)). Then $\mathfrak{U}_1(AB) \cong E_{p^2}$ is normal in G and $\mathfrak{U}_1(AB) \cap K = \{1\}$, a contradiction since K is the unique minimal normal subgroup of G and $\mathfrak{U}_1(AB)$ is normal in G .

Thus, $|G| > p^6$ for all p .

(ii) Let $|G| \geq p^7$. As above, set $K = K_3(G)$; it follows from Theorem 70.1 that $|G/K| \leq p^6$. Assume that $|G/K| \leq p^5$. Take a G -invariant subgroup $L < K$ with $|K : L| = p$. We have $|G/L| \leq p^6$ and G/L satisfies the assumptions of our theorem. By (i), we have a contradiction since $L > \{1\}$. Hence $|G/K| = p^6$; then $p = 2$ (Theorem 70.1), and G/K is isomorphic to the group of Theorem 70.1(d).

Let, in addition, $|G| = 2^7$ so that $|K| = 2$. Assume that L is another minimal normal subgroup of G . Then $|G/L| = 2^6$ so, by (i), G/L is of class 2. Then G , as a subgroup of $(G/K) \times (G/L)$, is also of class 2, a contradiction. Thus, K is the unique minimal normal subgroup of G ; in particular, $Z(G)$ is cyclic.

Let H be an arbitrary subgroup of order 2^5 in G . Since $\exp(G) \leq 2^3$ (by the above and Theorem 70.1), H is not cyclic. If $K \not\leq H$, then $KH = K \times H \in \Gamma_1$ and $d(KH) \geq 3$, a contradiction. Hence $H > K$ and so, by Theorem 70.1(d), $H > G' = \Phi(G)$ and H is normal in G . Since G/K is an \mathcal{A}_2 -group, H/K is abelian in view of $|(G/K) : (H/K)| = 4$.

Set $G' = W$. By Theorem 70.1(d), $\Omega_1(G/K) = W/K = Z(G/K) \cong E_{2^3}$. If $A/K < W/K$ is of order 2, then A is normal in G so $W \leq C_G(A)$ since $|\text{Aut}(A)|_2 = 2$. Thus, $W = \langle A \mid K < A < W, |A| = 4 \rangle \leq Z(W)$ so W is abelian. It follows that $W \in \{E_{2^4}, C_4 \times C_2 \times C_2\}$.

By Theorem 70.1(d), $G = \langle a, b, c \rangle$ and a, b, c are not involutions modulo K since $\Phi(G/K) = \Omega_1(G/K)$ so that $\langle x, W \rangle$ is of order 2^5 and class ≤ 2 for $x \in G - W$ since $\langle x, W \rangle / K$ is abelian (this fact will be used in the sequel) and $\langle a^2, b^2, c^2, K \rangle = G' (= W)$,

$$(***) \quad [a, b] \equiv c^2, \quad [a, c] \equiv b^2c^2, \quad [b, c] \equiv a^2b^2 \pmod{K}.$$

Also, for any $x, y \in G$,

$$\begin{aligned} [x, y]^2 &= [y, x]^{-2} = [y, x]^2, \quad [x^2, y]^{-1} = [x^2, y], \quad [x^2, y^{-1}] = [x^2, y], \\ [x^2, y] &= x^{-2}y^{-1}x^2y = x^{-2}(y^{-1}xy)^2 = x^{-2}(x[x, y])^2 \\ &= x^{-2}x^2[x, y]^2[[x, y], x] = [x, y]^2[x, y, x]. \end{aligned}$$

Using the above identity and the relations for G/K (see (**)), we get

$$[a^2, c] = [a, c]^2[[a, c], a] = [a, c]^2[b^2c^2k, a] = [a, c]^2[b^2, a][c^2, a],$$

where $k \in K \leq Z(G)$ and so

$$(11) \quad [a^2, c] = [a, c]^2[b^2, a][c^2, a].$$

In the same way we obtain the following relations:

$$(12) \quad [b^2, c] = [b, c]^2[b, c, b] = [b, c]^2[a^2b^2k, b] = [b, c]^2[a^2, b],$$

$$(13) \quad [b^2, a] = [b, a]^2[b, a, b] = [a, b]^2[c^2k, b] = [a, b]^2[c^2, b],$$

$$(14) \quad [c^2, a] = [c, a]^2[c, a, c] = [c, a]^2[b^2c^2k, c] = [a, c]^2[b^2, c],$$

$$(15) \quad [a^2, b] = [a, b]^2[a, b, a] = [a, b]^2[c^2k, a] = [a, b]^2[c^2, a],$$

$$(16) \quad [c^2, b] = [c, b]^2[c, b, c] = [c, b]^2[a^2b^2k, c] = [b, c]^2[a^2, c][b^2, c].$$

For any $x, y, z \in G$ we get (noting that W is abelian and $[x, y^{-2}] \in [x, \mathfrak{V}_1(G)] = [x, G'] \leq K \leq Z(G)$)

$$[x, y^{-1}] = [x, yy^{-2}] = [x, y^{-2}][x, y]^{y^{-2}} = [x, y^{-2}][x, y]$$

since G' is abelian and $y^{-2} \in \mathfrak{V}_1(G) = G'$, and so $[x, y^{-1}, z] = [[x, y^{-2}][x, y], z] = [x, y, z]$. Hence from the Hall–Witt identity $[a, b^{-1}, c]^b[b, c^{-1}, a]^c[c, a^{-1}, b]^a = 1$ we get $[a, b, c]^b[b, c, a]^c[c, a, b]^a = 1$ so $[c^2, c]^b[a^2b^2, a]^c[b^{-2}c^{-2}, b]^a = 1$, by (**), or, taking into account that $[b^2, a], [c^2, b] \in K \leq Z(G)$, we get

$$(17) \quad [b^2, a][c^2, b] = 1, \text{ or, what is the same, } [b^2, a] = [c^2, b],$$

It follows from (17) and (13) that $[a, b]^2 = 1$ so $[a^2, b] = [c^2, a]$, by (15). It follows from (15) and (12) that

$$[c^2, a] = [a, c]^2[b^2, c] = [a, c]^2[b, c]^2[a^2, b] = [a, c]^2[b, c]^2[c^2, a]$$

so, canceling, we get $[a, c]^2 = [b, c]^2$. Then, by (16), (12), (14), (11) we get

$$\begin{aligned} [c^2, b] &= [b, c]^2[a^2, c][b^2, c] = [a^2, b][a^2, c] = [c^2, a][a^2, c] \\ &= [a, c]^2[b^2, a][c^2, a][c^2, a] = [a, c]^2[c^2, b] \end{aligned}$$

so $[a, c]^2 = 1$. Thus, $[a, b]^2 = [a, c]^2 = [b, c]^2 = 1$ and one can rewrite (11–17) as follows:

$$(18) \quad [b^2, a] = [a^2, b][a^2, c],$$

$$(19) \quad [b^2, c] = [a^2, b],$$

$$(20) \quad [c^2, a] = [a^2, b],$$

$$(21) \quad [c^2, b] = [a^2, b][a^2, c].$$

In particular, since the abelian group $W = G' = \langle [a, b], [a, c], [b, c], K \rangle$ is generated by elements of order 2, we get $W \cong E_{2^4}$. Since $K = \langle k \rangle$ is the unique minimal normal subgroup of G and $K \leq Z(G) \leq W$, we get $Z(G) = K$. If $[a^2, b] = [a^2, c] = 1$, then the relations (18–21) and (****) imply that $W = \langle a^2, b^2, c^2, K \rangle \leq Z(G)$, a contradiction. It follows that we have exactly three possibilities for the values of $[a^2, b]$ and $[a^2, c]$ (below $K = \langle k \mid k^2 = 1 \rangle$):

$$(G_1) \quad [a^2, b] = k, \quad [a^2, c] = k;$$

$$(G_2) \quad [a^2, b] = k, \quad [a^2, c] = 1;$$

$$(G_3) \quad [a^2, b] = 1, \quad [a^2, c] = k.$$

In all three cases we have (see (***)): $[a, b] \equiv c^2$, $[a, c] \equiv b^2c^2$, $[b, c] \equiv a^2b^2 \pmod{K}$.

In case (G_1) we substitute $[a^2, b] = k$, $[a^2, c] = k$ in relations (18–21) and obtain

$$[b^2, a] = 1, \quad [b^2, c] = k, \quad [c^2, a] = k, \quad [c^2, b] = 1.$$

If $[a, b] = c^2k$, then we replace a with $a' = a^{-1} = aa^2$ and get

$$[a', b] = [aa^2, b] = [a, b]^{a^2}[a^2, b] = [a, b]k = c^2k^2 = c^2,$$

and so writing again a instead of a' , we may assume from the start that

$$(\alpha) \quad [a, b] = c^2.$$

If $[a, c] = b^2c^2k$, then we replace c with $c' = c^{-1}$ so that the relation (α) remains valid in view of $o(c) = 4$, and we get

$$[a, c'] = [a, cc^2] = [a, c^2][a, c]^{c^2} = k[a, c] = k^2b^2c^2 = b^2(c')^2,$$

and so we may assume from the start that

$$(\beta) \quad [a, c] = b^2c^2.$$

Finally, in case $[b, c] = a^2b^2k$, we replace b with $b' = b^{-1}$. Then the relation (α) remains unchanged: $[a, b'] = [a, bb^2] = [a, b^2][a, b]^{b^2} = [a, b]$, and also the relation

(β) remains unchanged and we get

$$[b', c] = [bb^2, c] = [b, c]^{b^2} [b^2, c] = [b, c]k = a^2 b^2 k^2 = a^2 (b')^2,$$

and so we may assume from the start that

$$(\gamma) \quad [b, c] = a^2 b^2.$$

The structure of $G = G_1$ is uniquely determined. If we set (identify)

$$a = (1, 2)(3, 13, 7, 9)(4, 10, 8, 11)(5, 6)(12, 16)(14, 15),$$

$$b = (1, 3)(2, 9)(4, 14, 8, 12)(5, 7)(6, 13)(10, 16, 11, 15),$$

$$c = (1, 4)(2, 10, 6, 11)(3, 12)(5, 8)(7, 14)(9, 15, 13, 16),$$

we see that the permutations a, b, c satisfy all relations for G_1 . Since

$$k = [a^2, b] = (1, 5)(2, 6)(3, 7)(4, 8)(9, 13)(10, 11)(12, 14)(15, 16)$$

and $\langle k \rangle = Z(G)$, we see that our permutations a, b, c induce a faithful permutation representation from G_1 into the alternating group A_{16} .

In case (G_2) we substitute $[a^2, b] = k, [a^2, c] = 1$ in relations (18–21) and obtain

$$[b^2, a] = k, \quad [b^2, c] = k, \quad [c^2, a] = k, \quad [c^2, b] = k.$$

If $[a, b] = c^2 k$, then we replace a with a^{-1} . If $[a, c] = b^2 c^2 k$, then we replace c with c^{-1} . Finally, in case $[b, c] = a^2 b^2 k$, we replace a with a^{-1} and b with b^{-1} . Doing so, we can assume (as before) from the start that $[a, b] = c^2, [a, c] = b^2 c^2, [b, c] = a^2 b^2$. The structure of $G = G_2$ is uniquely determined. Similarly, the permutations:

$$a = (1, 2)(3, 9, 7, 10)(13, 16, 14, 15)(4, 12)(5, 6)(8, 11),$$

$$b = (1, 3)(5, 7)(2, 9, 6, 10)(11, 15)(12, 16)(4, 13, 8, 14),$$

$$c = (1, 4)(2, 11, 6, 12)(5, 8)(9, 16)(10, 15)(3, 13, 7, 14),$$

induce a faithful permutation representation from G_2 into A_{16} .

In case (G_3) we substitute $[a^2, b] = 1, [a^2, c] = k$ in the relations (18) to (21) and obtain $[b^2, a] = k, [b^2, c] = 1, [c^2, a] = 1, [c^2, b] = k$. If $[a, b] = c^2 k$, then we replace b with b^{-1} . If $[a, c] = b^2 c^2 k$, then we replace a with a^{-1} . Finally, in case $[b, c] = a^2 b^2 k$, we replace c with c^{-1} . Doing so, we can assume from the start that $[a, b] = c^2, [a, c] = b^2 c^2, [b, c] = a^2 b^2$. The structure of $G = G_3$ is uniquely determined. The permutations:

$$a = (1, 2)(4, 14, 8, 11)(12, 15, 13, 16)(3, 10)(5, 6)(7, 9),$$

$$b = (1, 3)(4, 13)(2, 9, 6, 10)(5, 7)(8, 12)(11, 16, 14, 15),$$

$$c = (1, 4)(3, 12, 7, 13)(2, 11)(5, 8)(6, 14)(9, 16, 10, 15),$$

induce a faithful permutation representation from G_3 into A_{16} .

Considering G_1, G_2, G_3 as above subgroups of A_{16} , we see that the permutation $(2, 4, 11, 6, 8, 12, 9, 7, 14, 10)(3, 13)$ conjugates G_1 onto G_2 , and the permutation $(2, 11, 8, 6, 14, 7, 10, 4)(3, 9, 13, 12)$ conjugates G_1 onto G_3 . In particular, G_2 and G_3 are isomorphic to $G = G_1$. Since $K < \Phi(G)$, G satisfies the hypothesis since G/K does. The proof is complete. \square

Thus, groups of the title are classified for $p > 2$ (see also [Bla1, Theorem 3.1]).

Theorem 70.3. *Let G be a p -group with $d(G) > 2$, whose maximal subgroups are generated by two elements. If G is of class 3, then $p = 2$, $2^7 \leq |G| \leq 2^8$ and $G/K_3(G)$ is isomorphic to the group of order 2^6 of Theorem 70.1(d). If $|G| = 2^7$, then $|K_3(G)| = 2$ and G is isomorphic to the group of Theorem 70.2. If $|G| = 2^8$, then $K_3(G) = Z(G) \cong E_4$, $G' = \Phi(G) = \Omega_1(G) \cong E_{25}$ and such groups exist.*

Proof. Suppose that all maximal subgroups of a p -group G are generated by two elements but $d(G) = 3$. Assume, in addition, that G is of class 3.

By Theorem 70.2, $p = 2$, $|G| \geq 2^7$, $\{1\} < K = K_3(G) \leq Z(G)$, and G/K is isomorphic to the group of order 2^6 of Theorem 70.1(d). It follows that

$$G' = \Phi(G), \quad G/G' \cong E_8, \quad G'/K \cong E_8, \quad [G', G] = K, \\ \Omega_1(G/K) = Z(G/K) = G'/K.$$

Let $x \in G'$ and $g \in G$. Then $[x, g] \in K \leq Z(G)$ and so $[x, g]^2 = [x^2, g] = 1$ since $x^2 \in K$. Hence the abelian group K is generated by involutions and so K is elementary abelian. Let S be a maximal subgroup in K . Then G/S (of order 2^7) is isomorphic to the group of Theorem 70.2. In particular, $Z(G/S) = K/S$ and so $K = Z(G)$. Also, G'/S is elementary abelian. Hence $\Phi(G') \leq S$ for any maximal subgroup S of K . Since K is elementary abelian and noncyclic, we get $\Phi(G') = \{1\}$ and so $\Omega_1(G) = G'$ is elementary abelian.

We have $G = \langle a, b, c \rangle$, $\langle a^2, b^2, c^2 \rangle K = G'$ and for each maximal subgroup S of K , G/S is isomorphic to the group of Theorem 70.2. Suppose that $|K| \geq 2^3$. Then there exists a maximal subgroup S of K which contains $\langle [a^2, b], [a^2, c] \rangle$. But then a^2S is contained in $Z(G/S)$. This is a contradiction since $a^2 \notin K$ and $Z(G/S) = K/S$. We have proved that $|K| \leq 4$.

A group G of order 2^8 of Theorem 70.3 exists. For example, such a group is

$$G = \langle a, b, c \mid a^4 = b^4 = c^4 = k^2 = l^2 = m^2 = klm = 1, \\ [a, k] = [b, k] = [c, k] = 1, [a, l] = [b, l] = [c, l] = 1, [a, b] = c^2, \\ [a, c] = b^2c^2, [b, c] = a^2b^2, [a^2, b] = m, [a^2, c] = k, \\ [b^2, a] = l, [b^2, c] = m, [c^2, a] = m, [c^2, b] = l \rangle.$$

Here $\langle k, l \rangle = Z(G) = K_3(G) \cong E_4$ and $G' = \Phi(G) = \langle a^2, b^2, c^2, k, l \rangle = \Omega_1(G) \cong E_{25}$. We get a faithful permutation representation of G by setting:

$$a = (1, 2)(3, 21, 22, 15)(4, 23, 10, 18)(5, 8)(6, 11)(7, 17)(9, 14, 12, 26)$$

$$(13, 16, 25, 27)(19, 30, 20, 29)(24, 32, 31, 28),$$

$$b = (1, 3)(2, 14, 11, 15)(4, 24, 25, 20)(5, 9)(6, 12)(7, 22)(8, 21, 17, 26)$$

$$(10, 19, 13, 31)(16, 29, 27, 28)(18, 32, 23, 30),$$

$$c = (1, 4)(2, 16, 17, 18)(3, 19, 12, 20)(5, 10)(6, 13)(7, 25)(8, 27, 11, 23)$$

$$(9, 24, 22, 31)(14, 32, 21, 30)(15, 28, 26, 29).$$

In this way we see that the group G exists as a subgroup of A_{32} .

In view of $K < \Phi(G)$, G satisfies the hypothesis since G/K does. \square

Theorem 70.4. *Let G be a p -group with $d(G) > 2$ all of whose maximal subgroups are generated by two elements. If G is of class > 2 , then $p = 2$ and one of the following holds:*

(i) $G/K_4(G)$ is isomorphic to the uniquely determined group of order 2^7 given in Theorem 70.2.

(ii) $H = G/K_4(G)$ is isomorphic to one of the groups of order 2^8 described in Theorem 70.3 and more precisely, $H = \langle a, b, c \rangle$ with

$$a^4 = b^4 = c^4 = k^2 = l^2 = m^2 = klm = 1, \quad [a, k] = [b, k] = [c, k] = 1,$$

$$[a, l] = [b, l] = [c, l] = 1, \quad [a, b] = c^2k^\epsilon, \quad [a, c] = b^2c^2k^\epsilon, \quad [b, c] = a^2b^2,$$

$$[a^2, b] = m, \quad [a^2, c] = k, \quad [b^2, a] = l, \quad [b^2, c] = m, \quad [c^2, a] = m, \quad [c^2, b] = l,$$

where $\epsilon = 0, 1$. These two groups (for $\epsilon = 0$ and $\epsilon = 1$) exist as subgroups of the alternating group A_{32} and they are not isomorphic. We have in both cases $K_3(H) = Z(H) = \langle k, l \rangle \cong E_4$ and $H' = \Phi(H) = \Omega_1(H) = \langle a^2, b^2, c^2, k, l \rangle \cong E_{25}$. In case $\epsilon = 1$, H possesses an automorphism of order 7 which acts fixed-point-freely on $H/Z(H)$ and so $H/Z(H)$ is isomorphic to the Suzuki group of order 2^6 (given in Theorem 70.1(d)).

Proof. We may assume that $K_4(G) = \{1\}$ so that G is of class 3. Using Theorems 70.2 and 70.3, we see that G is either isomorphic to the group of order 2^7 given in Theorem 70.2 or a group of order 2^8 described in Theorem 70.3. It remains to determine completely the structure of G in the second case. In that case $G/K_3(G)$ is the special group of order 2^6 isomorphic to the group of Theorem 70.1(d), $K_3(G) = Z(G) \cong E_4$, and $G' = \Phi(G) = \Omega_1(G) \cong E_{25}$. We have $G = \langle a, b, c \rangle$, where a, b, c are elements of order 4 in $G - G'$ so that $\langle a^2, b^2, c^2 \rangle \times K_3(G) = G'$ and $[a, b] \equiv c^2$, $[a, c] \equiv b^2c^2$, $[b, c] \equiv a^2b^2 \pmod{K_3(G)}$. Also, for each maximal subgroup S of

$K_3(G)$, $|S| = 2$ and G/S is isomorphic to the group of order 2⁷ of Theorem 70.2. In particular, $Z(G/S) = Z(G)/S$ is of order 2.

We claim that each of the commutators $[a^2, b]$, $[a^2, c]$, $[b^2, a]$, $[b^2, c]$, $[c^2, a]$, $[c^2, b]$ are distinct from 1. Indeed, if (for example) $[a^2, b] = 1$, then we consider a maximal subgroup S^* of $Z(G)$ which contains $[a^2, c]$. Then $a^2 S^* \in Z(G/S^*)$, contrary to the fact that $Z(G/S^*) = Z(G)/S^*$ (and noting that $a^2 \notin Z(G)$).

Set $[a^2, b] = m$ and $[a^2, c] = k$. If $m = k$, then considering $G/\langle m \rangle$, we have $a^2 \langle m \rangle \in Z(G/\langle m \rangle)$, a contradiction. It follows that $k \neq m$ and so $K_3(G) = \langle k, m \rangle$ since $K_3(G) \cong E_4$. Set $l = km$ so that k, l, m are the three distinct involutions in $Z(G) = K_3(G)$. We compute (with some $z \in Z(G)$):

$$\begin{aligned} [b^2, c] &= [bb, c] = [b, c]^b [b, c] = (a^2 b^2 z)^b a^2 b^2 z = (a^2)^b a^2 \\ &= [b, a^2] = [a^2, b] = m, \\ [c^2, a] &= [c, a]^c [c, a] = (b^2 c^2 z)^c b^2 c^2 z = (b^2)^c b^2 = [c, b^2] = m, \\ [c^2, b] &= [c, b]^c [c, b] = (a^2 b^2 z)^c a^2 b^2 z = (a^2)^c a^2 (b^2)^c b^2 \\ &= [c, a^2] [c, b^2] = km = l, \\ [b^2, a] &= [b, a]^b [b, a] = (c^2 z)^b c^2 z = (c^2)^b c^2 = [b, c^2] = l. \end{aligned}$$

Hence we have obtained the following relations:

$$(\alpha^*) \quad \begin{aligned} [a^2, b] &= m, & [a^2, c] &= k, & [b^2, a] &= l, \\ [b^2, c] &= m, & [c^2, a] &= m, & [c^2, b] &= l, \end{aligned}$$

where $Z(G) = K_3(G) = \langle k, l \rangle \cong E_4$ and $m = kl$. Also, we may set

$$(\alpha^{**}) \quad [a, b]c^2 = k^p l^q, \quad [a, c]b^2 c^2 = k^r l^s, \quad [b, c]a^2 b^2 = k^t l^u,$$

where p, q, r, s, t, u are some integers mod 2.

For any $x \in G - G'$, $[x, G'] \leq Z(G)$ and so $\langle x, G' \rangle$ is of class ≤ 2 . This fact will be used many times. For any $x, y \in G - G'$ and any $g_1, g_2 \in G'$, we have

$$[(xg_1)^2, yg_2] = [(xg_1)^2, y] = [x^2 g_1^2 [g_1, x], y] = [x^2, y].$$

Therefore, if we replace a, b, c with $a' = aa^{2(q+s+u)}$, $b' = bb^{2(s+u)}$, $c' = cc^{2s}$, respectively, then the relations (α^*) remain preserved. However, the relations (α^{**})

are simplified, as the following computation shows:

$$\begin{aligned}
 [a', b'](c')^2 &= [aa^{2(q+s+u)}, bb^{2(s+u)}]c^2 \\
 &= [a, bb^{2(s+u)}]^{a^{2(q+s+u)}}[a^{2(q+s+u)}, bb^{2(s+u)}]c^2 \\
 &= [a, bb^{2(s+u)}][a^{2(q+s+u)}, bb^{2(s+u)}]c^2, \\
 [a, b^{2(s+u)}][a, b][a^{2(q+s+u)}, b^{2(s+u)}][a^{2(q+s+u)}, b]c^2 \\
 &= [a, b^2]^{s+u}[a, b][a^2, b]^{q+s+u}c^2 \\
 &= ([a, b]c^2)l^{s+u}m^{q+s+u} = k^pl^ql^{s+u}k^{q+s+u}l^{q+s+u} = k^{p+q+s+u},
 \end{aligned}$$

and we get in a similar way $[a', c'](b')^2(c')^2 = k^{q+r+u}$, $[b', c'](a')^2(b')^2 = k^{s+t+u}$.

Writing again a, b, c (instead of a', b', c'), we see that the relations (α^{**}) are simplified into:

$$(\alpha^{***}) \quad [a, b]c^2 = k^\epsilon, \quad [a, c]b^2c^2 = k^\eta, \quad [b, c]a^2b^2 = k^\zeta,$$

where ϵ, η, ζ are some integers mod 2. In this way we have obtained eight possibilities G_1, G_2, \dots, G_8 for the structure of G depending on the values of these integers:

(G_1)	$\epsilon = 0,$	$\eta = 0,$	$\zeta = 0;$
(G_2)	$\epsilon = 0,$	$\eta = 0,$	$\zeta = 1;$
(G_3)	$\epsilon = 0,$	$\eta = 1,$	$\zeta = 0;$
(G_4)	$\epsilon = 0,$	$\eta = 1,$	$\zeta = 1;$
(G_5)	$\epsilon = 1,$	$\eta = 0,$	$\zeta = 0;$
(G_6)	$\epsilon = 1,$	$\eta = 0,$	$\zeta = 1;$
(G_7)	$\epsilon = 1,$	$\eta = 1,$	$\zeta = 1;$
(G_8)	$\epsilon = 1,$	$\eta = 1,$	$\zeta = 0.$

We replace now a, b, c with

$$(\beta^*) \quad a^* = bb^2, \quad b^* = c, \quad c^* = aca^2b^2l,$$

respectively, and verify first that the relations (α^*) remain unchanged. For example:

$$[(a^*)^2, c^*] = [b^2, aca^2b^2l] = [b^2, ac] = [b^2, c][b^2, a]^c = ml^c = ml = k.$$

We want to see what happens with the relations (α^{***}) for arbitrary integers ϵ, η, ζ (mod 2). First we compute:

$$\begin{aligned}
 (ac)^2 &= a(ac)c = a(ac[c, a])c = a(acb^2c^2k^\eta)c = a^2(cb^2)c^3k^\eta \\
 &= a^2(b^2cm)c^3k^\eta = a^2b^2k^{\eta+1}l,
 \end{aligned}$$

which gives

$$\begin{aligned}(c^*)^2 &= (aca^2b^2l)^2 = (ac)^2(a^2b^2l)^2[a^2b^2l, ac] = a^2b^2k^{\eta+1}l[a^2b^2, c][a^2b^2, a]^c \\ &= a^2b^2k^{\eta+1}l[a^2, c][b^2, c][b^2, a]^c = a^2b^2k^{\eta+1}l.\end{aligned}$$

Then it is easy to transform the relations (α^{***}) :

$$\begin{aligned}[a^*, b^*](c^*)^2 &= [bb^2, c]a^2b^2k^{\eta+1}l = [b, c]b^2[b^2, c]a^2b^2k^{\eta+1}l \\ &= ([b, c]a^2b^2)mk^{\eta+1}l = k^\xi mk^{\eta+1}l = k^{\eta+\xi},\end{aligned}$$

and we get in a similar way:

$$[a^*, c^*](b^*)^2(c^*)^2 = k^{\epsilon+\eta+\xi+1}$$

and

$$[b^*, c^*](a^*)^2(b^*)^2 = k^{\eta+1}.$$

These results show that our group G_i defined with the constants ϵ, η, ζ in the relations (α^{***}) is isomorphic with the group G_j defined with the constants $\eta + \zeta, \epsilon + \eta + \zeta + 1, \eta + 1$. In particular, the group G_1 defined with $\epsilon = \eta = \zeta = 0$ is isomorphic to the group G_4 defined with the constants 0, 1, 1. Further, the group G_4 with $\epsilon = 0, \eta = 1, \zeta = 1$ is isomorphic with G_3 defined with the constants 0, 1, 0 and this one is isomorphic with G_5 . Then G_5 is isomorphic with G_2 , G_2 is isomorphic with G_6 and G_6 is isomorphic with G_7 . However, our replacement (β^*) sends G_8 onto G_8 and we verify that in fact (β^*) induces an automorphism of order 7 on G_8 which acts fixed-point-freely on $G_8/\mathbb{Z}(G_8)$. Hence $G/\mathbb{Z}(G)$ is isomorphic to the Suzuki group of order 2^6 given in Theorem 70.1(d).

The group G_1 is exactly the group occurring as an example in the proof of Theorem 70.3, where we have found a faithful permutation representation of G_1 of degree 32 (with even permutations). We get a faithful permutation representation of G_8 by setting:

$$\begin{aligned}a &= (1, 2)(3, 14, 21, 25)(4, 18, 10, 27)(5, 8)(6, 11)(7, 17) \\ &\quad (9, 24, 12, 15)(13, 26, 23, 16)(19, 30, 20, 29)(22, 32, 31, 28); \\ b &= (1, 3)(2, 14, 11, 15)(4, 22, 23, 20)(5, 9)(6, 12)(7, 21) \\ &\quad (8, 24, 17, 25)(10, 19, 13, 31)(16, 29, 26, 28)(18, 32, 27, 30); \\ c &= (1, 4)(2, 16, 17, 18)(3, 19, 12, 20)(5, 10)(6, 13)(7, 23) \\ &\quad (8, 26, 11, 27)(9, 22, 21, 31)(14, 32, 24, 30)(15, 28, 25, 29).\end{aligned}$$

In this way, we see that also the group G_8 exists as a subgroup of A_{32} .

Finally, considering G_1 and G_8 as subgroups of A_{32} , W. Lempken (Institut für experimentelle Mathematik, Essen) has shown that the groups G_1 and G_8 are not isomorphic. \square

Let G be a 2-group of class > 3 with $d(G) > 2$ but $d(H) = 2$ for all $H \in \Gamma_1$. Then, it is possible to prove that we must have $|G| \geq 2^9$ and we exhibit here an example of such a group G of order 2^9 and class 4, where $G = \langle a, b, c \rangle$ with the following defining relations:

$$\begin{aligned} a^8 &= b^4 = c^8 = 1, \quad a^4 = c^4 = u, \quad [a, u] = [b, u] = [c, u] = 1, \\ [a^2, b] &= m, \quad [a^2, c] = k, \quad m^2 = k^2 = 1, \quad km = l, \quad l^2 = 1, \\ [b^2, a] &= lu, \quad [b^2, c] = um, \quad [c^2, a] = um, \quad [c^2, b] = l, \quad [a, b] = c^2, \\ [a, c] &= b^2 c^2, \quad [b, c] = a^2 b^2, \quad [a^2, b^2] = 1, \quad [a^2, c^2] = 1, \quad [b^2, c^2] = u, \\ [m, a] &= 1, \quad [m, b] = 1, \quad [m, c] = u, \quad [k, a] = 1, \quad [k, b] = u, \\ [k, c] &= 1, \quad [l, a] = 1, \quad [l, b] = u, \quad [l, c] = u. \end{aligned}$$

Here $G' = \langle a^2, b^2, c^2, k, l \rangle$ is of order 2^6 , $K_4(G) = Z(G) = \langle u \rangle$ is of order 2, $K_3(G) = \langle k, l, u \rangle \cong E_8$, and $Z(G') = \langle a^2, k, l \rangle$ is abelian of type $(4, 2, 2)$. Finally, we have shown that this group G exists as a subgroup of the symmetric group of degree 64.

We can improve Theorem 70.4 in case (i).

Theorem 70.5. *Let G be a p -group with $d(G) > 2$ all of whose maximal subgroups are generated by two elements. If G is of class > 2 , then $p = 2$, and if $G/K_4(G)$ is isomorphic to the group of order 2^7 given in Theorem 70.2 (case (i) of Theorem 70.4), then $K_4(G) = \{1\}$.*

Proof. Assume that $K_4(G) \neq \{1\}$. To get a contradiction we may assume $|K_4(G)| = 2$ (by considering a suitable quotient group of G). Then $G/K_4(G)$ is isomorphic to the group of order 2^7 of Theorem 70.2. We may set $G = \langle a, b, c \rangle$, where

$$\begin{aligned} a^4 &\equiv b^4 \equiv c^4 \equiv k^2 \equiv 1, & [a, k] &\equiv [b, k] \equiv [c, k] \equiv 1, & [a, b] &\equiv c^2, \\ [a, c] &\equiv b^2 c^2, & [b, c] &\equiv a^2 b^2, & [a^2, b] &\equiv k, \\ [a^2, c] &\equiv k, & [b^2, a] &\equiv 1, & [b^2, c] &\equiv k, \\ [c^2, a] &\equiv k, & [c^2, b] &\equiv 1 \pmod{K_4(G)}. \end{aligned}$$

Also we may set $K_4(G) = \langle u \rangle \leq Z(G)$. Then $K_3(G) = \langle k, u \rangle$, $W = G' = \Phi(G) = \langle a^2, b^2, c^2, k, u \rangle$ is of order 2^5 and class ≤ 2 since $W/K_4(G) \cong E_{2^4}$.

Since $C_G(K_3(G))$ is a subgroup of index 2 in G , we get $K_3(G) \leq Z(W)$. From $[a^2, b] \equiv k \pmod{K_4(G)}$ with $k \notin K_4(G)$ follows $[a^2, b] = k_0$ with $k_0 \in K_3(G) - K_4(G)$. From $a^4 \equiv 1 \pmod{K_4(G)}$ follows $a^4 \in K_4(G) \leq Z(G)$ and so

$$1 = [a^4, b] = [a^2 a^2, b] = [a^2, b]^{a^2} [a^2, b] = k_0^{a^2} k_0 = k_0^2,$$

since $a^2 \in W$ and $K_3(G) = \langle k_0, u \rangle \leq Z(W)$. Hence k_0 is an involution and so we have proved that $K_3(G) \cong E_4$.

Using $[c, b^2] = ku^i$ and $[c^2, b] = u^j$, where i, j are some integers (mod 2), we compute

$$[c^2, b^2] = [cc, b^2] = [c, b^2]^c[c, b^2] = (ku^i)^c ku^i = k^c k = c^{-1} k c k = [c, k],$$

since k is an involution. On the other hand, we get

$$[c^2, b^2] = [c^2, bb] = [c^2, b][c^2, b]^b = u^j(u^j)^b = (u^j)^2 = 1,$$

and so $[c, k] = 1$.

Using $[a, b^2] \in K_4(G) \leq Z(G)$ and $[a^2, b] = ku^i$ with an integer $i \pmod{2}$, we compute

$$[a^2, b^2] = [aa, b^2] = [a, b^2]^a[a, b^2] = [a, b^2]^2 = 1,$$

$$[a^2, b^2] = [a^2, bb] = [a^2, b][a^2, b]^b = ku^i(ku^i)^b = kk^b = [k, b],$$

and so $[k, b] = 1$.

Finally, using $[a, c^2] = ku^j$ and $[a^2, c] = ku^l$ with some integers $j, l \pmod{2}$, we get

$$[a^2, c^2] = [aa, c^2] = [a, c^2]^a[a, c^2] = (ku^j)^a ku^j = k^a k = [a, k],$$

$$[a^2, c^2] = [a^2, cc] = [a^2, c][a^2, c]^c = ku^l(ku^l)^c = kk^c = [k, c].$$

Hence (by the above) $[a, k] = [k, c] = 1$. We have obtained $[k, a] = [k, b] = [k, c] = 1$, and so $K_3(G) = \langle k, u \rangle \leq Z(G)$. This is a contradiction since G was of class 4. \square

The group G of Theorem 70.2 of order 2^7 is an \mathcal{A}_4 -group since $\langle a^2, b \rangle$ is a non-abelian subgroup of order 2^4 (this subgroup is minimal nonabelian nonmetacyclic) and G has no nonabelian subgroups of order 8. Obviously, D_8 is not a subgroup of G since $\Omega_1(G) = E_{2^4} = G'$. Also, $Q = Q_8$ is not a subgroup of G (otherwise, $Q \cap G' = C_2$ and so $S = G'Q$ is a maximal subgroup of G and so $d(S) = 2$ so $\Phi(S) = G'$ and, by Taussky's theorem, S is of maximal class, a contradiction).

Both groups G of Theorem 70.4 of order 2^8 are \mathcal{A}_5 -groups since $\langle a^2, b \rangle$ is a non-abelian subgroup of order 2^4 (this subgroup is minimal nonabelian nonmetacyclic) and G has no nonabelian subgroups of order 8. Obviously, D_8 is not a subgroup of G since $\Omega_1(G) = E_{2^5} = G'$. Also, $Q = Q_8$ is not a subgroup of G (otherwise, $Q \cap G' = C_2$ and so $T = G'Q$ is a maximal subgroup of G hence $d(T) = 2$; then $\Phi(T) = G'$ so, by Taussky's theorem, T is of maximal class, a contradiction).

The above two paragraphs show that if a 2-group G is such that $d(G) = 3$ but $d(H) = 2$ for all $H \in \Gamma_1$ and the class of G is > 2 , then G is an \mathcal{A}_n -group with $n < 5$ if and only if G is the unique group of order 2^7 from Theorem 70.2, and this G is an \mathcal{A}_4 -group.

Determination of \mathcal{A}_2 -groups

We recall that a p -group G is called an \mathcal{A}_n -group if every subgroup of index p^n is abelian but at least one subgroup of index p^{n-1} is nonabelian. Here we determine \mathcal{A}_2 -groups of order $> p^4$ up to isomorphism in terms of generators and relations. This determination will follow five propositions covering all \mathcal{A}_2 -groups.

Proposition 71.1. *Suppose that G is an \mathcal{A}_2 -group of order $> p^4$. Then $|G'| = p$ if and only if G has at least two distinct abelian maximal subgroups and in that case one of the following holds:*

- (i) $G = H \times C_p$, where H is minimal nonabelian.
- (ii) $G = \langle a, b, c \rangle$, where

$$a^{p^m} = b^{p^n} = c^{p^2} = 1, \quad m \geq n \geq 1, \quad m \geq 2, \quad [a, b] = d, \quad c^p = d, \\ [a, d] = [b, d] = [a, c] = [b, c] = 1.$$

Here $H = \langle a, b \rangle$ is nonmetacyclic minimal nonabelian, $H' = G' = \langle d \rangle$, $G = H * C$, where $C = \langle c \rangle$ is cyclic of order p^2 and $H \cap C = \langle d \rangle = \langle c^p \rangle = H'$.

Proof. Let G be an \mathcal{A}_2 -group of order $> p^4$ with $|G'| = p$. By Lemmas 65.2(c) and 65.4(d), $|G'| = p$ if and only if the set Γ_1 has at least two abelian members. In that case the set Γ_1 has a nonabelian member H so that $G = HZ(G)$, where $Z(G) \cap H = Z(H)$. We have $|H| > p^3$, $H' = G'$, $Z(H) = \Phi(H) = \Phi(G)$, and $|H : Z(H)| = p^2$ since H is an \mathcal{A}_1 -group. Clearly, $|Z(G) : Z(H)| = p$.

Suppose that there is an element $c \in Z(G) - H$ of order p . Then $G = H \times \langle c \rangle$ and it is clear that all such groups are \mathcal{A}_2 -groups.

We assume in the sequel that $\Omega_1(Z(G)) \leq H$; then $d(Z(H)) = d(Z(G))$ so $|Z(H) : \Phi(Z(H))| = |Z(G) : \Phi(Z(G))| = p|Z(H) : \Phi(Z(G))|$ (note that $\Phi(Z(H)) < \Phi(Z(G)) \leq Z(H)$ since $Z(H)$ is maximal in $Z(G)$) and so $|\Phi(Z(G)) : \Phi(Z(H))| = p$. Hence, if $Z(G)/\Phi(Z(G)) \cong E_{p^d}$, then $Z(G)/\Phi(Z(H)) \cong C_{p^2} \times E_{p^{d-1}}$. This implies that for each $c \in Z(G) - Z(H)$, we have $c^p \in Z(H) - \Phi(Z(H))$.

(i) Assume, in addition, that H is metacyclic; then, by Lemma 65.1(b), we have $H = \langle a, b \mid a^{p^m} = b^{p^n} = 1, m \geq 2, n \geq 1, a^b = a^{1+p^{m-1}} \rangle$, where $H' = \langle a^{p^{m-1}} \rangle$ and $|H| = p^{m+n}$, $m + n > 3$, $|G| = p^{m+n+1}$. We have $Z(H) = \langle a^p \rangle \times \langle b^p \rangle = \Phi(H)$ and for each $c \in Z(G) - H$, $c^p \in \langle a^p, b^p \rangle - \langle a^{p^2}, b^{p^2} \rangle$ since $\langle a^{p^2}, b^{p^2} \rangle = \Phi(Z(H))$.

If $n = 1$, then $H \cong M_{p^{m+1}}$, $m > 2$, and $Z(H) = \langle a^p \rangle$ is cyclic. In this case, replacing an element $c \in Z(G) - Z(H)$ with c^i , $i \not\equiv 0 \pmod{p}$, if necessary, we may assume that $c^p = a^{-p}$ and so $(ca)^p = c^p a^p = 1$. Since $(ca)^b = ca^b = (ca)a^{p^{m-1}}$, it follows that $\langle ca, b \rangle$ is nonabelian of order p^3 . This is a contradiction, since $|G| \geq p^5$ and G is an \mathcal{A}_2 -group. We have proved that $n \geq 2$.

Suppose that there exists an element $x \in G - H$ of order p . Since $d(Z(G)) = d(Z(H))$, we get $x \notin Z(G)$ and so $[a, x] \neq 1$ or $[b, x] \neq 1$. If $[a, x] \neq 1$, then (noting that $\langle a \rangle$ is normal in G) $\langle a, x \rangle$ is nonabelian of order p^{m+1} . This is a contradiction since $|G| = p^{m+n+1}$ and $n \geq 2$. Hence we must have $[a, x] = 1$ and $[b, x] \neq 1$. In that case $\langle [b, x] \rangle = G' = H'$ and so $H^* = \langle b, x \rangle$ is a nonmetacyclic \mathcal{A}_1 -group of order p^{n+2} . Hence H^* must be a maximal subgroup of G containing $Z(H) = \Phi(G)$ but not containing $Z(G)$ (every member of the set Γ_1 , containing $Z(G)$, is abelian!), and so $|G| = p^{n+3}$. We get $m = 2$ and $G = H^*Z(G)$, where H^* is a nonmetacyclic \mathcal{A}_1 -group. This case will be considered in part (ii) of the proof.

Hence assume that $\Omega_1(G) \leq H$. By the paragraph preceding (i), for each $c \in Z(G) - Z(H)$, we get $c^p \in Z(H) - \Phi(Z(H))$, where $Z(H) = \Phi(H) = \mathfrak{U}_1(H)$ since H is metacyclic. If there is $h \in H$ such that $c^p = h^p$, then the abelian subgroup $\langle h, c \rangle$ is not cyclic since $\langle h \rangle$ and $\langle c \rangle$ are two distinct cyclic subgroups of $\langle h, c \rangle$ of the same order. Since $\langle h, c \rangle \cap H = \langle h \rangle$, there is an element of order p in $\langle h, c \rangle - H$, contrary to $\Omega_1(G) \leq H$. We conclude that $\langle c^p \rangle$ is a maximal cyclic subgroup of H . Since $c^p \in Z(H)$, the quotient group $H/\langle c^p \rangle$ is noncyclic so $c^p \leq \Phi(H) = \mathfrak{U}_1(H)$ since H is metacyclic. It follows that not every element in $\mathfrak{U}_1(H)$ is a p -th power of an element in H so H is irregular so $p = 2$ since H is of class 2 (Lemma 64.1(a)), and c^2 is not a square in H . Set $d = [a, b] \neq 1$, where $d^2 = 1$, and compute for any integers i, j : $(a^i b^j)^2 = a^{2i} b^{2j} [b^j, a^i] = a^{2i} b^{2j} d^{ij}$. If i or j is even, then $a^{2i} b^{2j} = (a^i b^j)^2$ is a square in H . Therefore $c^2 = a^{2k} b^{2l}$, where both k and l are odd. Consider the nonabelian subgroup $S = \langle a, b^{-l} c \rangle$ (recall that $c \in Z(G)$). We have $(b^{-l} c)^2 = b^{-2l} c^2 = b^{-2l} a^{2k} b^{2l} = a^{2k}$, and so $|S| = 2^{m+1}$. This is a contradiction, since $|G : S| = p^2 > p$ in view of $|G| = 2^{m+n+1}$ and $n \geq 2$.

(ii) It remains to consider the case where H is a nonmetacyclic \mathcal{A}_1 -group of order $\geq p^4$. We set

$$H = \langle a, b \mid a^{p^m} = b^{p^n} = 1, [a, b] = d, d^p = [a, d] = [b, d] = 1 \rangle,$$

where we may assume that $m \geq n \geq 1$. Here $|H| = p^{m+n+1}$ and so $|G| = p^{m+n+2}$. Since $|H| \geq p^4$, must be $m \geq 2$. We have $Z(H) = \Phi(H) = \langle a^p \rangle \times \langle b^p \rangle \times \langle d \rangle$ and $\Phi(Z(H)) = \langle a^{p^2} \rangle \times \langle b^{p^2} \rangle$ since $o(d) = p$. Also note that $\langle d \rangle$ is a maximal cyclic subgroup in H and for each $c \in Z(G) - Z(H)$, $c^p \in Z(H) - \Phi(Z(H))$. Note that $H \cap Z(G) = Z(H)$.

We want to show that there exists $c \in Z(G) - Z(H)$ so that $1 \neq c^p \in \langle d \rangle$.

Assume first that $n = 1$ so that $Z(H) = \langle a^p \rangle \times \langle d \rangle$ and for an element $c \in Z(G) - Z(H)$, $c^p = a^{ip} d^j$; recall that $o(c) > p$. If $i \equiv 0 \pmod{p}$, then $j \not\equiv 0$

(mod p) (otherwise, $o(c) = p$) and we may set $c^p = a^{i'p^2}d^j$. Then we compute $(a^{-i'p}c)^p = a^{-i'p^2}c^p = d^j \neq 1$, and we are done since $a^{-i'p}c \in Z(G) - Z(H) = Z(G) - H$. If $i \not\equiv 0 \pmod{p}$, then $S = \langle a^{-i}c, b \rangle$ is nonabelian and $(a^{-i}c)^p = a^{-ip}c^p = a^{-ip}a^{ip}d^j = d^j$. Hence $p \leq o(a^{-i}c) \leq p^2$. If $o(a^{-i}c) = p^2$, then $j \not\equiv 0 \pmod{p}$ and $\langle a^{-i}c \rangle \geq \langle d^j \rangle = G'$. In any case, $|S| = p^3$. This is a contradiction since $|G : S| \geq p^2$ and G is an \mathcal{A}_2 -group.

Thus, we may also assume that $n \geq 2$. We have for $c \in Z(G) - Z(H)$, $c^p = a^{ip}b^{jp}d^k$, where at least one of the integers i, j, k is $\not\equiv 0 \pmod{p}$ since $c^p \notin \Phi(Z(H))$.

If $i \equiv 0 \pmod{p}$ and $j \equiv 0 \pmod{p}$, then $k \not\equiv 0 \pmod{p}$ and $a^i, b^j \in Z(H) < Z(G)$ so

$$(a^{-i}b^{-j}c)^p = a^{-ip}b^{-jp}c^p = a^{-ip}b^{-jp}a^{ip}b^{jp}d^k = d^k \neq 1,$$

and we are done since $a^{-i}b^{-j}c \in Z(G) - Z(H)$.

Now assume that one of the integers i, j is $\equiv 0 \pmod{p}$ and the other one is $\not\equiv 0 \pmod{p}$. Note that a and b occur symmetrically since we have $m \geq 2$ and $n \geq 2$. Interchanging a and b (if necessary), we may assume that $i \not\equiv 0 \pmod{p}$ but $j \equiv 0 \pmod{p}$. In that case $T = \langle a^{-i}b^{-j}c, b \rangle$ is nonabelian and since $b^{-j}, c \in Z(G)$ we get $(a^{-i}b^{-j}c)^p = a^{-ip}b^{-jp}c^p = d^k$. Thus $p \leq o(a^{-i}b^{-j}c) \leq p^2$ and if $o(a^{-i}b^{-j}c) = p^2$, then $k \not\equiv 0 \pmod{p}$ and $\langle a^{-i}b^{-j}c \rangle \geq \langle d^k \rangle = G'$. In any case, $|T| = p^{n+2}$. This is a contradiction since $|G : T| = p^m > p$.

It remains to study the possibility $i \not\equiv 0 \pmod{p}$ and $j \not\equiv 0 \pmod{p}$. We consider again the nonabelian subgroup $T = \langle a^{-i}b^{-j}c, b \rangle$. If $p > 2$, then $(a^{-i}b^{-j}c)^p = a^{-ip}b^{-jp}c^p = d^k$. If $p = 2$, then

$$\begin{aligned} (a^{-i}b^{-j}c)^2 &= (a^{-i}b^{-j})^2c^2 = a^{-2i}b^{-2j}[b, a]^{ij}c^2 \\ &= a^{-2i}b^{-2j}d^{ij}a^{2i}b^{2j}d^k = d^{ij+k}. \end{aligned}$$

In any case, we have $|T| = p^{n+2}$, a contradiction since $|G : T| = p^m > p$.

We have proved that there exists $c \in Z(G) - H$ such that $1 \neq c^p \in \langle d \rangle$. Replacing c with another generator of $\langle c \rangle$, we may assume that $c^p = d$. The structure of G is uniquely determined. \square

Proposition 71.2. *Let G be a metacyclic \mathcal{A}_2 -group of order $> p^4$. Then $G' \cong C_{p^2}$ and we have one of the following possibilities:*

- (a) $G = \langle a, b \mid a^{p^m} = 1, m \geq 3, b^{p^n} = a^{\epsilon p^{m-1}}, n \geq 1, \epsilon = 0, 1, m+n \geq 5, a^b = a^{1+p^{m-2}} \rangle$, where in case $p = 2, m \geq 4$.
- (b) $p = 2, G = \langle a, b \mid a^8 = 1, b^{2^n} = a^{4\epsilon}, \epsilon = 0, 1, n \geq 2, a^b = a^{-1+4\eta}, \eta = 0, 1 \rangle$.

Proof. By Corollary 65.3, a metacyclic p -group G is an \mathcal{A}_2 -group if and only if $G' \cong C_{p^2}$. Let G_0 be the subgroup of order p in G' ; then G/G_0 is an \mathcal{A}_1 -group (Lemma

65.2(a)). But $|G/G_0| > p^3$ and so G/G_0 is a “splitting” metacyclic group (Lemma 65.1(b,c)). We have $G = AB$, where $A \geq G'$, $A \cap B = G_0$, A/G_0 (of order $\geq p^2$) and B/G_0 are cyclic. Since $G_0 < G' < A$ and G' is cyclic, A does not split over G_0 . Hence A is a cyclic normal subgroup of order p^m , $m \geq 3$, and we set $A = \langle a \rangle$. Let $b \in B$ be such that $\langle b \rangle$ covers A/G_0 so that $b^{p^n} \in G_0 = \langle a^{p^{m-1}} \rangle$, where $p^n = |B/G_0|$, $n \geq 1$. Changing a generator of $\langle a \rangle$ if necessary, one may assume $b^{p^n} = a^{\epsilon p^{m-1}}$ with $\epsilon = 0, 1$. Now, $\langle b \rangle$ induces an automorphism group of order p^2 on A so that $[A, B] \cong C_{p^2}$. In that case our result follows at once. \square

Proposition 71.3. *Let G be a nonmetacyclic \mathcal{A}_2 -group of order $> p^4$ possessing exactly one abelian maximal subgroup. Then $G' \cong E_{p^2}$ and assume, in addition, that $G' \not\leq Z(G)$. In that case $p > 2$, $d(G) = 2$, $K_3(G)$ is of order p , $G/K_3(G)$ is nonmetacyclic minimal nonabelian, and one of the following holds:*

(i) $G = \langle a, b \rangle$, where

$$a^p = b^{p^n} = 1, \quad n \geq 3, \quad [a, b] = c, \quad c^p = [a, c] = 1, \quad [b, c] = b^{p^{n-1}}.$$

Here $|G| = p^{n+2}$, $G' = \langle c, b^{p^{n-1}} \rangle \cong E_{p^2}$, $K_3(G) = \langle b^{p^{n-1}} \rangle$, $M = \langle a, c, b^p \rangle \in \Gamma_1$ is abelian of type (p, p, p^{n-1}) , and all members of the set $\Gamma_1 - \{M\}$ are metacyclic.

(ii) $G = \langle a, b \rangle$, where

$$\begin{aligned} a^p = b^{p^n} &= 1, \quad n \geq 2, \quad [a, b] = c, \quad [b, c] = d, \\ c^p = d^p &= [a, c] = [d, a] = [d, b] = 1. \end{aligned}$$

Here $|G| = p^{n+3}$, $G' = \langle c, d \rangle \cong E_{p^2}$, $K_3(G) = \langle d \rangle$, $M = \langle a, c, d, b^p \rangle \in \Gamma_1$ is abelian of type (p, p, p, p^{n-1}) .

(iii) $G = \langle a, b \rangle$, where

$$a^{p^2} = b^{p^n} = 1, \quad n \geq 2, \quad [a, b] = c, \quad [c, b] = a^{sp}, \quad c^p = [a, c] = 1,$$

and $s = 1$ or s is a fixed quadratic non-residue mod p . Here $|G| = p^{n+3}$, $G' = \langle c, a^p \rangle \cong E_{p^2}$, $K_3(G) = \langle a^p \rangle$, $M = \langle a, c, b^p \rangle \in \Gamma_1$ is abelian of type (p, p^2, p^{n-1}) , and all members of the set Γ_1 are nonmetacyclic.

Proof. Lemma 65.2(d,e), Lemma 65.4(c) and Theorem 65.7(c,d) imply that $G' \cong E_{p^2}$, $d(G) = 2$ and $p > 2$. Since $G' \not\leq Z(G)$, we have $|K_3(G)| = p$ and $G/K_3(G)$ is a nonmetacyclic \mathcal{A}_1 -group (Lemmas 65.2(e) and 64.1(m)).

By the structure of $G/K_3(G)$, there are cyclic subgroups $A/K_3(G) > \{1\}$ and $B/K_3(G) > \{1\}$ of $G/K_3(G)$ such that

$$\langle A, B \rangle = G, \quad A \cap G' = B \cap G' = A \cap B = (G'A) \cap B = (G'B) \cap A = K_3(G).$$

Let $A = \langle a, K_3(G) \rangle$ and $B = \langle b, K_3(G) \rangle$. The commutator $[a, b]$ is of order p since $ab \neq ba$ and $\exp(G') = p$ and $\langle [a, b] \rangle \cap K_3(G) = \{1\}$ since $G/K_3(G)$ is nonabelian. Since $G' \not\leq Z(G)$, both A and B cannot centralize G' . To fix ideas, assume that B does not centralize G' , which implies $[B, G'] = K_3(G)$. Since $G'B < G$ is nonabelian, we must have $|G : (G'B)| = p$. But $(G'B) \cap A = K_3(G)$ implies $|A| = p^2$, by the product formula. If also A does not centralize G' , then $G'A$ is nonabelian and so $G'A \in \Gamma_1$. In that case $|G| = p|G'A| = p \cdot p^3 = p^4$, a contradiction. We have proved that A centralizes G' . Let $B_1 \leq B$ be such that $K_3(G) \leq B_1$ and $|B : B_1| = p$. Let $M \in \Gamma_1$ be abelian. Since $G' < M$ and $G' \not\leq Z(G)$, we have $M = C_G(G')$. On the other hand, A centralizes G' and so $A < M$. Finally, $B_1 \leq \Phi(G) < M$ and so $M = G'AB_1$ (recall that $|G : B_1G'| = p^2$) and $A \not\leq B_1G'$ since $G = \langle A, B \rangle$. Since $|G| > p^4$ and $|AG'| = p^3$, we have $|B_1| \geq p^2$ and so $|B| \geq p^3$.

(i) Suppose first that B does not split over $K_3(G)$, i.e., B is cyclic. Set $B = \langle b \rangle$ so that $o(b) = p^n$ with $n \geq 3$ and $\langle b^{p^{n-1}} \rangle = K_3(G)$. The subgroup $BG' \cong M_{p^{n+1}}$ is maximal in G since $(BG')A = G$, $(BG') \cap A = K_3(G)$ and $|A| = p^2$. By Lemma 64.1(p), $d(M) > 2$ (otherwise, all members of the set Γ_1 are two-generator which is not the case since a nonmetacyclic \mathcal{A}_1 -group has a maximal subgroup that is not generated by two elements; see Lemma 65.1(a)); moreover, $d(M) = 3$ (consider $M \cap (BG')$ and so $\Omega_1(M) \cong E_{p^3}$. By the product formula, $G = B\Omega_1(M)$. It follows from $|AB| < |G|$ and $\langle A, B \rangle = G$ that B is not normal in G . Therefore, there is $a \in \Omega_1(M)$ that does not normalize B . One can take $A = \langle a, K_3(G) \rangle$. Set $[a, b] = c$, where c is an element of order p in $G' - K_3(G)$. Since $BG' \cong M_{p^{n+1}}$, one may assume that $b^c = b^{1+p^{n-1}}$ (if necessary, changing b by another element of order p^n in BG'). Thus we have obtained the group (i) of our proposition.

(ii) Suppose that B splits over $K_3(G)$ so that $B = K_3(G) \times \langle b \rangle$, where $o(b) = p^n$, $n \geq 2$. Consider first the subcase

(ii1) where A also splits over $K_3(G)$ so that $A = K_3(G) \times \langle a \rangle$ with $o(a) = p$. Then $[a, b] = c$, where $c \in G' - K_3(G)$ is of order p and $[b, c] = d$, where $\langle d \rangle = K_3(G)$. We have obtained the group (ii) of our proposition.

(ii2) It remains to consider the subcase where A does not split over $K_3(G)$ so that $A = \langle a \rangle$ is cyclic of order p^2 and $\langle a^p \rangle = K_3(G)$. We have again $[a, b] = c$, where $c \in G' - K_3(G)$ is of order p and $[c, b] = a^{sp}$, where $s \not\equiv 0 \pmod{p}$. For any $i \not\equiv 0 \pmod{p}$, we replace b with $b' = b^i$. Then $[a, b'] = [a, b^i] = [a, b]^i \gamma = c^i \gamma = c'$ with a suitable element $\gamma \in K_3(G) \leq Z(G)$. Hence $[c', b'] = [c^i \gamma, b^i] = [c, b]^i = a^{i^2 sp} = a^{s'p}$, where $s' = i^2 s \not\equiv 0 \pmod{p}$. It follows that we may assume (running through all $i \not\equiv 0 \pmod{p}$) that either $s' = 1$ or s' is a (fixed) quadratic non-residue mod p . Writing again b, c, s instead of b', c', s' , we have obtained the groups stated in part (iii) of our proposition. \square

Proposition 71.4. *Let G be a nonmetacyclic \mathcal{A}_2 -group of order $> p^4$ possessing exactly one abelian maximal subgroup. Then $G' \cong E_{p^2}$ and assume, in addition, that*

$G' \leq Z(G)$. In that case $d(G) = 3$, $Z(G) = \Phi(G)$, and one of the following holds:

(a) If G has no normal elementary abelian subgroups of order p^3 , then $p = 2$ and

$$G = \langle a, b, c \mid a^4 = b^4 = [a, b] = 1, c^2 = a^2, a^c = ab^2, b^c = ba^2 \rangle$$

is the minimal nonmetacyclic group of order 2^5 . Here G is a special group of exponent 4, $\Omega_1(G) = G' = Z(G) = \Phi(G) = \langle a^2, b^2 \rangle \cong E_4$, $C_4 \times C_4 \cong M = \langle a \rangle \times \langle b \rangle \in \Gamma_1$ is abelian, and all other six members of the set Γ_1 are metacyclic of exponent 4.

(b) If G has a normal elementary abelian subgroup E of order p^3 , then $E = \Omega_1(G)$ and one of the following holds:

(b1) $G = \langle a, b, d \rangle$ with

$$\begin{aligned} a^{p^\alpha} &= b^p = d^{p^2} = 1, \quad \alpha \geq 2, \\ [a, b] &= d^p a^{\epsilon p^{\alpha-1}}, \quad [d, b] = 1, \quad [a, d] = a^{p^{\alpha-1}}, \end{aligned}$$

where $\epsilon = 0$ unless $p = 2$ and $\alpha = 2$ in which case $\epsilon = 1$. Here

$$\begin{aligned} |G| &= p^{\alpha+3}, \quad G' = \langle d^p, a^{p^{\alpha-1}} \rangle \cong E_{p^2}, \\ E &= \Omega_1(G) = \langle b, d^p, a^{p^{\alpha-1}} \rangle \not\leq Z(G), \end{aligned}$$

and $\langle b, d, a^p \rangle \in \Gamma_1$ is abelian of type $(p, p^2, p^{\alpha-1})$.

(b2) $G = \langle a, b, c \rangle$ with

$$\begin{aligned} a^{p^\alpha} &= b^{p^2} = c^{p^2} = [b, c] = 1, \quad \alpha \geq 1, \\ [a, b] &= x, \quad [a, c] = y, \quad b^p = x^{\alpha'} y^\beta, \quad c^p = x^\gamma y^\delta, \\ x^p &= y^p = [a, x] = [a, y] = [b, x] = [b, y] = [c, x] = [c, y] = 1, \end{aligned}$$

where in case $p = 2$, $\alpha' = 0$, $\beta = \gamma = \delta = 1$, and in case $p > 2$, $4\beta\gamma + (\delta - \alpha')^2$ is a quadratic non-residue mod p . We have $|G| = p^{\alpha+4}$, $G' = \langle x, y \rangle \cong E_{p^2}$, $E = \Omega_1(G) = G' \langle a^{p^{\alpha-1}} \rangle$. Let $A \in \Gamma_1$ be abelian. Then in case $\alpha = 1$, $A = \langle b, c \rangle \cong C_{p^2} \times C_{p^2}$ and $E \not\leq Z(G)$ and in case $\alpha \geq 2$, $A = \langle a^p, b, c \rangle$ is abelian of type $(p^{\alpha-1}, p^2, p^2)$ and $E \leq Z(G)$.

Proof. Let G be a nonmetacyclic \mathcal{A}_2 -group of order $> p^4$ having exactly one abelian maximal subgroup. Then we have $G' \cong E_{p^2}$ (Lemmas 64.1(q), 65.4(d) and Theorem 65.7(a)), and we assume here, in addition, that $G' \leq Z(G)$. It follows from Lemma 65.2(a) that $d(G) = 3$. Next, $Z(G) = \Phi(G)$ (Lemma 65.4(c)), $G/Z(G) \cong E_{p^3}$, and if $H \neq K \in \Gamma_1$ are both nonabelian, then $Z(H) = Z(K) = Z(G)$ (Theorem 65.7(f)). It follows that if $x, y \in G$, then $|\langle x, y \rangle| \leq p \cdot o(x)o(y)$ (since $d(G) = 3$, $\langle x, y \rangle$ is either abelian or an \mathcal{A}_1 -subgroup). Also, if G has no normal elementary abelian subgroups of order p^3 , then G is minimal nonmetacyclic (Lemma 65.4(j)). In the last case, $p = 2$,

$|G| = 2^5$, and G is the group stated in part (a) of our proposition (Lemma 64.1(l) and Theorem 66.1).

From now on we assume that the group G has a normal subgroup $E \cong E_{p^3}$. By Lemma 65.4(k), either $\Omega_1(G) = E$ or $E < \Omega_1(G) = K \cong E_{p^4}$. Suppose that the second case occurs. Every maximal subgroup of G containing K must be abelian (Lemma 65.1) and $G/K > \{1\}$ is cyclic (Lemma 65.4(b)). Let $G = K\langle a \rangle$; then $K \cap \langle a \rangle = D$ is of order p . Indeed, $|D| \leq p$. Assume that $D = \{1\}$. Then, if $\langle a \rangle < T \in \Gamma_1$, then $\Omega_1(T) \geq \langle \Omega_1(\langle a \rangle), T \cap K \rangle$ is of order $\geq p^4$, so T is abelian (Lemma 65.1). Since $K \not\leq T$, the set Γ_1 has two distinct abelian members, contrary to the assumption. Thus, $p^s = |\langle a \rangle| \geq p^2$, $D \leq Z(G)$, and $|G| = p^{s+3}$. Since $K\langle a^p \rangle$ is abelian, $\langle a^p \rangle \leq Z(G)$. We have $G' \cong E_{p^2}$, $G' < K$, and $G' \leq Z(G)$ (by assumption). Since $G/Z(G) \cong E_{p^3}$ and $G'D \leq Z(G)$, we get $G' > D$ (otherwise, $d(G/G') = 2 < 3 = d(G)$). Therefore, $G'\langle a \rangle$ is an abelian normal subgroup of G of type (p^s, p) , $s \geq 2$, and $Z(G) = G'\langle a^p \rangle$. We have $C_K(a) < Z(G)$ and so $C_K(a) = G'$ and $C_G(a) = G'\langle a \rangle$. The subgroup $G'\langle a \rangle$ has exactly p cyclic subgroups of order p^s . Since $|G : (G'\langle a \rangle)| = p^2$, we get $N_K(\langle a \rangle) > G'$. Let $x \in N_K(\langle a \rangle) - G'$ so that x (of order p) induces an automorphism of order p on $\langle a \rangle$. But then $\langle a, x \rangle$ is a nonabelian subgroup of order p^{s+1} so its index in G equals p^2 , a contradiction. We have proved that $\Omega_1(G) = E \cong E_{p^3}$. Since $G' < E$, the quotient group G/E is abelian. Since $d(G/G') = 3$, G/E is also noncyclic.

In what follows A denotes the unique abelian maximal subgroup of G .

(i) First assume that $E \not\leq \Phi(G) (= Z(G))$; then $d(G/E) = 2$. If A does not contain E , then $G = AE$, $\Omega_1(A) = A \cap E = G' \cong E_{p^2}$ and so A is metacyclic. Hence each maximal subgroup of G is generated by two elements (Lemma 65.1) and $d(G) = 3$. Since G is of class 2 (by hypothesis), Theorem 70.1 shows that G is isomorphic to a group (b2) for $\alpha = 1$ in our proposition.

We may assume that $E < A$ and so each maximal subgroup of G which does not contain E is nonabelian metacyclic (Lemma 65.1, since all members of the set $\Gamma_1 - \{A\}$ are \mathcal{A}_1 -groups). Let M be a nonabelian maximal subgroup of G containing E (there are exactly p such subgroups since $d(G/E) = 2$). Then M is a nonmetacyclic \mathcal{A}_1 -group with $Z(M) = \Phi(M) = \Phi(G) = Z(G)$ (Theorem 65.7(f)). By Lemma 65.1, we have, since $E \not\leq Z(M)$ (otherwise, $E \leq Z(G)$), which is not the case since $d(G/E) = 2 < 3 = d(G/Z(G))$,

$$M = \langle a, b \mid a^{p^\alpha} = b^p = 1, \alpha \geq 2, [a, b] = c, c^p = [a, c] = [b, c] = 1 \rangle,$$

where

$$\langle c \rangle = M', \quad b \in E - G', \quad M = \langle b \rangle \cdot (\langle c \rangle \times \langle a \rangle),$$

$$Z(M) = Z(G) = \langle c \rangle \times \langle a^p \rangle, \quad |G| = p^{\alpha+3}, \quad G' = \langle a^{p^{\alpha-1}} \rangle \times \langle c \rangle.$$

In particular, G/E has a cyclic subgroup M/E of index p . Now, $\langle a, c \rangle (\geq G')$ is an abelian normal subgroup of type (p^α, p) and it has exactly p cyclic subgroups of

index p which are not normal in M (see the last assertion of Lemma 65.1). Therefore, $N_M(\langle a \rangle) = \langle a, c \rangle$ and so $N = N_G(\langle a \rangle)$ must cover G/M since $N \not\leq M$ in view of $|G : N| = c_\alpha(\langle a, c \rangle) = p = |G : M|$ (here $c_\alpha(X)$ is the number of cyclic subgroups of order p^α in a p -group X). Thus $N \in \Gamma_1$ with $M \cap N = \langle a, c \rangle$ and so $E \cap N = G'$. Therefore N is nonabelian metacyclic, $C_G(a) = \langle a, c \rangle$, N is an \mathcal{A}_1 -group, and so it is “splitting” metacyclic (Lemma 65.1). We have $\{1\} < N' < \langle a \rangle \cap G'$ and so $N' = \langle a^{p^{\alpha-1}} \rangle \leq \mathfrak{V}_1(N)$ (Lemma 65.1). It follows that $Z(G) = \langle a^p, c \rangle = Z(N) = \Phi(N) = \mathfrak{V}_1(N)$, and so there exists $d \in N - M = N - \langle a, c \rangle$ such that $d^p \in G' - \langle a^{p^{\alpha-1}} \rangle$ and $o(d) = p^2$ (note that $\Omega_1(N) \leq \langle a, c \rangle$). We have $N = \langle a, d \rangle$ and $N/\langle a \rangle$ is cyclic. Next, $C_G(E) = A$.

If $\alpha > 2$, then working in the abelian subgroup $\langle d, a^{p^{\alpha-2}} \rangle \cong C_{p^2} \times C_{p^2}$, we may choose an element $d' \in \langle d, a^{p^{\alpha-2}} \rangle - M$ such that $(d')^p = c$ and so we may assume from the start that $d^p = c = [a, b]$. If $u \in G$ is of order p^2 , then $|\langle u, E \rangle| = p^4$ so $\langle u, E \rangle$ is abelian, and we conclude that $u \in C_G(E) = A$. It follows that $\Omega_2(G) = E \langle u \in G \mid o(u) = p^2 \rangle \leq A$ so $[d, b] = 1$. Replacing d with $d' = d^i$ ($i \not\equiv 0 \pmod{p}$), we may assume that $a^{d'} = a^{d^i} = a^{1+p^{\alpha-1}}$. But then we also replace b with $b' = b^i$ and c with $c' = c^i$ and obtain $(d')^p = (d^p)^i = c^i = c' = [a, b']$ and the relation $[b', d'] = 1$ remains valid. Writing again d, b, c instead of d', b', c' , respectively, we obtain exactly the relations stated in part (b1) for $\alpha > 2$ of our proposition.

It remains to investigate the case $\alpha = 2$, where $|G| = p^5$, $G' = Z(G) = \Phi(G) \cong E_{p^2}$, $E = \Omega_1(G) \cong E_{p^3}$, $\exp(G) = p^2$. For each $x \in N - \langle a, c \rangle$, $x^p \in G' - \langle a^p \rangle$ (otherwise, $\langle a, x \rangle$ would be nonabelian of order p^3 ; here $N = N_G(\langle a \rangle)$). Since $G = EN$, we have $A = E(A \cap N)$, by the modular law. Note that $A \cap N$ is abelian of type (p^2, p) so it is generated by elements of order p^2 . Since $N = \langle a \rangle(A \cap N)$ (indeed, $M = \langle a \rangle E$ is nonabelian so $a \notin C_G(E) = A$), there exists $d \in (A \cap N) - \Omega_1(A \cap N)$ such that $\langle a, d \rangle$ is nonabelian. It follows that $d^p \notin \langle a^p \rangle$ (otherwise, $\langle a, d \rangle$ is nonabelian of order p^3 , contrary to the fact that G is an \mathcal{A}_2 -group). Replacing d with another generator of $\langle d \rangle$ if necessary, we may assume that $a^d = a^{1+p}$. Set $d^p = c^i a^{-jp}$, where $i \not\equiv 0 \pmod{p}$. We replace b with $b' = b^i$ and c with $c' = c^i$, so that we get $[a, b'] = [a, b^i] = [a, b]^i = c^i = c'$ and $d^p = c' a^{-jp}$. Thus, we may assume from the start that $[a, b] = c$ and $c = a^{jp} d^p$ with $j \in \mathbb{Z}$.

We shall determine the integer $j \pmod{p}$. Consider the nonabelian maximal subgroup $S = \langle b, ad^\xi \rangle$, where ξ is any integer (recall that $d(G) = 3$). The subgroup S is a nonmetacyclic (otherwise, $b \in \mathfrak{V}_1(S) = \Phi(S)$) \mathcal{A}_1 -group containing E with $Z(S) = Z(G) = G' = \langle a^p, d^p \rangle = \langle (ad^\xi)^p, [ad^\xi, b] \rangle$. If $p > 2$, then

$$(ad^\xi)^p = a^p (d^p)^\xi, \quad [ad^\xi, b] = [a, b] = c = a^{jp} d^p,$$

and so we must have (since the displayed two elements are independent) $\begin{vmatrix} 1 & \xi \\ j & 1 \end{vmatrix} \not\equiv 0 \pmod{p}$, which gives $1 - j\xi \not\equiv 0 \pmod{p}$ for every integer ξ . If $j \not\equiv 0 \pmod{p}$, then we can solve the congruence $j\xi \equiv 1 \pmod{p}$ for ξ and get a contradiction.

Hence $j \equiv 0 \pmod{p}$ and we may set in this case $j = 0$; then $c = a^{jp}d^p = d^p$. If $p = 2$, then taking $\xi = 1$, we have

$$(ad)^2 = a^2d^2[d, a] = a^2d^2a^2 = d^2, \quad [ad, b] = [a, b] = c = a^{2j}d^2$$

(by the above, $a^d = a^{1+p}$ for any p), and we must have $\begin{vmatrix} 0 & 1 \\ j & 1 \end{vmatrix} \not\equiv 0 \pmod{2}$, which gives $j \not\equiv 0 \pmod{2}$ and so we may set in this case $j = 1$; then $c = a^2d^2$. We have obtained the relations stated in part (b1) for $\alpha = 2$ of our proposition.

(ii) Suppose that $E_{p^3} \cong E = \Omega_1(G) \leq Z(G) = \Phi(G)$. Let $H \in \Gamma_1$ be nonabelian. Then $E < H$ and so H is a nonmetacyclic \mathcal{A}_1 -group:

$$H = \langle a, b \mid a^{p^\alpha} = b^{p^\beta} = 1, \quad [a, b] = c, \quad c^p = [a, c] = [b, c] = 1 \rangle,$$

where $E = \langle a^{p^{\alpha-1}}, b^{p^{\beta-1}}, c \rangle$. Since $E \leq Z(G) = Z(H) = \Phi(H)$ (Theorem 65.7(f)), we must have $\alpha \geq 2$ and $\beta \geq 2$ so $|G| = p|H| = p^{\alpha+\beta+2} \geq p^6$. Let $G_0 < G'$ be of order p such that $G_0 \neq H'$. Since $(G/G_0)' = G'/G_0$ is of order p and $d(G/G_0) = 3$, a nonabelian group G/G_0 is an \mathcal{A}_2 -group of order $\geq p^5$ with the commutator group of order p , where H/G_0 is an \mathcal{A}_1 -subgroup. By Proposition 71.1, there exists $d \in G - H$ such that $d^p \in G'$. Hence $o(d) = p^2$ and $d \notin Z(G)$ since $d \notin H$ and $\Omega_1(G) = E < H$. It follows that d does not centralize a or b . Without loss of generality, we assume that $[d, a] \neq 1$ and so nonabelian $\langle d, a \rangle \in \Gamma_1$ in view of $d(G) = 3$. Since $o(d) = p^2$ and $o(a) = p^\alpha$, we have $|\langle d, a \rangle| \leq p^{\alpha+2+1}$ in view of $o([d, a]) = p$, and therefore $|G| \leq p^{\alpha+4}$. Hence $|G| = p^{\alpha+\beta+2} \leq p^{\alpha+4}$ and so $\beta \leq 2$. This gives $\beta = 2$ and $|G| = p^{\alpha+4}$ with $\alpha \geq 2$. We have $Z(G) = E \langle a^p \rangle$.

Assume first that $\alpha > 2$; then $|G| > p^6$. In that case, any two elements $x, y \in G$ of orders $\leq p^2$ commute (otherwise, $\langle x, y \rangle \in \Gamma_1$, since $d(G) = 3$, is nonabelian with $|\langle x, y \rangle| \leq p \cdot o(x)o(y) \leq p^5$, a contradiction). Since $[b, d] = 1$ in view of $o(b) = o(d) = p^2$, we get $\langle b, d \rangle = \langle b \rangle \times \langle d \rangle$. Assume that this is false. Then $\langle b, d \rangle = \langle b \rangle \times \langle d_1 \rangle$ with $o(d_1) = p$. Since $b \in H$, $d \notin H$, we get $d_1 \notin H$, a contradiction: $\Omega_1(G) = E < H$. Consider $K = \langle a, d \rangle$, where $K \in \Gamma_1$ is nonabelian containing E (by assumption, $E < \Phi(G)$). Let $G_0 \neq K'$ be a subgroup of order p in G' . Then applying Proposition 71.1 on G/G_0 , we see that there is $b_0 \in G - K$ with $b_0^p \in G'$ and $o(b_0) = p^2$. Since $[d, b_0] = 1$ and there are no elements of order p in $G - K$, we see (as before) that $\langle d, b_0 \rangle = \langle d \rangle \times \langle b_0 \rangle$. But $G = \langle a, d, b_0 \rangle$, $b_0 \notin Z(G)$, and so $[a, b_0] \neq 1$. Replacing H with $H_0 = \langle a, b_0 \rangle (\neq K)$ and b with b_0 , we may assume from the start that $b^p \in G'$. Hence, we may assume that $\Omega_1(\langle b, d \rangle) = \Omega_1(\langle b, d \rangle) = G'$. Since $|G| = p^{\alpha+4}$ and $\bar{G} = G/G'$ is generated by $\bar{b}, \bar{d}, \bar{a}$ (bar convention) of orders at most p, p, p^α , respectively, and $|\bar{G}| = p^{\alpha+2}$, we get $o(\bar{a}) = p^\alpha$ which gives $\langle a \rangle \cap G' = \{1\}$ and so $\langle a \rangle \cap \langle b, d \rangle = \{1\}$ since $\Omega_1(\langle b, d \rangle) = G'$.

Suppose that $\alpha = 2$; then $|G| = p^6$, $\exp(G) = p^2$, $E = Z(G) = \Phi(G) = \Omega_1(G)$. Let $X < G'$ be of order p . Since $d(G/X) = 3$ and $(G/X)'$ is of order p , G/X is an \mathcal{A}_2 -group of order p^5 , and so we may apply again Proposition 71.1. There is $M \in \Gamma_1$

such that M/X is an A_1 -group and there is $c \in G - M$ such that $c^p \in G'$ and $[G, c] \leq X$. If $c^p \in X$, then $\langle c \rangle$ (of order p^2 ; recall that $\Omega_1(G) < M$) is normal in G . Since $c \notin Z(G) = E$, there is an element l of order p^2 with $[l, c] \neq 1$ and so $\langle [l, c] \rangle = \langle c^p \rangle$. But then $|\langle l, c \rangle| \leq o(l)o(c) \leq p^4$, a contradiction. Thus $c^p \in G' - X$. We consider now the subgroup $Y = \langle c^p \rangle$ of order p in G' and apply Proposition 71.1 to G/Y . As before, there is an element $b \in G$ such that $b^p \in G' - Y$. It follows $\langle b^p, c^p \rangle = G'$. The abelian group $\langle b, c \rangle/G'$ is generated by two elements of order p and so $|\langle b, c \rangle| \leq p^4$. Thus $\langle b, c \rangle$ is abelian and since $\langle b \rangle \cap \langle c \rangle = \{1\}$, we have $S = \langle b, c \rangle \cong C_{p^2} \times C_{p^2}$ and S is normal in G . But, $E = \Phi(G) = G'\mathfrak{O}_1(G)$ and so there is $a \in G$ such that $a^p \in E - G'$. Hence $\langle a \rangle \cap S = \{1\}$ and so $S\langle a \rangle = G$ since $o(a) = p^2$.

In any case (for all $\alpha \geq 2$) we have obtained the following configuration (where in case $\alpha > 2$ we write c instead of d). We have $G = \langle a \rangle \cdot (\langle b \rangle \times \langle c \rangle)$, with $a^{p^\alpha} = 1$, $\alpha \geq 2$, $b^{p^2} = c^{p^2} = 1$, $[b, c] = 1$, where G is a semidirect product with kernel $\langle b \rangle \times \langle c \rangle \cong C_{p^2} \times C_{p^2}$, $G' = \langle b^p, c^p \rangle$, and $A = \langle a^p, b, c \rangle$ is the unique abelian maximal subgroup of G (of type $(p^{\alpha-1}, p^2, p^2)$).

Set $[a, b] = x$, $[a, c] = y$. Then $G' = \langle x, y \rangle = \langle b^p, c^p \rangle (\leq Z(G))$ and so $b^p = x^{\alpha'} y^\beta$ and $c^p = x^\gamma y^\delta$, where, since b^p and c^p are independent, we get $\begin{vmatrix} \alpha' & \beta \\ \gamma & \delta \end{vmatrix} \not\equiv 0 \pmod{p}$.

The subgroup $\langle a, b^\xi c^\eta \rangle$ is nonabelian if and only if $[a, b^\xi c^\eta] = x^\xi y^\eta \neq 1$ which occurs if and only if both ξ and η are not multiples of p . In that case $L = \langle a, b^\xi c^\eta \rangle$ is a nonmetacyclic A_1 -subgroup of index p in G . Since $\langle x^\xi y^\eta \rangle = L'$ and L' is a maximal cyclic subgroup in L , we have $G' = \langle (b^\xi c^\eta)^p, x^\xi y^\eta \rangle$, where $(b^\xi c^\eta)^p = (b^p)^\xi (c^p)^\eta = x^{\alpha'\xi + \gamma\eta} y^{\beta\xi + \delta\eta}$. Hence, $\begin{vmatrix} \alpha'\xi + \gamma\eta & \beta\xi + \delta\eta \\ \xi & \eta \end{vmatrix} \equiv 0 \pmod{p}$ only if $\xi \equiv \eta \equiv 0 \pmod{p}$. This gives

$$(1) \quad \beta\xi^2 + (\delta - \alpha')\xi\eta - \gamma\eta^2 \equiv 0 \pmod{p}$$

only if $\xi \equiv \eta \equiv 0 \pmod{p}$. From (1) follows (setting $\xi = 1, \eta = 0$ or $\xi = 0, \eta = 1$) $\beta \not\equiv 0 \pmod{p}$ and $\gamma \not\equiv 0 \pmod{p}$.

Suppose first $p > 2$. Then we compute (using (1))

$$(2\beta\xi + (\delta - \alpha')\eta)^2 - (4\beta\gamma + (\delta - \alpha')^2)\eta^2 = 4\beta(\beta\xi^2 + (\delta - \alpha')\xi\eta - \gamma\eta^2) \equiv 0 \pmod{p}$$

only if $\xi \equiv \eta \equiv 0 \pmod{p}$. Hence

$$(2) \quad (2\beta\xi + (\delta - \alpha')\eta)^2 \equiv (4\beta\gamma + (\delta - \alpha')^2)\eta^2 \pmod{p}$$

only if $\xi \equiv \eta \equiv 0 \pmod{p}$. From (2) follows at once that $4\beta\gamma + (\delta - \alpha')^2$ is a quadratic non-residue mod p . Indeed, if $4\beta\gamma + (\delta - \alpha')^2$ is a quadratic residue modulo p , then we set $\eta = 1$ in (2) and then we solve the congruence $(2\beta\xi + (\delta - \alpha'))^2 \equiv 4\beta\gamma + (\delta - \alpha')^2 \pmod{p}$ for ξ and get a contradiction.

Suppose now that $p = 2$. We know already that $\beta = \gamma = 1$. Then (1) yields

$$(3) \quad \xi^2 + (\delta + \alpha')\xi\eta + \eta^2 \equiv 0 \pmod{2}$$

only if $\xi \equiv \eta \equiv 0 \pmod{2}$. Setting $\xi = \eta = 1$ in (3), we get $\delta + \alpha' = 1$. This gives $b^2 = x^{\alpha'}y$ and $c^2 = xy^{\alpha'+1}$, where $\alpha' = 0, 1$. Hence we have the following two possibilities:

$$(4) \quad b^2 = y, \quad c^2 = xy,$$

$$(5) \quad b^2 = xy, \quad c^2 = x.$$

However, interchanging b and c and also x and y , we see that the relations $[a, b] = x$ and $[a, c] = y$ remain unchanged but (4) goes onto (5). Hence, we may assume that we have relations (4) and so we get $\alpha' = 0$ and $\beta = \gamma = \delta = 1$. Our group G is uniquely determined. \square

Proposition 71.5. *Let G be a nonmetacyclic \mathcal{A}_2 -group of order $> p^4$ all of whose maximal subgroups are nonabelian. Then we have one of the following possibilities:*

(a) $d(G) = 3$, $p = 2$, and $G = \langle a, b, c \rangle$ with

$$\begin{aligned} a^4 = b^4 = c^4 &= 1, \quad [a, b] = c^2, \quad [a, c] = b^2c^2, \quad [b, c] = a^2b^2, \\ [a^2, b] = [a^2, c] &= [b^2, a] = [b^2, c] = [c^2, a] = [c^2, b] = 1, \end{aligned}$$

where $G' = \langle a^2, b^2, c^2 \rangle = Z(G) = \Phi(G) = \Omega_1(G) \cong E_{2^3}$, $\exp(G) = 4$ and all members of the set Γ_1 are nonmetacyclic \mathcal{A}_1 -groups. (From Theorem 70.4 follows that G is isomorphic to the Suzuki 2-group of order 2^6 .)

(b) $d(G) = 2$, $p > 2$, G is of order p^5 :

$$\begin{aligned} G &= \langle a, x \mid a^{p^2} = x^{p^2} = 1, [a, x] = b, [a, b] = y_1, [x, b] = y_2, \\ b^p &= y_1^p = y_2^p = [a, y_1] = [x, y_1] = [a, y_2] = [x, y_2] = 1, \\ a^p &= y_1^\alpha y_2^\beta, x^p = y_1^\gamma y_2^\delta \rangle, \end{aligned}$$

where in case $p > 3$, $4\beta\gamma + (\delta - \alpha)^2$ is a quadratic non-residue mod p . Here $G' = \langle b, y_1, y_2 \rangle = \Omega_1(G) \cong E_{p^3}$, $Z(G) = K_3(G) = \mathfrak{U}_1(G) = \langle y_1, y_2 \rangle \cong E_{p^2}$.

Proof. Let G be a nonmetacyclic \mathcal{A}_2 -group of order $> p^4$ all of whose maximal subgroups are nonabelian and therefore they are generated by two elements.

Suppose first that $d(G) = 3$. Then $G' \leq Z(G)$ (Lemma 65.4(a)). By Theorem 70.1, G is a uniquely determined group of order 2^6 as stated in part (a) of our proposition.

Now suppose that $d(G) = 2$. If $p = 2$, then G is metacyclic (Lemma 64.1(n)), a contradiction. Hence $p > 2$; then $\mathfrak{U}_1(G) = K_3(G)$, $|G : G'| = p^2$ (Lemma 64.1(m))

so $|G'| = p^3$ and $|G| = p^5$ (Lemma 65.2(d)). Since $G/K_3(G)$ is generated by its subgroups of index p^2 , $K_3(G) \leq Z(G)$ (Lemma 65.4(c)) and so G is of class 3. We have $K_3(G) = Z(G) \cong E_{p^2}$ and $G' \cong E_{p^3}$ (Lemma 65.7(d)).

Each $M \in \Gamma_1$ is a nonmetacyclic \mathcal{A}_1 -group with $G' = \Omega_1(M) \cong E_{p^3}$ and so $\Phi(G) = G' = \Omega_1(G)$ and $\exp(G) = p^2$ (Lemma 65.1). Let $G = \langle a, x \rangle$; then $a, x \in G - \Phi(G) = G - \Omega_1(G)$ and therefore $o(a) = o(b) = p^2$. We have $G' = \langle [a, x], K_3(G) \rangle$ and so $[a, x] = b \in G' - K_3(G)$ which gives $o(b) = p$. Set $[a, b] = y_1$ and $[x, b] = y_2$, where $y_1, y_2 \in K_3(G) = Z(G)$. But $\langle a, b \rangle Z(G)$ and $\langle x, b \rangle Z(G)$ are members of the set Γ_1 and so they are nonabelian. Hence $o(y_1) = o(y_2) = p$ (Lemma 65.1) and $\langle a, b \rangle Z(G) = \langle a, b \rangle$, $\langle x, b \rangle Z(G) = \langle x, b \rangle$. Since $\langle a, b \rangle$ and $\langle x, b \rangle$ are distinct members of the set Γ_1 , we have $\langle y_1 \rangle \neq \langle y_2 \rangle$ (Lemma 65.2(d)). It follows $\langle y_1, y_2 \rangle = Z(G)$. Since $a^p, x^p \in Z(G)$, we get $a^p = y_1^\alpha y_2^\beta$ and $x^p = y_1^\gamma y_2^\delta$.

Suppose that $p > 3$. Then G is regular (Lemma 64.1(a)) and since G' is elementary abelian, we get that G is p -abelian, i.e., $(lk)^p = l^p k^p$ for all $l, k \in G$ (see §7). Since $\langle a, x \rangle = G$, we have in this case $\langle a^p, x^p \rangle = \Omega_1(G) = Z(G) = \langle y_1, y_2 \rangle$. Consider the subgroup $S = \langle b, a^\xi x^\eta \rangle$ ($S < G$ since $b \in G'$; it follows that S is of class ≤ 2). Obviously, $a^\xi x^\eta \in G - G'$ if and only if not both ξ and η are divisible by p . In that case $[a^\xi x^\eta, b] = [a, b]^\xi [x, b]^\eta = y_1^\xi y_2^\eta \neq 1$, and so S is nonabelian; then $S \in \Gamma_1$ hence $E < S$. It follows that S is nonmetacyclic. Here we have used the fact that $[a, b], [x, b] \in Z(G)$. Since $Z(G) = Z(S)$ and S' is a maximal cyclic subgroup of S , we have $Z(S) = Z(G) = \langle y_1, y_2 \rangle = \langle (a^\xi x^\eta)^p, [a^\xi x^\eta, b] \rangle$. We compute

$$(a^\xi x^\eta)^p = (a^p)^\xi (x^p)^\eta = y_1^{\alpha\xi + \gamma\eta} y_2^{\beta\xi + \delta\eta} \quad \text{and} \quad [a^\xi x^\eta, b] = y_1^\xi y_2^\eta,$$

and so

$$(*) \quad \begin{vmatrix} \alpha\xi + \gamma\eta & \beta\xi + \delta\eta \\ \xi & \eta \end{vmatrix} \equiv 0 \pmod{p}$$

only if $\xi \equiv \eta \equiv 0 \pmod{p}$. From $(*)$ we get (as in the proof of Proposition 71.4) that $4\beta\gamma + (\delta - \alpha)^2$ is a quadratic non-residue modulo p . Our proposition is proved and all \mathcal{A}_2 -groups are determined. \square

The classification of \mathcal{A}_2 -groups is contained in Propositions 71.1–71.5. The subgroup structure of \mathcal{A}_2 -groups is given in §65.

It is impossible to compare our proof with Kazarin's proof since the last one is not published and only sketched in his PhD Thesis. The paper [She], also devoted to \mathcal{A}_2 -groups, is not accessible. In any case, our proof is based on other ideas. Indeed, the above authors were forced to use tables [HS]. Besides, Kazarin used Nazarova-Roiter's classification of p -groups with abelian subgroup of index p so his proof is not elementary. Instead of this, we use Theorem 70.1 which is new for $p = 2$.

Exercise 1. Let a p -group $G = A * C$, where $C \cong C_{p^2}$, is an \mathcal{A}_2 -group. Describe the intersection $A \cap C$. Consider in detail the case when A is metacyclic.

Exercise 2. Classify the metacyclic \mathcal{A}_1 -groups G of order 2^n such that there is an involution $x \in G$ which is not square.

Exercise 3. Find the \mathcal{A}_2 -groups G such that $|H^G : H| = p$ for all nonnormal $H < G$.

Exercise 4. Find the \mathcal{A}_2 -groups G such that $\exp(H^G) = \exp(H)$ for all $H < G$.

The following three theorems are due to the first author.

Theorem 71.6 ([BJ2]). *Let G be a nonmetacyclic two-generator 2-group. Then the number of two-generator members of the set Γ_1 is even.*

Proof. By hypothesis, G is nonabelian. If $A \in \Gamma_1$, then $\mathfrak{V}_2(G) \leq \mathfrak{V}_1(A) = \Phi(A)$ so $d(A/\mathfrak{V}_2(G)) = d(A)$. Therefore, without loss of generality, one may assume that $\mathfrak{V}_2(G) = \{1\}$; then $\exp(G) = 4$. Let $\Gamma_1(G) = \{A, B, C\}$. Since G is not metacyclic, one may assume that $d(C) = 3$ (Appendix 25 and Theorem 44.5). Assume that the theorem is false. Then we may assume that $d(A) = 2$ and $d(B) = 3$ (see Appendix 25). Let R be a G -invariant subgroup of index 2 in G' . Then G/R is minimal nonabelian (Lemma 65.2(a)) and nonmetacyclic (Theorem 36.1). Since $\exp(G/R) = 4$, we get $|G/R| \leq 2^5$ (Lemma 65.1). If $|G/R| = 2^5$, the set Γ_1 has no two-generator members (Lemma 65.1), contrary to the assumption. Thus, $|G/R| = 2^4$ so $|G/G'| = 8$. One may assume that $C/R = \Omega_1(G/R)$. Since B/R is abelian of type (4, 2) so two-generator and $d(B) = 3$, we get $R \neq \Phi(B)$. Clearly, $\Phi(B)$ is a G -invariant subgroup of index 8 in B . Write $\bar{G} = G/\Phi(B)$; then \bar{G} is not of maximal class since it contains $\bar{B} \cong E_8$. It follows that $\text{cl}(\bar{G}) = 2$. Since $|G/G'| = 8$, we get $|G' : \Phi(B)| = 2$. Since G' has only one G -invariant subgroup of index 2 (Remark 36.1), we conclude that $\Phi(B) = R$. This is a contradiction since B/R is abelian of type (4, 2) and $\exp(B/\Phi(B)) = 2$. Thus, the number of two-generator members of the set Γ_1 is even, as was to be shown. \square

Theorem 71.7. *Suppose that all nonabelian maximal subgroups of a 2-group G are metacyclic and $|G| > 2^4$. Then one of the following holds: (a) G is abelian. (b) G is metacyclic. (c) G is an \mathcal{A}_1 -group. (d) G is minimal nonmetacyclic. (e) $G = M \times C$, where M is a metacyclic \mathcal{A}_1 -group and $|C| = 2$.*

Proof. Assume that G is not of types (a)–(d). Then, by Theorem 71.6, $d(G) > 2$ and there is in G a maximal subgroup A that is not two-generator; in that case, by hypothesis, A is abelian. By assumption, there is in G a nonabelian maximal subgroup M ; then M is metacyclic so $d(G) = 3$. Since $M \cap A$ is a metacyclic maximal subgroup of A , we get $d(A) = 3$. Write $E = \Omega_1(A)$; then $E \triangleleft G$ and $E \cong E_8$. By hypothesis, all maximal subgroups of G that contain E , are abelian. Since G has at most three abelian maximal subgroups, we get $d(G/E) \leq 2$.

(i) Suppose that $d(G/E) = 2$. Let B/E be a maximal subgroup of G/E and $B \neq A$. Then B is abelian so $A \cap B = Z(G)$ has index 4 in G ; in that case, $|G'| = 2$ (Lemma 64.1(q)) and $E \leq Z(G)$. It follows from $|M'| = 2$ and $d(M) = 2$ that M is

an \mathcal{A}_1 -group. Let $C < E$ be a subgroup of order 2 not contained in $\Omega_1(M)$ ($\cong \text{E}_4$); then $G = M \times C$ is as stated in (e).

(ii) Now let G/E be cyclic; then $E \not\leq Z(G)$ since G is nonabelian. Since $d(G) = 3$, we get $|G'| = 2$. We have $E = \Omega_1(G)$ since $\Omega_1(G) < A$ in view of G/E is cyclic of order > 2 . Let, as above, M is a nonabelian maximal subgroup of G . By Lemma 65.2(a), M is an \mathcal{A}_1 -subgroup; moreover, $M \cong \text{M}_{2^n}$, $n > 3$, since $\Omega_1(M) = M \cap E \cong \text{E}_4$ and $M/\Omega_1(M) \cong G/E$ is cyclic of order > 2 , and we conclude that $Z(M)$ is cyclic. If $Z(G)$ is noncyclic, then $G = M \times C$, where $|C| = 2$, and G is as stated in (e). Next assume that $Z(G)$ is cyclic. We get $|G : Z(G)| = 2|G'| = 4$ (Lemma 64.1(q)). Then, by the product formula, $G = EZ(G)$ so G is abelian, a final contradiction. \square

Theorem 71.8. Suppose that a two-generator nonabelian p -group G contains an abelian maximal subgroup A . Set $R = \langle x^p \mid x \in G - A \rangle$. Then $R \leq Z(G)$ and G/R is of maximal class, unless G is an \mathcal{A}_1 -group.

Proof. Recall that if A is an abelian maximal subgroup of a nonabelian p -group G and $|G : G'| = p^2$, then G is of maximal class (this is proved by induction with help of Lemma 64.1(q)). We have $R \leq Z(G) \cap \Phi(G)$ since $C_G(x^p) \geq \langle x, A \rangle$ for all $x \in G - A$. Write $\bar{G} = G/R$; then \bar{G} is noncyclic. Since all elements of the set $\bar{G} - \bar{A}$ have the same order p , we get $\Omega_1(\bar{G}) \geq \langle \bar{G} - \bar{A} \rangle = \bar{G}$. It follows that $\bar{G}' = \Phi(\bar{G})$ so that $\bar{G}/\bar{G}' \cong \text{E}_{p^2}$ since $d(\bar{G}) = d(G) = 2$. Suppose that $\bar{G}' = \{\bar{1}\}$. Then $R = \Phi(G)$ so $G/Z(G) \cong \text{E}_{p^2}$. In that case, all maximal subgroups of G are abelian so G is an \mathcal{A}_1 -group. Now suppose that $\bar{G}' > \{\bar{1}\}$; then \bar{G} is nonabelian. In that case, as we have noticed, \bar{G} is of maximal class. \square

Problems

Problem 1. Classify the p -groups G such that, whenever $H < G$ is minimal non-abelian and $H \cong H_1 < G$, then $H_1 = H$.

Problem 2. Classify the p -groups all of whose \mathcal{A}_2 -subgroups are isomorphic. Moreover, study the p -groups all of whose \mathcal{A}_1 -subgroups of the same order are isomorphic.

Problem 3. Classify the non-Dedekindian p -groups all of whose nonnormal subgroups are abelian.

Problem 4. Classify the p -groups all of whose \mathcal{A}_2 -subgroups are metacyclic.

Problem 5. Let G be a p -group all of whose maximal subgroups are \mathcal{A}_2 -groups. Is it true that $|G|$ is bounded?

Problem 6. Classify the p -groups with at most two \mathcal{A}_2 -subgroups. (Note that p -groups with exactly one \mathcal{A}_2 -subgroup are not classified.)

Problem 7. Describe the automorphism groups of all \mathcal{A}_1 - and \mathcal{A}_2 -groups.

Problem 8. Study the p -groups G such that, whenever $A, B \in \Gamma_1$ are distinct, then $A \cap B$ is either abelian or minimal nonabelian.

Problem 9. Study the p -groups all of whose \mathcal{A}_2 -subgroups are not two-generator.

Problem 10. Study the subgroup structure of $A \times A$, where A is an \mathcal{A}_1 -group.

Problem 11. Classify the p -groups G which are lattice isomorphic with B , where B is (i) an \mathcal{A}_1 -group, (ii) an \mathcal{A}_2 -group.

Problem 12. Study the p -groups G such that, whenever $A < G$ is an \mathcal{A}_1 -subgroup, then $A < B \leq G$, where B is an \mathcal{A}_2 -subgroup.

Problem 13. Classify the p -groups of exponent $> p$ all of whose \mathcal{A}_2 -groups have exponent p (then these subgroups have order p^4).

Problem 14. Study the p -groups G such that $\Phi(G)$ is an \mathcal{A}_1 -group (\mathcal{A}_2 -group).

Problem 15. Study the p -groups G all of whose subgroups of fixed order p^n are \mathcal{A}_2 -groups. Is it possible to estimate $|G|$ in terms of n ?

Problem 16. Classify the p -groups with minimal nonabelian subgroup of index p .

\mathcal{A}_n -groups, $n > 2$

In this section we study \mathcal{A}_n -groups with $n > 2$. A p -group G is said to be an \mathcal{A}_n -group if all its subgroups of index p^n are abelian but G has a nonabelian subgroup of index p^{n-1} .

Main results of this section are due to the first author.

1^o. First we classify \mathcal{A}_n -groups G with $G' \cong C_{p^n}$, $n > 1$ (for $n = 2$, see Corollary 65.3).

Proposition 72.1. (a) *Let G be a metacyclic p -group with $|G'| = p^n$. Then G is an \mathcal{A}_n -group.*

(b) *Let G be an \mathcal{A}_n -group, $n > 1$, with cyclic derived subgroup G' of order $\geq p^n$. Then G is metacyclic and $|G'| = p^n$.*

Proof. We use induction on $|G|$.

(a) If $n = 1$, then G is an \mathcal{A}_1 -group (Lemma 65.2(a)). Now suppose that $n > 1$. Let $L = \mathfrak{V}_1(G')(\leq \Phi(G))$. By Lemma 65.2(a), G/L is minimal nonabelian so, if $H \in \Gamma_1$, then H/L is abelian, and we have $H' \leq L$. By induction, H is an \mathcal{A}_s -group with $s < n$. By Lemma 64.1(u), there is $F \in \Gamma_1$ with $|G' : F'| = p$ so F is an \mathcal{A}_{n-1} -group since $|F'| = p^{n-1}$. It follows that G is an \mathcal{A}_n -group.

(b) Set $|G'| = p^s$, $s \geq n$. In view of Lemma 65.2(a,b) and Theorem 65.7(a), one may assume that $n > 2$. Take $H \in \Gamma_1$. If $H' = G'$, then, by induction, H is an \mathcal{A}_s -group, a contradiction since $s \geq n$. Therefore, if $G' = \langle [x, y] \rangle$, then $G = \langle x, y \rangle$, i.e., $d(G) = 2$. By Lemma 64.1(u), there is $F \in \Gamma_1$ with $|G' : F'| = p$ so, by induction, F is an \mathcal{A}_{s-1} -group and so $s-1 \leq n-1$ since G is an \mathcal{A}_n -group. It follows that $s = n$ and F is metacyclic, by induction since it is an \mathcal{A}_{n-1} -group with cyclic F' of order $p^{n-1} > p$. Let $L = \mathfrak{V}_1(G')$ and $T = \mathfrak{V}_2(G')$. If $H \in \Gamma_1$, then H/L is abelian since G/L is an \mathcal{A}_1 -group (Lemma 65.2(a)). By Lemma 65.1, G/T is not an \mathcal{A}_1 -group. Then G/T has a maximal subgroup A/T that is nonabelian so $(A/T)' > \{1\}$. Since A' and G' are cyclic, we get $T < A'$ so, by the above, $|A'| = p^{n-1}$. By induction, A is metacyclic. Then A/T is an \mathcal{A}_1 -group (Lemma 65.2(a)). Thus, every maximal subgroup of G/T is either abelian or an \mathcal{A}_1 -group so G/T is an \mathcal{A}_2 -group. Since $|(G/T)'| = p^2$, G/T is metacyclic, by Lemma 65.7(a). Now, by Lemma 64.1(o), G is metacyclic since $T \leq \mathfrak{V}_2(G)$. \square

Let G be a nonabelian metacyclic group of order p^m and $p^k = \min \{|A| \mid A < G, A' > \{1\}\}$. Then G is an $\mathcal{A}_{m-(k-1)}$ -group (indeed, all subgroups of G of order p^{k-1} are abelian and G has a nonabelian subgroup A of order p^k) so $|G'| = p^{m-(k-1)}$ (Proposition 72.1(a)) whence $|G/G'| = p^{k-1}$. In that case, $G' < Z < G$, where Z is cyclic of index p^{k-2} in G . In particular, if $k = 3$, then G has a cyclic subgroup of index $p^{3-2} = p$ so it is either a 2-group of maximal class or $p > 2$ and $m = 3$ (Lemma 64.1(t)). The last result coincides with Proposition 10.19.

Let $p > 2$ and suppose that a metacyclic p -group G of order $p^m > p^4$ contains a normal nonabelian subgroup H of order p^4 and exponent p^2 . Then $H = \Omega_2(G)$ so all subgroups of G of order p^3 are abelian. It follows that G is an \mathcal{A}_{m-3} -group so $|G'| = p^{m-3}$ (Proposition 72.1) and G has a normal cyclic subgroup Z of index p^2 , $G' < Z$, such that G/Z is cyclic. We have $Z(H) \cong E_{p^2}$. Let L be a subgroup of order p in $Z(H)$, $L \neq H'$. Then $|G : C_G(L)| \leq p$. Since $C_G(L)/L$ contains a nonabelian subgroup H/L of order p^3 , we get $C_G(L)/L = H/L$ (Lemma 64.1(t)). In that case, $|G : H| = p$ so $|G| = p|G : H| = p^5$, and $Z(H) \not\leq Z(G)$ so $Z(G)$ is cyclic.

Let G be a metacyclic p -group and $M_{p^4} \cong H < G$. In that case, G has no cyclic subgroup of index p (Lemma 64.1(t)). Then G is an \mathcal{A}_{m-3} -group so $|G'| = p^{m-3}$ and G has a normal cyclic subgroup $Z \neq \Phi(G)$ of index p^2 .

Exercise. Describe the nonabelian metacyclic 2-groups of order $2^m > 2^5$ without normal subgroups of order 2^4 and exponent 4.

Solution. Suppose that G has no cyclic subgroups of index 2 (otherwise, G satisfies the condition). Then $\Omega_1(G) \cong E_4$. Write $\bar{G} = G/\Omega_1(G)$. Then \bar{G} has no normal abelian subgroups of type $(2, 2)$ so it is of maximal class (if \bar{G} is cyclic, then G has a cyclic subgroup of index 2 so $\cong M_{2^m}$). Suppose that \bar{G} is dihedral. By Proposition 10.17, all subgroups of G of order 8 are abelian. Since $\Omega_1(\bar{G}) = \bar{G}$, it follows that $\Omega_1(G) \leq Z(G)$. If $G/\Omega_1(G)$ is of maximal class, then G has no normal subgroups of order 2^4 and exponent 4 since any such subgroup must contain $\Omega_1(G)$. In the case under consideration, G is a U_2 -group (see §67).

2^o . In this subsection and subsection 3^o we estimate $|G'|$, where G is an \mathcal{A}_n -group, $n = 3, 4$.

If a p -group G is an \mathcal{A}_3 -group and $U, V \in \Gamma_1$ are distinct, then $|G'| \leq p|U'V'| \leq p^7$ (Lemmas 65.2(d) and 64.1(u)). Proposition 72.2 yields essentially better estimate, and that estimate is best possible.

Proposition 72.2. *If a p -group G is an \mathcal{A}_3 -group, then $|G'| \leq p^4$. For $p = 5$, there exists an \mathcal{A}_3 -group G with $|G'| = 5^4$.*

Proof. Assume that $|G'| > p^4$. Take $U \in \Gamma_1$. Then $|U'| \leq p^3$ and, if $|U'| = p^3$, then $U' \cong E_{p^3}$ (Theorem 65.7(a,d)).

(i) We claim that G' is regular. This is the case if $|G : G'| > p^2$ since then G' is abelian. Let $|G : G'| = p^2$ and let G' be nonabelian; then $p > 2$ (Taussky's theorem)

and G' is an \mathcal{A}_1 -group. In that case, G' is regular since $\text{cl}(G) \leq 2$ (Lemmas 65.1 and 64.1(a)); moreover, G' is metacyclic (Theorem 44.12).

(ii) We claim that if $H \leq G$, then $|H/\Omega_1(H)| \leq p^5$, and this inequality is strong if $H < G$. Indeed, there is an \mathcal{A}_2 -subgroup $A \in \Gamma_1$. Then $|A/\Omega_1(A)| \leq p^4$ (Lemma 65.4(a)) so $|G/\Omega_1(G)| \leq p^5$. Take $H < G$ such that $|H/\Omega_1(H)| \geq p^5$. By Lemmas 65.1 and 65.4(b), H is abelian so $\Omega_1(H)$ is elementary abelian of order $\geq p^5$. Then all members of the set Γ_1 containing $\Omega_1(H)$, are abelian (Lemmas 65.1 and 65.4(b)). By assumption, $|G'| > p^4 > p$ so H is the unique member of the set Γ_1 containing $\Omega_1(H)$ (Lemma 65.2(c)), and we conclude that $G/\Omega_1(H)$ is cyclic whence $G' < \Omega_1(H)$. Considering $H \cap F$, where $F \in \Gamma_1$ is nonabelian, we get $|\Omega_1(H)| \leq p^5$ so $|G'| < p^5$, a contradiction. (If $G = S(p^3) \times E_{p^2}$, where $S(p^3)$ is nonabelian of order p^3 and exponent $p > 2$, then G is an \mathcal{A}_3 -group, $|G| = p^5$ and $\exp(G) = p$.)

(iii) Assume that $|G'| > p^5$. Let $U, V \in \Gamma_1$ be distinct; then $|U'V'| \geq \frac{1}{p}|G'| \geq p^5$ (Lemma 64.1(u)) so one may assume that $|U'| = p^3$; then $|V'| \geq p^2$. If $|V'| = p^3$, then $\exp(U'V') = p$ since $\exp(U') = \exp(V') = p$ (Theorem 65.7(d), Lemma 64.1(a) and (i)), and $|U'V'| \geq p^5$, contrary to (ii). Thus, $|V'| = p^2$; then $U' \cap V' = \{1\}$, by the product formula. By (ii), since $|U'V'| \geq p^5$, we get $\exp(U'V') > p$ so V' is cyclic; then V is metacyclic (Theorem 65.7(a)), a contradiction since $E_{p^3} \cong U' < G' \leq \Phi(G) < V$. Thus, $|G'| = p^5$. Then the set Γ_1 has no abelian members, by Lemmas 65.2(d) and 64.1(u) (otherwise, if $A \in \Gamma_1$ is abelian and $H \in \Gamma_1 - \{A\}$, then $|H'| \leq p^3$ so $|G'| \leq p|A'H'| \leq p^4$, contrary to the assumption).

(iv) Assume that there are distinct $U, V \in \Gamma_1$ such that $\exp(U') = \exp(V') = p$. Then, using (i) and (ii), we get: $U'V'$ is of order p^4 and exponent p so $U'V' < G'$, and $\exp(G') = p^2$ since $|G'| = p^5$. In that case, $U/U'V'$ and $V/U'V'$ are cyclic (Lemma 65.4(b)). Thus, the nonabelian group $G/U'V'$ has two distinct cyclic subgroups $U/U'V'$ and $V/U'V'$ of index p so it is either ordinary quaternion or $\cong M_{p^n}$ (Lemma 64.1(t)). In the first case $|G : G'| = 4$ so G is a 2-group of maximal class (Lemma 64.1(s)), a contradiction. Assume that $G/U'V' \cong M_{p^n}$. Let $H/U'V'$ be the noncyclic subgroup of index p in $G/U'V'$. In that case, H is neither \mathcal{A}_1 - nor \mathcal{A}_2 -group (Lemmas 65.1 and 65.4(b)) so H is abelian, a contradiction (see the last sentence of part (iii)).

Now we are ready to complete the proof. By (iv), there is $V \in \Gamma_1$ such that $\exp(V') > p$; then V is metacyclic and V' is cyclic of order p^2 (Theorem 65.7(d,a)). Take $U \in \Gamma_1 - \{V\}$. Since $U' < V$, we get $|\Omega_1(U')| \leq p^2$ so $|U'| \leq p^2$ (Lemma 65.1 and Theorem 65.7(a,d)). Then $U' \cap V' = \{1\}$ (Lemmas 65.2(d) and 64.1(u)). Since $U'V' = U' \times V' < V$ and V is metacyclic, $U' \cong C_{p^2}$ (Corollary 65.3 and Lemma 64.1(u)). Thus, all members of the set Γ_1 are metacyclic. Since G is nonmetacyclic (Proposition 72.1(a)), we get, $|G'| \leq p^2$ (Lemma 64.1(l)), a contradiction.

Below we present an \mathcal{A}_3 -group G with $|G'| = p^4$ for $p = 5$ (this example was constructed by the second author).

Let G be the group of order 5^6 with the following generators and relations:

$$\begin{aligned} \langle b, h \mid b^{25} = h^{25} = 1, [h, b] = a, a^5 = 1, [a, b] = c, c^5 = 1, \\ [b, c] = d, d^5 = 1, [c, a] = [h, d] = [b, d] = [h, c] = 1, \\ [h, a] = s, s^5 = 1, [h, s] = [b, s] = 1, d = h^5, b^5 = s \rangle. \end{aligned}$$

Here $G' = \langle a, c, d, s \rangle \cong E_{5^4}$, $K_3(G) = \langle c, d, s \rangle \cong E_{5^3}$, $K_4(G) = \langle d \rangle$ is of order 5, and $Z(G) = \langle d, s \rangle \cong E_{5^2}$. All maximal subgroups of G are \mathcal{A}_2 -groups and so G is an \mathcal{A}_3 -group. Finally, we have shown that this group G exists as a subgroup of the symmetric group of degree 625. \square

In the following proposition we investigate \mathcal{A}_3 -groups with derived subgroup of order p^4 in some detail. We show that then G' is nonmetacyclic. Note that $|G| \geq p^6$ with strong inequality if $p = 2$ (Taussky's theorem).

Proposition 72.3. *Suppose that a p -group G is an \mathcal{A}_3 -group with $|G'| = p^4$.*

- (a) *G' is abelian.*
- (b) *If $\exp(G') = p$, then $p > 2$, G/G' is abelian of type (p^n, p) ($n \geq 1$) and $G' \cong E_{p^4}$. If, in addition, $n > 1$, then $\Omega_1(G) = G'$.*
- (c) *G' is not metacyclic.*

Proof. By Proposition 72.1, G' is noncyclic so G is not metacyclic.

(i) Assume that G' is metacyclic. Let us prove that then $p = 2$, the set Γ_1 has only one nonmetacyclic member and G has no normal elementary abelian subgroups of order 8. Since the set Γ_1 has a nonmetacyclic member (Lemma 64.1(l)), there is $U \in \Gamma_1$ such that $\exp(U') \leq p$ (Theorem 65.7(a,d)); then $|U'| \leq |\Omega_1(G')| = p^2$ so $U' \leq Z(G')$ (indeed, every G -invariant subgroup L of order $\leq p^2$ in G' is contained in $Z(G')$: consider $C_G(L)$). Take $V \in \Gamma_1 - \{U\}$. By Lemma 64.1(u), $|G' : U'V'| \leq p$ so $|U'V'| \geq p^3$ hence $\exp(U'V') > p$ since G' is metacyclic. It follows that $\exp(V') > p$. Since V' is abelian in view of $|V'| \leq p^3$, $U'V'$ is also abelian (recall that $U' \leq Z(G')$), V' is cyclic of order $> p$ (Theorem 65.7(d)) so V is a metacyclic \mathcal{A}_2 -group and $|V'| = p^2$ (Corollary 65.3). It follows that all members of the set Γ_1 are nonabelian.

If $E \triangleleft G$, where E is of order p^3 and exponent p , then there is only one maximal subgroup of G containing E , by the previous paragraph, so G/E is cyclic. Then $G' < E$, a contradiction since $|G'| = p^4 > |E|$. Thus, E does not exist. Assume that $p > 2$. Then, by Theorem 13.7 (see also Theorem 69.4), G is a 3-group of maximal class and $|G| = 3^2|G'| = 3^6$. In that case, G has a nonabelian subgroup of index 3^3 (Theorem 9.6), a contradiction. Thus, $p = 2$.

(ii) Assume that G' is nonabelian; then $|G : G'| = p^2$ and $G' = \Phi(G)$ is an \mathcal{A}_1 -group. By Theorem 44.12, G' must be metacyclic so $p = 2$, by (i); then G is of

maximal class (Taussky's theorem) so $Z(G')$ is cyclic, a contradiction (Lemma 1.4). Thus, G' is abelian.

(iii) Let $\exp(G') = p$. Then, by (ii), $G' \cong E_{p^4}$. If $|G : G'| = p^2$, then $p > 2$ (Lemma 64.1(s)).

Now assume that $|G : G'| > p^2$ and assume, in addition, that G/G' has two distinct noncyclic maximal subgroups U/G' and V/G' . Then U is either abelian or an \mathcal{A}_2 -group with the derived subgroup of order p , the same is true for V (Lemma 65.4(b)). Then $|G'| \leq p^3$ (Lemma 64.1(u)), a contradiction. Thus, G/G' has exactly p cyclic subgroups of index p , so it is abelian of type (p^n, p) with $n > 1$. Let H/G' be the noncyclic maximal subgroup of G/G' . Then H is either abelian or an \mathcal{A}_2 -group with $|H'| = p$. If $F \in \Gamma_1 - \{H\}$, then $|F'| \geq p^2$ (Lemmas 64.1(u) and 65.2(d)) and so F is an \mathcal{A}_2 -group. If $|F'| = p^3$, then F has no maximal abelian subgroups (Lemma 65.2(d)). But, if F_1 is a maximal subgroup of F containing G' , then F_1 must be abelian (Lemma 65.1). This contradiction shows that $|F'| = p^2$ and then $|H'| = p$. Looking at the determination of \mathcal{A}_2 -groups (see §71), we see that F must be isomorphic to a group (ii) of Proposition 71.3. In particular, $p > 2$. (H must be isomorphic with a group of Proposition 71.1(i); then H must be a nonmetacyclic \mathcal{A}_1 -group).

Assume that there is $x \in G - G'$ of order p . Then $D = \langle x, G' \rangle \cong E_{p^5}$ since $|G : D| \geq p^2$ and $\Omega_1(D) = D$. If $D \leq M \in \Gamma_1$, then M is abelian (Lemmas 65.1 and 65.4(a)). Take $N \in \Gamma_1 - \{M\}$. By Lemma 64.1(u) applied to $M, N (\in \Gamma_1)$, $|N'| \geq p^3$. Considering $N \cap M$ and using Lemma 65.4(b), we conclude that N/G' is cyclic and $|N'| \leq p^2$, contrary to the result of the previous sentence. Thus, x does not exist so $\Omega_1(G) = G'$.

(iv) By (i), $p = 2$ and the set Γ_1 has only one nonmetacyclic member H and G has no normal elementary abelian subgroups of order 8. Take $V \in \Gamma_1 - \{H\}$; then V is metacyclic so $|V'| \leq 4$ (Corollary 65.3 and Lemma 65.1). Then H is nonabelian (apply Lemma 64.1(u) to $H, V \in \Gamma_1$). If H is an \mathcal{A}_1 -group, then $\Omega_1(H) \cong E_8 \triangleleft G$ (Lemma 65.1), contrary to (i). If H is an \mathcal{A}_2 -group with $|H'| = 2$, then $\Omega_1(H) \cong E_8$ or E_{16} (Proposition 72.1), contrary to (i). Hence, H must be an \mathcal{A}_2 -group of Proposition 71.4. If H is minimal nonmetacyclic of order 2^5 , then $|G| = 2|H| = 2^6$ so $|G : G'| = 4$ and G is of maximal class (Lemma 64.1(s)), a contradiction. In other cases of Proposition 71.4, $\Omega_1(H) \cong E_8$, a final contradiction. \square

3^o . It follows from Proposition 72.2 and Lemma 64.1(u) that if a p -group G is an \mathcal{A}_4 -group, then $|G'| \leq p^9$. In this subsection we improve essentially that estimate.

Since every p -group of order $< p^7$ is an \mathcal{A}_i -group with $i \leq 4$, in what follows we consider only \mathcal{A}_4 -groups of order $\geq p^7$; then our \mathcal{A}_4 -group is not of maximal class (Theorems 9.5 and 9.6).

Lemma 72.4. *Suppose that a p -group G of order $> p^6$ is an \mathcal{A}_4 -group with non-abelian G' . Let $|G : G'| = p^i$; then $i \in \{2, 3\}$.*

(a) If $i = 2$, then $p > 2$ and G' is either metacyclic or an \mathcal{A}_2 -subgroup with $d(G) = 3$.

(b) If $i = 3$, then G' is a metacyclic \mathcal{A}_1 -subgroup.

Proof. We have $|G : G'| = p^i$, $i \in \{2, 3\}$.

If $i = 3$, then G' is an \mathcal{A}_1 -group so $d(G') = 2$ (Lemma 65.1); then G' is metacyclic (Theorem 44.12).

Now suppose that $i = 2$. If $p = 2$, then G is of maximal class (Lemma 64.1(s)), a contradiction. Thus, $p > 2$. Assume that G' is nonmetacyclic; then $d(G') > 2$ (Theorem 44.12) and G' is an \mathcal{A}_2 -subgroup with $d(G) = 3$. \square

Proposition 72.5. *If a p -group G is an \mathcal{A}_4 -group, then $|G'| \leq p^7$.*

Proof. Assume that $|G'| = p^9$. For $U \in \Gamma_1$, we have $|U'| = p^4$ so U' is nonmetacyclic, abelian (Lemma 64.1(u), Propositions 72.2, 72.3 and 72.1); in particular, all members of the set Γ_1 are \mathcal{A}_3 -groups (Lemmas 65.1 and 65.2(c)). If $V \in \Gamma_1 - \{U\}$, then $U' \cap V' = \{1\}$ (Lemma 64.1(u)) so $U'V' = U' \times V'$ is abelian of order p^8 . Set $L = \Omega_1(U'V')$; then $|\Omega_1(L)| \geq p^6$ (Proposition 72.3) and $L < U$. If $A < U$ is nonabelian subgroup, then $|A \cap L| \geq p^5$, contrary to Lemmas 65.1 and 65.4(b). Thus, $|G'| \leq p^8$.

Next we assume that $|G'| = p^8$. If $U, V, W \in \Gamma_1$ are distinct with $|U'| \geq |V'| \geq |W'|$, then using Lemma 64.1(u) twice, we get $|U'| = |V'| = p^4$ and $|U' \cap V'| \leq p$ since $|U'V'| \geq \frac{1}{p}|G'| = p^7$. Then U and V are both \mathcal{A}_3 -groups and U' and V' are nonmetacyclic abelian (Proposition 72.3(a,c)) so $\text{cl}(U'V') \leq 2$ (Fitting's lemma), hence, if $p > 2$, then $U'V'$ is regular (Lemma 64.1(a)). Now let $p = 2$. If $U'V' = G'$, then G' is abelian since then $G' = U' \times V'$ (here we use Proposition 72.3(a) again). Suppose that $U'V' < G'$. Then $|G : U'V'| > |G : G'| \geq 8$, by Lemma 64.1(s), so $U'V'$ is abelian again.

Set $L = \Omega_1(U'V')$ so that $\exp(L) = p$. By the previous paragraph, $|L| \geq p^5$. If U_1 is a maximal subgroup of U containing L , then U_1 must be abelian (Lemma 65.4(b)). Since $|U'| > p$, U/L is cyclic (indeed, U_1 is the unique abelian maximal subgroup of U), and so $U' < L$. Hence $\exp(U') = p$ and Proposition 72.3(c) implies that $U' = \Omega_1(U)$. This is a contradiction since $U' < L < U$ and $\exp(L) = p$. \square

Now we improve the estimate of Proposition 72.5.

Theorem 72.6. *If a p -group G is an \mathcal{A}_4 -group, then $|G'| \leq p^6$.*

Proof. Assume, by the way of contradiction, that a p -group G is an \mathcal{A}_4 -group with $|G'| = p^7$. By Propositions 72.2, 72.3(a) and Lemma 64.1(u), $p^2 \leq |U'| \leq p^4$ and U' is abelian for all $U \in \Gamma_1$.

(i) We claim that the subgroup G' is nonmetacyclic and then $d(G') > 2$ (Theorem 44.12). Suppose that this is false. By Proposition 72.1, $|U'| = p^3$ for all $U \in \Gamma_1$ and so $U'V' = U' \times V'$ for distinct $U, V \in \Gamma_1$ (Lemma 64.1(u)). It follows that each

U' is cyclic (otherwise, $U' \times V'$ is nonmetacyclic) and so U is metacyclic (Proposition 72.1(b)). But then G is minimal nonmetacyclic (Proposition 72.1(a)), contrary to Lemma 64.1(l).

(ii) If $|G/G'| > p^2$, then G' is abelian and $p^3 \leq |\Omega_1(G')| \leq p^4$. Indeed, since $d(G') > 2$, by (i) and Theorem 44.12, G' is not an \mathcal{A}_1 -group and so G' must be abelian. Since G/G' is noncyclic, there is $U \in \Gamma_1$ such that U/G' is noncyclic. Let V_1 and V_2 be two distinct maximal subgroups of U containing G' . If $|\Omega_1(G')| > p^4$, then V_1 and V_2 cannot be \mathcal{A}_1 -groups or \mathcal{A}_2 -groups (Lemmas 65.1 and 65.4(a,b)) and so they are abelian. It follows that $|U'| \leq p$ (Lemma 64.1(q)), a contradiction. Thus $|\Omega_1(G')| \leq p^4$, and $|\Omega_1(G')| \geq p^3$ follows from $d(G') > 2$ and commutativity of G' .

(iii) If G' is nonabelian, then $G/G' \cong E_{p^2}$, by (ii), so $p > 2$ since G is not of maximal class (Taussky's theorem), and G' is an \mathcal{A}_2 -group with $d(G') = 3$, by (i). Hence G' is isomorphic to a group of Proposition 71.1 or Proposition 71.4(b). In any case, $\Omega_1(G') \cong E_{p^3}$ or E_{p^4} , which follows from §71.

(iv) If $U \in \Gamma_1$ and $|U'| = p^4$, then U' is abelian of type (p^2, p, p) . If $V \in \Gamma_1$ and $|V'| = p^3$, then V' is abelian noncyclic since V is nonmetacyclic, in view of $G' < V$. Indeed, U' is abelian nonmetacyclic (Proposition 72.3). Suppose that $U' \cong E_{p^4}$. Then Proposition 72.3(c) (noting that $|U| = \frac{1}{p}|G| > p^6$) implies that $\Omega_1(U) = U'$. Take $W \in \Gamma_1 - \{U\}$. Then $U' \leq \Phi(U) \leq \Phi(G) < W$ so W is nonmetacyclic. Next, $|U'W'| \geq \frac{1}{p}|G'| = p^6$ (Lemma 64.1(u)) and we must have $W' \leq U$, $\Omega_1(W') \leq U'$ (see (iii)) so $|W'| \geq p^3$. By Proposition 72.1(b), W' is noncyclic so $|U' \cap W'| \geq p^2$. But then $|U' \cap W'| = p^2$ and $|W'| = p^4$ (Lemma 64.1(u)). Since W' is abelian and nonmetacyclic (Proposition 72.3(c)), we have $|\Omega_1(W')| \geq p^3$ and so $\Omega_1(W') \not\leq U'$, contrary to what has just been proved.

(v) We claim that $|\Omega_1(G')| \leq p^4$. Indeed, assume that $|\Omega_1(G')| \geq p^5$. Then G' is not an \mathcal{A}_i -group, $i = 1, 2$ (Lemmas 65.1 and 65.4(a,b)) so G' is abelian and $E = \Omega_1(G')$ is elementary abelian of order $\geq p^5$. By (ii), $G/G' \cong E_{p^2}$ so $p > 2$ (Taussky's theorem). For each $U \in \Gamma_1$, $p^2 \leq |U'| \leq p^4$ (Lemma 64.1(u)) so U is an \mathcal{A}_3 -group (indeed, the nonabelian U cannot be an \mathcal{A}_i -group, $i \leq 2$, since $E < U$; see Lemma 65.4(a,b)). If U/E is not cyclic, U has a maximal subgroup $U_0 \neq G'$ containing E (note that G' is maximal in U). Then U_0 must be abelian and so $|U'| \leq p$ (Lemma 65.2(c)), a contradiction. Hence U/E is cyclic; then $U' < E$ and so U' is elementary abelian for each $U \in \Gamma_1$. Then (iv) forces that $U' \cong E_{p^3}$ for each $U \in \Gamma_1$ and $U'V' = U' \times V'$ for any two distinct $U, V \in \Gamma_1$. In particular, $E = \Omega_1(G')$ is elementary abelian of order $\geq p^6$. Let an \mathcal{A}_2 -subgroup A be maximal in U . But in that case $|A \cap E| \geq p^5$ since $G' < U$, contrary to Lemma 65.4(a,b).

(vi) We claim that, for each $U \in \Gamma_1$, U' is abelian of exponent p^2 . Also, $\Omega_1(G') \cong E_{p^4}$ and, if G' is nonabelian, then $G' = H \times C_p$, where H is a nonmetacyclic \mathcal{A}_1 -group of order p^6 . Indeed, assume that there is $U \in \Gamma_1$ with $U' \cong E_{p^3}$, and take $V \in \Gamma_1 - \{U\}$. Since $|U'V'| \geq p^6$ (Lemma 64.1(u)), we have $|V' : (U' \cap V')| \geq p^3$. If $|V'| = p^3$, then $U' \cap V' = \{1\}$ and V' is noncyclic, by Proposition 72.1(b) and (i),

since $G' < V$. If $|V'| = p^4$, then $|U' \cap V'| \leq p$ (Lemma 64.1(u)) and $\Omega_1(V') \cong E_{p^3}$, by (iv). In any case, $|\Omega_1(U'V')| \geq p^5$, contrary to (v). Suppose that $W \in \Gamma_1$ with $W' \cong E_{p^2}$ and take $V_0 \in \Gamma_1 - \{W\}$. Then $|V'_0| = p^4$, $W' \cap V'_0 = \{1\}$ (Lemma 64.1(u)), so again $|\Omega_1(W'V'_0)| \geq p^5$, by (iv), which is a contradiction. We have proved that if $U \in \Gamma_1$ and $|U'| = p^2$, then $U' \cong C_{p^2}$ and if $|U'| = p^3$, then $U' \cong C_{p^2} \times C_p$. This together with (iv) proves our first assertion on $\exp(U')$.

Suppose that $U \in \Gamma_1$ is such that $|U'|$ is as large as possible. Let $|U'| = p^4$; then U' is abelian of type (p^2, p, p) , by (iv). Let $V \in \Gamma_1 - \{U\}$ be such that $|V' : (U' \cap V')| \geq p^2$. If $|V'| = p^2$, then $U' \cap V' = \{1\}$ and we have $|\Omega_1(U'V')| \geq p^4$. If $|V'| = p^3$, then $|U' \cap V'| \leq p$ and so there are elements of order p in $V' - U'$ since V' is abelian of type (p^2, p) , by the previous paragraph. If $|V'| = p^4$, then $|U' \cap V'| \leq p^2$ (Lemma 64.1(u)) and again there are elements of order p in $V' - U'$ since V' is abelian of type (p^2, p, p) , by (iv). In any case, we get $|\Omega_1(U'V')| \geq p^4$. Suppose now that $|U'| = p^3$. If $W \in \Gamma_1 - \{U\}$, then $|W'| = p^3$, $U'W' = U' \times W'$ (Lemma 64.1(u)) and both U' and W' are noncyclic ((i) and Proposition 72.1). Hence we get $|\Omega_1(U'W')| \geq p^4$ again. These results together with (iii) and (v) give that $\Omega_1(G') \cong E_{p^4}$. If G' is nonabelian, then using (iii), we see that G' must be isomorphic to a group of Proposition 71.1(i) and we are done.

(vii) The group G is an irregular 3-group of order 3^9 . Each maximal subgroup of G is two-generator and $\mathfrak{U}_1(G) = K_3(G)$ is of index 3^3 in G . In particular, $G/G' \cong E_9$. Indeed, let $U \in \Gamma_1$ and let $A < U$ be maximal. Since $\Omega_1(G') \cong E_{p^4}$, we have $|A \cap \Omega_1(G')| \geq p^3$ since $G' < U$, and so A is nonmetacyclic. This implies that A' is elementary abelian (Lemma 65.1 and Theorem 65.7(d)) and so $A' \leq \Omega_1(U') < U'$ since $\exp(U') = p^2$, by (vi), and we get $d(U) = 2$ (Lemma 64.1(y)). Thus, all members of the set Γ_1 are two-generator.

Assume that $d(G) > 2$. Using Theorem 70.1 and 70.2, we get in case $p > 2$ that $|G| \leq p^5$, a contradiction. If $p = 2$, then it follows from $|G| \geq 2^{10}$ that $\text{cl}(G) > 2$. The quotient group $G/K_4(G)$ is of order 2^7 or 2^8 . If $|G/K_4(G)| = 2^8$, then we know that $G/K_4(G)$ is an \mathcal{A}_5 -group, a contradiction (see the text following Theorem 70.5). If $|G/K_4(G)| = 2^7$, then Theorem 70.5 implies that $K_4(G) = \{1\}$, a contradiction.

We have proved that $d(G) = 2$. Since G is not metacyclic, we get $p > 2$ (Lemma 64.1(n)). By Lemma 64.1(p), $\mathfrak{U}_1(G) = K_3(G)$ is of index p^3 in G . On the other hand, $|\Omega_1(G')| = p^4 > |G/\mathfrak{U}_1(G)|$ so G is irregular (Lemma 64.1(a)). This implies that $p = 3$ (Theorem 9.8(a)), $G/G' \cong E_9$ and $|G| = 3^9$.

(viii) Let $U, V \in \Gamma_1$ be distinct. Then $|U'V'| \geq \frac{1}{3}|G'| = 3^6$ (Lemma 64.1(u)) and we claim that $|U'V'| = 3^6$. Since $H = K_3(G) = [G, G'] \leq U'V'$, we have $H = U'V' = \mathfrak{U}_1(G)$ in view of $|G : H| = 3^3$. Also, $\Omega_1(G') = \Omega_1(H)$ and H is abelian of exponent 3^2 . Finally, G/H is nonabelian of order 3^3 and exponent 3. Suppose that there are distinct $U, V \in \Gamma_1$ such that $U'V' = G'$. We may assume that $|U'| = 3^4$ and V' covers G'/U' . If $|V'| = 3^3$, then $G' = U' \times V'$. But then, by (iv), $|\Omega_1(G')| \geq 3^5$, contrary to (v). If $|V'| = 3^4$, then $|U' \cap V'| = 3$. But $|\Omega_1(V')| = 3^3$ and again we get $|\Omega_1(G')| \geq 3^5$, a contradiction. Hence, for each distinct $U, V \in \Gamma_1$,

we have $|U'V'| = 3^6$. Since $U'V' \triangleleft G$ and $G'/(U'V') \leq Z(G/(U'V'))$, we have $H = [G, G'] \leq U'V'$. By (vii), $H = U'V' = \Omega_1(G)$ (recall that $|G : G'| = 3^2$). Since $|\Omega_1(U'V')| \geq 3^4$, we have $|\Omega_1(U'V')| = 3^4$, by (v), and so $E = \Omega_1(H) = \Omega_1(G') \cong E_{34}$. If H would be nonabelian, then H is an \mathcal{A}_1 -group, contrary to Lemma 65.1. Thus, H is abelian and so $\exp(H) = 3^2$ since $\exp(U') = \exp(V') = 3^2$ and $H = U'V'$.

We are now able to get the final contradiction. Take $U \in \Gamma_1$. Since G/H is non-abelian of order 3^3 and exponent 3, we get $U/H \cong E_9$, where $H = K_3(G) = \Omega_1(G)$. On the other hand, $d(U) = 2$ (by (vii)) and so $\Phi(U) = H$. Let X be any of the four maximal subgroups of U . Then $|X : H| = 3$ and $E = \Omega_1(H) \cong E_{34}$ is a normal subgroup of X . Suppose that $|X'| \geq 3^2$ so that X is an \mathcal{A}_2 -subgroup. By the results of §71, X must be isomorphic to a group of Proposition 71.3(ii). In particular, X (of order 3^7) has the unique abelian maximal subgroup of type $(3^3, 3, 3, 3)$. This is a contradiction since H is a unique maximal abelian subgroup of X and $\exp(H) = 3^2$ (by (viii)). We have proved that $|X'| \leq 3$ for any maximal subgroup X of U . This implies that $|U'| \leq 3^3$ for any $U \in \Gamma_1$ (Lemma 64.1(u)).

We have proved that for each $U \in \Gamma_1$, U' is abelian of type $(3^2, 3)$ and so $H = U' \times V'$, where $V \in \Gamma_1 - \{U\}$. This implies that H is abelian of type $(3^2, 3^2, 3, 3)$ and each maximal subgroup X of U must be an \mathcal{A}_2 -group with $|X'| = 3$ (Lemmas 65.1 and 64.1(u)). By the results of §71, X must be the following group of Proposition 71.1(i):

$$X = \langle a, b \mid a^{3^3} = b^{3^2} = 1, [a, b] = c, c^3 = [a, c] = [b, c] = 1 \rangle \times C_3,$$

where $\Omega_1(X) = \langle a^{3^2}, b^3, c \rangle \times C_3 = E = \Omega_1(H)$ and $X' = \langle c \rangle$ is a maximal cyclic subgroup in X (see Lemma 65.1).

We have $U' < H$ and set $U' \cap E = E_0$ so that $E_0 \cong E_9$. Also set $\langle e_0 \rangle = \Omega_1(U')$ so that $\langle e_0 \rangle$ is a subgroup of order 3 in E_0 and $\langle e_0 \rangle$ is not a maximal cyclic subgroup in H . Let X_1, X_2, X_3, X_4 be all maximal subgroups of U and note that each one is isomorphic to the above group X . Then X'_1, X'_2, X'_3, X'_4 must be four distinct subgroups of order 3 in E_0 (Lemma 64.1(u)). It follows that for some $i \in \{1, 2, 3, 4\}$, $X'_i = \langle e_0 \rangle$. This is a contradiction since $\langle e_0 \rangle$ is not a maximal cyclic subgroup in H (and H is contained in X_i); see the last sentence of the previous paragraph. \square

§73

Classification of modular p -groups

We recall that a p -group G is *modular* if and only if any two subgroups of G are permutable (for general groups there is another definition). Sections of modular p -groups are modular. A nonabelian Dedekindian p -group G is a modular 2-group of the form $G = Q \times E$, where $Q \cong Q_8$ and $\exp(E) \leq 2$ (Theorem 1.20). Such groups are called *Hamiltonian*. Nonmodular p -groups of order p^3 are D_8 and the nonabelian group $S(p^3)$ of order p^3 and exponent $p > 2$.

If G is a minimal nonmodular p -group, then there is $N \triangleleft G$ such that G/N is either $S(p^3)$ ($p > 2$) or D_8 (see Theorem 44.13).

The aim of this section is to correct the original Iwasawa's proof [Iwa] of the theorem on the structure of modular p -groups. ((Iwasawa's proof contains essential gaps. Two gaps were filled by Napolitani [Nap], remaining ones – by the second author, who wrote this corrected proof. There exists another proof of Iwasawa's theorem, due to R. Schmidt [Sch, Chapter 2]; that proof is based on entirely other ideas and is essentially shorter.) Our proof is self-contained.

The following proposition is obvious.

Proposition 73.1. *Let G be a modular p -group. Then $\Omega_1(G)$ is elementary abelian.*

In particular, modular p -groups, $p > 2$, are powerful (apply Lemma 73.1 to $G/\Omega_1(G)$; see [LM] and §26). It follows from Theorem A.24.4 that non-Hamiltonian modular 2-groups G are also powerful (see [LM] and §26.2). Indeed, by that theorem, G is Q_8 -free. One may assume that $\exp(G) = 4$. Assume that G has a minimal nonabelian subgroup H . Then $8 < |H| < 32$ since $\exp(H) = 4$. Using Lemma 65.1, we see that H has a nonabelian epimorphic image of order 8, contrary to what has just been said. Thus, H does not exist so G is abelian.

Proposition 73.2. *Let G be a modular p -group. Then $\exp(\Omega_n(G)) \leq p^n$ and the group $\Omega_n(G)/\Omega_{n-1}(G)$ is elementary abelian for all n .*

Use induction on n and Proposition 73.1.

By Theorem 44.13, a p -group G is modular if and only if it is D_8 -free if $p = 2$ and $S(p^3)$ -free if $p > 2$.

Remark. A two-generator modular p -group G is metacyclic. Assume that G is not metacyclic. In view of Lemma 64.1(m), one may assume that $K_3(G)\Phi(G') = \{1\}$;

then G is minimal nonabelian such as in Lemma 65.1(a) with $m + n > 2$, $|G| = p^{m+n+1}$. Then $G = \langle a, b \rangle = \langle a \rangle \langle b \rangle$ has order $p^{m+n} < p^{m+n+1} = |G|$, a contradiction.

Since metacyclic p -groups, $p > 2$, are modular, it follows from the remark that a p -group G , $p > 2$, is modular if and only if every its two-generator subgroup is metacyclic. It is interesting to classify the 2-groups satisfying this property. Note that dihedral 2-groups are metacyclic but nonmodular. The group M_{2^n} is modular. A central product of two modular p -group is not necessary modular (for example, the group $Q_{2^3} * C_4$ is not modular).

Proposition 73.3. *Nonabelian modular groups G of order p^4 are: (a) M_{p^4} , (b) $M_{p^3} \times C_p$, $p > 2$, (c) $G = \langle a, b \mid a^{p^2} = b^{p^2} = 1, a^b = a^{1+p} \rangle$, $p > 2$, (d) $Q_8 \times C_2$.*

Proposition 73.4. *Suppose that G is a modular 2-group containing a normal elementary abelian subgroup E such that $G/E \cong Q_8$. Then $G = Q \times E$ with $Q \cong Q_8$ and so G is Hamiltonian.*

Proposition 73.5. *Let G be a modular 2-group which is not Hamiltonian. Then each quotient group $\Omega_i(G)/\Omega_{i-2}(G)$ is abelian. In particular, $\Omega_2(G)$ is abelian.*

Proof. Let G be a modular 2-group of exponent 4. If G does not contain a quaternion subgroup, then Proposition 73.3 implies that any two elements of G commute and so G is abelian. Suppose that $Q_8 \cong Q \leq G$. In that case, G is Hamiltonian, by Theorem A.24.4, and we are done. The result follows since all sections of G are modular. \square

Proposition 73.6. *Let G be a modular p -group of exponent p^μ ($\mu \geq 2$) which is not Hamiltonian. Then*

$$(*) \quad (uv)^{p^{\mu-1}} = u^{p^{\mu-1}} v^{p^{\mu-1}}$$

for any $u, v \in G$, i.e., G is $p^{\mu-1}$ -abelian.

Proof. (i) Suppose that $\mu = 2$. If $p = 2$, then $G = \Omega_2(G)$ is abelian (Proposition 73.5). Suppose that $p > 2$ and let $a, b \in G$. Then $H = \langle a, b \rangle = \langle a \rangle \langle b \rangle$ of order $\leq p^4$ is metacyclic (Lemma 64.1(m)), $|H'| = p$ so $(ab)^p = a^p b^p [b, a]^{\binom{p}{2}} = a^p b^p$.

The general case follows by induction on μ . Let $\mu > 2$. Since $G/\Omega_1(G)$ is of exponent $p^{\mu-1}$, we have, for $x, y \in G$, $(xy)^{p^{\mu-2}} = x^{p^{\mu-2}} y^{p^{\mu-2}} z$, where $z \in \Omega_1(G)$. Since $x^{p^{\mu-2}}, y^{p^{\mu-2}} \in \Omega_2(G)$ and $\exp(\Omega_2(G)) = p^2$, we get

$$\begin{aligned} (xy)^{p^{\mu-1}} &= ((xy)^{p^{\mu-2}})^p = (x^{p^{\mu-2}} y^{p^{\mu-2}} z)^p \\ &= x^{p^{\mu-1}} y^{p^{\mu-1}} z^p = x^{p^{\mu-1}} y^{p^{\mu-1}}. \end{aligned} \quad \square$$

Proposition 73.7. *Let G be a non-Hamiltonian modular group of exponent p^μ ($\mu \geq 2$). Set $|\Omega_\alpha(G) : \Omega_{\alpha-1}(G)| = p^{\omega_\alpha}$ for $\alpha = 1, \dots, \mu$. Take elements $a_1, \dots, a_{\omega_\mu}$ (of order p^μ) of G so that they form $(\text{mod } \Omega_{\mu-1}(G))$ a basis for the elementary abelian group $\Omega_\mu(G)/\Omega_{\mu-1}(G)$. Now, $a_1^p, \dots, a_{\omega_\mu}^p$ can be extended $(\text{mod } \Omega_{\mu-2}(G))$ to a basis $a_1^p, \dots, a_{\omega_\mu}^p, a_{\omega_\mu+1}, \dots, a_{\omega_{\mu-1}}$ of $\Omega_{\mu-1}(G)/\Omega_{\mu-2}(G)$ and so on. Every element of G can be written in a unique way as a product of powers of these elements a_1, a_2, \dots . In other words, the elements a_1, a_2, \dots form a basis of G . Looking at the series $\Omega_1(G), \dots, \Omega_\mu(G)$, we see that the constants $o(a_1), o(a_2), \dots$ are uniquely determined (up to the ordering). Next, if a_1, \dots, a_d is so constructed basis, then $\prod_{i=1}^d o(a_i) = |G|$.*

Proof. Working in $G/\Omega_{\mu-2}(G)$, we may assume for a moment that $\Omega_{\mu-2}(G) = \{1\}$ so that $\exp(G) = p^2$. We have to show that (commuting) elements $a_1^p, \dots, a_{\omega_\mu}^p$ are linearly independent in $\Omega_{\mu-1}(G)$ ($= \Omega_1(G) \cong E_{p^{\omega_\mu-1}}$). Indeed, if $a_1^{n_1 p} \dots a_{\omega_\mu}^{n_{\omega_\mu} p} = 1$ for some integers $n_1, \dots, n_{\omega_\mu}$, then, by Proposition 73.6, we get $(a_1^{n_1} \dots a_{\omega_\mu}^{n_{\omega_\mu}})^p = 1$, and so $a_1^{n_1} \dots a_{\omega_\mu}^{n_{\omega_\mu}} \equiv 1 \pmod{\Omega_{\mu-1}(G)}$, and we conclude that $n_i \equiv 0 \pmod{p}$. Hence $a_1^p, \dots, a_{\omega_\mu}^p$ are linearly independent in $\Omega_{\mu-1}(G)$ and so they are extendible to a basis $a_1^p, \dots, a_{\omega_\mu}^p, a_{\omega_\mu+1}, \dots, a_{\omega_{\mu-1}}$ of $\Omega_{\mu-1}(G)$ ($= \Omega_1(G)$).

Now, in general, (without assuming $\mu = 2$) we consider the elements

$$a_1^{p^2}, \dots, a_{\omega_\mu}^{p^2}, a_{\omega_\mu+1}^p, \dots, a_{\omega_{\mu-1}}^p \in \Omega_{\mu-2}(G)$$

and working in $\Omega_{\mu-1}(G)/\Omega_{\mu-3}(G)$ (of exponent p^2) we again show that these elements are linearly independent modulo $\Omega_{\mu-3}(G)$ and therefore they are extendible with elements $a_{\omega_{\mu-1}+1}, \dots, a_{\omega_{\mu-2}} \in \Omega_{\mu-2}(G)$ in such a way that

$$a_1^{p^2}, \dots, a_{\omega_\mu}^{p^2}, a_{\omega_\mu+1}^p, \dots, a_{\omega_{\mu-1}}^p, a_{\omega_{\mu-1}+1}, \dots, a_{\omega_{\mu-2}}$$

considered modulo $\Omega_{\mu-3}(G)$, form a basis of $\Omega_{\mu-2}(G)/\Omega_{\mu-3}(G)$. Then in the obvious way we continue with the construction of a “basis” a_1, a_2, \dots of G .

Since for any two “basis” elements a_i and a_j we have $\langle a_i \rangle \langle a_j \rangle = \langle a_j \rangle \langle a_i \rangle$, every element of G can be written as a product of powers of elements a_1, a_2, \dots . Moreover, each element of G can be written in a unique way as a product of powers of elements a_1, a_2, \dots (in that order). Indeed, by the construction of these elements, we have $o(a_1) \cdot o(a_2) \cdots = |G|$ and so the elements a_1, a_2, \dots form a basis of G . \square

Proposition 73.8. *Let G be a modular p -group which is not Hamiltonian. Let $a \in \Omega_1(G)^\#$ (this assumption is essential: it cannot be avoided even in the case where G is the abelian group of type (p^3, p)). Then there is a basis a_1, \dots, a_r of G such that $a \in \langle a_1 \rangle$.*

Proof. We use induction on $|G|$. Let a_1, \dots, a_r be a basis of G such that $o(a_1) \geq o(a_2) \geq \cdots \geq o(a_r)$. Let $a \in \Omega_1(G)^\#$. Set $\langle a_1, \dots, a_{r-1} \rangle = G_1$ so that G_1 is a

complement of $\langle a_r \rangle$ in G . If $a \in \Omega_1(\langle a_r \rangle)$, we are done. If $a \in G_1$, then, by induction, there is a basis b_1, \dots, b_{r-1} of G_1 such that $a \in \langle b_1 \rangle$. But then b_1, \dots, b_{r-1}, a_r is a basis of G and we are done.

It remains to consider the case $a = cd = dc$, where $c \in \Omega_1(G_1)^\#$ and $d \in \Omega_1(\langle a_r \rangle)^\#$. By induction, there is a basis c_1, \dots, c_{r-1} of G_1 such that $c \in \langle c_{r-1} \rangle$. Set $o(a_r) = p^s$. If $s = 1$, then we replace a_r with a . Since $\langle a \rangle \cap G_1 = \{1\}$ and $o(a) = o(a_r) = p$, c_1, \dots, c_{r-1}, a is a basis of G and we are done. Suppose $s \geq 2$ and replace a_r with a'_r so that $d = (a'_r)^{p^{s-1}}$. Then $c_1, \dots, c_{r-1}, a'_r$ is also a basis of G . Since $o(a_1) \geq o(a_2) \geq \dots \geq o(a_r)$ (and these numbers are invariants of G), we have also $o(c_{r-1}) \geq o(a'_r) = p^s$. Thus, there is an element $l \in \langle c_{r-1} \rangle$ of order p^s such that $l^{p^{s-1}} = c$.

Since $\langle l, a'_r \rangle$ is a modular subgroup of exponent p^s (noting that $\exp(\Omega_s(G)) \leq p^s$), it follows from Proposition 73.6 that $(la'_r)^{p^{s-1}} = l^{p^{s-1}}(a'_r)^{p^{s-1}} = cd = a$, and so $o(la'_r) = o(a'_r) = p^s$. On the other hand, $\langle c_1, \dots, c_{r-1}, la'_r \rangle = G$ and $G_1 \cap \langle la'_r \rangle = \{1\}$. Hence $c_1, \dots, c_{r-1}, la'_r$ is a basis of G and $a \in \langle la'_r \rangle$. \square

Proposition 73.9. *Let G be a modular p -group which is not Hamiltonian. If $|G'| = p$, then $G = G_1 \times G_2$, where $G_1 = \langle a_1, a_2 | a_1^{p^m} = a_2^{p^n} = 1, a_1^{a_2} = a_1^{1+p^{m-1}}, m > 1, n \geq 1 \rangle$ and G_2 is abelian of exponent $\leq p^{m-1}$ with $m > 2$ if $p = 2$. Hence $A = \langle a_1, G_2 \rangle$ is an abelian normal subgroup of $G = \langle A, a_2 \rangle$ and $a^{a_2} = a^{1+p^{m-1}}$ for all $a \in A$.*

Proof. By Proposition 73.8, we may choose a basis a_1, a_2, \dots, a_s of G so that $G' \leq \langle a_1 \rangle$. Since $\langle a_i, a_j \rangle \cap G' \leq \langle a_i, a_j \rangle \cap \langle a_1 \rangle = 1$ ($i, j > 1$), we see that $\langle a_2, \dots, a_s \rangle$ is abelian. Let a_2 be an element of the smallest order among those basis elements a_2, \dots, a_s which do not commute with a_1 . By Lemma 65.2(a), $\langle a_1, a_2 \rangle$ is minimal nonabelian. So, in view of Lemma 65.1, we may put $[a_1, a_2] = z$, where $z = a_1^{p^{m-1}}$ and $o(a_1) = p^m$, $m \geq 2$. (We get $\langle a_1 \rangle \neq G'$ since G is nonabelian.)

We have $[a_1, a_i] = z^{k_i}$ with $k_i \in \{0, 1, \dots, p-1\}$ ($i > 2$), where (by assumption) $o(a_i) \geq o(a_2)$ whenever $k_i \neq 0$. Then we replace the basis elements a_3, \dots, a_s with the elements $a_2^{-k_i} a_i = b_i$ ($3 \leq i \leq s$). We have $o(b_i) = o(a_i)$ and

$$[a_1, b_i] = [a_1, a_2^{-k_i} a_i] = [a_1, a_2]^{-k_i} [a_1, a_i] = z^{-k_i} z^{k_i} = 1$$

and so the abelian subgroup $\langle b_3, \dots, b_s \rangle$ centralizes $\langle a_1, a_2 \rangle$. It is clear that $\{a_1, a_2, b_3, \dots, b_s\}$ is also a basis of G . Indeed, $\langle a_1, a_2, b_3, \dots, b_s \rangle = G$ and

$$|G| = o(a_1)o(a_2)o(a_3)\dots o(a_s) = o(a_1)o(a_2)o(b_3)\dots o(b_s).$$

Denoting b_3, \dots, b_s again with a_3, \dots, a_s , we may assume from the start that $G = G_1 \times G_2$, where $G_1 = \langle a_1, a_2 \rangle$ and $G_2 = \langle a_3, \dots, a_s \rangle$.

For $i \geq 3$ we have

$$(a_1 a_i)^{a_2} = a_1^{a_2} a_i = (a_2^{-1} a_1 a_2) a_i = a_1 (a_1^{-1} a_2^{-1} a_1 a_2) a_i = a_1 z a_i = z (a_1 a_i).$$

Now, $(G' \leq) A = \langle a_1, a_3, \dots, a_s \rangle \triangleleft G$, $G = A\langle a_2 \rangle$, and $A \cap \langle a_2 \rangle = \{1\}$. Consider the subgroup $H = \langle a_1 a_i, a_2 \rangle$ ($i > 2$) which is nonabelian. Since $H = \langle a_1 a_i \rangle \langle a_2 \rangle$ and $\langle a_1 a_i \rangle \leq A$, we have $H \cap A = \langle a_1 a_i \rangle$ and so a_2 normalizes $\langle a_1 a_i \rangle$. Thus $(a_1 a_i)^{a_2} = z(a_1 a_i) = (a_1 a_i)^x$ (x integer) and so $z = a_1^{p^{m-1}} \in \langle a_1 a_i \rangle$. This implies that the order of a_i ($i > 2$) is at most p^{m-1} .

For each $a \in A$, we have $a = a_1^r b$ with an integer r and $b \in G_2$ so that

$$\begin{aligned} a^{a_2} &= (a_1^r b)^{a_2} = (a_1^{1+p^{m-1}})^r b = (a_1^r)^{1+p^{m-1}} b^{1+p^{m-1}} \\ &= (a_1^r b)^{1+p^{m-1}} = a^{1+p^{m-1}}. \end{aligned}$$

If $p = 2$ and $m = 2$, then $K = \langle a_1, a_2 \mid a_1^4 = a_2^{2^n} = 1, a_1^{a_2} = a_1^3 = a_1^{-1} \rangle$ is not modular, since $K/\langle a_2^{2^{n-1}} \rangle \cong D_8$. Hence, if $p = 2$, then $m > 2$. Our proposition is proved. \square

Proposition 73.10. *Let G be a modular p -group which is not Hamiltonian. Then each subgroup and each factor group is modular and is not Hamiltonian.*

Subgroups and epimorphic images of modular p -groups are modular so the assertion follows since, by Theorem A.24.4, G is Q₈-free.

Proposition 73.11. *Let $t, x \in G$, where $\exp(G) = p^\mu$. If $x^t = x^{1+p^s} z$, where $z \in \Omega_1(Z(G))^\#$ and $1 \leq s < \mu - 1$ is a natural number which is ≥ 2 if $p = 2$, then $x^{t^{p^{\mu-1-s}}} = x^{1+p^{\mu-1}}$. In particular, if $o(x) \leq p^{\mu-1}$, then $[x, t^{p^{\mu-1-s}}] = 1$.*

Proof. By induction on i , we first prove that $x^{t^i} = x^{(1+p^s)^i} z^i$. Indeed, we have

$$x^{t^{i+1}} = (x^{(1+p^s)^i} z^i)^t = (x^{1+p^s} z)^{(1+p^s)^i} z^i = x^{(1+p^s)^{i+1}} z^{i+1}.$$

This gives $x^{t^{p^{\mu-1-s}}} = x^{(1+p^s)^{p^{\mu-1-s}}}$, since $s < \mu - 1$ and so $z^{p^{\mu-1-s}} = 1$.

It remains to prove the following congruence:

$$(1) \quad (1 + p^s)^{p^{\mu-1-s}} \equiv 1 + p^{\mu-1} \pmod{p^\mu}.$$

According to P. Roquette, everything depends on the following formula:

$$(2) \quad (a + bp^s)^p \equiv a^p + a^{p-1}bp^{s+1} \pmod{p^{s+2}},$$

where a, b are integers, p prime, $s \geq 1$ and, if $p = 2$, then $s \geq 2$. Indeed, we get

$$(3) \quad (a + bp^s)^p = a^p + pa^{p-1}bp^s + \sum_{2 \leq i \leq p-1} \binom{p}{i} a^{p-i} b^i p^{si} + b^p p^{sp}.$$

Therefore each member of the above sum is $\equiv 0 \pmod{p^{1+si}}$ and so $\equiv 0 \pmod{p^{s+2}}$ since $1 + si \geq s + 2$ in view of $i \geq 2$. For the last term on the right-hand side of (3)

we have $sp \geq s + 2$ for $p \geq 3$ and this holds also for $p = 2$ because in that case we have assumed $s \geq 2$. Thus, the last term is also $\equiv 0 \pmod{p^{s+2}}$, and (2) is proven.

It follows from (2) that

$$(4) \quad z \equiv 1 + p^s \pmod{p^{s+1}} \text{ implies } z^p \equiv 1 + p^{s+1} \pmod{p^{s+2}}.$$

To prove (4) we set $z = 1 + p^s + bp^{s+1} = a + bp^{s+1}$, where $a = 1 + p^s$ and b is an integer. From (2) follows (with $s + 1$ instead of s and noting that always $s + 1 \geq 2$) $z^p = (a + bp^{s+1})^p \equiv a^p + a^{p-1}bp^{s+2} \pmod{p^{s+3}}$ and so $z^p \equiv a^p \equiv (1 + p^s)^p \pmod{p^{s+2}}$. Again using (2) (for $a = b = 1$), we get $(1 + p^s)^p \equiv 1 + p^{s+1} \pmod{p^{s+2}}$, proving (4).

With iteration we get from (4) (with $k = 1, 2, 3, \dots$)

$$(5) \quad z \equiv 1 + p^s \pmod{p^{s+1}} \text{ implies } z^{p^k} \equiv 1 + p^{s+k} \pmod{p^{s+k+1}}.$$

If we set in (5) $z = 1 + p^s$, $k = \mu - 1 - s$, where $s < \mu - 1$, we get (1). \square

Proposition 73.12. *Let G be a non-Hamiltonian modular p -group. Then each element of $\mathfrak{V}_i(G)$ ($i \geq 1$) can be written as a^{p^i} for some $a \in G$.*

Proof. We prove first this result for $i = 1$, working by induction on $|G|$. Let $x \in \mathfrak{V}_1(G)$ so that $x = a_1^{p^1}a_2^{p^1} \dots a_s^{p^1}$ with some $a_i \in G$. Now, $G/\mathfrak{V}_2(G)$ is of exponent p^2 and so, using Proposition 73.6, we get $x = (a_1a_2 \dots a_s)^{p^1}l$ where $l \in \mathfrak{V}_2(G)$. We set $a_1a_2 \dots a_s = b$, $H = \langle b, \mathfrak{V}_1(G) \rangle$, and $l = c_1^{p^2}c_2^{p^2} \dots c_r^{p^2}$ with some $c_1, c_2, \dots, c_r \in G$. Thus $x = b^{p^1}(c_1^{p^1})^{p^1} \dots (c_r^{p^1})^{p^1} \in \mathfrak{V}_1(H)$. We have $H \neq G$, unless G is cyclic, so $x = a^p$ for some $a \in H$, by induction.

Assume that $i > 1$ and use induction on i . Let $y \in \mathfrak{V}_i(G)$ so that $y = b_1^{p^{i-1}} \dots b_t^{p^{i-1}} = (b_1^{p^{i-1}})^p \dots (b_t^{p^{i-1}})^p$ for some $b_1, \dots, b_t \in G$. Here $b_j^{p^{i-1}} \in \mathfrak{V}_{i-1}(G)$, $j = 1, \dots, t$, so $y \in \mathfrak{V}_1(\mathfrak{V}_{i-1}(G))$. By the above, $y = c^p$ with $c \in \mathfrak{V}_{i-1}(G)$. By induction, $c = d^{p^{i-1}}$ and so $y = d^{p^i}$. \square

Proposition 73.13. *Let G be a non-Hamiltonian modular p -group. If we have $G = \langle a_1, \dots, a_r \rangle$, then $\mathfrak{V}_i(G) = \langle a_1^{p^i}, \dots, a_r^{p^i} \rangle$.*

Proof. One may assume that $\{a_i\}_1^r$ is a minimal basis. First let $i = 1$. We have $\langle a_1 \rangle \dots \langle a_r \rangle = G$ so by the product formula applied $r-1$ times, $|G : \langle a_1^p \rangle \dots \langle a_r^p \rangle| = p^r$. Since $p^r = |G : \Phi(G)| = |G : \mathfrak{V}_1(G)|$, we are done.

Suppose that $i > 2$. By induction on i , $\mathfrak{V}_{i-1}(G) = \langle a_1^{p^{i-1}}, \dots, a_r^{p^{i-1}} \rangle$. If $y \in \mathfrak{V}_{i-1}(G)$, then $y = a^{p^{i-1}}$, $a \in G$ (Proposition 73.12) and so $y^p = a^{p^i} \in \mathfrak{V}_i(G)$. This gives $\mathfrak{V}_1(\mathfrak{V}_{i-1}(G)) \leq \mathfrak{V}_i(G)$. On the other hand, if $g \in \mathfrak{V}_i(G)$, then by Proposition 73.12, $g = b^{p^i} = (b^{p^{i-1}})^p$, $b \in G$, and so $g \in \mathfrak{V}_1(\mathfrak{V}_{i-1}(G))$ which gives $\mathfrak{V}_i(G) = \mathfrak{V}_1(\mathfrak{V}_{i-1}(G))$. By the above, this gives $\mathfrak{V}_i(G) = \langle a_1^{p^i}, \dots, a_r^{p^i} \rangle$. \square

Proposition 73.14 (compare with [Sch, Lemma 2.3.4]). *Let G be a p -group and let $A \triangleleft G$ be abelian and such that $G/A = \langle tA \rangle$ is cyclic, all subgroups of A are normal in G and, if $p = 2$, when $\Omega_2(A) \leq Z(G)$. Then G is modular.*

Proof. Suppose that G is a counterexample of minimal order. Then, by induction, $H < G$ is modular since $H/(H \cap A) \cong AH/A(\leq G/A)$ is cyclic and H satisfies the hypothesis with respect to $H \cap A$. Hence, G is minimal nonmodular. Then, by Theorem 44.18, there exists $N \triangleleft G$ with $G/N \in \{D_8, S(p^3)\}$. Since G/AN is a cyclic epimorphic image of G/N , we have $|G : AN| \leq p$. But every subgroup of AN/N is normal in G/N , and this implies that $p = 2$ and AN/N is the cyclic subgroup of order 4 in $G/N \cong D_8$. Hence $A/(A \cap N) \cong C_4$ so $A = (A \cap N)\langle u \rangle$, and A is modular, by the above. Let $G = A\langle v \rangle$. Then $G = \langle u, v \rangle$ since $\langle u, v \rangle$ is nonmodular since it has an epimorphic image $\cong D_8$. Since $v^2 \in A$, $\phi : u \rightarrow u^v$ is an automorphism of order 2. Let $o(u) = 2^m$, $o(v) = 2^n$. By Theorem 1.2, we have to consider one of the following three possibilities:

- (i) $u^v = u^{-1}$. Then $u^{2^{m-2}} = (u^{2^{m-2}})^v = u^{-2^{m-2}}$ so $u^{2^{m-1}} = 1$, a contradiction.
- (ii) $u^v = u^{-1+2^{m-1}}$, $m > 2$. Then $u^{2^{m-2}} = (u^{2^{m-2}})^v = u^{2^{m-2}(-1+2^{m-1})}$ so $u^{2^{m-1}(-1+2^{m-2})} = 1$, a contradiction.
- (iii) $u^v = u^{1+2^{m-1}}$, $m > 2$, i.e., $G \cong M_{2^{m+1}}$. In that case, G is modular, contrary to the assumption. \square

Theorem 73.15 ([Iwa]). *A non-Hamiltonian p -group G is modular if and only if it contains an abelian normal subgroup N with cyclic quotient group G/N and there exists an element t in G with $G = \langle N, t \rangle$ and a positive integer s which is at least 2 in the case $p = 2$ such that $a^t = a^{1+p^s}$ for all $a \in N$.*

Proof (Iwasawa–Napolitani–Janko). If G is as in the theorem, it is modular, by Proposition 73.14.

Suppose, conversely, that G is a modular p -group which is not Hamiltonian. This property is inherited by sections (Proposition 73.10), so we may assume that the theorem is true for groups of smaller order. By Proposition 73.6, the mapping $g \mapsto g^{p^{\mu-1}}$, where $p^\mu = \exp(G)$, is a homomorphism of G . The image of this homomorphism is $\mathfrak{V}_{\mu-1}(G) \neq 1$. There is a G -invariant subgroup $Z = \langle z \rangle$ of order p in $\mathfrak{V}_{\mu-1}(G)$. By induction, G/Z contains an abelian normal subgroup N/Z with properties stated in the theorem. There is an element $t \in G$ such that $G = \langle N, t \rangle$ and $a^t = a^{1+p^s}z^k$ for all $a \in N$, where $k \in \mathbb{N} \cup \{0\}$ depends on a .

There are two major possibilities for the structure of N . The subgroup N is either (I) abelian or (II) nonabelian.

Case (I). N is abelian. Here $z \in \mathfrak{V}_{\mu-1}(G)$ is the $p^{\mu-1}$ -th power of an element c in G , $z = c^{p^{\mu-1}}$. There are two possibilities for the position of c in G .

(α) It is possible to choose $c \in N$.

Since $o(c) = p^\mu$, c is an element of a basis of G (Proposition 73.7). In particular, $\langle c \rangle$ has a complement T in G which is generated by remaining elements of those basis of G that contains c . We have $G = T\langle c \rangle$ with $T \cap \langle c \rangle = \{1\}$ and so $N = (T \cap N) \times \langle c \rangle$, by the modular law, and T covers G/N since $TN \leq T\langle c \rangle = G$. The quotient group $T/(T \cap N) \cong G/N$ is cyclic, and we choose $t_1 \in T \cap (Nt)$ so that $T = \langle T \cap N, t_1 \rangle$; then $G = \langle N, t_1 \rangle$. Since $t^{-1}t_1 \in N$ and N is abelian, t and t_1 induce the same automorphism on N . In view of $Z \cap T = \{1\}$, we have $a^t = a^{t_1} = a^{1+p^s}$ for all $a \in T \cap N$.

If also $c^t = c^{1+p^s}$, then the fact that $N = (T \cap N) \times \langle c \rangle$ is abelian implies $x^t = x^{1+p^s}$ for all $x \in N$ and the theorem is proved. Therefore assume that $c^t = c^{1+p^s}z^k = c^{1+p^s+kp^{\mu-1}}$, where $k \not\equiv 0 \pmod{p}$. We may assume that $k \in \{1, 2, \dots, p-1\}$ and so $p-k \in \{1, 2, \dots, p-1\}$.

We claim that $\mathfrak{V}_{\mu-1}(T \cap N) = \{1\}$. Otherwise, there is $a \in T \cap N$ of order p^μ . We have $\langle a \rangle \cap \langle c \rangle = \{1\}$ and $\langle ca \rangle \cap \langle c \rangle = \{1\}$. Both elements ca and c are of order p^μ and they, clearly, are “linearly independent” modulo $\Omega_{\mu-1}(G)$. Hence, by the process of constructing a basis of G in Proposition 73.7, there is a basis of G containing both c and ca . Let T_1 be a complement of $\langle c \rangle$ in G containing ca . By the preceding argument, $(ca)^t = (ca)^{1+p^s}$ and so $(ca)^t = c^t a^t = c^t a^{1+p^s} = c^{1+p^s} a^{1+p^s}$, which gives $c^t = c^{1+p^s}$, contrary to what has been assumed in the previous paragraph.

We have proved that $\mathfrak{V}_{\mu-1}(T \cap N) = \{1\}$ or, what is the same, $\exp(T \cap N) \leq p^{\mu-1}$. Hence, if $s \geq \mu-1$, then $G/\langle z \rangle$ is abelian. Assuming that G is nonabelian (otherwise, there is nothing to prove), we conclude that $G' = \langle z \rangle$ is of order p and so Proposition 73.9 implies the validity of the theorem.

It remains to examine the case $s < \mu-1$ (and $s \geq 2$ for $p=2$). We use Proposition 73.11 and get $x^{t^{p^{\mu-1-s}}} = x^{1+p^{\mu-1}}$, whenever $x^t = x^{1+p^z}z'$ with $z' \in Z$. From this relation we get, iterating $(p-k)$ times,

$$\begin{aligned} x^{t^{(p-k)p^{\mu-1-s}}} &= x^{(t^{p^{\mu-1-s}})^{p-k}} = x^{(1+p^{\mu-1})^{p-k}} \\ &= x^{1+(p-k)p^{\mu-1} + \binom{p-k}{2}p^{2(\mu-1)} + \dots} = x^{1-kp^{\mu-1}}. \end{aligned}$$

Thus, setting $t^* = t^{1+(p-k)p^{\mu-1-s}}$, we get

$$\begin{aligned} c^{t^*} &= c^{t^{(p-k)p^{\mu-1-s}} \cdot t} = (c^{1-kp^{\mu-1}})^t = (c^t)^{(1-kp^{\mu-1})} \\ &= (c^{1+p^s+kp^{\mu-1}})^{(1-kp^{\mu-1})} = c^{1+p^s+kp^{\mu-1}-kp^{\mu-1}-kp^{\mu-1+s}-k^2p^{2\mu-2}} \\ &= c^{1+p^s}. \end{aligned}$$

Finally, for each $a \in T \cap N$ (noting that $a^{p^{\mu-1}} = 1$ holds) we obtain also $a^{t^*} = (a^{t^{(p-k)p^{\mu-1-s}}})^t = (a^{1-kp^{\mu-1}})^t = a^t = a^{1+p^s}$. Thus $y^{t^*} = y^{1+p^s}$ for each $y \in N$. Since $G = \langle N, t^* \rangle$, we are done.

(β) **It is not possible to choose c in N .**

We claim that $\langle c, N \rangle = G$. Indeed, if $\langle c, N \rangle < G$, then we can choose a generator t_1 of $\langle t \rangle$ such that $t_1^{p^h} \equiv c \pmod{N}$ with $h > 0$. Hence $c = bt_1^{p^h}$, where $b \in N$. It follows $b = ct_1^{-p^h}$ and then applying Proposition 73.6 we get $b^{p^{\mu-1}} = (ct_1^{-p^h})^{p^{\mu-1}} = c^{p^{\mu-1}}t_1^{-p^{h+\mu-1}} = c^{p^{\mu-1}} = z$, where $b \in N$ and $o(b) = p^\mu$, a contradiction.

It follows that a suitable generator c_0 of $\langle c \rangle$ operates on N in the same way as t and so we may assume that c itself operates on N as t . In what follows we shall identify t and c . This means that we shall assume that $o(t) = p^\mu$, $t^{p^{\mu-1}} = z$, and so for each $a \in N$ we have $a^t = a^{1+p^s}t^{kp^{\mu-1}}$ with $k \in \{0, 1, \dots, p-1\}$ depending on a .

Let $\{a_1, a_2, \dots, a_r\}$ be a basis of N such that $Z = \langle z \rangle \leq \langle a_1 \rangle$ (such a basis exists by Proposition 73.8). For each a_i , $i = 1, 2, \dots, r$, we have either $a_i^t = a_i^{1+p^s}$ or $a_i^t = a_i^{1+p^s}t^{k_i p^{\mu-1}}$, $k_i \not\equiv 0 \pmod{p}$.

We shall prove that it is possible to assume that $a_i^t = a_i^{1+p^s}$ for $i \geq 3$. For this purpose, we order the basis elements a_2, \dots, a_r so that:

(1 β) there exists v such that $a_i^t = a_i^{1+p^s}$ if and only if $i = v+1, \dots, r$;

(2 β) if $v > 1$, then $o(a_2) \leq o(a_j)$ for each j with $2 \leq j \leq v$.

If $v \leq 2$, the above statement is obviously true. Supposing $v > 2$, we observe that for each i , $2 \leq i \leq v$, $\{a_2, a_2^q a_i\}$ (q integer) is a basis of $\langle a_2, a_i \rangle$. Since

$$\begin{aligned} (a_2^q a_i)^t &= (a_2^t)^q a_i^t = (a_2^{1+p^s} t^{k_2 p^{\mu-1}})^q (a_i^{1+p^s})^{k_i p^{\mu-1}} \\ &= (a_2^q)^{1+p^s} t^{k_2 q p^{\mu-1}} a_i^{1+p^s} t^{k_i p^{\mu-1}} = (a_2^q a_i)^{1+p^s t^{(k_2 q+k_i)p^{\mu-1}}} \end{aligned}$$

and $k_2 \not\equiv 0 \pmod{p}$, we can solve the congruence equation $k_2 q + k_i \equiv 0 \pmod{p}$, in $q = q_i$ (depending on i) so that $(a_2^{q_i} a_i)^t = (a_2^{q_i} a_i)^{1+p^s}$. Hence the set $\{a_1, a_2, a_2^{q_3} a_3, \dots, a_2^{q_v} a_v, a_{v+1}, \dots, a_r\}$ is a basis with the desired property.

We consider first the following special possibility:

(β_1) $a_2^t = a_2^{1+p^s} t^{k_2 p^{\mu-1}}$, $k_2 \not\equiv 0 \pmod{p}$, $a_2^{p^{\mu-1}} \neq 1$, and $a_i^{p^{\mu-1}} = 1$ for all $i \geq 3$. We shall prove that in this case either the theorem holds or we can choose our abelian normal subgroup $N = \langle a_1, a_2, \dots, a_r \rangle$ in such a way that also $a_2^t = a_2^{1+p^s}$. Here we distinguish two subcases (i) $s \geq \mu - 1$ and (ii) $s < \mu - 1$.

(i) $s \geq \mu - 1$. If $a_1^t = a_1^{1+p^s} t^{k_1 p^{\mu-1}}$ with $k_1 \not\equiv 0 \pmod{p}$, then we multiply a_2 with $a_1^{\bar{q}}$, where \bar{q} is a solution of the congruence equation $k_1 \bar{q} + k_2 \equiv 0 \pmod{p}$ and we replace the basis $\{a_1, a_2, \dots, a_r\}$ of N with the basis $\{a_1, \hat{a}_2 = a_1^{\bar{q}} a_2, a_3, \dots, a_r\}$ noting that $o(a_1) \leq p^{\mu-1}$ (since in our case (β), $z \leq \langle a_1 \rangle$ is not a $p^{\mu-1}$ -th power of

any element in N). Then we compute

$$\begin{aligned} (\hat{a}_2)^t &= (a_1^{\bar{q}} a_2)^t = (a_1^{1+p^s} t^{k_1 p^{\mu-1}})^{\bar{q}} a_2^{1+p^s} t^{k_2 p^{\mu-1}} \\ &= a_1^{\bar{q}(1+p^s)} a_2^{1+p^s} t^{(k_1 \bar{q} + k_2) p^{\mu-1}} = (a_1^{\bar{q}} a_2)^{1+p^s} = (\hat{a}_2)^{1+p^s}, \end{aligned}$$

as required. If, however, $a_1^t = a_1^{1+p^s} = a_1$ (noting that $s \geq \mu - 1$ and $a_1^{p^{\mu-1}} = 1$), then $G' = \langle t^{p^{\mu-1}} \rangle$ or $G' = \langle a_2^{p^{\mu-1}} t^{k_2 p^{\mu-1}} \rangle$ depending whether $s > \mu - 1$ or $s = \mu - 1$. Here we have also used our assumption that $a_i^{p^{\mu-1}} = 1$ and the fact that $a_i^t = a_i^{1+p^s}$ for all $i \geq 3$. But then our theorem follows from Proposition 73.9.

(ii) $s < \mu - 1$. We replace here the subgroup N with the subgroup $N^* = \langle a_1, a_2^*, a_3, \dots, a_r \rangle$, where $a_2^* = a_2^\alpha t^{p^{\mu-1-s}}$ with α being a solution of the congruence $\alpha k_2 \equiv 1 \pmod{p}$. Note that $\alpha \not\equiv 0 \pmod{p}$ and $t^{\alpha k_2 p^{\mu-1}} = t^{p^{\mu-1}} = z$. We note that $t^{k_2 p^{\mu-1}} = z^{k_2} \in Z(G)$ and $a_2^{p^s}$ ($s \geq 1$) is of order $\leq p^{\mu-1}$ and therefore $a_2^{p^s}$ and $t^{p^{\mu-1-s}}$ commute (Proposition 73.11). Then we compute

$$\begin{aligned} (a_2^*)^t &= (a_2^\alpha t^{p^{\mu-1-s}})^t = (a_2^t)^\alpha t^{p^{\mu-1-s}} = (a_2^{1+p^s} t^{k_2 p^{\mu-1}})^\alpha t^{p^{\mu-1-s}} \\ &= a_2^{\alpha(1+p^s)} t^{\alpha k_2 p^{\mu-1}} t^{p^{\mu-1-s}} = a_2^\alpha a_2^{\alpha p^s} t^{p^{\mu-1}} t^{p^{\mu-1-s}} \\ &= a_2^\alpha a_2^{\alpha p^s} t^{p^{\mu-1-s}} (t^{p^{\mu-1-s}})^{p^s} = (a_2^\alpha t^{p^{\mu-1-s}})(a_2^{\alpha p^s} (t^{p^{\mu-1-s}})^{p^s}). \end{aligned}$$

The subgroup $H = \langle a_2, t^{p^{\mu-1-s}} \rangle$ is of class 2. Indeed, by Proposition 73.11, $a_2^{t^{p^{\mu-1-s}}} = a_2^{1+p^{\mu-1}}$ and so $H' = \langle a_2^{p^{\mu-1}} \rangle$ is of order p . Therefore,

$$\begin{aligned} (a_2^*)^{p^s} &= (a_2^\alpha t^{p^{\mu-1-s}})^{p^s} = a_2^{\alpha p^s} (t^{p^{\mu-1-s}})^{p^s} [t^{p^{\mu-1-s}}, a_2]^{p^s \choose 2} \\ &= a_2^{\alpha p^s} (t^{p^{\mu-1-s}})^{p^s}, \end{aligned}$$

since (in any case) p divides ${p^s \choose 2}$. Substituting this last result in the above relation, we get $(a_2^*)^t = a_2^*(a_2^*)^{p^s} = (a_2^*)^{1+p^s}$.

The subgroup N^* is abelian. Indeed, $t^{p^{\mu-1-s}}$ commutes with each a_i , $i \neq 2$, because each such a_i is of order $\leq p^{\mu-1}$ (Proposition 73.11). Also, $G = \langle N^*, t \rangle$, $(N^*)^t = N^*$, and so N^* is normal in G with G/N^* cyclic. We observe that a_2 is of order p^μ and so $\langle a_2^* \rangle \cap \langle a_1, a_3, \dots, a_r \rangle = \{1\}$, which implies that $\{a_1, a_2^*, a_3, \dots, a_r\}$ is a basis of N^* . Indeed, by Proposition 73.6, $(a_2^*)^{p^{\mu-1}} = (a_2^\alpha t^{p^{\mu-1-s}})^{p^{\mu-1}} = (a_2^{p^{\mu-1}})^\alpha t^{p^{2\mu-2-s}} = a_2^{\alpha p^{\mu-1}}$ is an element of order p ($\alpha \not\equiv 0 \pmod{p}$) and $\langle a_2^{\alpha p^{\mu-1}} \rangle \cap \langle a_1, a_3, \dots, a_r \rangle = \{1\}$, where we have used the fact that $2\mu - 2 - s \geq \mu$. All the statements in case (β_1) are proved. Indeed, a_2^* is of order p^μ , all other basis elements a_i of N^* are of order $\leq p^{\mu-1}$ and so $\mathfrak{U}_{\mu-1}(N^*) = \langle a_2^{p^{\mu-1}} \rangle$ is of order p . Hence $z \in \langle a_1 \rangle$ cannot be a $p^{\mu-1}$ -th power of any element of N^* .

In view of what was proved so far in the case (β) , it remains to consider the following two possibilities:

(β_2) There exists an a_i , $i \geq 2$, such that $a_i^{p^{\mu-1}} \neq 1$ and $a_i^t = a_i^{1+p^s}$.

(β_3) All a_i are of order $\leq p^{\mu-1}$ and, in addition, $a_j^t = a_j^{1+p^s}$ for $j \geq 3$. (We are in case (β) and so also a_1 is of order $\leq p^{\mu-1}$ since $z \in \langle a_1 \rangle$ and z is not a $p^{\mu-1}$ -th power of any element in N .)

Assume that the condition (β_2) is satisfied. Hence there exists an $a_{\underline{i}}$, $\underline{i} \geq 2$, such that $a_{\underline{i}}^t = a_{\underline{i}}^{1+p^s}$ and $a_{\underline{i}}^{p^{\mu-1}} \neq 1$. Here $t^{p^{\mu-1}} = z \in \langle a_1 \rangle$ and therefore $\langle t \rangle \cap \langle a_{\underline{i}} \rangle = \{1\}$. Since $t^{p^{\mu-1}} \neq 1$ and $a_{\underline{i}}^{p^{\mu-1}} \neq 1$, we get $(ta_{\underline{i}})^{p^{\mu-1}} = t^{p^{\mu-1}}a_{\underline{i}}^{p^{\mu-1}} \neq 1$ so $\langle ta_{\underline{i}} \rangle \cap \langle a_{\underline{i}} \rangle = \{1\}$. It follows that elements $a_{\underline{i}}$, $ta_{\underline{i}}$ are contained in a basis of G since $a_{\underline{i}}$ and $ta_{\underline{i}}$ are both of order p^μ and they are “linearly independent” mod $\Omega_{\mu-1}(G)$ (see the proof of Proposition 73.7). Therefore, there exists a complement T of $\langle a_{\underline{i}} \rangle$ in G containing $ta_{\underline{i}}$. We have $N = (N \cap T) \times \langle a_{\underline{i}} \rangle$ and $ta_{\underline{i}}$ operates in the same way as t on $N \cap T$. If $ta_{\underline{i}}$ does not transform each element of $N \cap T$ into its $(1 + p^s)$ -th power, then there exists $\bar{a} \in N \cap T$ such that $\bar{a}^{ta_{\underline{i}}} = \bar{a}^t = \bar{a}^{1+p^s}t^{\bar{k}p^{\mu-1}}$ with $\bar{k} \not\equiv 0 \pmod{p}$, and so $t^{p^{\mu-1}} \in T$. Since $(ta_{\underline{i}})^{p^{\mu-1}} = t^{p^{\mu-1}}a_{\underline{i}}^{p^{\mu-1}} \in T$, it follows that $a_{\underline{i}}^{p^{\mu-1}} \in T$, a contradiction. Hence $a^t = a^{1+p^s}$ for each $a \in T \cap N$ and $a_{\underline{i}}^t = a_{\underline{i}}^{1+p^s}$. But $N = (T \cap N) \times \langle a_{\underline{i}} \rangle$ is abelian and so $x^t = x^{1+p^s}$ for all $x \in N$ and we are done.

Assume, finally, that the condition (β_3) is satisfied. We distinguish here two subcases: (i) $s < \mu - 1$ and (ii) $s \geq \mu - 1$.

(i) Suppose that $s < \mu - 1$. If $a_1^t = a_1^{1+p^s}t^{k_1p^{\mu-1}}$, $k_1 \not\equiv 0 \pmod{p}$ and $a_i^t = a_i^{1+p^s}$ for $i \geq 2$, then we replace a_1 with $a_1^* = a_1^\alpha t^{p^{\mu-1-s}}$, where α is such that $\alpha k_1 \equiv 1 \pmod{p}$. Applying Proposition 73.11, we prove that $N^* = \langle a_1^*, a_2, \dots, a_r \rangle$ is an abelian normal subgroup of G with $G = \langle N^*, t \rangle$, $(a_1^*)^t = (a_1^*)^{1+p^s}$, and $a_i^t = a_i^{1+p^s}$ for $i \geq 2$ (where $\{a_1^*, a_2, \dots, a_r\}$ is not necessarily a basis of N^*). Indeed, $t^{p^{\mu-1-s}}$ commutes with each a_i , $i = 1, \dots, r$, and so N^* is abelian. It remains to compute

$$\begin{aligned} (a_1^*)^t &= (a_1^\alpha t^{p^{\mu-1-s}})^t = (a_1^t)^\alpha t^{p^{\mu-1-s}} = (a_1^{1+p^s}t^{k_1p^{\mu-1}})^\alpha t^{p^{\mu-1-s}} \\ &= (a_1^\alpha)^{1+p^s}t^{\alpha k_1 p^{\mu-1}}t^{p^{\mu-1-s}} = (a_1^\alpha)^{1+p^s}t^{p^{\mu-1}}t^{p^{\mu-1-s}} \\ &= (a_1^\alpha)^{1+p^s}(t^{p^{\mu-1-s}})^{1+p^s} = (a_1^\alpha t^{p^{\mu-1-s}})^{1+p^s} = (a_1^*)^{1+p^s}. \end{aligned}$$

If $a_2^t = a_2^{1+p^s}t^{k_2p^{\mu-1}}$ with $k_2 \not\equiv 0 \pmod{p}$, then we replace a_2 with $a_2^* = a_2^\alpha t^{p^{\mu-1-s}}$, where α is such that $\alpha k_2 \equiv 1 \pmod{p}$. Applying Proposition 73.11 again, we see that $N^* = \langle a_1, a_2^*, a_3, \dots, a_r \rangle$ is an abelian normal subgroup of G with $G = \langle N^*, t \rangle$ (where $\{a_1, a_2^*, a_3, \dots, a_r\}$ is not necessarily a basis of N^*). It remains

only to compute

$$\begin{aligned}(a_2^*)^t &= (a_2^\alpha t^{p^{\mu-1-s}})^t = a_2^{\alpha(1+p^s)} t^{\alpha k_2 p^{\mu-1}} t^{p^{\mu-1-s}} \\ &= a_2^{\alpha(1+p^s)} t^{p^{\mu-1}} t^{p^{\mu-1-s}} = (a_2^\alpha t^{p^{\mu-1-s}})^{1+p^s} = (a_2^*)^{1+p^s}.\end{aligned}$$

Then our theorem either holds or we have the case considered already in the previous paragraph (noting that the order of a_2^* is $\leq p^{\mu-1}$).

(ii) Suppose that $s \geq \mu - 1$. Since $o(a_i) \leq p^{\mu-1}$ for all i , then G is either abelian or $G' = \langle z \rangle = Z$ is of order p . Then the theorem follows from Proposition 73.9.

Case (II). N is nonabelian. The idea here is to reduce this case to Case (I). By Proposition 73.9, N has the following structure. There is a basis $\{a_1, a_2, \dots, a_r\}$ of N such that

$$\begin{aligned}a_1^{p^m} &= a_2^{p^n} = 1, \quad m > 1, n \geq 1, & a_1^{a_2} &= a_1^{1+p^{m-1}}, \\ a_i a_j &= a_j a_i \quad \text{for } i, j \geq 3, & a_i^{p^{m-1}} &= 1 \quad \text{for } i \geq 3, \\ N &= \langle a_1, a_2 \rangle \times \langle a_3, \dots, a_r \rangle, & \text{and if } p = 2, \text{ then } m > 2.\end{aligned}$$

Here $Z = \langle a_1^{p^{m-1}} \rangle = N' \leq Z(G)$ and, for each $a \in N$, we have $a^t = a^{1+p^s} a_1^{kp^{m-1}}$, where $k \pmod{p}$ depends on a .

Replacing t by a suitable $ta_1^\alpha a_2^\beta$ (α and β are integers \pmod{p}), we may assume

$$(6) \quad a_1^t = a_1^{1+p^s} \quad \text{and} \quad a_2^t = a_2^{1+p^s}.$$

Indeed, we have $a_1^t = a_1^{1+p^s} a_1^{k_1 p^{m-1}}$ and $a_2^t = a_2^{1+p^s} a_1^{k_2 p^{m-1}}$, where $k_1, k_2 \in \{0, 1, \dots, p-1\}$. It follows from $a_1^{a_2} = a_1 a_1^{p^{m-1}}$ that $a_2^{a_1} = a_2 a_1^{-p^{m-1}}$, and these two relations imply $a_1^{a_2^\beta} = a_1^{1+\beta p^{m-1}}$ and $a_2^{a_1^\alpha} = a_2 a_1^{-\alpha p^{m-1}}$. We shall choose α and β so that $\alpha \equiv k_2 \pmod{p}$ and $\beta \equiv -k_1 \pmod{p}$. Then we compute (noting that $s \geq 1$)

$$\begin{aligned}a_1^{ta_1^\alpha a_2^\beta} &= (a_1^{1+p^s} a_1^{k_1 p^{m-1}})^{a_2^\beta} = (a_1^{1+\beta p^{m-1}})^{1+p^s} a_1^{k_1 p^{m-1}} \\ &= a_1^{1+p^s + (\beta+k_1)p^{m-1}} = a_1^{1+p^s}\end{aligned}$$

and similarly $a_2^{ta_1^\alpha a_2^\beta} = (a_2^{1+p^s} a_1^{k_2 p^{m-1}})^{a_1^\alpha a_2^\beta} = a_2^{1+p^s} a_1^{(-\alpha+k_2)p^{m-1}} = a_2^{1+p^s}$.

Since $Z \leq \mathfrak{U}_{\mu-1}(G)$, where $p^\mu = \exp(G)$, a generator $z = a_1^{p^{m-1}}$ of Z is a $p^{\mu-1}$ -th power of some element c . Suppose that $a_1^{p^{m-1}} = c^{p^{\mu-1}}$ and $c = a_1^{e_1} a_2^{e_2} \dots a_r^{e_r} t^{f_0}$. Then

$$(7) \quad a_1^{p^{m-1}} = c^{p^{\mu-1}} = a_1^{e_1 p^{\mu-1}} a_2^{e_2 p^{\mu-1}} t^{f_0 p^{\mu-1}}.$$

Suppose that $a_1^{p^{\mu-1}} \neq 1$. Then $m = \mu$. If $s = \mu - 1$ and $a_2^{p^{\mu-1}} = 1$, then $G' = \langle a_1^{p^{\mu-1}} \rangle$ is of order p and our theorem holds by Proposition 73.9.

(i) If $a_1^{p^{\mu-1}} \neq 1$, $s = \mu - 1$, and $a_2^{p^{\mu-1}} \neq 1$, then we replace a_2 by $a_2^* = a_2 t^{-1}$. From (6) we get $a_1^{t^{-1}} = a_1^{1-p^{\mu-1}}$, and so

$$a_1^{a_2^*} = a_1^{a_2 t^{-1}} = (a_1 a_1^{p^{\mu-1}})^{t^{-1}} = a_1 a_1^{-p^{\mu-1}} a_1^{p^{\mu-1}} = a_1,$$

since $a_1^{p^{\mu-1}} \in Z(G)$. Assume that, for an $i \geq 3$, we have $a_i^t = a_i^{1+p^{\mu-1}} a_1^{k_i p^{\mu-1}} = a_i a_1^{k_i p^{\mu-1}}$ with $k_i \not\equiv 0 \pmod{p}$. This gives $[a_i, t] = a_i^{k_i p^{\mu-1}}$ and so $H = \langle a_i, t \rangle$ contains $Z = \langle a_1^{p^{\mu-1}} \rangle$. But Z is normal in G and so $H' = Z$ is of order p . By Lemma 65.2(a), H is minimal nonabelian and by Remark, following Proposition 73.2, H is metacyclic. Therefore $\Omega_1(H) \cong E_{p^2}$ which implies $\Omega_1(H) = \langle \Omega_1(\langle a_i \rangle), a_1^{p^{\mu-1}} \rangle$. In particular, $\Omega_1(\langle t \rangle) \leq \Omega_1(H)$. Also $[a_i, t^{-1}] = [a_i, t]^{-1} = a_1^{-k_i p^{\mu-1}}$, and so $a_i^{t^{-1}} = a_i a_1^{-k_i p^{\mu-1}}$.

Now consider the subgroup $K = \langle a_i, a_2^* \rangle$. We have $a_i^{a_2^*} = a_i^{a_2 t^{-1}} = a_i^{t^{-1}} = a_i a_1^{-k_i p^{\mu-1}}$ and so $[a_i, a_2^*] = a_1^{-k_i p^{\mu-1}}$, which is a generator of Z . Thus K contains Z and since Z is normal in G , we have $K' = Z$. It follows that K is also minimal nonabelian and metacyclic and we have $\Omega_1(K) = \langle \Omega_1(\langle a_i \rangle), a_1^{p^{\mu-1}} \rangle = \Omega_1(H)$. In particular, $\Omega_1(\langle a_2^* \rangle) \in \Omega_1(H)$. We compute, using Proposition 73.6, $(a_2^*)^{p^{\mu-1}} = (a_2 t^{-1})^{p^{\mu-1}} = a_2^{p^{\mu-1}} t^{-p^{\mu-1}}$ and since $t^{p^{\mu-1}} \in \Omega_1(H)$, we get $1 \neq a_2^{p^{\mu-1}} \in \Omega_1(H) = \langle \Omega_1(\langle a_i \rangle), a_1^{p^{\mu-1}} \rangle$. This is a contradiction since $\{a_1, \dots, a_r\}$ is a basis of N .

We have proved that t centralizes $\langle a_3, \dots, a_r \rangle$. This implies that the subgroup $N^* = \langle a_1, a_2^*, a_3, \dots, a_r \rangle$ is abelian. Since t normalizes $\langle a_2 \rangle$, it follows that t centralizes $a_2^{p^{\mu-1}}$. We compute

$$\begin{aligned} (a_2^*)^t &= (a_2 t^{-1})^t = a_2^t t^{-1} = a_2^{1+p^{\mu-1}} t^{-1} = (a_2 t^{-1}) a_2^{p^{\mu-1}} \\ &= a_2^* a_2^{p^{\mu-1}} = (a_2^*)^{1+p^{\mu-1}} t^{p^{\mu-1}}, \end{aligned}$$

since $(a_2^*)^{p^{\mu-1}} = (a_2 t^{-1})^{p^{\mu-1}} = a_2^{p^{\mu-1}} t^{-p^{\mu-1}}$. Also, $G = \langle N^*, t \rangle$. If $t^{p^{\mu-1}} = 1$, then t normalizes the abelian subgroup N^* and $x^t = x^{1+p^{\mu-1}}$ for each $x \in N^*$ and we are done. Suppose that $t^{p^{\mu-1}} \neq 1$. Note that t induces an automorphism of order p on N and so t^p centralizes N . In particular, $t^{p^{\mu-1}} \in Z(G)$. Hence $A = N^* \langle t^{p^{\mu-1}} \rangle$ is a normal abelian subgroup of G , $G = A \langle t \rangle$, and for each $a \in A$, $a^t \equiv a^{1+p^{\mu-1}} \pmod{\langle t^{p^{\mu-1}} \rangle}$. Finally, $t^{p^{\mu-1}} \in \mathcal{V}_{\mu-1}(G)$ and this is exactly the situation studied in Case (I).

(ii) Suppose that $a_1^{p^{\mu-1}} \neq 1$ ($m = \mu$) and $s < \mu - 1$. In this case we replace a_2 by $a_2^* = a_2 t^{-p^{\mu-1-s}}$. Since $o(a_i) \leq p^{\mu-1}$ for $i > 2$, Proposition 73.11 implies that $\langle a_2^*, a_3, \dots, a_r \rangle$ is abelian. Again, Proposition 73.11 gives $a_1^{t^{p^{\mu-1-s}}} = a_1 a_1^{p^{\mu-1}}$, and conjugating this relation with $t^{-p^{\mu-1-s}}$ (noting that $a_1^{p^{\mu-1}} \in Z(G)$) we get $a_1 = a_1^{t^{-p^{\mu-1-s}}} a_1^{p^{\mu-1}}$ and so $a_1^{t^{-p^{\mu-1-s}}} = a_1^{1-p^{\mu-1}}$. We compute

$$\begin{aligned} a_1^{a_2^*} &= a_1^{a_2 t^{-p^{\mu-1-s}}} = (a_1^{1+p^{\mu-1}})^{t^{-p^{\mu-1-s}}} = (a_1^{1-p^{\mu-1}})^{1+p^{\mu-1}} \\ &= a_1^{1-p^{2\mu-2}} = a_1 \end{aligned}$$

since $2\mu - 2 \geq \mu$ and so $N^* = \langle a_1, a_2^*, a_3, \dots, a_r \rangle$ is an abelian subgroup of G . It remains to compute $(a_2^*)^t$.

Let us consider the subgroup $H = \langle a_2, t^{p^{\mu-1-s}} \rangle$. Since, by Proposition 73.11, $a_2^{t^{p^{\mu-1-s}}} = a_2^{1+p^{\mu-1}}$, it follows that $H' = \langle a_2^{p^{\mu-1}} \rangle$ is of order $\leq p$. By Proposition 73.11, $a_2^{p^s}$ ($s \geq 1$ and if $p = 2$ then $s \geq 2$) commutes with $t^{p^{\mu-1-s}}$ and so working in the subgroup H of class ≤ 2 , we get

$$\begin{aligned} (a_2^*)^{1+p^s} &= (a_2 t^{-p^{\mu-1-s}})^{1+p^s} = a_2 t^{-p^{\mu-1-s}} (a_2 t^{-p^{\mu-1-s}})^{p^s} = \\ &= a_2 t^{-p^{\mu-1-s}} a_2^{p^s} t^{-p^{\mu-1}} = a_2^{1+p^s} t^{-p^{\mu-1-s}} t^{-p^{\mu-1}}. \end{aligned}$$

On the other hand, $(a_2^*)^t = (a_2 t^{-p^{\mu-1-s}})^t = a_2^{1+p^s} t^{-p^{\mu-1-s}}$, and so by the above we get finally $(a_2^*)^t = (a_2^*)^{1+p^s} t^{p^{\mu-1}}$.

We have $G = \langle N^*, t \rangle$. If $t^{p^{\mu-1}} \in \langle a_1^{p^{\mu-1}} \rangle$, then the abelian subgroup N^* is normal in G and we have reduced this case to Case (I). So suppose $t^{p^{\mu-1}} \notin \langle a_1^{p^{\mu-1}} \rangle$. By Proposition 73.11, $t^{p^{\mu-1-s}}$ centralizes a_3, \dots, a_r and $t^{p^{\mu-1-s}}$ induces an automorphism of order $\leq p$ on $\langle a_1 \rangle$ and $\langle a_2 \rangle$ and so $t^{p^{\mu-1}} = (t^{p^{\mu-1-s}})^{p^s} \in Z(G)$. Hence $N^{**} = \langle N^*, t^{p^{\mu-1}} \rangle$ is a normal abelian subgroup of G , $G = \langle N^{**}, t \rangle$, and, for each $x \in N^{**}$, we get $x^t = x^{1+p^s} t^{k_x p^{\mu-1}} a_1^{l_x p^{\mu-1}}$, where k_x, l_x are integers depending on x . Also, t and a_1 are both of order p^μ and they are “linearly independent” modulo $\Omega_{\mu-1}(G)$. Indeed, if $t^{n_1} a_1^{n_2} \in \Omega_{\mu-1}(G)$ (n_1, n_2 integers), then (Proposition 73.6) $(t^{p^{\mu-1}})^{n_1} (a_1^{p^{\mu-1}})^{n_2} = 1$ and so $n_1 \equiv n_2 \equiv 0 \pmod{p}$. Hence there is a basis a_1, t, \dots of G (Proposition 73.7). In particular, there is a complement T of $\langle a_1 \rangle$ in G containing t . Since $\langle a_1 \rangle \leq N^{**}$, we get $N^{**} = \langle a_1 \rangle \times (N^{**} \cap T)$, by the modular law. Take $a \in N^{**} \cap T$ and assume that $a^t = a^{1+p^s} t^{k_a p^{\mu-1}} a_1^{l_a p^{\mu-1}}$ with $l_a \not\equiv 0 \pmod{p}$. Then $a_1^{p^{\mu-1}} \in T$, a contradiction. Hence, for each $a \in N^{**} \cap T$, we get $a^t = a^{1+p^s} t^{k_a p^{\mu-1}}$. But N^{**} is abelian and so $x^t = x^{1+p^s} t^{k_x p^{\mu-1}}$ for all $x \in N^{**}$. Since $\langle t^{p^{\mu-1}} \rangle \in Z(G)$ and $t^{p^{\mu-1}} \in \mathcal{V}_{\mu-1}(G)$, we have again reduced this case to Case (I).

(iii) Suppose, finally, that $a_1^{p^{\mu-1}} = 1$. Then from relation (7) follows

$$(8) \quad a_1^{p^{m-1}} = a_2^{e_2 p^{\mu-1}} t^{f_0 p^{\mu-1}}, \quad t^{p^{\mu-1}} \neq 1, \quad f_0 \not\equiv 0 \pmod{p}$$

since $\{a_1, a_2\}$ is a basis of the minimal abelian subgroup $\langle a_1, a_2 \rangle$. Also, $t^{p^{\mu-1}} \in \Omega_1(\langle a_1, a_2 \rangle) = \langle a_1^{p^{m-1}}, \Omega_1(\langle a_2 \rangle) \rangle$ but $t^{p^{\mu-1}} \notin \Omega_1(\langle a_2 \rangle)$.

Denote $p^l = |\langle a_1, a_2, t \rangle : \langle a_1, a_2 \rangle|$ and note that (6) implies that t normalizes $\langle a_2 \rangle$ (and $\langle a_1 \rangle$) and so $t^{p^l} \in N_{\langle a_1, a_2 \rangle}(\langle a_2 \rangle) = \langle a_1^p \rangle \times \langle a_2 \rangle$. Replacing a_1 with a_1^i ($i \not\equiv 0 \pmod{p}$), we may assume (writing again a_1 instead of a_1^i) that

$$(9) \quad t^{p^l} = a_1^{-p^k} a_2^{-hp^f}, \quad \text{where } k \geq 1, \quad h \not\equiv 0 \pmod{p}.$$

Since $[a_1^{p^k}, a_2^{p^f}] = 1$ and $\Omega_1(\langle t \rangle) \not\leq \Omega_1(\langle a_2 \rangle)$, we get $o(a_2^{-hp^f}) \leq o(a_1^{-p^k})$ and so $o(t^{p^l}) = o(a_1^{-p^k})$. On the other hand, $o(t^{p^l}) = p^{\mu-l}$ and $o(a_1^{-p^k}) = p^{m-k}$ and so $\mu - l = m - k$. By assumption, $\mu > m$, where $p^m = o(a_1)$, and so $l > k \geq 1$.

If $f = 0$, then we consider the normal abelian subgroup $M = \langle a_1, a_3, \dots, a_r \rangle$ of G . Since $a_2^{-h} = a_1^{p^k} t^{p^l}$, $h \not\equiv 0 \pmod{p}$, we have $G = \langle M, t \rangle$. For each $x \in M$, $x^t = x^{1+p^s} a_1^{k_x} p^{m-1}$, where (8) gives $a_1^{p^{m-1}} = (a_2^{e_2} t^{f_0})^{p^{\mu-1}} \in Z(G)$. This case is reduced to Case (I). Therefore we assume in the sequel that $f \geq 1$.

The element t centralizes $t^{p^l} = a_1^{-p^k} a_2^{-hp^f}$, where $h \not\equiv 0 \pmod{p}$, $k \geq 1$, $f \geq 1$. On the other hand, t normalizes $\langle a_1 \rangle$ and $\langle a_2 \rangle$ and so (since $\{a_1, a_2\}$ is a basis of the subgroup $\langle a_1, a_2 \rangle$) t centralizes $\langle a_1^{p^k} \rangle$ and $\langle a_2^{p^f} \rangle$. This implies that t^p centralizes $\langle a_1^{p^{k-1}} \rangle$ and $\langle a_2^{p^{f-1}} \rangle$. We have $t^{p^{l-1}} \in \langle t^p \rangle$ since $l > k \geq 1$ and so $l \geq 2$. Thus $t^{p^{l-1}}$ centralizes $\langle a_1^{p^{k-1}}, a_2^{p^{f-1}} \rangle$.

We consider an element

$$(10) \quad g = t^{p^{l-1}} a_1^{xp^{k-1}} a_2^{yp^{f-1}}$$

and show that there exist integers $x \not\equiv 0 \pmod{p}$ and $y \not\equiv 0 \pmod{p}$ such that $g^p = 1$. (Hence the coset $t^{p^{l-1}} \cdot \langle a_1, a_2 \rangle$ contains elements of order p .) Note that $t^{p^{l-1}}$ centralizes $\langle a_1^{xp^{k-1}}, a_2^{yp^{f-1}} \rangle$ and from (9) follows

$$(11) \quad t^{p^l} a_1^{p^k} a_2^{hp^f} = 1.$$

We get from (10) in any case $g^p = t^{p^l} (a_1^{xp^{k-1}} a_2^{yp^{f-1}})^p$, and so if $[a_1^{p^{k-1}}, a_2^{p^{f-1}}] = 1$, then we take $x = 1$ and $y = h$ so that (with the help of (11)) follows $g^p = t^{p^l} a_1^{p^k} a_2^{hp^f} = 1$. If $[a_1^{p^{k-1}}, a_2^{p^{f-1}}] \neq 1$, then $k = f = 1$ (since $\langle a_1, a_2 \rangle$ is minimal nonabelian) and $[a_1, a_2]^p = 1$. If $p > 2$, then $\langle a_1, a_2 \rangle$ is p -abelian and so setting again $x = 1$ and $y = h$ we get $g^p = t^{p^l} a_1^{p^k} a_2^{hp^f} = 1$. However, if $p = 2$, then $[a_1, a_2] = a_1^{2^{m-1}}$ is an involution in $Z(G)$ and here we set $x = 1 - 2^{m-2}$ (noting that

in this case $m > 2$ according to Proposition 73.9) and $y = h$. We obtain in that case also

$$\begin{aligned} g^2 &= t^{2^l} (a_1^{1-2^{m-2}} a_2^h)^2 = t^{2^l} a_1^{2(1-2^{m-2})} a_2^{2h} [a_2, a_1]^{(1-2^{m-2})h} \\ &= t^{2^l} a_1^{2-2^{m-1}+2^{m-1}} a_2^{2h} = 1, \end{aligned}$$

since $[a_2, a_1]^{(1-2^{m-2})h} = [a_2, a_1] = a_1^{2^{m-1}}$.

We consider the subgroup $K = \langle t^{p^{l-k}}, a_1 \rangle$ noting that $l > k \geq 1$. Using Proposition 73.13 and (9), we get $\mathfrak{V}_{k-1}(K) = \langle t^{p^{l-1}}, a_1^{p^{k-1}} \rangle$ and

$$\mathfrak{V}_k(K) = \langle t^{p^l}, a_1^{p^k} \rangle = \langle a_1^{-p^k} a_2^{-hp^f}, a_1^{p^k} \rangle = \langle a_1^{p^k}, a_2^{p^f} \rangle \leq Z(\langle a_1, a_2 \rangle).$$

Since $K/\mathfrak{V}_k(K)$ is of exponent p^k , Proposition 73.6 implies that $K/\mathfrak{V}_k(K)$ is p^{k-1} -abelian. Take the element

$$(12) \quad t^{p^{l-1}} a_1^{xp^{k-1}} \in \mathfrak{V}_{k-1}(K)$$

where $x \not\equiv 0 \pmod{p}$ is the integer from (10). Using Proposition 73.12, we see that there exists an element $g^* = t^{\alpha p^{l-k}} a_1^\beta$ (α, β integers) in K such that

$$(13) \quad (g^*)^{p^{k-1}} = t^{p^{l-1}} a_1^{xp^{k-1}}.$$

On the other hand, using the fact that $K/\mathfrak{V}_k(K)$ is p^{k-1} -abelian, we get

$$(14) \quad (g^*)^{p^{k-1}} = (t^{\alpha p^{l-k}} a_1^\beta)^{p^{k-1}} = t^{\alpha p^{l-1}} a_1^{\beta p^{k-1}} s,$$

where

$$(15) \quad s = a_1^{\gamma p^k} a_2^{\delta p^f} \in \mathfrak{V}_k(K) \ (\gamma, \delta \text{ integers}).$$

Using (12), (14), and (15), we get

$$(16) \quad a_1^{xp^{k-1}} = t^{(\alpha-1)p^{l-1}} a_1^{p^{k-1}(\beta+\gamma p)} a_2^{\delta p^f}.$$

It follows that $t^{(\alpha-1)p^{l-1}} \in \langle a_1, a_2 \rangle$ and so $\alpha-1 \equiv 0 \pmod{p}$. We may set $\alpha-1 = d$ (d integer), where $\alpha \not\equiv 0 \pmod{p}$ and together with (14) we get

$$(17) \quad t^{(\alpha-1)p^{l-1}} = t^{dp^l} = a_1^{-dp^k} a_2^{-hp^f}.$$

From (16) and (17) (noting that $x \not\equiv 0 \pmod{p}$) follows also $\beta \not\equiv 0 \pmod{p}$ since $\{a_1, a_2\}$ is a basis of $\langle a_1, a_2 \rangle$.

Substituting (13) in (15), we get $g = (g^*)^{p^{k-1}} a_2^{\gamma p^f - 1}$ and so the element g of order p (not being contained in $\langle a_1, a_2 \rangle$) is contained in the subgroup $H = \langle g^*, a_2 \rangle$.

On the other hand, H is modular with $d(H) = 2$ and so $|\Omega_1(H)| = p^2$ and therefore $\Omega_1(H) = \langle g, a_2^{p^{n-1}} \rangle$, where $\Omega_1(\langle a_2 \rangle) = \langle a_2^{p^{n-1}} \rangle$.

From $a_1^{a_2} = a_1^{1+p^{m-1}}$ follows $a_2^{a_1} = a_2 a_1^{-p^{m-1}}$ and $a_2^{a_1^\beta} = a_2 a_1^{-\beta p^{m-1}}$. From $a_2^t = a_2^{1+p^s}$ we get $a_2^{t^{\alpha p^{l-k}}} = a_2^u$ with a certain integer $u \not\equiv 0 \pmod{p}$. Then we compute

$$a_2^{g^*} = a_2^{t^{\alpha p^{l-k}} a_1^\beta} = (a_2^u)^{a_1^\beta} = (a_2^{a_1^\beta})^u = (a_2 a_1^{-\beta p^{m-1}})^u = a_2^u a_1^{-\beta u p^{m-1}},$$

since $a_1^{p^{m-1}} \in Z(G)$. Hence $a_1^{-\beta u p^{m-1}} \in H$ and $-\beta u \not\equiv 0 \pmod{p}$ implies $a_1^{p^{m-1}} \in H$. Thus $a_1^{p^{m-1}} \in \Omega_1(H) = \langle g, a_2^{p^{n-1}} \rangle$. This is a contradiction since $\langle g, a_2^{p^{n-1}} \rangle \cap \langle a_1, a_2 \rangle = \langle a_2^{p^{n-1}} \rangle$. The theorem is proved. \square

Minimal nonmodular p -groups are described in [Jan1].

Corollary 73.16 (v. d. Waall). *Every non-Dedekindian modular 2-group has a characteristic subgroup of index 2.*

Proof. By Theorem A.24.4, G is Q_8 -free. Now the result follows from Ward's Theorem 56.1. \square

As follows from v. d. Waall's result, if $p > 2$ and G is nonabelian modular, it contains a characteristic subgroup of index p .

Exercise. Let H be a powerful 2-group. If a 2-group G is lattice isomorphic with H via ϕ , then G is also powerful. (*Hint.* Use Proposition 73.5.)

p -groups with a cyclic subgroup of index p^2

The title groups have been determined in [Nin] (see also the old paper [HT1] by Hua and Tuan), where these groups are given in terms of generators and relations without any comments about its subgroup structure and therefore this result was not very useful for applications. We shall classify here the title groups in a structural form.

If a group G of order 2^4 has no cyclic subgroups of index 4, it is elementary abelian. Therefore, it suffices to classify the 2-groups with cyclic subgroup of index 4, which have the order $> 2^4$.

Theorem 74.1. *Let G be a nonabelian group of order p^m , $p > 2$, $m > 3$, and exponent p^{m-2} . Then one and only one of the following holds:*

- (a) G is metacyclic, $|G/\mathfrak{U}_2(G)| = p^4$.
- (b) $m > 4$, G is an L_3 -group.
- (c) $m = 4$, G is regular, $\Omega_1(G)$ is of order p^3 and exponent p .
- (d) $m = 4$, G is irregular, $p = 3$, G is of maximal class.

Proof (Berkovich). Let $Z < G$ be a cyclic subgroup of index p^2 in G .

Suppose that G has a normal subgroup E of order p^3 and exponent p ; then $G = EZ$ with $|E \cap Z| = p$. We know that $\exp(\text{Aut}(E))_p = p$ and so $|G : C_G(E)| \leq p$. Therefore, if $m > 4$, then $\Omega_1(G) = E$ and G is an L_3 -group.

Now let $m = 4$. If G is regular, then $|\Omega_1(G)| \in \{p^2, p^3\}$. In the first case, G is metacyclic (Lemma 64.1(a,m)). In the second case, $\Omega_1(G)$ is of exponent p (Lemma 64.1(a)). Next suppose that G is irregular. Then $p = 3$ (Lemma 64.1(a)). (Note that a 3-group of maximal class and order 3^4 has a cyclic subgroup of index 3^2 , since it is irregular.)

In what follows we assume that $m > 4$ and G has no normal subgroups of order p^3 and exponent p . According to Theorem 13.7 (see also Theorem 69.4), G is either metacyclic or a 3-group of maximal class. Let us consider these possibilities.

Let G be metacyclic. In that case, G is regular. Since G has no cyclic subgroups of index p , the subgroup $\mathfrak{U}_1(G)$ is noncyclic. Therefore, $|G/\mathfrak{U}_2(G)| = p^4$. Let us show that $\mathfrak{U}_2(G)$ is cyclic. If not, $G/\mathfrak{U}_3(G)$ is of order p^6 and exponent p^3 , which is not the case since $\exp(G) = p^{m-2}$. Conversely, if G is metacyclic with $|G/\mathfrak{U}_2(G)| = p^4$ and $\mathfrak{U}_2(G)$ is cyclic, it has a cyclic subgroup of index p^2 since $\mathfrak{U}_2(G) = \{x^{p^2} \mid x \in G\}$ (Lemma 64.1(a)).

Now let G be a 3-group of maximal class, $m > 4$. Then G_1 , the fundamental subgroup of G , is metacyclic and $\exp(G_1) = \exp(G)$ (see §9). It follows that G_1 has a cyclic subgroup of index 3. In that case, $\mathfrak{U}_1(G_1)$ is cyclic of index p^2 in G_1 so $|\mathfrak{U}_1(G)| \geq 3^2$. This is a contradiction since a p -group of maximal class and order $> p^3$, $p > 2$, has no normal cyclic subgroups of order $> p$. \square

Theorem 74.2. *Let G be a nonabelian group of order 2^m , $m > 4$, and exponent 2^{m-2} . Then one of the following holds:*

- (a) *G is an L_3 -group.*
- (b) *G is the uniquely determined group of order 2^5 with $\Omega_2(G) \cong D_8 \times C_2$. The group G has a normal elementary abelian self centralizing subgroup $E = \langle z, u, e \rangle$ of order 8 and an element a of order 8 such that $G = E\langle a \rangle$, where $a^4 = z$, $e^a = eu$, and $u^a = z$. Here $\Phi(G) = \langle a^2, u \rangle$ is abelian of type $(4, 2)$, $G' = \Omega_1(\Phi(G)) \cong E_4$, $Z(G) = \mathfrak{U}_1(\Phi(G))$ is of order 2, and $c_3(G) = 4$.*
- (c) *G is a U_2 -group (all such groups are completely determined in §67). If $m > 5$, then $c_{m-2}(G) = 2$.*
- (d) *$G = WZ$ with $W \cap Z \cong C_4$, where W is an abelian normal subgroup of type $(4, 4)$ and $Z \cong C_{2^{m-2}}$. We have $W = \Omega_2(G)$ and G is metacyclic. Also, $2 \leq |Z : C_Z(W)| \leq 4$, (since $\exp(\text{Aut}(W))_2 \leq 4$; see §33) and $c_{m-2}(G) = 4$.*
- (e) *$G = QZ$, where $Q \cong Q_8$ is a normal subgroup of G , $Q \cap Z = Z(Q)$, $Z = \langle b \rangle \cong C_{2^{m-2}}$ and b either centralizes Q or b induces on Q an involutory outer automorphism in which case $m > 5$. Also we have $c_{m-2}(G) = 4$.*
- (f) *G is the uniquely determined group of order 2^5 with $\Omega_2(G) = \langle a, b \rangle \times \langle u \rangle$, where $\langle a, b \rangle \cong Q_8$ and u is an involution with $C_G(u) = \Omega_2(G)$. Let $\langle z \rangle = Z(Q)$; then $a^2 = b^2 = z$. There is an element y of order 8 in G such that $y^2 = ua$, $u^y = uz$, $a^y = a^{-1}$, $b^y = bu$. Here $\Phi(G) = \langle y^2, u \rangle$ is abelian of type $(4, 2)$, $G' = \Omega_1(\Phi(G)) \cong E_4$, $Z(G) = \mathfrak{U}_1(G)$ is of order 2, and $c_3(G) = 4$.*

Proof (Janko). Suppose that G has a normal subgroup $E \cong E_8$; then $G = EZ$ with $Z \cong C_{2^{m-2}}$ and $E \cap Z \cong C_2$. If K/E is the subgroup of order 2 in G/E , then $\Omega_1(G) \leq K$. Therefore, if K is abelian, we get $\Omega_1(G) = E$, and so G is an L_3 -group. Now let $C_G(E) = E$. Since $\exp(\text{Aut}(E))_2 = 4$, we get $|G| = 2^5$ and $Z = \langle a \rangle$ is of order 8. In that case, $|Z(G)| = 2$. Therefore, setting $z = a^4$, one can choose $e, u \in E$ so that $E = \langle e, u, z \rangle$, $e^a = eu$ and $u^a = uz$. The structure of G is determined and we get the group (b) stated in the theorem.

From now on we assume that G has no normal elementary abelian subgroups of order 8. Since G is neither cyclic nor of maximal class, it has a normal four-subgroup W_0 . Suppose that G/W_0 is cyclic (of order 2^{m-2}), then $G = W_0S$ with $S \cong C_{2^{m-2}}$ and $W_0 \cap S = \{1\}$ since G has no cyclic subgroups of index 2. But then $W_0 \times \Omega_1(S) \cong E_8$ is normal in G , contrary to our assumption. Hence, G/W_0 is noncyclic. Let $Z < G$ be cyclic of order 2^{m-2} . Then $W_0 \cap Z \cong C_2$ and so W_0Z is maximal

in G . It follows that G/W_0 has a cyclic subgroup $(W_0Z)/W_0$ of order $2^{m-3} \geq 4$ and index 2. Set $F/W_0 = \Phi(G/W_0)$ so that $F < W_0Z$ and F/W_0 is cyclic of order ≥ 2 . Since $C_{W_0Z}(W_0) \geq F$ (indeed, $|W_0Z : C_{W_0Z}(W_0)| \leq 2$), it follows that $\Omega_1(W_0Z) = W_0$. Let M/W_0 be any cyclic subgroup of index 2 in G/W_0 . Since $M > F$ and $\Omega_1(M) \leq \Omega_1(F) = W_0$, we get $\Omega_1(M) = W_0$. If G/W_0 is of maximal class, then G is an U_2 -group and all such groups have been determined in §67. Note, that if $m > 5$, then all cyclic subgroups of order 2^{m-2} are contained in the L_2 -subgroup W_0Z so $c_{2^{m-2}}(G) = c_{2^{m-2}}(W_0Z) = 2$.

We may assume that G/W_0 is not of maximal class. It follows that G/W_0 is either abelian of type $(2^{m-3}, 2)$ or $G/W_0 \cong M_{2^{m-2}}$ in which case $m > 5$ (Lemma 64.1(t)). In any case, G/W_0 has exactly two cyclic subgroups M_1/W_0 and M_2/W_0 of index 2 and the third maximal subgroup M_3/W_0 is abelian of type $(2^{m-3}, 2)$. Hence M_3 cannot contain cyclic subgroups of index 2. But $\Omega_1(M_i) = W_0$ and so M_i is either abelian of type $(2^{m-2}, 2)$ or $M_i \cong M_{2^{m-1}}$, $i = 1, 2$. In any case, $c_{m-2}(M_i) = 2$ and two cyclic subgroups of order 2^{m-2} in M_i generate M_i , $i = 1, 2$. Since $\exp((M_1 \cap M_2)/W_0) = 2^{m-4}$, it follows that $M_1 \cap M_2$ does not contain any cyclic subgroup of order 2^{m-2} . We get (see the proof of Theorem 1.10) $c_{m-2}(G) = c_{m-2}(M_1) + c_{m-2}(M_2) = 2+2 = 4$ and G is generated by its four cyclic subgroups of order 2^{m-2} .

We are now in a position to use Theorem 54.2. The groups (d) and (a) of our theorem correspond to possibilities (a) and (b) of Theorem 54.2, respectively. In case (c) of Theorem 54.2, we have here only the possibility $|G| = 2^5$ with $\Omega_2(G) \cong Q_8 \times C_2$ (since in case $\Omega_2(G) = D_8 \times C_2$ the group G would have a normal elementary abelian subgroup of order 8). This leads to the group (f) of our theorem, and we are done. \square

Exercise. Let $p > 2$ and let G be a nonmetacyclic group of order $p^m > p^4$ with non-normal cyclic subgroup L of order p^{m-2} . Suppose that G is not minimal nonabelian. Prove that G has a maximal subgroup $H \cong M_{p^{m-1}}$.

Solution. We have $p > 2$. The quotient group G/L_G is isomorphic to a Sylow p -subgroup of the symmetric group S_{p^2} so L_G is cyclic of order $> p$ since $m > 4$. It follows from Theorem 9.6 that G is not a p -group of maximal class. Then, by Theorem 69.3, G has a normal subgroup R of order p^3 and exponent p . Since G has a cyclic subgroup of index p^2 , then $\Omega_1(G) = R$, G/R is cyclic so $\exp(\Omega_k(G)) \leq p^k$ for all $k \in \mathbb{N}$. By Proposition 10.28, G is generated by minimal nonabelian subgroups. It follows that G has a minimal normal subgroup H of exponent p^{m-2} . By hypothesis, $H < G$. Then H has a cyclic subgroup of index p , and the result follows from Theorem 1.2.

§75

Elements of order ≤ 4 in p -groups

All results of this section are due to the second author.

If G is a finite p -group and $n \in \mathbb{N}$ a fixed natural number, then we define $\Omega_n^*(G) = \langle x \in G \mid o(x) = p^n \rangle$. It is a known fact that $\Omega_2(G)$ has a strong influence on the structure of a finite 2-group G . For example, if $\Omega_2(G)$ is metacyclic, then the 2-group G is also metacyclic (this follows from the classification of minimal nonmetacyclic p -groups; see Theorem 66.1). In §52, all 2-groups G with the property $|\Omega_2(G)| = 2^4$ are classified. If $|\Omega_2(G)| \leq 2^3$, then we get for a 2-group G four infinite classes of groups (see Lemma 42.1). In this section we consider for the first time the case, where for $\Omega_2(G)$ we could have an infinite class of 2-groups. More precisely, we assume that G is a finite 2-group with $\Omega_2(G) \cong C_2 \times D$, where D is any 2-group of maximal class. Then either $G = \Omega_2(G)$ or $|G : \Omega_2(G)| = 2$ and the structure of G is uniquely determined (Theorem 75.1). In fact, the most difficult part of the proof is to show that $|G : \Omega_2(G)| = 2$. The exact determination of the structure of G is obtained by applying a classification of so called U_2 -groups given in §67. A 2-group H is said to be a U_s -group ($s \geq 2$) with respect to the kernel R if H has a normal elementary abelian subgroup R of order 2^s , H/R is of maximal class and whenever T/R is a cyclic subgroup of index 2 in H/R , then $\Omega_1(T) = R$.

We shall determine also the structure of a finite 2-group G with $\Omega_2^*(G) \cong C_2 \times Q_{2^n}$, where Q_{2^n} is a generalized quaternion group of order 2^n , $n \geq 4$ (see ‘Research problems and themes I’, #563). If $\Omega_2(G) > \Omega_2^*(G)$, then we show that $G = \Omega_2(G) \cong C_2 \times SD_{2^{n+1}}$, where $SD_{2^{n+1}}$ is the semidihedral group of order 2^{n+1} (Theorem 75.2). The case $n = 3$ was treated in §55.

Finally, we show that a finite p -group G , all of whose noncyclic subgroups H have the property $H = \Omega_1(H)$, is either cyclic or of exponent p or $p = 2$ and G is a dihedral group D_{2^n} , $n \geq 3$ (Theorem 75.3). Here the case $p > 2$ is almost trivial but some proving must be done in case $p = 2$; see also Exercise 1.113.

Theorem 75.1. *Let G be a 2-group with $\Omega_2(G) = \langle u \rangle \times D$, where u is an involution, D is any 2-group of maximal class, and $|D| = 2^n$, $n \geq 4$. If $G \neq \Omega_2(G)$, then $|G : \Omega_2(G)| = 2$, D is dihedral or generalized quaternion, $C_G(u) = \Omega_2(G)$, G is a nonmetacyclic U_2 -group with respect to the kernel $R = \langle u \rangle \times Z(D)$, $G/R \cong SD_{2^n}$, $Z(G) = Z(D)$, and $d(G) = 2$. More precisely, we set $D = \langle a', b \mid (a')^{2^{n-1}} = 1, (a')^{2^{n-2}} = z, (a')^{2^{n-3}} = v, b^2 = z^\epsilon, \epsilon = 0, 1, (a')^b = (a')^{-1} \rangle$, and then*

there is an element $a \in G - \Omega_2(G)$ such that $a^2 = a'$, $u^a = uz$, $a^b = a^{-1}vu$, and this determines the structure of G uniquely. (For $n < 4$, such groups G have been determined in Lemma 42.1.)

Proof. Set $H = \Omega_2(G)$ so that $H = \langle u \rangle \times D$ with $|D| = 2^n$, $n \geq 4$. Let Z be the unique cyclic subgroup of index 2 in D , where $|Z| = 2^{n-1} \geq 8$. Since D has no normal four-subgroups, it follows that G has no normal elementary abelian subgroups of order 8. We know that D has no normal abelian subgroups of type $(4, 2)$ and so H (and also G) has no normal abelian subgroups of type $(4, 4)$. Set $\langle z \rangle = \Omega_1(Z)$ so that $\langle z \rangle = Z(D)$. Let $\langle v \rangle$ be the cyclic subgroup of order 4 in Z , where $v^2 = z$. Since $\langle v \rangle \leq \Omega_1(H) = \Omega_1(Z)$, it follows that $\langle v \rangle$ is normal in G and so $z \in Z(G)$. Obviously, $W_0 = \langle u \rangle \times \langle z \rangle = Z(H)$ and so W_0 is normal in G . Therefore, $W = W_0\langle v \rangle$ is normal in G , $W_0 = \Omega_1(W)$, and W is a normal abelian subgroup of G of type $(4, 2)$. We see that W_0 is the unique normal four-subgroup in H and then W is the unique normal abelian subgroup of H of type $(4, 2)$. It follows that W_0 is the unique normal four-subgroup in G and W is the unique normal abelian subgroup of G of type $(4, 2)$.

We are now in a position to use Proposition 50.6(a). It follows that $N = C_G(W)$ is abelian of type $(2^m, 2)$, where $m \geq n - 1$, $N \cap H = W_0Z = \langle u \rangle \times Z$, G/N is isomorphic to a subgroup of D_8 , and $W = \Omega_2(N)$. Let r be an element in $D - Z$ so that $r^2 \in \langle z \rangle$ and $v^r = v^{-1}$. Hence r induces an involutory automorphism on the abelian group N and r inverts $W = \Omega_2(N)$. This implies that $C_N(r) = W_0 = \Omega_1(W)$ and so, using Theorems 67.1, 67.2 and 67.3, we see that r inverts N/W_0 . Suppose that $N \neq W_0Z$. Take an element $x \in N - (W_0Z)$. We have $x^r = x^{-1}w_0$ with some $w_0 \in W_0$. But then $(rx)^2 = rxrx = r^2x^r x = r^2x^{-1}w_0x = r^2w_0 \in W_0$, and so $o(rx) \leq 4$. This is a contradiction since $rx \notin H = \Omega_2(G)$.

We have proved that $N = W_0Z$. Since $\langle v \rangle$ is normal in G , $v^r = v^{-1}$, and $u^r = u$ for any $r \in D - Z$, it follows that $C_G(v)$ covers G/H . If $G \neq H$, there is $s \in C_G(v) - H$ with $u^s = uz$, $v^s = v$, so that $G/(W_0Z)$ is a four-group of automorphisms of W induced with $\langle s, r \rangle$.

From now on we assume $G \neq H$. In that case $|G : H| = 2$, $C_G(W) = W_0Z$, $G/(W_0Z) \cong E_4$, and for each $x \in G - H$, $u^x = uz$ so that $C_G(u) = \langle u \rangle \times D = H$. It remains to determine the structure of G . Since $S = C_G(v)$ covers G/H and $C_H(v) = W_0Z$, it follows that S is a nonabelian maximal subgroup of G with $S \cap H = W_0Z$. Hence $\Omega_2(S) = W$ and so we may apply Lemma 42.1 for $p = 2$. It follows that either $S \cong M_{2^{n+1}}$ or $S = \langle a, b \mid a^{2^{n-1}} = b^8 = 1, a^b = a^{-1}, a^{2^{n-2}} = b^4 \rangle$, $n \geq 4$. In the second case,

$$\langle b^2 \rangle = \langle v \rangle = Z(S), \quad \langle a^2 \rangle = S', \quad \Phi(S) = Z(S)\langle a^2 \rangle, \quad \Omega_1(S) = \Omega_1(W) = \langle u, z \rangle,$$

$z = a^{2^{n-2}}$ and $C_S(\Omega_1(S)) = \langle b^2, a \rangle$ is the unique abelian maximal subgroup of S and so $\langle b^2, a \rangle = W_0Z = \langle u \rangle \times Z$. Since W_0Z contains exactly two cyclic subgroups Z_1, Z_2 of index 2, one of them, say $Z_1 = \langle a \rangle$, is inverted by the element $b \in S - (W_0Z)$. But $Z_1 \cap Z_2 \geq \langle v \rangle$ and so b inverts $\langle v \rangle$, contrary to $S = C_G(v)$.

We have proved that $S \cong M_{2^{n+1}}$. In particular, S has a cyclic subgroup S_1 of index 2 containing $\langle v \rangle$ and so S/W_0 is a cyclic subgroup of index 2 in G/W_0 . But G/W_0 contains $DW_0/W_0 = H/W_0 \cong D/\langle z \rangle$, where $D/\langle z \rangle$ is a group of maximal class. Thus G/W_0 is of maximal class and order 2^n ($n \geq 4$) and so S/W_0 is the unique cyclic subgroup of index 2 in G/W_0 . Since $\Omega_1(S) = W_0$, it follows that G is a U_2 -group with the kernel W_0 .

We are now in the position to use the classification of U_2 -groups given in §67 (see Theorems 67.1 and 67.3). It follows that only the group G given in Theorem 67.3(d) satisfies our assumptions:

$$\begin{aligned} G = \langle a, b \mid a^{2^n} = 1, a^{2^{n-1}} = z, a^{2^{n-2}} = v, b^2 = z^\epsilon, \epsilon = 0, 1, \\ a^b = a^{-1}vu, u^2 = [u, b] = 1, u^a = uz, n \geq 4 \rangle, \end{aligned}$$

where $W_0 = \langle u, z \rangle$, $G/W_0 \cong SD_{2^n}$, $Z(G) = \langle z \rangle \cong C_2$, G is non-metacyclic, and $d(G) = 2$. Also, $C_G(u) = \langle u \rangle \times D = \Omega_2(G)$, where $D = \langle a^2, b \rangle$. For $\epsilon = 0$, D is dihedral and for $\epsilon = 1$, D is generalized quaternion. Our theorem is proved. \square

Of course, groups of Theorem 75.1 have no normal elementary abelian subgroups of order 8. Therefore, to prove that theorem, we must find all groups of §50 satisfying the hypothesis of Theorem 75.1. However, such proof will be not easier than the presented proof.

Theorem 75.2. *Let G be a 2-group with $\Omega_2^*(G) = Q_{2^n} \times C_2$, where $n \geq 4$. If $\Omega_2(G) \neq \Omega_2^*(G)$, then $\Omega_2(G) = G \cong SD_{2^{n+1}} \times C_2$. (If $n = 3$, then such groups G have been determined in Theorem 55.1.)*

Proof. Set $H = \Omega_2^*(G) = \langle u \rangle \times Q$, where u is an involution and $Q \cong Q_{2^n}$, $n \geq 4$. Assume $\Omega_2(G) \neq H$. Let $\langle a \rangle$ be the unique cyclic subgroup of index 2 in Q and we set

$$Q = \langle a, b \mid a^{2^{n-1}} = b^4 = 1, a^{2^{n-2}} = z, a^{2^{n-3}} = v, b^2 = z, a^b = a^{-1} \rangle,$$

where $Q_1 = \langle a^2, b \rangle$ and $Q_2 = \langle a^2, ab \rangle$ are the other two maximal subgroups of Q and $Q_1 \cong Q_2 \cong Q_{2^{n-1}}$. Also, $Z(H) = \langle u, z \rangle$ is normal in G . Since $\langle v \rangle \leq \langle a^2 \rangle = \Omega_1(H)$, $\langle v \rangle$ and $\langle a^2 \rangle$ are normal subgroups in G and $\langle z \rangle \leq Z(G)$.

Since $\Omega_2(G) \neq H$, there exists an involution $t \in G - H$ and we set $K = H\langle t \rangle$. If $u^t = uz$, then $Z(H)\langle t \rangle \cong D_8$ and so $o(ut) = 4$, a contradiction since the element ut of order 4 is not contained in $H = \Omega_2^*(G)$. Hence t centralizes $Z(H)$. Since t cannot commute with any element of order 4 in H , we get $C_H(t) = Z(H) = \langle u, z \rangle$.

We act with t on the abelian group $\langle u \rangle \times \langle a \rangle$ and apply §55. It follows that t inverts the quotient group $\langle u, a \rangle / Z(H)$ and so $a^t = a^{-1}s$ with $s \in Z(H)$. We compute $(ta)^2 = (tat)a = a^{-1}sa = s$, and so $s = 1$ (since ta cannot be of order 4 in view $ta \notin H$) and $a^t = a^{-1}$. Hence t inverts the maximal subgroup $\langle u, a \rangle$ of H containing $Z(H)$.

Suppose that $(Q_1Z(H))^t = Q_1Z(H)$. In that case $b^t = ba^{2i}u^j$, where i, j are suitable integers. Working in Q , there is $a^k \in \langle a \rangle$ (k is an integer) such that $b^{a^k} = ba^{-2i}$ and so $b^{ta^k} = (ba^{2i}u^j)^{a^k} = ba^{-2i}a^{2i}u^j = bu^j$, where $t' = ta^k$ is an involution in $K - H$. We compute $(t'b)^2 = (t'bt')b = bu^jb = u^jz$, and so $o(t'b) = 4$, a contradiction. Hence $(Q_1Z(H))^t = Q_2Z(H)$. It follows $b^t = aba^{2r}u^s$ (r, s are some integers) and so $\langle b, b^t \rangle = Q^* \cong Q \cong Q_{2^n}$ with $K = \langle u \rangle \times (Q^*\langle t \rangle)$, where $Q^*\langle t \rangle \cong SD_{2^{n+1}}$.

Let $N = N_G(Q_1Z(H))$ so that $|G : N| = 2$, $H \leq N$, and $G = N \cdot \langle t \rangle$. Suppose $N \neq H$. By the above argument, $N - H$ cannot contain involutions and so $\Omega_2(N) = H$. By Theorem 75.1, we get $|N : H| = 2$ and N is a uniquely determined group. In particular, by the structure of N , if $y \in N - H$, $(Q_1Z(H))^y = Q_2Z(H)$, contrary to $N = N_G(Q_1Z(H))$. Hence, $N = H$ and so $G = H\langle t \rangle = K$ and we are done. \square

Let G be a 2-group. Of course, $\Omega_2^*(\Omega_2^*(G)) = \Omega_2^*(G)$. Therefore, if $\Omega_2^*(G) = C_2 \times D$, where D is of maximal class and order > 8 , then D is a generalized quaternion group.

Remark. Let, as in Theorem 75.1, $\Omega_2(G) = C_2 \times D$, where D is a 2-group of maximal class. If D is dihedral, then $c_2(G) = 2$, and such groups are classified (see §43). It follows from the results of §54 that the 2-groups G with $\Omega_2(G) = E_4 \times D$, where D is dihedral, also known. Similarly, if $n > 3$ and $\Omega_{n-1}(G) = C_2 \times M_{2^n}$ or $\Omega_{n-1}^*(G) = C_2 \times M_{2^n}$, then $c_{n-1}(G) = 4$, and the classification of such groups follows from results of §55.

Theorem 75.3. *Let G be a p -group all of whose noncyclic subgroups are generated by its elements of order p . Then one of the following holds: G is cyclic, G is of exponent p , G is a dihedral 2-group D_{2^n} of order 2^n .*

Proof. Suppose that $p > 2$ and assume that G is neither cyclic nor of exponent p . Let Z be a maximal cyclic subgroup of order p^s , $s \geq 2$. Since $Z \neq G$, there is a subgroup $Y > Z$ with $|Y : Z| = p$. It follows that Y is either abelian of type (p^s, p) or $Y \cong M_{p^{s+1}}$. In any case, $\Omega_1(Y) \cong E_{p^2}$ so $\Omega_1(Y) < Y$, a contradiction.

From now on assume $p = 2$. We may also assume that G is not cyclic, $\exp(G) \geq 4$, and G is not of maximal class. Let R be a normal four-subgroup of G . If $C_G(R)$ has an element v of order 4, then $R\langle v \rangle$ contains an abelian subgroup of type $(4, 2)$, a contradiction. Hence $H = C_G(R)$ is elementary abelian and $|G : H| = 2$. We have $\exp(G) = 4$ and let $s \in G - H$ be an element of order 4 so that $s^2 \in H$. Since G has no abelian subgroups of type $(4, 2)$, it follows that $\langle s \rangle$ is a maximal abelian subgroup of G . Then, by Suzuki (Proposition 1.8), G is of maximal class, contrary to the assumption. \square

Problem. Classify the 2-groups G satisfying one of the following conditions:

- (i) $\Omega_2(G) = E \times D$, where E is elementary abelian and D is of maximal class.
- (ii) $\Omega_2^*(G) = E \times D$, where E is elementary abelian and D is of maximal class.

- (iii) $\Omega_{n-1}^*(G) = E \times M_{2^n}$, where $n > 3$ and E is elementary abelian.
- (iv) $\Omega_n(G) = E \times C_{2^n}$, where $n > 1$ and E is elementary abelian.
- (v) $\Omega_n^*(G) = E \times C_{2^n}$, where $n > 1$ and E is elementary abelian.

p -groups with few \mathcal{A}_1 -subgroups

1^o. Recall that G is an \mathcal{A}_n -group if it contains a nonabelian subgroup of index p^{n-1} but all its subgroups of index p^n are abelian (see §72). For example, a p -group G of maximal class and order p^m is an \mathcal{A}_{m-2} -group since it contains a nonabelian subgroup of order p^3 (see Theorems 9.5 and 9.6).

Let $\alpha_n(G)$ be the number of \mathcal{A}_n -subgroups in a p -group G . If G is an \mathcal{A}_n -group, then $\alpha_i(G) > 0$ for $i = 1, \dots, n-1$, $\alpha_n(G) = 1$ and $\alpha_j(G) = 0$ for $j > n$. For $H < G$, we set $\beta_1(G, H) = \alpha_1(G) - \alpha_1(H)$. For example, if $H < G$ is abelian, then $\beta_1(G, H) = \alpha_1(G)$. If $H < G$, then Γ_i^H denotes the set of all members of the set Γ_i which contain H . Given $H < G$, let $\Gamma_i(H) = \{U < H \mid \Phi(H) \leq U, |H : U| = p^i\}$. If G is a p -group of maximal class containing an abelian subgroup of index p , then $\alpha_1(G) = p^{m-3}$.

It is fairly difficult to compute $\alpha_1(G)$ even for groups with not very complicated structure. Below we compute $\alpha_1(G)$ for three families of groups.

Let X be a group and $\varphi_2(X)$ the number of noncommuting ordered pairs $(x, y) \in X \times X$ such that $\langle x, y \rangle = X$ (it follows that $\varphi_2(X) > 0$ if and only if X is nonabelian and two-generator). Let $k(X)$ be the class number of X . We claim that (see §2; this identity is due to Mann)

$$(1) \quad \sum_{H \leq X} \varphi_2(H) = |X|(|X| - k(X)).$$

Indeed, let $\{K_1, \dots, K_r\}$ (here $r = k(X)$) be the set of conjugacy classes of X . Then the number of commuting ordered pairs of G equals

$$(2) \quad \sum_{i=1}^r \left(\sum_{x \in K_i} |C_X(x)| \right) = \sum_{i=1}^r |K_i| \frac{|X|}{|K_i|} = r|X| = |X|k(X)$$

so the number of noncommuting ordered pairs of elements of X is identical with $|X|^2 - |X|k(X)$. On the other hand, that number also equals $\sum_{H \leq X} \varphi_2(H)$.

Examples. 1. Let us find $\alpha_1(G)$, where G is extraspecial of order p^{2m+1} . We have $k(G) = |\mathrm{Z}(G)| + \frac{|G-\mathrm{Z}(G)|}{p} = p^{2m} + p - 1$. Let $E \leq G$ be nonabelian and two-generator. Then $E' = G'$ and $E/E' \cong \mathrm{E}_{p^2}$ since $E/E' \leq G/E' = G/G' \cong \mathrm{E}_{p^{2m}}$. It follows that $|E| = p^3$ so E is an \mathcal{A}_1 -subgroup. We have

$$\varphi_2(E) = (|E - \Phi(E)|)(|E| - p|\Phi(E)|) = (p^3 - p)(p^3 - p^2) = p^3(p^2 - 1)(p - 1).$$

It follows from (1) that

$$\begin{aligned}\alpha_1(G)\varphi_2(E) &= \alpha_1(G)p^3(p^2 - 1)(p - 1) = p^{2m+1}(p^{2m+1} - p^{2m} - p + 1) \\ &= p^{2m+1}(p - 1)(p^{2m} - 1),\end{aligned}$$

and we get $\alpha_1(G) = p^{2m-2} \cdot \frac{p^{2m}-1}{p^2-1}$. In particular, if $|G| = p^5$, i.e., $m = 2$, then $\alpha_1(G) = p^2(p^2 + 1)$.

2. Let G be a nonabelian group of order p^m all of whose nonabelian two-generator subgroups have the same order p^3 . Then, using (1), we get $\alpha_1(G) = \frac{p^{m-3}(p^m - k(G))}{(p-1)(p^2-1)}$.

3. Let $G = S \times E_{p^n}$, where S is nonabelian of order p^3 . Then $|G| = p^{n+3}$, $k(G) = p^n(p^2 + p - 1)$. If $A < G$ is an \mathcal{A}_1 -subgroup, then $|A| = p^3$. Therefore, by the formula in Example 2, we get $\alpha_1(G) = \frac{p^n[p^{n+3} - p^n(p^2 + p - 1)]}{(p^2-1)(p-1)} = p^{2n}$.

Epimorphic images of an \mathcal{A}_n -group are \mathcal{A}_k -groups with $k \leq n$. Indeed, if $N \triangleleft G$, where G is an \mathcal{A}_n -group, then all subgroups of index p^n in G/N are abelian.

The main result of this section is the following

Theorem A ([Ber30]). *Let G be a nonabelian p -group. If $\alpha_1(G) \leq p^2 + p + 1$, then G is an \mathcal{A}_n -group, $n \in \{1, 2, 3\}$.*

Exercise 1. Prove that if G is metacyclic, distinct $F, H \in \Gamma_1$ are \mathcal{A}_r -, \mathcal{A}_s -groups respectively, and $r \leq s$, then G is an \mathcal{A}_{s+1} -group.

Solution. Since G' is cyclic, we get $F' \leq H'$. It follows from the above, Lemma 64.1(u) that $|G'| = p|H'| = p^{s+1}$ so G is an \mathcal{A}_{s+1} -group, by Theorem 72.1.

Exercise 2. Let G be a nonabelian p -group. Suppose that its maximal subgroups M_1, \dots, M_k contain all \mathcal{A}_1 -subgroups of G . Is it true that $k \geq p$?

Exercise 3. Suppose that maximal subgroups M_1, \dots, M_p together contain all \mathcal{A}_1 -subgroups of a nonabelian p -group G . Is it true that $|G : (\bigcap_{i=1}^p M_i)| = p^2$?

Exercise 4. Let $G = M \times C$, where M is nonabelian of order p^3 and C is cyclic of order p^2 . Prove that G has an \mathcal{A}_1 -subgroup of order p^4 and find the number of such subgroups in G .

2^o. *Proof of Theorem A.* We begin with the following

Remark 1. Let G be neither abelian nor an \mathcal{A}_1 -group and let $F_1 \in \Gamma_1$ be nonabelian. We claim that $\beta(G, F_1) \geq p - 1$. By Exercise 1.6(a), the set Γ_1 has at least p nonabelian members. Let $F_2 \in \Gamma_1 - \{F_1\}$ be nonabelian and set $D = F_1 \cap F_2$. Since $D \not\leq Z(G)$, at least p members of the set Γ_1^D , say F_1, \dots, F_p , are nonabelian. Let $U_i \leq F_i$ be an \mathcal{A}_1 -subgroup such that $U_i \not\leq D$, $i = 1, \dots, p$ (such U_i exists, by Proposition 10.28). Then U_1, \dots, U_p are distinct \mathcal{A}_1 -subgroups of G and $U_2, \dots, U_p \not\leq F_1$ so $\beta_1(G, F_1) \geq p - 1$. (For more detailed description of such groups, see Lemma 76.5.)

Lemma 76.1 (= Exercise 1.8a (L. Redei)). *Let G be an \mathcal{A}_1 -group. Then $G = \langle a, b \rangle$, $Z(G) = \Phi(G)$, $|G'| = p$ and one of the following holds:*

(a) $a^{p^m} = b^{p^n} = c^p = 1$, $[a, b] = c$, $[a, c] = [b, c] = 1$, $|G| = p^{m+n+1}$, $G = \langle b \rangle \cdot (\langle a \rangle \times \langle c \rangle) = \langle a \rangle \cdot (\langle b \rangle \times \langle c \rangle)$ (semidirect products with kernels in brackets) is nonmetacyclic. Here $G' = \langle c \rangle$, $Z(G) = \Phi(G) = \langle a^p \rangle \times \langle b^p \rangle \times \langle c \rangle$. If $m + n > 2$, then $\Omega_1(G) = \langle \Omega_1(\langle a \rangle), \Omega_1(\langle b \rangle), c \rangle \cong E_{p^3}$.

(b) $a^{p^m} = b^{p^n} = 1$, $m > 1$, $a^b = a^{1+p^{m-1}}$, $|G| = p^{m+n}$ is metacyclic. Here $G' = \langle a^{p^{m-1}} \rangle$, $Z(G) = \Phi(G) = \langle a^p \rangle \times \langle b^p \rangle$, $\Omega_1(G) = \langle a^{p^{m-1}}, b^{p^{n-1}} \rangle \cong E_{p^2}$. If $\Omega_1(G) \not\leq Z(G)$, then $n = 1$ so $G \cong M_{p^{m+1}}$.

(c) $a^4 = 1$, $a^2 = b^2$, $a^b = a^{-1}$, $G \cong Q_8$.

If $|\Omega_1(G)| \leq p^2$, then G is metacyclic. The group G is nonmetacyclic if and only if G' is a maximal cyclic subgroup of G . Next, $|G/\Omega_1(G)| \leq p^3$ with equality if and only if G is from (a) and $p > 2$. If, in (a), $u \in G - \Phi(G)$, then $\langle u \rangle \not\leq G$. All members of the set Γ_1 have ranks at most 3. If N is normal in G and G/N is not cyclic, then $N \leq Z(G)$.

In what follows G is a nonabelian group of order p^m .

Let us prove that if, in Lemma 76.1, G' is not a maximal cyclic subgroup of G , then G is metacyclic. Let $G' < L < G$, where L is cyclic of order p^2 . By Theorem 6.1, $L/G' \leq C/G'$, where C/G' is a cyclic direct factor of G/G' ; in particular, G/C is cyclic. It remains to show that C is cyclic. We get $G' = \Phi(L) \leq \Phi(C)$. It follows that $C/\Phi(C)$ as an epimorphic image of a cyclic group C/G' , is cyclic. In that case, C is also cyclic, as was to be shown.

In what follows G is a nonabelian group of order p^m .

Lemma 76.2. *Suppose that a p -group G is neither abelian nor an \mathcal{A}_1 -group and $\Gamma_1 = \{H_1, \dots, H_p, A\}$, where A is abelian. Then $H'_1 = \dots = H'_p$ and G/H'_1 is an \mathcal{A}_1 -group so $|G'| = p|H'_1|$. In particular, $d(H_i) \leq 3$ for all i . If, in addition, $d(H_i) = 2$ for $i = 1, \dots, p$, and L is a G -invariant subgroup of index p in H'_1 , then G/L is an \mathcal{A}_2 -group.*

Proof. By Remark 1, H_1, \dots, H_p are nonabelian. Let $|H'_1| \leq \dots \leq |H'_p|$. Since $(H_1/H'_1) \cap (A/H'_1) \leq Z(G/H'_1)$, we get $G/H'_1/Z(G/H'_1) \cong E_{p^2}$ so all maximal subgroups of G/H'_1 must be abelian so $H'_1 = \dots = H'_p$ since $d(G) = 2$. Assume that G/H'_1 is abelian; then $G' = H'_1$. Let L be a G -invariant subgroup of index p in G' . Then, by Lemma 65.2(a), G/L is an \mathcal{A}_1 -group since $d(G/L) = 2$, so $H'_1 \leq L < G' = H'_1$, a contradiction. Thus, G/H'_1 is an \mathcal{A}_1 -group so $|G'| = p|H'_1|$. By Lemma 76.1, $d(H_i) = d(H_i/H'_1) \leq 3$. Next suppose that $d(H_i) = 2$ for $i = 1, \dots, p$ and L is taken as above; then H_i/L is an \mathcal{A}_1 -group (Lemma 65.2(a)) so G/L is an \mathcal{A}_2 -group. \square

Lemma 76.3. *If all members of the set Γ_2 are abelian, then $d(G) \leq 3$. If, in addition, $d(G) = 3$, then $\Phi(G) \leq Z(G)$.*

Proof. Suppose that $d(G) > 3$. Take $F \in \Gamma_1$; then F contains at least $p^2 + p + 1$ (abelian) members of the set Γ_2 so it is abelian (Exercise 1.6(a)). In that case, since G is not two-generator, it is abelian (Lemma 76.1), contrary to the hypothesis. Now suppose that $d(G) = 3$. Then $C_G(\Phi(G)) \geq \langle H \mid H \in \Gamma_2 \rangle = G$, completing the proof. \square

In what follows we make use of the following fact: If N is a normal subgroup of a p -group G , $|G/N| > p^2$ and G/N is generated by subgroups of index p^2 , whose inverse images in G are abelian, then $N \leq Z(G)$. Indeed, $C_G(N) \geq \langle H < G \mid N < H, |G : H| = p^2 \rangle = G$.

Lemma 76.4. *Let G be a nonmetacyclic \mathcal{A}_2 -group of order $p^m > p^4$. Then*

- (a) $d(G) \leq 3$, $|G'| \leq p^3$, $\exp(G') = p$, $G/Z(G)$ is of order p^3 and exponent p .
- (b) $\alpha_1(G) \in \{p, p+1, p^2, p^2+p, p^2+p+1\}$.
- (c) *If $\alpha_1(G) < p^2$, then $p > 2$, $d(G) = 2$, and $\text{cl}(G) = 3$.*
 - (c1) *If $\alpha_1(G) = p$, then $G/(G' \cap Z(G))$ is an \mathcal{A}_1 -group, $G' \cong E_{p^2}$.*
 - (c2) *If $\alpha_1(G) = p+1$, then $|G| = p^5$, $G' = \Omega_1(G) \cong E_{p^3}$, $Z(G) = K_3(G) = \mathfrak{V}_1(G) \cong E_{p^2}$.*
- (d) *If $\alpha_1(G) = p^2$, then $d(G) = 3$, $G/Z(G) \cong E_{p^2}$, $|G'| = p$.*
- (e) *If $\alpha_1(G) = p^2+p$, then $d(G) = 3$, $G' \cong E_{p^2}$, $G' \leq Z(G) = \Phi(G)$.*
- (f) *If $\alpha_1(G) = p^2+p+1$, then $p = 2$, $|G| = 2^6$, G is special with $G' = Z(G) = \Phi(G) = \Omega_1(G) \cong E_8$.*

Proof. (a) Two inequalities follow from Lemmas 76.1 and 64.1(u). Next, $\exp(G') = p$ (Theorem 65.7(d)). If $d(G) = 3$, then $\Phi(G) \leq Z(G)$, by the paragraph preceding the lemma. If $p > 2$, then $|G/\mathfrak{V}_1(G)| > p^2$ (Theorem 9.11) so $G/\mathfrak{V}_1(G)$ is generated by subgroups of index p^2 , and we get $\mathfrak{V}_1(G) \leq Z(G)$. Hence, the last assertion of (a) holds for $p > 2$. Now suppose that $p = 2$ and $d(G) = 2$. However, this case does not occur according to Propositions 71.1 to 71.5. Indeed, the results of §71 imply that an \mathcal{A}_2 -group of order $2^m > 2^4$ with $d(G) = 2$ must be metacyclic (this is also true for $m \leq 4$, by Lemma 64.1(i)).

Assertions (b) to (f) are direct consequences of §71. Indeed, if G is a group of Proposition 71.1, then $\alpha_1(G) = p^2$, $d(G) = 3$, $G/Z(G) \cong E_{p^2}$, and $|G'| = p$. If G is a group of Proposition 71.3, then $\alpha_1(G) = p$, $p > 2$, $d(G) = 2$, $\text{cl}(G) = 3$, $G' \cong E_{p^2}$, and $\bar{G} = G/(G' \cap Z(G))$ is an \mathcal{A}_1 -group since $d(\bar{G}) = 2$ and $|\bar{G}'| = p$ (Lemma 65.2(a)). If G is a group of Proposition 71.4, then $\alpha_1(G) = p^2 + p$, $d(G) = 3$, $G' \cong E_{p^2}$, and $G' \leq Z(G) = \Phi(G)$. If G is a group of Proposition 71.5 (a), then $\alpha_1(G) = p^2 + p + 1$, $p = 2$, $d(G) = 3$, $|G| = 2^6$, G is special with $G' = Z(G) = \Phi(G) = \Omega_1(G) \cong E_8$; moreover, G is isomorphic to a Sylow 2-subgroup of the Suzuki simple group $\text{Sz}(8)$. If G is a group of Proposition 71.5(b),

then $p > 2$, $d(G) = 2$, $\text{cl}(G) = 3$, $\alpha_1(G) = p + 1$, $|G| = p^5$, $G' = \Omega_1(G) \cong E_{p^3}$, $Z(G) = K_3(G) = \mathcal{V}_1(G) \cong E_{p^2}$. Our proof is complete since the \mathcal{A}_2 -groups of Proposition 71.2 are metacyclic. \square

Let us give a proof, independent of §71, that if G is a nonmetacyclic \mathcal{A}_2 -group with $\alpha_1(G) < p^2$, then $\text{cl}(G) = 3$. It follows from Exercise 1.6(a) that $d(G) = 2$. Assume that $\text{cl}(G) = 2$. Then $G' \leq Z(G)$. Since G is nonmetacyclic, we get $\exp(G') = p$, by Lemma 76.4(a). In that case, G is an \mathcal{A}_1 -group (Lemma 65.2(a)), a contradiction. It remains to prove that $\text{cl}(G) = 3$. This is the case if $|G'| = p^2$. Now let $|G'| = p^3$ (see Lemma 76.4(a)); then $\alpha_1(G) = p + 1$ and G is nonmetacyclic with all two-generator members of the set Γ_1 since the latter has no abelian members (Lemma 64.1(u)). It follows that $G/\mathcal{V}_1(G)$ is nonabelian of order p^3 and exponent p and $\mathcal{V}_1(G) = K_3(G)$ so $|G : G'| = p^2$ (Lemma 64.1(p)), and we get $|G| = |G : G'||G'| = p^5$. Since all subgroups of order p^3 that contain $K_3(G)$, are abelian (G is an \mathcal{A}_2 -group!) and generate G , we get $K_3(G) = Z(G)$ since $|G : Z(G)| > p^2$, and so $\text{cl}(G) = 3$.

Remarks. Suppose that $A, B \in \Gamma_1$ are distinct.

2. If A is abelian and B an \mathcal{A}_1 -group, then $|G/Z(G)| \leq p^3$. If, in addition, A is the unique abelian member of the set Γ_1 , then $G/Z(G)$ is either of order p^3 and exponent p or $G/Z(G) \cong D_8$. Indeed, $|G'| \leq p^2$ (Lemmas 64.1(u) and 76.1) so $|G : Z(G)| \leq p^3$ (Lemma 64.1(q)). If A is the unique abelian member of the set Γ_1 , then $|G : Z(G)| = p^3$ so $G/Z(G)$ has at most one cyclic subgroup of index p , and the last assertion follows.

3. If A, B are \mathcal{A}_1 -subgroups, then $|G/Z(G)| \leq p^4$. Indeed, put $D = A \cap B$. Then $Z(A) = \Phi(A) \leq \Phi(G) \leq A \cap B = D$ and similarly $Z(B) < D$ so, comparing orders, we conclude that $Z(A)$ and $Z(B)$ are maximal in D (Lemma 76.1). It follows that $U = Z(A) \cap Z(B)$ has index at most p^2 in D and $U \leq Z(G)$ since $C_G(U) \geq AB = G$, and we get $|G/Z(G)| \leq |G/U| \leq |G/D||D/U| \leq p^4$.

The following lemma is the key result.

Lemma 76.5. *Suppose that H is a nonabelian maximal subgroup of a p -group G . Then $\beta_1(G, H) \geq p - 1$. If $\beta_1(G, H) = p - 1$, then the following holds:*

- (a) $d(G) = 2$, $\Gamma_1 = \{H_1 = H, H_2, \dots, H_p, A = H_{p+1}\}$, where A is abelian and all members of the set $\Gamma_1 - \{H, A\}$ are \mathcal{A}_1 -groups.
- (b) $H'_1 = \dots = H'_p$ is of order p .
- (c) G/H'_1 is an \mathcal{A}_1 -group so $|G'| = p^2$. We also have $d(H_1) \leq 3$. If G is nonmetacyclic, then G/H'_1 is also nonmetacyclic.
- (d) $G/Z(G)$ is either nonabelian of order p^3 and exponent p or $G/Z(G) \cong D_8$, $Z(H_i) = Z(G)$ and H_i/G' is cyclic, $i = 2, \dots, p$. In particular, $\text{cl}(G) = 3$.
- (e) If $G' \cong C_{p^2}$, then H_2, \dots, H_p, A are metacyclic and G has no normal subgroups of order p^3 and exponent p . If $p > 2$, then G is metacyclic (in that case, G is an \mathcal{A}_2 -group, by Corollary 65.3).

(f) If $G' \cong E_{p^2}$, then $\text{cl}(G) = 3$.

In what follows we assume that G is not an \mathcal{A}_2 -group: then $|G| = p^m > p^4$. Since $|G'| = p^2$, G is nonmetacyclic.

(g) $d(H) = 3$.

In what follows we assume, in addition, that $p = 2$. Then, since G is not of maximal class, we get $|G : G'| > 4$, by Taussky's theorem.

(h) $d(A) = 2$ so A is metacyclic.

(i) G has no normal elementary abelian subgroups of order 8.

(j) H_2 is metacyclic.

(k) $U = \Omega_1(H_2) = \Omega_1(A) < \Phi(G)$ is the unique normal abelian four-subgroup of G .

(l) If $Z(G)$ is cyclic, then $H_2 \cong M_{2^{m-1}}$ and $G' \not\leq Z(G)$. In that case, if $\tilde{G} = G/H'$ and $\tilde{T} = \Omega_1(\tilde{H})$, then $\tilde{T} = \Omega_1(\tilde{G}) \cong E_8$ and $T = Q * L$, where $L \cong C_4$, $Q \cong Q_8$, $Q \triangleleft G$ and G/Q is cyclic so $G' < Q$ is cyclic of order 4. Since $\Omega_1(G) = T$, it follows that G has exactly 7 involutions. Next, G/G' is abelian with cyclic subgroup of index 2 and G has no elementary abelian subgroups of order 8.

(m) Suppose that $Z(G)$ is noncyclic. Then $G' \cong C_4$ is a maximal cyclic subgroup of G . Let T be as in (l). Then $|T| = 16$ and $T = Q \times L$, where Q is nonabelian of order 8. Next, H_2/G' is cyclic since $G' \not\leq Z(G) = Z(H) = \Phi(H)$ and H_2 has no cyclic subgroups of index 2. The quotient group A/G' is also cyclic.

(n) G' is a maximal cyclic subgroup of G .

Proof. The set $\Gamma_1(H) \cap \Gamma_2$ contains a member N ; then $N \not\leq Z(G)$ since H is non-abelian. Set $\Gamma_1^N = \{H_1 = H, \dots, H_p, H_{p+1}\}$. Since at most one member of the set Γ_1^N is abelian, one may assume that H_1, \dots, H_p are nonabelian. By Remark 1, $\beta_1(G, H) \geq p - 1$. Next we suppose that $\beta_1(G, H) = p - 1$.

(a–c) If $U_i \leq H_i$ is an \mathcal{A}_1 -subgroup not contained in N (see Theorem 10.28), then U_2, \dots, U_p are pairwise distinct. It follows that U_{p+1} does not exist so $H_{p+1} = A$ is abelian. Then $N = H \cap A$ is also abelian, and we get $p - 1 = \beta_1(G, H) \geq \sum_{i=2}^p \alpha_1(H_i)$. It follows that $\alpha_1(H_i) = 1$ ($i = 2, \dots, p$) so H_2, \dots, H_p are \mathcal{A}_1 -groups and the subgroups H_1, \dots, H_p together contain all \mathcal{A}_1 -subgroups of G . Assume that $F \in \Gamma_1 - \Gamma_1^N$. The intersection $F \cap H_i$ is abelian since H_i is an \mathcal{A}_1 -subgroup, $i = 2, \dots, p$. Therefore, if F is nonabelian, then all \mathcal{A}_1 -subgroups of F are contained in H_1 . In that case, $F \leq H_1$ (Theorem 10.28), a contradiction. Thus, all members of the set $\Gamma_1 - \Gamma_1^N$ are abelian. Assuming that $d(G) > 2$, we see that the set Γ_1 has at least $(p^2 + p + 1) - p = p^2 + 1 > p + 1$ abelian members, contrary to Exercise 1.6(a). Thus, $\Gamma_1 = \Gamma_1^N = \{H_1, \dots, H_p, A\}$ so $d(G) = 2$ and $\Phi(G) = N$, completing the proof of (a). Now (b) follows from (a) and Lemma 76.2. By Lemma 76.2 again, G/H'_1 is an \mathcal{A}_1 -group and hence $|G'| = p|H'_1| = p^2$. In that

case, $d(H_1) = d(H_1/H'_1) \leq 3$ (Lemma 76.1). The last assertion in (c) follows from Theorem 36.1.

(d) It follows from $d(G) = 2$ that $|G : Z(G)| > p^2$. By Remark 2, $G/Z(G)$ is either nonabelian of order p^3 and exponent p or $G/Z(G) \cong D_8$ since A is the unique abelian member of the set Γ_1 . Now let $i \in \{2, \dots, p\}$. In view of $d(G) = 2$, we get $Z(G) \leq \Phi(G) < H_i$ so $Z(G) \leq Z(H_i)$, and the equality $|Z(G)| = |Z(H_i)|$ implies $Z(G) = Z(H_i) (= \Phi(H_i))$. Therefore, since $G' \not\leq Z(G)$, then H_i/G' is cyclic.

(e) Suppose that $G' \cong C_{p^2}$. Then H_i is metacyclic since H'_i is not a maximal cyclic subgroup in H_i in view of $H'_i < G', i = 2, \dots, p$ (Lemma 76.1). Assume that G has a normal subgroup R of order p^3 and exponent p . For $i = 2, \dots, p$, we get $H_i R = G$ so $G/(R \cap H_i) = (H_i/(R \cap H_i)) \times (R/(R \cap H_i))$, and we conclude that $H_i/(R \cap H_i)$ is cyclic; then $G/(R \cap H_i)$ is abelian. On the other hand, $G/(R \cap H_i)$ is nonabelian since $C_{p^2} \cong G' \not\leq R \cap H_i \cong E_{p^2}$, and this is a contradiction. Thus, R does not exist so A is metacyclic. Let $p > 2$. Since G' is cyclic, G is regular (Theorem 7.1(c)) so $p^2 = |\Omega_1(G)| = |G/\Omega_1(G)|$ whence G is metacyclic (Theorem 9.11).

(f) If $G' \cong E_{p^2}$, then $G' \not\leq Z(G)$ ((a) and Lemma 65.2(a)) so $\text{cl}(G) = 3$.

(g) By hypothesis, H is not an \mathcal{A}_1 -group (otherwise, G is an \mathcal{A}_2 -group). By Lemma 65.2(a), $d(H) > 2$. Since G/H' is an \mathcal{A}_1 -group, we get $d(H) \leq 3$, and our claim is proved.

In what follows we assume that $p = 2$ so $|G : G'| > 4$ since G is not of maximal class (Taussky).

(h) By Theorem 71.6, the number of two-generator members in the set Γ_1 is even. Since $|\Gamma_1| = 3$ and $d(H_2) = 2 < 3 = d(H)$, by (g), we get $d(A) = 2$, so A is metacyclic. Clearly, A is noncyclic.

(i) Assume that $E_8 \cong E \triangleleft G$. Then $E \cap A = \Omega_1(A)$, by (h). We have $C_G(E \cap A) = EA = G$ so $E \cap A \leq Z(G)$. Since $E \not\leq A \in \Gamma_1$ and $|\Gamma_1| = 3$, the number of maximal subgroups of G/E is < 3 so G/E is cyclic. In that case, $A = L \times Z$, where $|L| = 2$ and Z is cyclic so A/L is a cyclic subgroup of index 2 in G/L (we have $L < \Omega_1(A) \leq Z(G)$). Since $L < Z(G)$ and $G/Z(G) \cong D_8$, G/L is of maximal class (Theorem 1.2). However, G/L has a normal subgroup $E/L \cong E_4$ and $|G/L| \geq 2^4$, and this is a contradiction. Thus, E does not exist.

(j) Assume that H_2 is nonmetacyclic. Then $\Omega_1(H_2) \cong E_8$ (Lemma 65.1) and $\Omega_1(H_2) \triangleleft G$, contrary to (i).

(k) Since the two-generator 2-group G has no cyclic subgroups of index 2, the subgroup $\Phi(G)$ is noncyclic. We have $H_2 \cap A = \Phi(G)$ is noncyclic so $U = \Omega_1(H_2) = \Omega_1(A) \cong E_4$. Assume that $V \neq U$ is a G -invariant four-subgroup. Then $V \not\leq H_2, A$ so G/V is cyclic. Since G has no cyclic subgroups of index 2 and $|G| > 2^4$, we get $\Omega_1(G) = UV \cong E_8$, contrary to (i). Thus, V does not exist.

Let $\bar{G} = G/H'$ and $\bar{T} = \Omega_1(\bar{H})$; then $\bar{T} \cong E_8$ is normal in \bar{G} since \bar{H} is abelian of rank 3, by (g). Since \bar{G} is minimal nonabelian, by (c), we get $\Omega_1(\bar{G}) = \bar{T}$ so $\Omega_1(G) \leq T$. Assume that $|G| > 2^5$. Then $\bar{G}/\bar{T} \cong G/T$ is cyclic since $T \not\leq A, H_2$,

by (h) and (j). Since $d(T) = 3$, it follows that T is nonabelian, by (i). By (k), $U < T$, where U is the unique normal abelian four-subgroup of G . Let $Q < T$ be minimal nonabelian; then $|Q| = 8$, $T = QZ(T)$ (Lemma 64.1(i)) and $Z(T) \triangleleft G$ since $T \triangleleft G$.

(l) Suppose that $Z(G)$ is cyclic. Then the noncyclic abelian subgroup $\Phi(G)$ has a cyclic subgroup $Z(G)$ of index 2 (recall that $8|Z(G)| = |G| = 4|\Phi(G)|$ and $Z(G) < \Phi(G)$ since $d(G) = 2$) so $\Omega_1(\Phi(G)) = U \not\leq Z(H_2)$ (otherwise, $C_G(U) \geq H_2 A = G$ and $E_4 \cong U \leq Z(G)$, contrary to the assumption) so $H_2 \cong M_{2m-1}$ (Lemma 76.1). Let T be defined as in the previous paragraph. Then $Z(T)$ is cyclic (otherwise, since $Z(T) \triangleleft G$, we get $Z(T) = U$, by (k), and $C_G(U) \geq TA = G$; then $Z(G)$ is noncyclic, a contradiction), so, by the product formula, $H = QZ(G)$, where $Q \cong Q_8$ (Appendix 16) since $Q \not\leq A, H_2$. Since Q is the unique subgroup isomorphic to Q_8 in T (Appendix 16), we get $Q \triangleleft G$, and then G/Q is cyclic since $d(G) = 2$ and $Q \not\leq A$. In that case, $G' < Q$ is of order 4 so $G' \cong C_4$ and $G' \not\leq Z(G) = Z(H_2)$. Then G/G' , as abelian group of type $(|G/Q|, 2)$, has exactly two cyclic subgroups H_2/G' and A/G' of index 2 (H/G' is not cyclic since $d(H) = 3$). Assume that $E_8 \cong E < G$. Then $E \cap A = \Omega_1(A) = U$ so $C_G(U) \geq EA = G$, contrary to the cyclicity of $Z(G)$. Thus, G has no elementary abelian subgroups of order 8. By the above and Appendix 16, T has exactly 7 involutions so G has also 7 involutions since $\Omega_1(G) = T$ (see Theorem 43.10).

(m) Suppose that $Z(G)$ is noncyclic; then $U = \Omega_1(Z(G))$. We have $G' \neq U$ (otherwise, G is an \mathcal{A}_1 -group, by (a) and Lemma 65.2(a), a contradiction). Since U is the unique normal four-subgroup of G , we get $G' \cong C_4$. Let $T/H' = \Omega_1(H/H')$ be as in (l); then $T/H' \cong E_8$ (see the proof of (l)), T is nonabelian and $T = QZ(T)$, where Q is nonabelian of order 8 (Lemma 64.1(i)). As above, G/T is cyclic so $G' < T$. Since $U < T \cap Z(G)$, we get $T = Q \times L$, where $|L| = 2$. We know that $\Omega_1(G) = \Omega_1(T)$. Since $Z(T) = U \neq G'$, we get $G' \not\leq Z(T)$ so $G' \not\leq Z(G)$ hence $\text{cl}(G) = 3$. Since $U < H_2$, H_2 has no cyclic subgroups of index 2 (otherwise, $\Omega_1(H_2) = U \leq Z(G)$ so H_2 is abelian). Next, H_2/G' is cyclic since $G' \not\leq Z(G) = Z(H) = \Phi(H)$. Since G/G' is abelian with cyclic subgroup of index 2, it follows that A/G' is cyclic (otherwise, H/G' is cyclic so H is metacyclic, which is a contradiction).

(n) By (l) and (m), $G' \cong C_4$. Assume that $G' < Z$, where $Z \cong C_8$. Then $G'/H' < Z/H'$ so G'/H' is not a maximal cyclic subgroup of the \mathcal{A}_1 -group G/H' . It follows that G/H' is metacyclic (Lemma 76.1). In that case, G is metacyclic, by Theorem 36.1, which is a contradiction. Thus, $G' < G$ is maximal cyclic. \square

Remarks. 4. Let G be a p -group and let members H_1, \dots, H_k , $k > 1$, of the set Γ_1 contain together all \mathcal{A}_1 -subgroups of G . Suppose that there exists $A \in \Gamma_1 - \{H_1, \dots, H_k\}$ such that $A \cap H_i$ is abelian for all $i = 2, \dots, k$. Then A is abelian. Assuming that this is false, we can take an \mathcal{A}_1 -subgroup $U \leq A$ such that $U \not\leq H_1$ (Proposition 10.28). Since, for $i = 2, \dots, k$, also $U \not\leq H_i$ (recall that $A \cap H_i$ is abelian, by hypothesis), we get a contradiction.

5. For a nonabelian p -group G , the following two conditions are equivalent: (a) G

is of maximal class with abelian subgroup A of index p . (b) Whenever $H \leq G$ is nonabelian of order p^k , then $\alpha_1(H) = p^{k-3}$. In the proof we use induction on $|G|$. Let us prove that (a) \Rightarrow (b). By Fitting's lemma, all members of the set $\Gamma_1 - \{A\}$ are of maximal class so, by Hall's enumeration principle and induction,

$$\alpha_1(G) = \sum_{H \in \Gamma_1 - \{A\}} \alpha_1(H) = p \cdot p^{m-1-3} = p^{m-3}.$$

Next, let $L < G$ be nonabelian. Then $L \leq H \in \Gamma_1$ and the subgroup H of maximal class has an abelian subgroup $H \cap A$ of index p so, by induction, L is of maximal class and $\alpha_1(L) = p^{l-3}$, where $|L| = p^l$. Now we prove that (b) \Rightarrow (a). In that case, all proper nonabelian subgroups of G are of maximal class, by induction. Take $T \leq G$, where T is an \mathcal{A}_1 -subgroup of G . Setting $|T| = p^k$, we get $1 = \alpha_1(T) = p^{k-3}$ so $k = 3$, i.e., all \mathcal{A}_1 -subgroups of G have the same order p^3 . Assume that G is not of maximal class. Then we get $C_H(T) \not\leq T$ (Lemma 64.1(i)). Let F be a subgroup of order p^2 in $C_H(T)$ such that $Z(T) < F$. Then $|FT| = p^4$ and $\alpha_1(FT) = p^2 \neq p = p^{4-3}$, a contradiction. Thus, G is of maximal class. Next, let $R \triangleleft G$ be of order p^2 and set $U = C_G(R)$; then $|G : U| = p$ and, by induction, U is abelian since it is not of maximal class.

6. Let $d(G) = 3$ and $\Phi(G) \not\leq Z(G)$; then the set Γ_2 has a nonabelian member N (Lemma 76.3). We claim that the set Γ_2 contains at least p^2 nonabelian members. Let $A_1, A_2 \in \Gamma_2$ be distinct abelian; then $A = A_1 A_2 \in \Gamma_1$ contains exactly $p + 1$ members of the set Γ_2 and all of them are abelian since $\Phi(G) = A_1 \cap A_2 \leq Z(A)$. Assume that $B \in \Gamma_2 - \Gamma_1(A)$ is abelian. Then $C_G(\Phi(G)) \geq AB = G$, contrary to the hypothesis. Thus, $\Gamma_1(A) \cap \Gamma_2$ is the set of all abelian members of the set Γ_2 so the last set contains exactly $|\Gamma_2| - (p + 1) = p^2$ nonabelian members. Thus, in our case, the set Γ_2 has $p^2, p^2 + p$ or $p^2 + p + 1$ nonabelian members.

7. Let G be a nonabelian p -group with $d = d(G) > 3$. Let $\mathfrak{T} = \{T_1, \dots, T_r\} \subseteq \Gamma_2$ and $\mathfrak{M} = \{M_1, \dots, M_s\} \subseteq \Gamma_1$ be the sets of nonabelian members of the sets Γ_2, Γ_1 , respectively ($\mathfrak{T} \neq \emptyset$, by Lemma 76.3, $\mathfrak{M} \neq \emptyset$, by Exercise 1.6(a)). We claim that $r > (p - 1)s$. Let μ_i be the number of members of the set \mathfrak{M} , containing T_i , $i = 1, \dots, r$, and let γ_j be the number of members of the set \mathfrak{T} contained in M_j , $j = 1, \dots, s$. Then, by double counting,

$$\mu_1 + \dots + \mu_r = \gamma_1 + \dots + \gamma_s,$$

and, in view of $\mu_i = p + 1$ for all i , that formula can be rewritten as follows:

$$(3) \quad (p + 1)r = \gamma_1 + \dots + \gamma_s.$$

Note that M_j contains exactly $p^{d-2} + p^{d-3} + \dots + p + 1$ members of the set Γ_2 . Since, by Exercise 1.6(a), the set $\Gamma_1(M_j)$ contains at most $p + 1$ abelian members, we

get $\gamma_j \geq p^{d-2} + \dots + p^2$ for $j = 1, \dots, s$, and we deduce from (3) the following inequality: $(p+1)r \geq (p^{d-2} + \dots + p^2)s$. We get

$$r \geq \frac{p^{d-2} + \dots + p^2}{p+1}s \geq \frac{p^2}{p+1}s = \frac{(p^2-1)+1}{p+1}s > (p-1)s,$$

as was to be shown. By Exercise 1.6(a), we have $s \geq |\Gamma_1| - (p+1) = p^{d-1} + \dots + p^2$.

8. Given a set \mathfrak{M} of subgroups of a p -group G , let $\alpha_1(\mathfrak{M})$ denote the number of \mathcal{A}_1 -subgroups that contain together members of the set \mathfrak{M} . Suppose that G is neither abelian nor an \mathcal{A}_1 -group. We claim that if, for each $K \in \Gamma_2$, we have $\alpha_1(\Gamma_1^K) \leq p+1$, then G is an \mathcal{A}_2 -group. By hypothesis, there is $K \in \Gamma_2$ which is not contained in $Z(G)$. Indeed, this is the case if $d(G) = 2$. If $d(G) > 2$, our claim is obvious. Set $\Gamma_1^K = \{H_1, \dots, H_{p+1}\}$ and let $\alpha_1(H_1) \geq \dots \geq \alpha_1(H_{p+1})$. Since at most one member of the set Γ_1^K is abelian, H_1, \dots, H_p are nonabelian. Assume that $\alpha_1(H_1) > 1$; then $\alpha_1(H_1) = p$, by Remark 1 and hypothesis. We get

$$p+1 \geq \alpha_1(\Gamma_1^K) = \alpha_1(H_1) + \sum_{i=2}^{p+1} \beta_1(H_i, K) = p + \sum_{i=2}^{p+1} \beta_1(H_i, K)$$

so $\beta_1(H_2, K) = 1$ and we get $p = 2$ and $\beta_1(H_3, K) = 0$ (Remark 1) whence H_3 is abelian, and we conclude that K is abelian; in that case, H_2 is an \mathcal{A}_1 -group. Thus, all members of the set Γ_2 are abelian so $d(G) \leq 3$ (Lemma 76.3). Assume that G is not an \mathcal{A}_2 -group. If $d(G) = 2$, then $\Gamma_1 = \Gamma_1^K = \{H_1, H_2, A\}$, where $\alpha_1(H_1) = 2$, $\alpha_1(H_2) = 1$ and A is abelian. In this case, $\beta_1(G, H_1) = 1$ so $|H'_1| = 2$ (Lemma 76.5), and the equality $\alpha_1(H_1) = 2$ is impossible (Lemma 76.4(c)), a contradiction. Now assume that $d(G) = 3$; then $|\Gamma_1(H_1) \cap \Gamma_2| = p+1 > 1$ so $|H'_1| = 2$ (Lemma 64.1(q)), and again we get a contradiction.

Lemma 76.6. *Suppose that $\alpha_1(G) > 1$. Then $\alpha_1(G) \geq p$.*

- (a) *If $\alpha_1(G) = p$, then G is an \mathcal{A}_2 -group with $d(G) = 2$ and $|G'| = p^2$. If G is nonmetacyclic, it is of class 3.*
- (b) *If $\alpha_1(G) = p+1$, then G is an \mathcal{A}_2 -group with $d(G) = 2$. If G is not metacyclic, then $p > 2$, G is of order p^5 with $G' \cong E_{p^3}$ and of class 3.*

Proof. The inequality $\alpha_1(G) \geq p$ follows from Remark 1. By Remark 8, G is an \mathcal{A}_2 -group. All remaining assertions follows from Lemma 76.4(c). \square

Lemma 76.7. *Let $N \in \Gamma_2$ and $\Gamma_1^N = \{H_1, \dots, H_{p+1}\}$. Then:*

- (a) *$\alpha_1(G) \geq \alpha_1(N) + \sum_{i=1}^{p+1} \beta_1(H_i, N)$.*
- (b) *If N is nonabelian, then $\beta_1(G, N) \geq p^2 - 1$.*
- (c) *If $\alpha_1(G) < p^2$, then $N_G(K)/K$ has only one subgroup of order p for each nonabelian $K < G$.*

Proof. (a) is obvious, (b) follows from (a) and Remark 1. It remains to prove (c). Assume that $K < G$ is nonabelian and $N_G(K)/K$ contains an abelian subgroup L/K of type (p, p) ; then $1 + \beta_1(L, K) \leq \alpha_1(K) + \beta_1(L, K) = \alpha_1(L) \leq \alpha_1(G) \leq p^2 - 1$ so $\beta_1(L, K) < p^2 - 1$, contrary to (b). Thus, L/K does not exist so $N_G(K)/K$ has only one subgroup of order p so it is either cyclic or generalized quaternion. \square

Lemma 76.8. Suppose that G is an \mathcal{A}_n -group, $n > 2$. (a) If $d(G) > 2$ then $\alpha_1(G) \geq p^2$. (b) If $d(G) = 3$ and $\Phi(G) = Z(G)$, then $\alpha_1(G) \geq 2p^2 + p - 1$. (c) If $d(G) = 3$ and $|G : Z(G)| = p^2$, then $\alpha_1(G) \geq 2p^2 - 1$.

Proof. (a) There is $N \not\leq Z(G)$ for some $N \in \Gamma_2$ since $\langle M \mid M \in \Gamma_2 \rangle = G$. If all such N are abelian, then $\alpha_1(G) = \sum_{H \in \Gamma_1} \alpha_1(H) \geq p(|\Gamma_1| - (p + 1)) \geq p^3 > p^2$ (Exercise 1.6(a) and Lemma 76.6). If N is nonabelian, then $\alpha_1(G) \geq p^2$ (Lemma 76.7(b)).

(b) If $L \in \Gamma_1$ is nonabelian, then $|L : Z(L)| = |L : Z(G)| = p^2$ so $|L'| = p$ (Lemma 64.1(q)). Suppose that L is neither abelian nor an \mathcal{A}_1 -group (such an L exists since $n > 2$). Then, by Lemma 76.4, $\alpha_1(L) \geq \alpha_1(H) \geq p^2$, where $H \leq L$ is an \mathcal{A}_2 -subgroup. In view of $|G : Z(G)| = p^3$, the set Γ_1 has at most one abelian member (Lemma 64.(u)) so this set has at least $p^2 + p$ nonabelian members, and, by Hall's enumeration principle, $\alpha_1(G) = \alpha_1(L) + \sum_{M \in \Gamma_1 - \{L\}} \alpha_1(M) \geq p^2 + p^2 + p - 1 = 2p^2 + p - 1$ (we have here equality if and only if $\alpha_1(L) = p^2$ and all nonabelian members of the set $\Gamma_1 - \{L\}$ are \mathcal{A}_1 -groups).

(c) In our case, $|G'| = p$ and all members of the set Γ_2 are abelian, the set Γ_1 has exactly p^2 nonabelian members (Remark 6). If $L \in \Gamma_1$ is neither abelian nor an \mathcal{A}_1 -group, then $\alpha_1(L) \geq p^2$ (see the proof of (b)) so we get $\alpha_1(G) = \alpha_1(L) + \sum_{M \in \Gamma_1 - \{L\}} \alpha_1(M) \geq p^2 + (p^2 - 1) = 2p^2 - 1$. \square

Theorem 76.9. A p -group G with $1 < \alpha_1(G) < p^2$ is a two-generator \mathcal{A}_2 -group. In particular, $\alpha_1(G) \in \{p, p + 1\}$.

Proof. Suppose that G is a counterexample of minimal order; then $p^2 > \alpha_1(G) > p + 1$ (Lemma 76.6(a,b)) so $p > 2$. By Lemma 76.8(a), $d(G) = 2$ so $\Phi(G) > Z(G)$. By Lemma 76.7(c), $\Phi(G)$ is abelian. By Proposition 10.28 and induction, G is an \mathcal{A}_3 -group. Then there is $H \in \Gamma_1$, which is an \mathcal{A}_2 -group, and so, by Proposition 10.28, Lemmas 76.4 and 76.6, $d(H) = 2$, $|H'| > p$ and $\alpha_1(H) \in \{p, p + 1\}$.

(i) Assume that $A, U \in \Gamma_1$, where A is abelian and U is an \mathcal{A}_1 -group. Then $G/Z(G)$ is of order p^3 and exponent p (Remark 2), and $Z(G) < \Phi(G) < H$. In that case, $|H : Z(G)| = p^2$ so $|H'| = p$ (Lemma 64.1(q)), contrary to what has been said in the previous paragraph. Thus, a pair (A, U) does not exist.

Let $F_1, \dots, F_s, V_1, \dots, V_u$ be all nonabelian members of the set Γ_1 , where $\alpha_1(F_i) = p$ and $\alpha_1(V_k) = 1$ (since $\Phi(G)$ is abelian, the set Γ_1 has no members H with $\alpha_1(H) = p + 1$, by Lemma 76.4). Since the set Γ_1 has at most one abelian member (Lemma 64.1(u)), we get $s + u \geq |\Gamma_1| - 1 = p$.

(ii) Assume that $A \in \Gamma_1$ is abelian. Then $u = 0$, by (i), so $s = p$ and, since $\Phi(G)$ is abelian, $p^2 > \alpha_1(G) = \sum_{i=1}^p \alpha_1(F_i) = p \cdot p = p^2$, a contradiction.

Thus, all members of the set Γ_1 are nonabelian, i.e., $s + u = p + 1$. As in the previous paragraph, $s < p$ so $u \geq 2$. Then G and all members of the set Γ_1 are two-generator so G is either metacyclic or $G/\text{K}_3(G)$ is nonabelian of order p^3 and exponent p and then $|G : G'| = p^2$ (Lemma 64.1(p)).

(ii1) Assume that G is metacyclic. Then $V_1, V_2 \in \Gamma_1$ are distinct \mathcal{A}_1 -subgroups so G is an \mathcal{A}_2 -group (Exercise 1), a contradiction. Thus, G is nonmetacyclic.

(ii2) Since $u > 1$, then $|G'| \leq p|V'_1V'_2| = p^3$ so $|G| = |G : G'||G'| \leq p^5$. Since G is not an \mathcal{A}_2 -group, we get $|G| = p^5$. In that case, G has a nonabelian subgroup of order p^3 . Since all nonabelian groups of order p^3 are \mathcal{A}_1 -groups, we get by Proposition 2.3, $\alpha_1(G) \geq p^2$, a final contradiction. \square

Let G be a p -group of maximal class and order p^5 with abelian subgroup of index p . Then $\alpha_1(G) = p^2$ and G is an \mathcal{A}_3 -group.

Remark 9. Let a p -group G be neither abelian nor an \mathcal{A}_1 -group. If, for each $K \in \Gamma_2$, we have $\alpha_1(\Gamma_1^K) \leq p^2$, then G is either an \mathcal{A}_2 - or \mathcal{A}_3 -group. Indeed, let $H_1 \in \Gamma_1$ be nonabelian and take $K \in \Gamma_1(H_1) \cap \Gamma_2$. Set $\Gamma_1^K = \{H_1, \dots, H_{p+1}\}$. Since at most one member of the set Γ_1^K is abelian, we get $\alpha_1(H_1) < p^2$, i.e., H_1 is either \mathcal{A}_1 - or \mathcal{A}_2 -group (Theorem 76.9) so G is an \mathcal{A}_n -group, $n \in \{2, 3\}$.

Theorem 76.10. If $\alpha_1(G) = p^2$, then G is an \mathcal{A}_n -group, $n \in \{2, 3\}$. Next suppose that G is an \mathcal{A}_3 -group. Then $|G'| = p^3$ and $\alpha_1(H) \in \{1, p\}$ for every nonabelian $H < G$.

(a) If the set Γ_2 has a nonabelian member N , then N is an \mathcal{A}_1 -group and one of the following holds:

- (a1) G is metacyclic with $\alpha_1(H) = p$ for all $H \in \Gamma_1$, i.e., all members of the set Γ_1 are \mathcal{A}_2 -groups.
- (a2) $d(G) = 3$, $\Gamma_1 = \{F_1, \dots, F_{p^2+p}, A\}$, where $\alpha_1(F_i) = p$ for all i and A is abelian, $Z(G) = Z(N)$ is of index p^4 and the set Γ_2 has exactly p^2 nonabelian members which are \mathcal{A}_1 -groups.

(b) If all members of the set Γ_2 are abelian, then $d(G) = 2$ and one of the following holds:

- (b1) G is metacyclic, $\Gamma_1 = \{H_1, \dots, H_p, A\}$, where $\alpha_1(H_i) = p$ for all i , $H'_1 = \dots = H'_p$, A is abelian.
- (b2) $\Gamma_1 = \{H_1, \dots, H_p, A\}$, where $\alpha_1(H_i) = p$, $H'_1 = \dots = H'_p$ is of order p^2 , A is abelian, G' is noncyclic, G/H'_1 is an \mathcal{A}_1 -group.
- (b3) $p = 2$, $\Gamma_1 = \{H_1, H_2, H_3\}$, $\alpha(H_1) = 2$, $\alpha(H_2) = \alpha(H_3) = 1$. We have $|G/Z(G)| = 16$.

Proof. Suppose that G is not an \mathcal{A}_2 -group; then G is an \mathcal{A}_3 -group (Proposition 10.28 and Theorem 76.9).

(a) Suppose that the set Γ_2 has a nonabelian member N . Let $\Gamma_1^N = \{H_1, H_2, \dots, H_{p+1}\}$; then all members of the set Γ_1^N are neither abelian nor \mathcal{A}_1 -groups. Using Remark 1, we get

$$p^2 = \alpha_1(G) \geq \alpha_1(N) + \sum_{i=1}^{p+1} \beta_1(H_i, N) \geq 1 + (p-1)(p+1) = p^2,$$

and hence $\alpha_1(N) = 1$, $\beta_1(H_i, N) = p-1$, $\alpha_1(H_i) = p$, $d(H_i) = 2$ and $|H'_i| = p^2$ for all i , H_1, \dots, H_{p+1} are \mathcal{A}_2 -groups (Remark 1, Lemmas 74.4 and 76.6(a)) and these $p+1$ subgroups contain together all \mathcal{A}_1 -subgroups of G . If G is metacyclic, it is as in (a1). Next we assume that G is nonmetacyclic. We also have $d(G) \leq d(H_1) + 1 = 3$.

Suppose, in addition, that $d(G) = 2$ so $N = \Phi(G)$. Then G and all members of the set Γ_1 are two-generator (Lemma 76.6(a)). Since G is nonmetacyclic, we get $p > 2$ and $|G : G'| = p^2$ (Lemma 64.1(p)). By the above and Lemma 76.6(a), H_i has the unique abelian maximal subgroup A_i , all i . Then the subgroups $A_1 \neq A_2$ are normal in G ; therefore, $A = A_1 A_2$ is of class at most 2 (Fitting's lemma). By Lemma 64.1(l), G is not minimal nonmetacyclic so we may assume that H_1 is not metacyclic. Since $A > A_1$ and $\text{cl}(G) \geq \text{cl}(H_1) > 2$ (Lemma 76.4(c)), we get $A \in \Gamma_1$. Then $A_1 = H_1 \cap A = \Phi(G) = N$, a contradiction since N is nonabelian.

Thus, $d(G) = 3$. Then, by Remark 6, the set Γ_2 has at least p^2 nonabelian members, say L_1, \dots, L_{p^2} , and all L_i are \mathcal{A}_1 -groups since G is an \mathcal{A}_3 -group and $|G : L_i| = p^2$. Since $\alpha_1(G) = p^2$, all \mathcal{A}_1 -subgroups of G are members of the set Γ_2 so each nonabelian $H \in \Gamma_1$ is an \mathcal{A}_2 -group. If U_1, \dots, U_{p+1} are all abelian members of the set Γ_2 , then $A = U_1 U_2 \in \Gamma_1$, by the product formula, and $|A'| \leq p$ (Lemma 64.1(q)) so A is not an \mathcal{A}_2 -group since $\alpha_1(A) < \alpha_1(G) = p^2$ (Lemma 76.4). It follows that A is abelian; moreover, A is the unique abelian member of the set Γ_1 (Lemma 76.8(b)). Thus, $\Gamma_1 = \{F_1, \dots, F_{p^2+p}, A\}$, where $\alpha_1(F_i) = p$ and $|F'_i| = p^2$ (Lemma 76.6). Next, in view of $d(F_i) = 2$, we get $Z(F_i) < \Phi(F_i) = \Phi(G) < A$; then $C_G(Z(F_i)) \geq F_i A = G$ so $Z(F_i) \leq Z(G)$ and, by Lemma 64.1(q), $|F_i : Z(F_i)| = p |F'_i| = p^3$. Thus, $|G : Z(G)| \leq p^4$. By Lemma 64.1(q), $|G : Z(G)| = p |G'| \geq p |F'_1| \geq p^3$. Since $G/Z(G)$ is noncyclic and A is the unique abelian member of the set Γ_1 , it follows that $Z(G) \leq F_i$ for some i . By the above, $Z(F_i) \leq Z(G)$ so $Z(G) = Z(F_i)$, and we get $|G : Z(G)| = |G : F_i| |F_i : Z(G)| = p^4$ so $|G'| = \frac{1}{p} |G : Z(G)| = p^3$ and G is as stated in (a2) since, if $N < F_i$, then $Z(N) = \Phi(N) < \Phi(G) < A$ so $C_G(Z(N)) \geq AN = G$ hence $Z(N) \leq Z(G)$ and $|G : Z(N)| = p^4 = |G : Z(G)|$.

(b) Suppose that all members of the set Γ_2 are abelian. Then $p^2 = \alpha_1(G) = \sum_{M \in \Gamma_1} \alpha_1(M)$ since the intersection of any two distinct members of the set Γ_1 is abelian (here we use Hall's enumeration principle). It follows from Remark 6 and

Lemma 76.8(b,c) that $d(G) = 2$ (indeed, if $d(G) = 3$, then $\Phi(G) \leq Z(G)$, by Lemma 76.3, and, by Lemma 76.8(b,c), $\alpha_1(G) \geq 2p^2 - 1 > p^2$).

Let $\{H_1, \dots, H_s, V_1, \dots, V_u\}$ be the set of nonabelian members of the set Γ_1 , where $\alpha_1(H_i) = p$, $\alpha_1(V_j) = 1$ (since $\Phi(G) \in \Gamma_2$ is abelian, the set Γ_1 has no member H with $\alpha_1(H) = p + 1$; see Lemma 76.4). By assumption, $s > 0$. Next, $|G'| \geq |H'_i| = p^2$ so the set Γ_1 has at most one abelian member (Lemma 64.1(q)).

We have $p^2 = \alpha_1(G) = sp + u \leq sp + (p + 1 - s) = s(p - 1) + (p + 1)$. If $s < p$, then $p^2 \leq (p - 1)^2 + p + 1 = p^2 - p + 2$ so $p = 2$, $s = 1$, $u = 2$. Then $\alpha_1(H_1) = 2$ so $\text{cl}(H_1) = 3$ (Lemma 76.4). By Remark 3, $|G/Z(G)| \leq p^4$. Since $Z(G) < H_1$ and $\text{cl}(H_1) = 3$, we get $|H_1 : Z(G)| > p^2$ so $|G/Z(G)| = p^4$. Assume that $|G'| = p^2$. Then G/V'_1 is an \mathcal{A}_1 -group (Lemma 65.2(a)) hence H_1/V'_1 is abelian and $H'_1 = V'_1$ is of order p , a contradiction. Since $|G'| \leq 2|V'_1V'_2| \leq 8$, we get $|G'| = 8$ so G is as in (b3). Thus, $s \geq p$.

Since $s < p + 1$, we get $s = p$. It follows from $p^2 = \alpha_1(G) = sp + u = p^2 + u$ that $u = 0$. Thus, $\Gamma_1 = \{H_1, \dots, H_p, A\}$, where A is abelian and $\alpha_1(H_i) = p$ for $i = 1, \dots, p$.

Suppose that G is metacyclic. Then $|G : Z(G)| = p|G'| = p^4$ (Lemma 64.1(q) and Theorem 72.1) and G is as stated in (b1).

Suppose that G is not metacyclic. Then G/H'_i is an \mathcal{A}_1 -group for all i (Lemma 76.2) whence $|G'| = p|H'_1| = p^3$. By Proposition 72.1(b), G' is noncyclic so G is as stated in (b2). \square

Theorem 76.11. Suppose that G is a p -group with $p^2 < \alpha_1(G) \leq p^2 + p - 1$. Then G is a two-generator \mathcal{A}_3 -group with $|G'| > p$ and one of the following holds:

- (a) $\Gamma_1 = \{H_1, H_2, \dots, H_p, A\}$, where A is abelian, H_1 is an \mathcal{A}_2 -group with $d(H_1) = 3$, $\alpha_1(H_1) = p^2$, $\alpha_1(H_i) = 1$, $i = 2, \dots, p$, $H'_1 = \dots = H'_p$ is of order p , G/H'_1 is an \mathcal{A}_1 -group so $|G'| = p^2$, $\alpha_1(G) = p^2 + p - 1$.
- (b) $\Gamma_1 = \{H_1, \dots, H_p, B\}$, where $\alpha_1(H_i) = p$, $i = 1, \dots, p$, $\alpha_1(B) = 1$, $\alpha_1(G) = p^2 + 1$. If G is nonmetacyclic, then $p > 2$, $|G : G'| = p^2$ and $|G| \in \{p^5, p^6\}$.
- (c) G is metacyclic, $\Gamma_1 = \{F_1, \dots, F_s, H_1, \dots, H_u\}$, where $s + u = p + 1$, $\alpha_1(F_i) = p$, $s \geq 2$, $\alpha_1(H_j) = p + 1$, $\alpha_1(\Phi(G)) = 1$ and $|G'| = p^3$.

Proof. By Lemma 76.4(b), G is not an \mathcal{A}_2 -group.

Assume that G is not an \mathcal{A}_3 -group. Then there exists a nonabelian $H \in \Gamma_1$ which is an \mathcal{A}_n -group, $n \geq 3$. By Theorem 76.9, $\alpha_1(H) \geq p^2$. Then, by Lemma 76.5,

$$p^2 + p - 1 \geq \alpha_1(G) = \alpha_1(H) + \beta_1(G, H) \geq p^2 + p - 1$$

so $\alpha_1(G) = p^2 + p - 1$ and $\alpha_1(H) = p^2$, $\beta_1(G, H) = p - 1$ so $|H'| = p$. Let $L < H$ be an \mathcal{A}_2 -subgroup. Since $|L'| = p$, we get, by Lemma 76.4, $\alpha_1(L) \geq p^2 = \alpha_1(H)$, contrary to Proposition 10.28. Thus, H is an \mathcal{A}_2 -group so G is an \mathcal{A}_3 -group. This argument also shows that the set Γ_1 has no member U with $\alpha_1(U) > p^2$.

If $U \in \Gamma_1$, $\alpha_1(U) = p^2$, then $\beta_1(G, U) = p - 1$ so, by Lemma 76.5, G is as in (a).

Next we assume that $\alpha_1(U) < p^2$ for all $U \in \Gamma_1$; then $d(G) \leq d(U) + 1 = 3$ (Lemma 76.1 and Theorem 76.9). Let

$$\Gamma_1 = \{F_1, \dots, F_s, H_1, \dots, H_t, B_1, \dots, B_u, A_1, \dots, A_v\}, \quad s + t > 0,$$

where $\alpha_1(F_i) = p$, $\alpha_1(H_j) = p + 1$ (see Lemma 76.6), $\alpha_1(B_k) = 1$ and A_l are abelian. Since $s + t > 0$ and $|F'_i|, |H'_j| > p$, we get $v \leq 1$ (Lemma 64.1(u)). We have

(*) If $t > 0$, then $u = v = 0$ since the set $\Gamma_1(H_1)$ has no abelian members.

(**) If $d(G) = 2$, then $uv = 0$. Indeed, if $uv > 0$, then all maximal subgroups of G/B'_1 are abelian, by Exercise 1.6(a), a contradiction since $|T'| \geq p^2$ for $T \in \{F_1, \dots, F_s, H_1, \dots, H_t\}$ (Lemma 76.4).

(i) Suppose that $d(G) = 2$. Then $uv = 0$, by (**). Put $N = \Phi(G)$.

(ii) Suppose, in addition, that N is nonabelian so it is an \mathcal{A}_1 -group since $|G : N| = p^2$. Then $s + t = |\Gamma_1| = p + 1$,

$$\begin{aligned} p^2 + p - 2 &\geq \beta_1(G, N) = \sum_{M \in \Gamma_1} \beta_1(M, N) = s(p - 1) + tp \\ &= s(p - 1) + (p + 1 - s)p = p^2 + p - s, \end{aligned}$$

and we get $s \geq 2$ and $t \leq p - 1$. Let U_i be (the unique so normal in G) abelian maximal subgroup of F_i , $i = 1, 2$, and set $A = U_1 U_2$. Since $F_1 \cap F_2 = \Phi(G)$ is nonabelian, we get $U_1 \neq U_2$. Then $A (> U_1)$ is of class ≤ 2 (Fitting). If $A \in \Gamma_1$, then $\Phi(G) = A \cap F_1 = A_1$ is abelian, a contradiction. Thus, $A = G$, so $\text{cl}(G) = 2$. In that case, all members of the set Γ_1 are metacyclic (Lemma 76.4) so G is also metacyclic (Lemma 64.1(e,f,h)), and G is as in (c).

(ii) In what follows we assume that $N = \Phi(G)$ is abelian; then $t = 0$. If $s = p + 1$, then $\alpha_1(G) = sp = (p + 1)p > p^2 + p - 1$, a contradiction. Thus, $u + v > 0$. Since $|G'| \geq |F'_1| = p^2$, we get $v \leq 1$ (Lemma 64.1(u)).

If $v = 1$, then $u = 0$, by (**); then $s = p$ and we get $p^2 + 1 \leq \alpha_1(G) = sp = p^2$, a contradiction. Thus, $v = 0$ so $s + u = p + 1$ and $u = p + 1 - s > 0$. We have

$$p^2 + 1 \leq \alpha_1(G) = \sum_{M \in \Gamma_1} \alpha_1(M) = ps + u = (p - 1)s + p + 1 \leq p^2 + p - 1.$$

It follows that $p \leq s \leq p + 1 - \frac{1}{p-1}$, and so $s = p$ and $u = 1$. In that case, $\alpha_1(G) = ps + u = p^2 + 1$, $\Gamma_1 = \{F_1, \dots, F_p, B\}$, where $\alpha_1(F_i) = p$, $\alpha_1(B) = 1$. Thus, G and all members of the set Γ_1 are two-generator so G is either metacyclic or $p > 2$ and $G/K_3(G)$ is nonabelian of order p^3 and exponent p (Lemma 64.1(n,p)).

Suppose that G is not metacyclic; then $|G : G'| = p^2$. In that case, $|G'| \leq p|F'_1 B'| \leq p^4$ so $|G| = |G : G'||G'| \leq p^6$. Since G is an \mathcal{A}_3 -group, we get $|G| \in \{p^5, p^6\}$ so G is as in (b).

(ii) Now let $d(G) = 3$. By Lemma 76.8(b,c), $\Phi(G) \not\leq Z(G)$. Then, by Lemma 76.3 and the last sentence of Remark 6, the set Γ_2 has exactly p^2 nonabelian members which are \mathcal{A}_1 -groups so this set has two distinct abelian members U_1 and U_2 . Then $M = U_1 U_2 \in \Gamma_1$, by the product formula and $|\Gamma_1(M) \cap \Gamma_2| = p + 1$. It follows from $U_1 \cap U_2 \leq Z(M)$ that all members of the set $\Gamma_1(M) \cap \Gamma_2$ are abelian so the set Γ_2 has exactly $p + 1$ abelian members, say U_1, \dots, U_{p+1} . We have $|M'| \leq p$ (Lemma 64.1(u)) and $\Gamma_2 = \{L_1, \dots, L_{p^2}, U_1, \dots, U_{p+1}\}$, where all L_i are \mathcal{A}_1 -groups, all $U_i < M$. Since $L_i \cap M = \Phi(G)$ is abelian for all i , we get $\alpha_1(M) + p^2 \leq \alpha_1(G) \leq p^2 + p - 1$ so $\alpha_1(M) \leq p - 1$ and M is either abelian or \mathcal{A}_1 -group (Remark 1).

(ii1) Suppose that M is abelian. Then $v = 1$ (Lemma 64.1(u)) and so $t = 0$. Also, $u = 0$ since all $p + 1$ abelian members of the set Γ_2 lie in M . Hence, $s = |\Gamma_1| - v = p^2 + p$. By the hypothesis and Hall's enumeration principle (Theorem 5.2),

$$p^2 < \alpha_1(G) = \sum_{H \in \Gamma_1} \alpha_1(H) - p \sum_{H \in \Gamma_2} \alpha_1(H) = ps - p \cdot p^2 = p(p^2 + p) - p^3 = p^2,$$

a contradiction. Thus, $v = 0$.

(ii2) Now let M be an \mathcal{A}_1 -group; then $u = 1$ since all $U_i < M$. We get $t = 0$, by (*), so $s = |\Gamma_1| - u = p^2 + p$. Therefore, by Hall's enumeration principle,

$$\begin{aligned} p^2 + 1 &\leq \alpha_1(G) = \sum_{H \in \Gamma_1} \alpha_1(H) - p \sum_{H \in \Gamma_2} \alpha_1(H) \\ &= 1 + sp - p \cdot p^2 = 1 + (p^2 + p)p - p^3 = p^2 + 1. \end{aligned}$$

Note that $d(G) = 3$ but all members of the set Γ_1 are two-generator. We have $cl(G) \geq cl(F_1) = 3$. Then $p = 2$ (Theorem 70.1) and $G/K_4(G)$ is of order 2^7 or 2^8 (Theorem 70.4). However, by remarks following Theorem 70.5, the above groups of order 2^7 and 2^8 are \mathcal{A}_4 -groups and \mathcal{A}_5 -groups, respectively, a contradiction. \square

Lemma 76.12. *Let G be an \mathcal{A}_4 -group and let $R \in \Gamma_2$ be an \mathcal{A}_2 -group. Then $\alpha_1(G) > p^2 + p + 1$, unless $p = 2$ and G satisfies the following conditions:*

- (a) $d(G) = 3$, $\alpha_1(G) = 2^2 + 2 + 1 = 7$.
- (b) $\Gamma_2 = \{R, R_1, R_2, R_3, A_1, A_2, A_3\}$, where $\alpha_1(R) = 4$, $|R'| = 2$, $d(R) = 3$, R_1, R_2, R_3 are \mathcal{A}_1 -groups and A_1, A_2, A_3 are abelian.
- (c) $\Gamma_1 = \{F_1, F_2, F_3, H_1, H_2, H_3, A\}$, where A is abelian and
 - (c1) $\Gamma_1(F_i) = \{R, R_i, A_i\}$, $\alpha_1(F_i) = 2^2 + 1 = 5$, $|F'_i| = 4$, $R' = R'_i$, F_i/R' is an \mathcal{A}_1 -group, i.e., F_i is a group of Theorem 76.11(a), $i = 1, 2, 3$.
 - (c2) $\Gamma_1(H_1) = \{A_1, R_2, R_3\}$, $\Gamma_1(H_2) = \{A_2, R_3, R_1\}$, $\Gamma_1(H_3) = \{A_3, R_1, R_2\}$ so $\alpha_1(H_i) = 2$ and $|H'_i| = 4$ hence H_i is an \mathcal{A}_2 -group, $i = 1, 2, 3$.
- (d) $Z(G) < \Phi(G)$, $|G'| = 8$, $|G/Z(G)| = 16$, $Z(G) = Z(R_i)$, $i = 1, 2, 3$.

All nonabelian members of the set Γ_1 are two-generator.

Proof. Let $\Gamma_1^R = \{F_1, \dots, F_{p+1}\}$; then F_1, \dots, F_{p+1} are \mathcal{A}_3 -groups. By Theorem 76.9, $\alpha_1(F_i) \geq p^2$ for all i . By Lemma 76.6, $\alpha_1(R) \geq p$.

If $\alpha_1(R) = p$, then $\beta_1(F_i, R) \geq p^2 - p$ for all i , and we are done since

$$\alpha_1(G) \geq \alpha_1(R) + \sum_{i=1}^{p+1} \beta_1(F_i, R) \geq p + (p^2 - p)(p + 1) = p^3 > p^2 + p + 1.$$

Now suppose that $\alpha_1(R) = p + 1$. Then $\alpha_1(F_i) \geq p^2 + p$, by Theorems 76.10 and 76.11, so $\beta_1(F_i, R) \geq p^2 - 1$ for all i , and we are done since

$$\alpha_1(G) \geq \alpha_1(R) + \sum_{i=1}^{p+1} \beta_1(F_i, R) \geq p + 1 + (p^2 - 1)(p + 1) = p^3 + p^2 > p^2 + p + 1.$$

If $\alpha_1(R) > p + 1$, then $\alpha_1(R) \geq p^2$ (Theorem 72.1 and 76.4). Since F_i is an \mathcal{A}_3 -group with $R \in \Gamma_1(F_i)$, we get $\beta_1(F_i, R) \geq p - 1$ (Lemma 76.5), and so

$$(4) \quad \begin{aligned} \alpha_1(G) &\geq \alpha_1(R) + \sum_{i=1}^{p+1} \beta_1(F_i, R) \geq p^2 + (p - 1)(p + 1) \\ &= 2p^2 - 1 \geq p^2 + p + 1. \end{aligned}$$

If $p > 2$, then $\alpha_1(G) \geq 2p^2 - 1 > p^2 + p + 1$, and we are done in this case.

Now let $2p^2 - 1 = p^2 + p + 1$; then $p = 2$ and $\alpha_1(G) = 7$. In that case, as it follows from (4), $\alpha_1(R) = 4$ and $\beta_1(F_i, R) = 1$ so $\alpha_1(F_i) = 5$ for $i = 1, 2, 3$. By Lemma 76.5 applied to the pair $R < F_i$, we get $|R'| = 2$, $d(F_i) = 2$ and $\Gamma_1(F_i) = \{R, R_i, A_i\}$, where R_i is an \mathcal{A}_1 -group with $R' = R'_i$ and A_i is abelian, $|F'_i| = 4$, i.e., F_i is a group of Theorem 76.11(a), $i = 1, 2, 3$. By Lemma 76.5, $d(G) \leq 1 + d(F_1) = 3$.

Assume that $d(G) = 2$. Since all members of the set Γ_1 are also two-generator, G is metacyclic since $p = 2$ (Lemma 64.1(n)). In that case, $|G'| = 2^4$ so $|F'_i| = 2^3$ (Theorem 72.1), contrary to what has been said in the previous paragraph.

Thus, $d(G) = 3$. Then $\Phi(F_i) = \Phi(G)$ and so $\{R, R_1, R_2, R_3, A_1, A_2, A_3\} = \bigcup_{i=1}^3 \Gamma_1(F_i) = \Gamma_2$, where A_1, A_2, A_3 are abelian so $\Phi(G)$ is abelian, $\alpha_1(R_i) = 1$ ($i = 1, 2, 3$).

Set $A = A_1 A_2$; then $A \in \Gamma_1$ and $A_3 < A$ (if $A_3 \not\leq A$ then $C_G(\Phi(G)) \geq AA_3 = G$ so $\Phi(G) \leq Z(G)$, a contradiction since $|R : \Phi(G)| = 2$ and R is nonabelian). Since F_1, F_2, F_3 together contain all \mathcal{A}_1 -subgroups of G and $A \cap F_i$ is abelian for $i = 2, 3$, then A is abelian (Remark 4).

Set $\Gamma_1 - \Gamma_1^R = \{H_1, H_2, H_3, A\}$. One may assume that $A_i < H_i$, $i = 1, 2, 3$. Since $H_i \cap A > \Phi(G)$ is an abelian maximal subgroup of H_i and $H_i \cap A \in \Gamma_2$, then $R_i \not\leq H_i$ since $R_i A_i = F_i \neq H_i$, $i = 1, 2, 3$. Since $R \not\leq H_i$ and $|\Gamma_1(H_i) \cap \Gamma_2| = 3$, $i = 1, 2, 3$, we get

$$H_1 = \{A_1, R_2, R_3\}, \quad H_2 = \{A_2, R_1, R_3\}, \quad H_3 = \{A_3, R_1, R_2\}.$$

Now, R, R_1, R_2, R_3 together contain all \mathcal{A}_1 -subgroups of G . Each of the four \mathcal{A}_1 -subgroups S_1, S_2, S_3, S_4 of R satisfies $S_j \Phi(G) = R, j = 1, 2, 3, 4$, since $\Phi(G)$ is an abelian maximal subgroup of R , and so, in view of $R \not\leq H_i$, no one of S_1, S_2, S_3, S_4 is contained in $H_i, i = 1, 2, 3$. Thus, $\alpha_1(H_i) = 2, i = 1, 2, 3$. By Lemma 76.6(a), H_i is an \mathcal{A}_2 -group with $d(H_i) = 2$ and $|H'_i| = 4, i = 1, 2, 3$. Hence, all nonabelian members of the set Γ_1 are two-generator.

By Lemma 64.1(u), $|G'| \leq 2|H'_1 A'| = 8$ and so Lemma 64.1(q) implies that $|G : Z(G)| = 2|G'| \leq 2^4$. On the other hand, $G = R_i A$ with $A \cap R_i = \Phi(G)$. We have $Z(R_i) = \Phi(R_i) < \Phi(G) < A, |\Phi(G) : Z(R_i)| = 2$, by the product formula, and $C_G(Z(R_i)) \geq R_i A = G$. Thus, $Z(R_i) \leq Z(G), i = 1, 2, 3$. Assume that $|G : Z(G)| < 2^4$; then $|G : Z(G)| = 2^3$. In that case, all members of the set Γ_1 , containing $Z(G)$, must be abelian or \mathcal{A}_1 -subgroups since nonabelian members of the set Γ_1 are two-generator. Since A is the unique abelian member of the set Γ_1 , this set also contains an \mathcal{A}_1 -group, contrary to what has been said about Γ_1 . Thus, $Z(G) = Z(R_i) (i = 1, 2, 3)$ so $|G : Z(G)| = 2^4$ and $|G'| = 8$ (Lemma 64.1(q)). \square

Definition 1. A 2-group G of Lemma 76.12 is called a 2-group of type $\mathfrak{G}_{7,1}$.

We shall see (see Appendix, below) that groups of type $\mathfrak{G}_{7,1}$ do not exist.

Lemma 76.13. Let a p -group G be an \mathcal{A}_n -group, $n > 2$, let $H_1 \in \Gamma_1$ and $\beta_1(G, H_1) = p$; then H_1 is nonabelian (Lemma 76.6). In that case, $d(G) = 2$ so $\Gamma_1 = \{H_1, \dots, H_{p+1}\}$, and one of the following holds:

- (a) If H_2 is neither abelian nor an \mathcal{A}_1 -group, then $p = 2, \alpha_1(H_2) = 2, H_3$ is abelian, $H'_1 = H'_2$ is of order 4, G/H'_2 is an \mathcal{A}_1 -group so $|G'| = 8$ and $|G/Z(G)| = 16$.
- (b) All p members of the set $\Gamma_1 - \{H_1\}$ are \mathcal{A}_1 -groups, $H'_1 = H'_2 = \dots = H'_{p+1}$ and G/H'_1 is an \mathcal{A}_1 -group so $|G'| = p^2$.
- (c) All p members of the set $\Gamma_1 - \{H_1\}$ are \mathcal{A}_1 -groups and H'_2, \dots, H'_{p+1} are pairwise distinct. Set $Q = H'_2 \dots H_{p+1}$; then $Q \cong E_{p^2}$, G/Q is an \mathcal{A}_1 -group so $H'_1 \leq Q$ and $|G'| = p^3$.

Proof. Let $R \in \Gamma_1(H_1) \cap \Gamma_2$ and set $\Gamma_1^R = \{H_1, H_2, \dots, H_{p+1}\}$. Since H_1 is nonabelian (Lemma 76.6(a)), we get $R \not\leq Z(G)$ so the set Γ_1^R has at most one abelian member.

(i) Suppose that R is nonabelian; then all subgroups H_i are nonabelian and we have $\beta_1(H_i, R) \geq p - 1$ for $i > 1$ (Remark 1), and we get $p = \beta_1(G, H_1) \geq \sum_{i=2}^{p+1} \beta_1(H_i, R) \geq p(p - 1)$ so that $p = 2$ and $\beta_1(H_i, R) = 1$ for $i = 2, 3$. Therefore, by Lemma 76.5, applied to the pair $R < H_i, i = 2, 3$, we have

$$|R'| = 2, \quad d(H_i) = 2, \quad |H'_i| = 4, \quad \Gamma_1(H_2) = \{R, L_2, A_2\}, \\ \Gamma_1(H_3) = \{R, L_3, A_3\},$$

where $\alpha_1(L_i) = 1$ and A is abelian. Since, in view of $\beta(G, H_1) = 2$, H_1, H_2, H_3 contain together all \mathcal{A}_1 -subgroups of G , the members of the set Γ_1 are not \mathcal{A}_1 -groups. Next, $A_2, A_3 \triangleleft G$. Set $A = A_2 A_3$; then $\text{cl}(A) \leq 2$ (Fitting). Since $\text{cl}(G) \geq \text{cl}(H_2) = 3 > 2$, we get $A \in \Gamma_1$. Then A is abelian since $A \cap H_i = A_i$ is abelian for $i = 2, 3$ (Remark 4). Therefore, in view of $|G'| \geq |H'_2| = 4$, A is the unique abelian member of the set Γ_1 (Lemma 64.1(u)).

Since $R \not\leq A$, we get $d(G) > 2$ so $d(G) = 3$ since $d(H_2) = 2$; then $|\Gamma_1(H_i) \cap \Gamma_2| = 3$, $i = 1, 2, 3$, hence $\Gamma_1(H_2) \cup \Gamma_1(H_3) \subset \Gamma_2$. We have $H_i \cap A = A_i \in \Gamma_2$ and A_i is the unique abelian member of the set $\Gamma_1(H_i)$, $i = 2, 3$. Also put $A_1 = H_1 \cap A (\in \Gamma_2)$ and $\Gamma_1^{A_i} = \{H_i, F_i, A\}$, $i = 1, 2, 3$. It follows that $\Gamma_1 = \{H_1, H_2, H_3, F_1, F_2, F_3, A\}$.

Since $F_1 \cap H_1 = A_1$ and $\alpha_1(F_1) = 2 = \beta_1(G, H_1)$, F_1 is an \mathcal{A}_2 -group (Lemma 76.6). For $i = 2, 3$, set $S_i = F_1 \cap H_i$; then $S_i \in \Gamma_2$ and, since $S_i \neq A_1$, the unique abelian member of the set $\Gamma_1(F_1)$, S_i is an \mathcal{A}_1 -subgroup (Lemma 76.5). We also have $S_i \neq R$, $i = 2, 3$, and $S_2 \neq S_3$ so $\Gamma_1(F_1) \cap \Gamma_2 = \{S_2, S_3, A_1\}$. One may assume, without loss of generality, that $\Gamma_1^{S_2} = \{F_1, H_2, F_2\}$; then $\Gamma_1^{S_3} = \{F_1, H_3, F_3\}$. By Lemma 76.5, $d(H_i) = d(F_j) = 2$, $i = 2, 3$ and $j = 1, 2, 3$.

Let $\Gamma_1(H_1) \cap \Gamma_2 = \{R, U, A_1\}$. Then $H_1 \cap F_i = U$ for $i = 2, 3$ so $\Gamma_1^U = \{H_1, F_2, F_3\}$. By the above, $\Gamma_2 = \{R, S_2, S_3, U, A_1, A_2, A_3\}$ and

$$\begin{aligned} A_1 &= H_1 \cap F_1 \cap A, & A_2 &= H_2 \cap F_2 \cap A, & A_3 &= H_3 \cap F_3 \cap A, \\ R &= H_1 \cap H_2 \cap H_3, & U &= H_1 \cap F_2 \cap F_3, & S_2 &= H_2 \cap F_1 \cap F_2, \\ S_3 &= H_3 \cap F_1 \cap F_3. \end{aligned}$$

By Lemma 64.1(u), $|G'| \leq 2|H'_2 A'| = 8$. Assume that $|G'| = 4$. Then all non-abelian maximal subgroups of G have the same derived subgroup which is equal to G' . By Lemma 64.1(q), $|G : Z(G)| = 8$. If $K/Z(G)$ is a maximal subgroup of $G/Z(G)$ such that $K \neq A$, then $|K'| = 2$ (Lemma 64.1(q)), a contradiction. Thus, $|G'| = 8$ so $|G/Z(G)| = 16$ (Lemma 64.1(q)). If $Z(G) \not\leq H \in \Gamma_1$, then $G = HZ(G)$ so $|G'| = |H'| = 4$, which is a contradiction. Thus, $Z(G) < \Phi(G)$. Since $R \cap U = \Phi(G)$, we get $|U'| = 2$ (Lemma 64.1(q)).

Let us consider the quotient group $\bar{G} = G/Z(G)$ which is of rank 3 and order 16. The subgroups $\bar{R}, \bar{S}_2, \bar{S}_3$ and \bar{U} are four-groups so \bar{G} has at least 9 involutions. Since $\exp(\bar{G}) = 4$, it follows that \bar{G} is nonabelian. Let \bar{D} be a minimal nonabelian subgroup of \bar{G} . Then, by Lemma 64.1(i), $\bar{G} = \bar{D}Z(\bar{G})$, and now it is easy to see that $\bar{G} \cong D_8 \times C_2$ (see Appendix 16). Then \bar{G} contains exactly two distinct elementary abelian subgroups of order 8. Let $\bar{K} \cong E_8$ be such that $\bar{K} \neq \bar{A}$. Then $K \in \Gamma_1$ is nonabelian of rank ≥ 3 , contrary to what has been proved already.

Thus, all members of the set $\Gamma_1(H_1) \cap \Gamma_2$ are abelian.

(ii) Since R is abelian, we have

$$p = \beta_1(G, H_1) \geq \sum_{i=2}^{p+1} \beta_1(H_i, R) = \sum_{i=2}^{p+1} \alpha_1(H_i).$$

Thus, for nonabelian $H \in \Gamma_1^R - \{H_1\}$ we have $\alpha_1(H) \in \{1, p\}$ so $d(H) = 2$ (Lemmas 76.1 and 76.6), and so $d(G) \leq 1 + d(H) = 3$.

(ii1) Assume that H_2 is neither abelian nor an \mathcal{A}_1 -group. Then $\alpha_1(H_2) = p = \beta_1(G, H_1)$ (Lemma 76.6) so H_i is abelian for $i > 2$. Next, H_2 is an \mathcal{A}_2 -subgroup and $|G'| \geq |H'_2| = p^2$ (Lemma 76.6) so the set Γ_1 has at most one abelian member (Lemma 64.1(u)). In that case, $p = 2$ and $\Gamma_1^R = \{H_1, H_2, H_3 = A\}$; here A is abelian, $\alpha_1(H_2) = 2$ and $|H'_2| = 4$ (Lemmas 76.6 and 76.4).

Assume that $d(G) = 2$. Then $H'_1 = H'_2$ has order 4 and G/H'_2 is an \mathcal{A}_1 -group (Lemmas 76.6 and 76.2) so $|G'| = 8$, $|G/Z(G)| = 2|G/G'| = 16$, and G is as in (a).

Now suppose that $d(G) = 3$. Then $|\Gamma_2 \cap \Gamma_1(H_1)| = 2 + 1 = 3$. Take $S \in (\Gamma_2 \cap \Gamma_1(H_1)) - \{R\}$; then S is abelian, by (i). Set $\Gamma_1^S = \{H_1, F_2, F_3\}$. Since H_1 and H_2 together contain all \mathcal{A}_1 -subgroups of G , F_2 and F_3 are not \mathcal{A}_1 -subgroups (they are nonabelian since A is the unique abelian maximal subgroup of G). Since $F_i \cap H_1 = S$ ($\in \Gamma_1(H_1)$) is abelian, we get $1 < \alpha_1(F_i) \leq \beta_1(G, H_1) = 2$ so $\alpha_1(F_i) = 2$ and F_i is an \mathcal{A}_2 -group, $i = 2, 3$ (Lemma 76.6(a)). Then F_2 and F_3 together contain 4 distinct \mathcal{A}_1 -subgroups and all of them are not contained in H_1 (indeed, $F_2 \cap H_1 = S = F_3 \cap H_1$ is abelian), i.e., $\beta_1(G, H_1) \geq 4 > 2$, contrary to the hypothesis.

Thus, all nonabelian members of the set $\Gamma_1^R - \{H_1\}$ are \mathcal{A}_1 -groups. It follows that all nonabelian members of the set $\Gamma_1 - \{H_1\}$ are \mathcal{A}_1 -groups.

(ii2) Assume that $d(G) = 3$. Then $p = \beta_1(G, H_1) = \sum_{F \in \Gamma_1 - \{H_1\}} \alpha_1(F) \geq p^2 - 1$ since the set $\Gamma_1 - \{H_1\}$ has at least $p^2 - 1$ nonabelian members (Lemma 64.1(q)) which are \mathcal{A}_1 -subgroups. However, $p^2 - 1 > p$, and we get a contradiction.

Thus, $d(G) = 2$. Then H_2, \dots, H_{p+1} are \mathcal{A}_1 -groups, by (ii1) and hypothesis.

(ii3) Let $H'_2 = H'_3$ ($\cong C_p$). In that case, $C_G(H'_2) \geq H_2 H_3 = G$ so $H'_2 \leq Z(G)$. Then all maximal subgroups of the quotient group G/H'_2 are abelian (Exercise 1.6(a)) so G/H'_2 is nonabelian hence an \mathcal{A}_1 -group (Lemma 65.2(a)). We get

$$H'_1 = \dots = H'_{p+1}, \quad |G'| = |(G/H'_2)'||H'_2| = p \cdot p = p^2,$$

and G is as in (b).

(ii4) Now let H'_2, \dots, H'_{p+1} be all distinct. Set $Q = H'_2 H'_3$. Then, as above, all maximal subgroups of the quotient group G/Q are abelian so $H'_2 \dots H'_{p+1} = Q \cong E_{p^2}$ and $H'_1 < Q$. To fix ideas, assume that $H'_2 \neq H'_1$. Then H_1/H'_2 is nonabelian and $\beta_1(G/H'_2, H_1/H'_2) = p-1$ so, by Lemma 76.5, $|G'| = |(G/H'_2)'||H'_2| = p^2 \cdot p = p^3$ and G/Q is an \mathcal{A}_1 -group. Thus, G is as in (c). \square

Now we are ready to complete the proof of Theorem A for odd p .

Theorem 76.14. *Let G be a p -group, $p > 2$. Suppose that $\alpha_1(G) \in \{p^2 + p, p^2 + p + 1\}$. Then G is an \mathcal{A}_n -group, $n \in \{2, 3\}$.*

Proof. Assume that the theorem is false. Then there is an \mathcal{A}_k -group $M \in \Gamma_1$ with $k > 2$, and so $\alpha_1(M) \geq p^2$ (Theorem 76.9), hence $\beta_1(G, M) \leq p + 1$.

Assume that $|M'| = p$; then $d(M) > 2$ (Lemma 65.2(a)). Let $S < M$ be an \mathcal{A}_2 -subgroup. Then, by Lemma 76.4, $\alpha_1(S) \geq p^2$. If $S \notin \Gamma_1(M)$, then, by Lemma 76.5,

$$\alpha_1(M) \geq \alpha_1(S) + 2(p - 1) \geq p^2 + p + (p - 2) \geq p^2 + p + 1$$

so, by Theorem 10.28, $\alpha_1(G) > \alpha_1(M) \geq p^2 + p + 1$, a contradiction. Thus, $S \in \Gamma_1(M)$. By Lemma 76.5, $\beta_1(M, S) \geq p$ and $\beta_1(G, M) \geq p - 1$, so

$$\alpha_1(G) \geq \alpha_1(S) + \beta_1(G, M) + \beta_1(M, S) \geq p^2 + p + p - 1 > p^2 + p + 1$$

since $p > 2$, a contradiction. It follows that

(A*) $|M'| \geq p^2$ so $\beta_1(G, M) \geq p$ (Lemma 76.5). Therefore,

$$p^2 + p + 1 \geq \alpha_1(G) = \alpha_1(M) + \beta_1(G, M) \geq \alpha_1(M) + p,$$

hence $p^2 \leq \alpha_1(M) \leq p^2 + 1$ and so M is an \mathcal{A}_3 -group of Theorem 76.10 or Theorem 76.11; then G is an \mathcal{A}_4 -group.

By Lemma 76.12, since $p > 2$, we have

(B*) Any member of the set Γ_2 is either abelian or an \mathcal{A}_1 -group.

(i) Let $\alpha_1(M) = p^2$; then M is a group of Theorem 76.10 so $|M'| = p^3$, and $\beta_1(G, M) \in \{p, p + 1\}$. By (B*), M is not a group of Theorem 76.10(a1) since the set $\Gamma_1(M) \cap \Gamma_2$ has no members which are \mathcal{A}_2 -groups.

(i1) Let M be a group of Theorem 76.10(a), i.e., $d(M) = 3$, $|M'| = p^3$, $\Gamma_1(M) = \{F_1, \dots, F_{p^2+p}, A\}$, where $\alpha_1(F_i) = p$ for all i and A is abelian. By (B*), $F_i \notin \Gamma_2$, $i = 1, \dots, p^2$, so $|\Gamma_1(M) \cap \Gamma_2| = 1$ hence $A = \Phi(G)$ and $d(G) = 2$. Let $\Gamma_1 = \{M_1 = M, M_2, \dots, M_{p+1}\}$; then at most one member of the set Γ_1 is abelian and $\beta_1(G, M) = \sum_{i=2}^{p+1} \alpha_1(M_i)$ since $\Phi(G) = A$ is abelian.

Let $\alpha_1(G) = p^2 + p$; then $\beta_1(G, M) = p$ so $|M'| \leq p^2$ (Lemma 76.13), contrary to the first paragraph of (i).

Thus, we have $\alpha_1(G) = p^2 + p + 1$. In view of $\beta_1(G, M) = p + 1 > p = |\{M_2, \dots, M_{p+1}\}|$, one may assume that M_2 is neither abelian nor an \mathcal{A}_1 -group (Dirichlet's principle); then $\alpha_1(M_2) = p$. It follows from

$$p + 1 = \beta_1(G, M) = \alpha_1(M_2) + \sum_{i=3}^{p+1} \alpha_1(M_i) = p + \sum_{i=3}^{p+1} \alpha_1(M_i)$$

that $|\Gamma_1| - 3$ members of the set Γ_1 are abelian and exactly one its member, say M_3 , is an \mathcal{A}_1 -group. Since $|G'| \geq |M'| = p^3 > p$, the set Γ_1 has at most one abelian member (Lemma 64.1(u)) so we get $p = 3$. Then $\Gamma_1 = \{M_1 = M, M_2, M_3, M_4 = A\}$, where A is abelian. However, by Lemma 76.2, we get $M'_3 = M'$, a contradiction since $|M'| = p^3 > p = |M'_3|$.

(i2) Let M be a group of Theorem 76.10(b1,b2), i.e., $d(M) = 2$, $\Gamma_1(M) = \{F_1, \dots, F_p, A\}$, where $\alpha_1(F_i) = p$, $F'_1 = \dots = F'_p$ has order p^2 , A is abelian. It follows from (B*) that $F_i \notin \Gamma_1(M) \cap \Gamma_2$ for all i so $A = \Phi(G)$ and $d(G) = 2$. Let $\Gamma_1 = \{M_1 = M, \dots, M_{p+1}\}$. As in (i1), one has to consider two possibilities: $\alpha_1(G) \in \{p^2 + p, p^2 + p + 1\}$.

Let $\alpha_1(G) = p^2 + p$; then $\beta_1(G, M) = p$ so $|M'| \leq p^2$ (Lemma 76.13), contrary to the first paragraph of (i).

Now let $\alpha_1(G) = p^2 + p + 1$. In that case, $\beta_1(G, M) = p + 1$. Therefore, as in (i1), one may assume that M_2 is neither abelian nor an \mathcal{A}_1 -group. In that case, as in (i1), we get $p = 3$ and $\Gamma_1 = \{M_1 = M, M_2, M_3, M_4 = A\}$, where A is abelian, $\alpha_1(M_3) = 1$. By Lemma 76.2, we get $M'_3 = M'$, a contradiction since $|M'| \geq p^2 > p = |M'_3|$.

All the above, together with (A*) and (B*), yields

(C*) $\alpha_1(M) = p^2 + 1$, i.e., M is a group of Theorem 76.11(b).

(ii) In view of (C*), Theorem 76.11(b) and Lemma 76.5, we must have $\beta_1(G, M) \geq p$ so that $\alpha_1(G) = p^2 + p + 1$; then $\beta_1(G, M) = p$.

By Theorem 76.11(b), $d(M) = 2$, $\Gamma_1(M) = \{F_1, \dots, F_p, B\}$, where $\alpha_1(F_i) = p$, $i = 1, \dots, p$, $\alpha_1(B) = 1$. By (B*), $\Phi(G) = B$ so $d(G) = 2$. Set $\Gamma_1 = \{M = M_1, \dots, M_{p+1}\}$; then $\beta_1(M_i, B) \geq p - 1$, $i > 1$ (Lemma 76.5). We have

$$\alpha_1(G) = \alpha_1(M) + \sum_{i=2}^{p+1} \beta_1(M_i, B) \geq p^2 + 1 + (p - 1)p > p^2 + p + 1,$$

a final contradiction. □

Theorem 76.15. *A 2-group G satisfying $\alpha_1(G) = 6$ is an \mathcal{A}_n -group, $n \in \{2, 3\}$.*

Proof. Assume that this is false. Then, by Theorems 76.9–76.11, G is an \mathcal{A}_4 -group so there is an \mathcal{A}_3 -group $H \in \Gamma_1$. Since $\alpha_1(H) \geq 4$ (Theorem 76.9) and $\beta_1(G, H) > 0$ (Proposition 10.28), we get $\alpha_1(H) \in \{4, 5\}$ so $\beta_1(G, H) \in \{2, 1\}$.

(i) Let $\alpha_1(H) = 4$; then $\beta_1(G, H) = 2$, $|H'| \leq 4$ (Lemma 76.13). On the other hand, H is a group of Theorem 76.10, and so $|H'| = 8$, a contradiction.

(ii) Let $\alpha_1(H) = 5$. Then H is a group of Theorem 76.11 so $|H'| \geq 4$. However, $\beta_1(G, H) = 1$ so $|H'| = 2$ (Lemma 76.5), a final contradiction. □

Appendix by Z. Janko: Nonexistence of groups of types $\mathfrak{G}_{7,1}$ and $\mathfrak{G}_{7,2}$

Theorem A.1. *2-groups of type $\mathfrak{G}_{7,1}$ do not exist.*

Proof. Let G be a 2-group of type $\mathfrak{G}_{7,1}$, i.e., G is a 2-group of Lemma 76.12 with $\alpha_1(G) = 7$. We shall use freely the notation and the results of Lemma 76.12.

By Lemma 76.4(c), H_i is metacyclic for $i = 1, 2, 3$ since $p = 2$ and $\alpha_1(H_i) = 2$. Here we note that $|G| \geq 2^6$ and so $|H_i| \geq 2^5$ since $R \in \Gamma_2$ and R is an \mathcal{A}_2 -group and so $|R| \geq 2^4$. In particular, $R_1, R_2, R_3, A_1, A_2, A_3$ are also metacyclic. Next, R is nonmetacyclic since $d(R) = 3$.

Since A_1 is a maximal subgroup of A and $d(A_1) = 2$, we have $d(A) \leq 3$. Assume that $d(A) = 2$. In that case, all members of the set Γ_1 are two-generator so we can use the results of §70. By Theorem 70.1, $\text{cl}(G) > 2$. Then Theorem 70.2 implies that $(G/K_3(G))' \cong E_8$. But $K_3(G) \neq \{1\}$ and so $|G'| > 8$, contrary to Lemma 76.12(d). Hence we have $d(A) = 3$ and so $\Omega_1(A) \cong E_8$.

Since H_i is metacyclic and $|H_i| \geq 2^5$ ($i = 1, 2, 3$), we can use Proposition 71.2. It follows that $H'_i \cong C_4$ (Exercise 1) and H_i is isomorphic to one of the following groups:

$$(5) \quad H_i = \langle a, b \mid a^{2^m} = 1, m \geq 4, b^{2^n} = a^{\epsilon 2^{m-1}}, n \geq 2, \epsilon = 0, 1, \\ a^b = a^{1+2^{m-2}} \rangle,$$

$$(6) \quad H_i = \langle a, b \mid a^8 = 1, b^{2^n} = a^{4\epsilon}, n \geq 2, \epsilon = 0, 1, a^b = a^{-1+4\eta}, \eta = 0, 1 \rangle.$$

However, in case (5) we get $\Omega_1(H_i) = \langle a^2, b^2 \rangle$ (this subgroup is abelian) and we see that $\langle a, b^2 \rangle, \langle a^2, b \rangle, \langle a^2, b^2 \rangle \langle ab \rangle$ are three maximal subgroups of H_i and they are all \mathcal{A}_1 -groups, contrary to $\alpha_1(H_i) = 2$ (Lemma 76.12). (Indeed, to check that a nonabelian metacyclic p -group is an \mathcal{A}_1 -group, it suffices, in view of Lemma 65.2(a), to show that its derived subgroup has order p . For example, if, in (5), $K = \langle a, b^2 \rangle$, then $a^{b^2} = a^{(1+2^{m-2})^2} = a^{1+2^{m-1}}$ so $K' = \langle a^{2^{m-1}} \rangle$ has order 2 and K is an \mathcal{A}_1 -group.) We have proved that H_i must be isomorphic to a group given in (6). Here we distinguish two essentially different cases $\epsilon = 0$ (splitting case) and $\epsilon = 1$ (non-splitting case).

(i) We consider first the splitting case $\epsilon = 0$ so that

$$H_1 = \langle a, b \mid a^8 = b^{2^n} = 1, n \geq 2, a^b = a^{-1}z^\eta, z = a^4, \eta = 0, 1 \rangle,$$

and we also set $u = b^{2^{n-1}}$ and $v = a^2$ so that $v^2 = z$ and u are involutions. Since $|H_1| = 2^{n+3}$, we have $|G| = 2^{n+4}, n \geq 2$. But $A_1 = \langle b^2 \rangle \times \langle a \rangle$ is the unique abelian maximal subgroup of H_1 and so $A \cap H_1 = A_1$. The fact that $d(A) = 3$ implies that there is an involution $t \in A - A_1$ so that $\Omega_1(A) = \langle u, z, t \rangle$ because $\Omega_1(H_1) = \langle u, z \rangle < \Omega_1(A)$. We have $Z(H_1) = \langle b^2, z \rangle = Z(G)$ (indeed, $Z(G) \leq H_1$ and $|Z(G)| = |Z(H_1)|$) and $\Phi(H_1) = \langle b^2 \rangle \times \langle v \rangle = \Phi(G)$ since $\Phi(H_1) \leq \Phi(G)$ and $d(G) = 3$; in particular, $u = b^{2^{n-1}} \in Z(G)$. Also, $H'_1 = \langle v \rangle \cong C_4$ is normal in G and $|G'| = 8$ (Lemma 76.12). Since $\Phi(G) = \langle b^2 \rangle \times \langle v \rangle$ and $H_1 > G' > \langle v \rangle$, it follows, by the modular law, that $G' = \langle u \rangle \times \langle v \rangle$ is abelian of type $(2, 4)$. Note that R_1, R_2, R_3 are

metacyclic of order 2^{n+2} because $\Gamma_1(H_1) = \{A_1, R_2, R_3\}$, $\Gamma_1(H_2) = \{A_2, R_1, R_3\}$ and H_1 and H_2 are metacyclic of order 2^{n+3} .

We have $G = \langle H_1, t \rangle = \langle a, b, t \rangle$, $\langle [a, b] \rangle = \langle v \rangle$, $[a, t] = 1$ (recall that $a, t \in A$) and, since $G/\langle v \rangle$ is nonabelian, we get $[b, t] \in G' - \langle v \rangle$. On the other hand, $\Omega_1(A) = \langle u, z, t \rangle$ is normal in G and so $[b, t] = t^b t \in \Omega_1(A)$. It follows that $[b, t] = uz^\delta$ with $\delta \in \{0, 1\}$ since $[b, t] = b^{-1}b^t \in H_1 \cap \Omega_1(A) = \Omega_1(H_1)$ and $[b, t] \in G' - \langle v \rangle$ (recall that $z = v^2$). Also note that $R \in \Gamma_2$ is an A_2 -group of order 2^{n+2} and therefore four \mathcal{A}_1 -subgroups S_1, S_2, S_3, S_4 which are contained in R are of order 2^{n+1} . Since $\alpha_1(G) = 7$, $\{S_1, S_2, S_3, S_4, R_1, R_2, R_3\}$ is the set of all \mathcal{A}_1 -subgroups in G . In particular, all \mathcal{A}_1 -subgroups of G of order $< 2^{n+2}$ are contained in R .

Let $\delta = 1$ so that $[b, t] = uz$. Since $uz \in \langle b^2, z \rangle = Z(G)$, $\langle uz \rangle \triangleleft G$ and so $\langle b, t \rangle / \langle uz \rangle$ is abelian which implies that $\langle b, t \rangle' = \langle uz \rangle \cong C_2$. It follows that $\langle b, t \rangle$ is an \mathcal{A}_1 -subgroup (Lemma 65.2(a)) containing $\langle b^{2^{n-1}} = u, z, t \rangle \cong E_8$ and so $\langle b, t \rangle$ is nonmetacyclic. Also, $\langle b, t \rangle$ is of order $\geq 2^{n+2}$ (since $\langle u, z, t \rangle \cap \langle b \rangle = \langle u \rangle$) and so $\langle b, t \rangle$ is of order 2^{n+2} and therefore $\langle b, t \rangle$ is one of R_1, R_2, R_3 (see the last sentence of the previous paragraph). This is a contradiction since R_1, R_2, R_3 are metacyclic.

Suppose that $\delta = 0$; then $[b, t] = u = b^{2^{n-1}}$ is an involution, and therefore we have either $\langle b, t \rangle \cong M_{2n+1}$ ($n > 2$) or $\langle b, t \rangle \cong D_8$ ($n = 2$). It follows that $\langle b, t \rangle$ is an \mathcal{A}_1 -subgroup of order 2^{n+1} and so $\langle b, t \rangle < R$. On the other hand, $R > \Phi(G)$ and so $R \geq \Phi(G)\langle b, t \rangle$. But $\Phi(G)\langle b, t \rangle \in \Gamma_1$. This is a contradiction since $R \in \Gamma_2$.

(ii) We consider now the non-splitting case $\epsilon = 1$ so that

$$H_1 = \langle a, b \mid a^8 = 1, b^{2^n} = a^4 = z, n \geq 2, a^b = a^{-1}z^\eta, \eta = 0, 1 \rangle$$

and we set $v = a^2$, $w = b^{2^{n-1}}$ and $u = vw$. We see again that $A_1 = \langle b^2, a \rangle = A \cap H_1$ is the unique abelian maximal subgroup in H_1 . Since $d(A) = 3$ and $\Omega_1(A_1) = \Omega_1(H_1) = \langle u, z \rangle$, there is an involution $t \in A - A_1$ such that $\Omega_1(A) = \langle u, z, t \rangle \cong E_8$. Also, $|H_1| = 2^{n+3}$, $|G| = 2^{n+4}$ and the metacyclic \mathcal{A}_1 -subgroups R_1, R_2, R_3 are of order 2^{n+2} . Since $R \in \Gamma_2$ and R is an A_2 -group with $\alpha_1(R) = 4$, four \mathcal{A}_1 -subgroups S_1, S_2, S_3, S_4 , which are contained in R , are of order 2^{n+1} .

We have $Z(H_1) = \langle b^2 \rangle \cong C_{2^n}$, $Z(H_1) = Z(G)$, $\Phi(G) = \Phi(H_1) = \langle b^2 \rangle \langle v \rangle$ since $\Phi(H_1) \leq \Phi(G)$ and $d(G) = 3$. Also, $H'_1 = \langle v \rangle \cong C_4$ is normal in G , $|G'| = 8$ (Lemma 76.12) and so $G' = \langle v, w \rangle = \langle u \rangle \times \langle v \rangle$ is abelian of type $(4, 2)$.

We have $G = \langle H_1, t \rangle = \langle a, b, t \rangle$, $\langle [a, b] \rangle = \langle v \rangle$, where $t \in \Omega_1(A) - \Omega_1(H_1)$, $[a, t] = 1$ and, since $G/\langle v \rangle$ is nonabelian (recall that $o(v) = 4 < 8 = |G'|$), we get $[b, t] \in G' - \langle v \rangle$. On the other hand, $\Omega_1(A) = \langle u, z, t \rangle$ is normal in G and so

$$b^{-1}b^t = [b, t] = t^b t \in \Omega_1(A) \cap H_1 = \Omega_1(H_1) = \Omega_1(G') = \langle u \rangle \times \langle z \rangle.$$

Since $z = v^2 \in \langle v \rangle$, it follows that $[b, t] = u$ or uz . Note that $o(b) = 2^{n+1} \geq 8$ and so, taking into account that $u^b = (vw)^b = v^{-1}w = vwz = uz$, we have $\Phi(G) = \langle b^2, v \rangle < \langle b, u \rangle \cong M_{2n+2}$ noting that $b^{2^{n-1}} = w$, $v = uw^{-1}$ and so $v \in \langle b, u \rangle$. Therefore $\langle b, u \rangle$ is an \mathcal{A}_1 -subgroup of order 2^{n+2} contained in H_1 and consequently

$\langle b, u \rangle = R_2$ or R_3 . Since t normalizes $\langle b, u \rangle$, we have $|\langle b, t \rangle : \langle b, u \rangle| = 2$ and so $\langle b, t \rangle$ is of order 2^{n+3} which implies that $\langle b, t \rangle$ is a maximal subgroup of G with $\langle b, t \rangle' \geq \langle z, u \rangle$ and so $\langle b, t \rangle' = \langle z, u \rangle \cong E_4$. It follows that $\langle b, t \rangle$ is a nonmetacyclic member of the set Γ_1 . Hence $\langle b, t \rangle = F_2$ or F_3 and so $\langle b, t \rangle$ is an A_3 -group. On the other hand, $\tilde{A} = \langle b^2 \rangle \times \langle u \rangle \times \langle t \rangle$ is an abelian nonmetacyclic subgroup of order 2^{n+2} in $\langle b, t \rangle$. Hence \tilde{A} is the unique abelian maximal subgroup of $\langle b, t \rangle$ and so $\tilde{A} = A_2$ or A_3 (see, in Lemma 76.12, lists of the members of the sets $\Gamma_1(F_2)$ and $\Gamma_1(F_3)$). This is a contradiction since A_1, A_2, A_3 are metacyclic. \square

Definition 2. A 2-group G is said to be a group of type $\mathfrak{G}_{7,2}$, if it satisfies the following conditions:

- (1 $\mathfrak{G}_{7,2}$) $d(G) = 2$, $\Gamma_1 = \{H_1, H_2, H_3\}$, $\alpha_1(H_1) = 4$, $\alpha_1(H_2) = 2$, $\alpha_1(H_3) = 1$.
- (2 $\mathfrak{G}_{7,2}$) $\Gamma_1(H_1) = \{F_1, \dots, F_6, A\}$, where $\alpha_1(F_i) = 2$, $i \leq 6$, $A = \Phi(G)$ is abelian, $|H'_1| = 8$. We have $\beta_1(G, H_1) = 3$ so $\alpha_1(G) = 7$.
- (3 $\mathfrak{G}_{7,2}$) $|G : Z(G)| = 2^5$, $Z(G) = Z(H_1) < \Phi(H_1)$.
- (4 $\mathfrak{G}_{7,2}$) $H'_1 = H'_2 \times H'_3$, G/H'_1 is an A_1 -group so $|G'| = 2^4$, $\beta_1(G/H'_2, H_1/H'_2) = 1$, $\beta_1(G/H'_3, H_1/H'_3) = 2$.

It follows from Definition 2 that a 2-group G of type $\mathfrak{G}_{7,2}$, if it exists, is an A_4 -group. It will be proved in the Appendix that groups of type $\mathfrak{G}_{7,2}$ do not exist.

Theorem A.2. *Groups of type $\mathfrak{G}_{7,2}$ do not exist.*

Proof. We prove first that a two-generator 2-group X which is an A_2 -group is metacyclic. Indeed, if $|X| > 2^4$, then the result follows from Lemma 76.4(c). So let $|X| = 2^4$ and let Y be a nonabelian subgroup of order 2^3 . Since $d(X) = 2$, we have $C_X(Y) \leq Y$. It follows from Lemma 64.1(i) that X is of maximal class and so X is metacyclic and we are done.

Let G be a 2-group of type $\mathfrak{G}_{7,2}$, where we use the notation from Definition 2. By Lemma 76.6(a), H_2, F_1, \dots, F_6 are all two-generator A_2 -groups. Therefore, the groups H_2, F_1, \dots, F_6 are all metacyclic. But $A = \Phi(G) < H_2$ and so A is also metacyclic. Hence H_1 is minimal nonmetacyclic and so, by Theorem 66.1, H_1 is an A_2 -group of order 2^5 . This is a contradiction since H_1 contains a proper subgroup F_1 which is an A_2 -group. \square

Now we are ready to prove

Theorem 76.16. *If a 2-group G satisfies $\alpha_1(G) = 7$, then G is an A_n -group, $n \in \{2, 3\}$.*

Proof. Let G be a counterexample of minimal order. If $H \in \Gamma_1$, then $\alpha_1(H) < \alpha_1(G) = 7$, so, by Lemma 76.6 and Theorems 76.9–76.11, 76.15, H is either abelian or an A_n -group, $n \leq 3$. Therefore, G is an A_4 -group so one can choose $H \in \Gamma_1$ so that H is an A_3 -group. In that case, $4 \leq \alpha_1(H) \leq 6$ (Theorem 76.9) so H is one of

the \mathcal{A}_3 -groups of Theorems 76.10, 76.11 or 76.15. Since $\mathfrak{G}_{7,1}$ -groups do not exist, by Appendix, it follows from Lemma 76.12 that

(i) The set Γ_2 has no members which are \mathcal{A}_2 -groups. It follows that H is not a group of Theorems 76.10(a1) and 76.11(c).

(ii) Let $H \in \Gamma_1$ be a group of Theorem 76.10(a2,b1,b2). In that case, $\alpha_1(H) = 4$, $|H'| = 8$, the set $\Gamma_1(H)$ has exactly one abelian member A and all other its members are \mathcal{A}_2 -groups. It follows from (i) that $A = \Phi(G)$ so, in view of $|G : A| = 2^2$, we get $d(G) = 2$, and then $Z(G) < \Phi(G) = A$. Set $\Gamma_1 = \{H_1 = H, H_2, H_3\}$; then $A \in \Gamma_1(H_i)$, $i = 1, 2, 3$, so

$$\alpha_1(H_2) + \alpha_1(H_3) = \beta_1(G, H) = \alpha_1(G) - \alpha_1(H) = 7 - 4 = 3.$$

One may assume that $\alpha_1(H_2) = 2$ and $\alpha_1(H_3) = 1$ ($\alpha_1(H_2) \neq 3$ since the set $\Gamma_1(H_2)$ has one abelian member). Thus, H_2 is an \mathcal{A}_2 -group (Lemma 76.6(a)) and H_3 is an \mathcal{A}_1 -group. We have $d(H_2) = 2 = d(H_3)$ (Lemmas 76.1 and 76.6(a)).

Assume that H is a group from Theorem 76.10(b1,b2); then $d(H) = 2$. In that case, by the above, G and all members of the set Γ_1 are two-generator so G is metacyclic (Lemma 64.1(n)). Since H_2 is an \mathcal{A}_2 -group and H_3 is an \mathcal{A}_1 -group, Exercise 1 shows that G is an \mathcal{A}_3 -group, a contradiction.

Thus, H is a group from Theorem 76.10(a2). Then $d(H) = 3$, $|H'| = 8$, $\Gamma_1(H) = \{F_1, \dots, F_6, A\}$, where $\alpha_1(F_i) = 2$ and $d(F_i) = 2$ for $i \leq 6$ and A is abelian, $|H : Z(H)| = 2|H'| = 16$ (Lemma 64.1(q)). By §65, $H_2/Z(H_2) \in \{D_8, C_4 \times C_4\}$ since $d(H_2) = 2$.

Suppose that $H_2/Z(H_2) \cong D_8$. Then $Z(H_2) \leq \Phi(H_2) \leq \Phi(G) = A$ since $d(H_2) = 2$, and so $|A : Z(H_2)| = 4$. Since H_3 is an \mathcal{A}_1 -group, we get $Z(H_3) = \Phi(H_3) < \Phi(G) = A$ and $|A : \Phi(H_3)| = 2$. Then $Z(H_2) \cap Z(H_3) \leq Z(G)$ and $|A : Z(G)| \leq 8$ so $|G : Z(G)| = |G : A||A : Z(G)| \leq 2^5$. By the above, $|H : Z(G)| = 2^4$ so $Z(G) = Z(H)$ has index 2^5 in G .

Now suppose that $H_2/Z(H_2)$ is abelian of type $(4, 4)$. We have $Z(H_2) < \Phi(H_2) < \Phi(G) < H_3$. Assume that $Z(H_2) \not\leq Z(H_3)$. Then $H_3/Z(H_2)$ is cyclic since $Z(H_3) = \Phi(H_3)$ (Lemma 76.1). Thus, $G/Z(H_2)$ has the cyclic subgroup $H_3/Z(H_2)$ of index 2 and the abelian subgroup $H_2/Z(H_2)$ of type $(4, 4)$ and index 2, which is impossible. It follows that $Z(H_2) \leq Z(H_3)$ so $Z(H_2) \leq Z(G)$, and we get $|G : Z(G)| = |G : H_2||H_2 : Z(H_2)| \leq 2 \cdot 2^4 = 2^5$. Since $Z(G) < \Phi(G) < H_2$, we get $Z(H_2) = Z(G)$ and so $|G : Z(G)| = 2^5$. Comparing the orders, we get $Z(G) = Z(H)$.

Since $|H'| = 8$ and $|F'_i| = 4$, the equality $F_i Z(G) = H$ is impossible for $i \leq 6$. It follows that $Z(G) < F_i$ for all i . In particular, $Z(G) < \Phi(H)$. We see that G is a group of type $\mathfrak{G}_{7,2}$. By the Appendix, groups of type $\mathfrak{G}_{7,2}$ do not exist, and this is a contradiction.

(iii) Now let $\alpha_1(H) = 2^2 + 1$, i.e., H is a group of Theorem 76.11. As we have noticed in (i), H is not a group of Theorem 76.11(c). We have $|H'| > 2$ (Theorem 76.11) and $\beta_1(G, H) = 2$.

(iii1) Let $H \in \Gamma_1$ be a group of Theorem 76.11(a), i.e., $d(H) = 2$, $|H'| = 4$, $\Gamma_1(H) = \{F_1, F_2, A\}$, where $d(F_1) = 3$, $\alpha_1(F_1) = 4$, $|F'_1| = 2$, $\alpha_1(F_2) = 1$ and A is abelian. If $d(G) = 3$, then $F_1 \in \Gamma_1(H) \subset \Gamma_2$, contrary to (i). Thus, $d(G) = 2$ so $\Gamma_1 = \{H_1 = H, H_2, H_3\}$. We have $\Phi(G) \in \{F_2, A\}$, by (i).

Assume that $F_2 = \Phi(G)$. Then

$$7 = \alpha_1(G) = \alpha_1(H_1) + \sum_{i=2}^3 \beta_1(H_i, F_2) = 5 + \sum_{i=2}^3 \beta_1(H_i, F_2)$$

so $\beta_1(H_2, F_2) + \beta_1(H_3, F_2) = 2$. By Remark 1, we get $\beta_1(H_i, F_2) = 1$, $i = 2, 3$. In that case, $\alpha_1(H_i) = 2$ so $|H'_i| = 4$, $d(H_i) = 2$, $i = 2, 3$ (Lemma 76.6(a)). Thus, G and all members of the set Γ_1 are two-generator so G is metacyclic (Lemma 64.1(n)). Then, by Exercise 1, applied to H_2 and H_3 , G is an \mathcal{A}_3 -group so G is not a counterexample.

Therefore, we must have $\Phi(G) = A$. Then we have $\alpha_1(H_2) + \alpha_1(H_3) = 2$. If $\alpha_1(H_i) = 1$, $i = 2, 3$, then G and all members of the set Γ_1 are two-generator so G is metacyclic (Lemma 64.1(n)). In that case, by Exercise 1, G must be \mathcal{A}_2 -group so it is not a counterexample.

Thus, $\alpha_1(H_2) = 2$ so $|H'_2| = 4$ and H_3 is abelian. By Lemma 76.2, $H' = H'_2$ and G/H' is an \mathcal{A}_1 -group. It follows that $|G'| = 2|H'| = 8$ so $|G : Z(G)| = 16$ (Lemma 64.1(q)). Since $d(G) = 2$, we get $Z(G) < \Phi(G) < H_i$ so $|H_i : Z(G)| = 8$, $i = 1, 2, 3$. Since $H_1/Z(G)$ is noncyclic and two-generator, we get $Z(G) < \Phi(H_1) < F_i$, $i = 1, 2$. Then $|F_i : Z(G)| = 4$, $i = 1, 2$. Since $d(F_1) = 3$ and $Z(F_1) > \Phi(F_1)$, we get, by Lemma 76.8(c), $\alpha_1(F_1) \geq 2 \cdot 2^2 - 1 = \alpha_1(G)$, contrary to Proposition 10.28.

(iii2) Let $H \in \Gamma_1$ be a group from Theorem 76.11(b). Retaining the notation of Theorem 76.11, we get, in view of (i), $\Phi(G) = B$ so $d(G) = 2$. Set $\Gamma_1 = \{H_1 = H, H_2, H_3\}$. Then, as above, $\beta_1(H_i, R) = 1$, and we conclude that $\alpha_1(H_i) = 2$ and $d(H_i) = 2$ for $i = 2, 3$ (Lemma 76.6(a)). In that case, G and all members of the set Γ_1 are two-generator so G is metacyclic (Lemma 64.1(n)). Then, by Exercise 1, applied to H_2 and H_3 , G is an \mathcal{A}_3 -group so G is not a counterexample.

(iv) It remains to consider the case where $H \in \Gamma_1$ is a group of Theorem 76.15, i.e., $\alpha_1(H) = 6$. In that case, $\beta_1(G, H) = 1$ so $|H'| = 2$ and $|G'| = 4$, $d(G) = 2$, $\Gamma_1 = \{H_1 = H, H_2, A\}$, where H_2 is an \mathcal{A}_1 -group and A is abelian (Lemma 76.5). By Lemma 64.1(q), $|G : Z(G)| = 8$ and, since $Z(G) < \Phi(G) < H$, we get $|H : Z(G)| = 4$ so $|H : Z(H)| = 4$. Since H is not an \mathcal{A}_1 -group, we get $d(H) = 3$. Then, by Lemma 76.8(c), $\alpha_1(H) \geq 2 \cdot 2^2 - 1 > 6$, a final contradiction. \square

Theorem A follows immediately from Lemma 76.6, Theorems 76.9–76.11, 76.14–76.16 and the Appendix.

If G is a 2-group of maximal class and order 2^6 , then $\alpha_1(G) = 8$ and G is an \mathcal{A}_4 -group. I do not know if, for odd p , there exists an \mathcal{A}_4 -group G with $\alpha_1(G) = (p^2 + p + 1) + 1$.

If G is a nonabelian p -group such that for each $K \in \Gamma_2$, we have $\alpha_1(\Gamma_1^K) < p^2 + 2p + 1$, then G is an \mathcal{A}_n -group, $n \leq 4$. Assume that this is false. Then there is $H \in \Gamma_1$ such that H is an \mathcal{A}_k -group with $k \geq 4$. By Theorem A, $\alpha_1(H) \geq p^2 + p + 2$. If $K \in \Gamma_1(H)$ is abelian, then, since the set Γ_1^K has at most one abelian member, we have $\alpha_1(\Gamma_1^K) = \alpha_1(H) + \sum_{M \in \Gamma_1^K - \{H\}} \alpha_1(M) \geq (p^2 + p + 2) + (p - 1) = p^2 + 2p + 1$ (Remark 1), a contradiction. If K is nonabelian, then, by Remark 1,

$$\begin{aligned} \alpha_1(\Gamma_1^K) &= \alpha_1(H) + \sum_{M \in \Gamma_1^K - \{H\}} \beta_1(M, K) \\ &\geq (p^2 + p + 2) + p(p - 1) = 2p^2 + 2 > p^2 + 2p + 1, \end{aligned}$$

a final contradiction.

3°. A lower estimate of $\alpha_1(G)$ in terms of $d(G)$. To facilitate the proof of Theorem B, we begin with the following remarks.

Remarks. 10. Let G be a nonabelian p -group, $d(G) = 3$ and $H \in \Gamma_1$. Let us prove that $\beta_1(G, H) \geq p(p - 1)$. This is the case if H is abelian since then $\beta_1(G, H) = \alpha_1(G) \geq p^2 > p(p - 1)$ (Theorem 76.9). Next we assume that H is nonabelian. If $\alpha_1(G) = p^2$, then $\alpha_1(H) \leq p$ (Theorem 76.10) so $\beta_1(G, H) \geq p^2 - p = p(p - 1)$. Now let $\alpha_1(G) \geq p^2 + 1$. The result is true if $\alpha_1(H) \leq p + 1$. So, in view of Lemma 76.6 and Theorem 76.9, one may assume that $\alpha_1(H) \geq p^2$. Take $R \in \Gamma_1(H) \cap \Gamma_2$. Assuming that R is nonabelian, we get, using Remark 1, $\beta_1(G, H) \geq \sum_{F \in \Gamma_1^R - \{H\}} \beta_1(F, R) \geq p(p - 1)$ since all $p + 1$ members of the set Γ_1^R are nonabelian. If R is abelian, then the set Γ_1^R has at least p nonabelian members so, by Lemma 76.6, $\beta_1(G, H) \geq \sum_{F \in \Gamma_1^R - \{H\}} \alpha_1(F) \geq p^2 \geq (p - 1)p$.

11. Suppose that G is a p -group such $d = d(G) \geq 3$. We claim that if $H \in \Gamma_1$ is nonabelian, then $\beta_1(G, H) \geq p^{d-2}(p - 1)$. We use induction on d . Remark 10 is the basis of induction so assume that $d > 3$. If $X \in \Gamma_1$, then $d(X) \geq d - 1 \geq 3$. Since $|\Gamma_1(H) \cap \Gamma_2| = p^{d-2} + \cdots + p + 1 > p + 1$, the set $\Gamma_1(H) \cap \Gamma_2$ has a nonabelian member R (Exercise 1.6(a)). Then all members of the set $\Gamma_1^R = \{H_1 = H, \dots, H_{p+1}\}$ are nonabelian. Let $d(H_i) = d_i$, where $d_i \geq d - 1$. By induction, $\beta_1(H_i, R) \geq p^{d_i-2}(p - 1) \geq p^{d-3}(p - 1)$, $i > 1$. Therefore, $\beta_1(G, H) \geq \sum_{i=2}^{p+1} \beta_1(H_i, R) \geq p^{d-3}(p - 1) \cdot p = p^{d-2}(p - 1)$, as required.

Theorem B. Suppose that a p -group G is neither abelian nor an \mathcal{A}_1 -group and $d = d(G)$. Then $\alpha_1(G) \geq p^{d-1}$.

Proof. By Lemma 76.6 and Theorem 76.9, the theorem is true for $d \leq 3$ so we may assume in what follows that $d > 3$. If $X \in \Gamma_1$, then $d(X) \geq d - 1$. We proceed by induction on d . If $H \in \Gamma_1$ is nonabelian and such that $d(H) \geq d$, then, by induction, $\alpha_1(H) \geq p^{d-1}$, and we are done. Therefore, one may assume that, for all nonabelian $H \in \Gamma_1$, we have $d(H) < d$; then, for such H we

have $d(H) = d - 1 (\geq 3)$. It follows from Lemma 76.3 that there is a nonabelian $R \in \Gamma_2$. Set $\Gamma_1^R = \{H_1, \dots, H_{p+1}\}$. By induction, $\alpha_1(H_i) \geq p^{d-2}$ and, by Remark 11, $\beta_1(H_i, R) \geq p^{d-3}(p-1)$ for all i . Therefore, $\alpha_1(G) \geq \alpha_1(H_1) + \sum_{i=2}^{p+1} \beta_1(H_i, R) \geq p^{d-2} + p^{d-3}(p-1) \cdot p = p^{d-1}$. \square

4^o. Groups of exponent p. We assume that all groups, considered in this subsection, have exponent p . If G is an \mathcal{A}_1 -group of exponent p , then $|G| = p^3$.

Now let G be an \mathcal{A}_2 -group; then $|G| = p^4$. If the set Γ_1 has exactly one abelian member, then $\text{cl}(G) = 3$ and $\alpha_1(G) = p$. If the set Γ_1 has two distinct abelian members, then $G = S \times C$ and $\alpha_1(G) = p^2$, where $|C| = p$.

Remarks. 12. Suppose that G is a nonabelian group of exponent p and order $\geq p^5$ and $H \in \Gamma_1$. By Proposition 2.3, $p^2 \mid \alpha_1(H)$, $p^2 \mid \alpha_1(G)$ so $p^2 \mid \beta_1(G, H)$.

13. We claim that if G is nonabelian of order p^6 and exponent p , then $\alpha_1(G) \geq p^3$. Let $R \in \Gamma_2$ be such that $R \neq Z(G)$. Set $\Gamma_1^R = \{H_1, \dots, H_{p+1}\}$. If R is nonabelian, then, by Remark 12 and Proposition 10.28, $\alpha_1(G) \geq \alpha_1(R) + \sum_{i=1}^{p+1} \beta_1(H_i, R) > p^2(p+1) > p^3$. If R is abelian, one may assume that H_1, \dots, H_p are nonabelian so $\alpha_1(H_i) \geq p^2$ ($i = 1, \dots, p$), by Proposition 2.3. In that case we have $\alpha_1(G) \geq \sum_{i=1}^p \alpha_1(H_i) \geq p^2 \cdot p = p^3$. Now let $R = Z(G)$. Then $G = A \times E$, where A is an \mathcal{A}_1 -group and $E \cong E_{p^3}$ so, by Remark 3, $\alpha_1(G) = p^6$.

Theorem C. *If G is nonabelian of order p^m and exponent p , $m > 3$, then:*

- (a) *If $H \in \Gamma_1$, then $\beta_1(G, H) \geq p^{m-4}(p-1)$.*
- (b) *$\alpha_1(G) \geq p^{m-3}$.*
- (c) *If $\alpha_1(G) = p^{m-3}$, then G is of maximal class with abelian subgroup of index p and $m \leq p$.*

Proof. In all three cases we proceed by induction on m .

(a) One may assume that $m > 4$, in view of Remark 1. Let $H \in \Gamma_1$ be nonabelian and $R \in \Gamma_1(H) \cap \Gamma_2$. Then the set $\Gamma_1^R = \{H_1 = H, \dots, H_{p+1}\}$ has at most one abelian member.

Suppose that H_{p+1} is abelian; then R is also abelian. In that case, by induction, $\beta_1(G, H) \geq \sum_{i=2}^p \alpha_1(H_i) \geq p^{(m-1)-3} \cdot (p-1) = p^{m-4}(p-1)$.

Now suppose that the set Γ_1^R has no abelian members. Then, by induction, we get $\beta_1(G, H) \geq \sum_{i=2}^{p+1} \beta_1(H_i, R) \geq p^{(m-1)-4}(p-1) \cdot p = p^{m-4}(p-1)$, and (a) is proven.

(b) In view of Remarks 12 and 13, one may assume that $m > 6$. There is $R \in \Gamma_2$ such that $R \neq Z(G)$ since G is neither abelian nor \mathcal{A}_1 -group. Set

$$\Gamma_1^R = \{H_1, \dots, H_{p+1}\}.$$

Suppose that R is abelian. One may assume in that case that H_1, \dots, H_p are non-abelian. By induction, we have

$$\alpha_1(G) = \sum_{i=1}^p \alpha_1(H_i) \geq p^{(m-1)-3} \cdot p = p^{m-3}.$$

Now let R be nonabelian. Then, by induction and (a), we have

$$\alpha_1(G) = \alpha_1(R) + \sum_{i=1}^{p+1} \beta_1(H_i, R) \geq p^{(m-2)-3} + p^{(m-1)-4}(p-1)(p+1) = p^{m-3},$$

completing the proof of (b).

- (c) Let $\alpha_1(G) = p^{m-3}$. As in (b), we prove that there is an abelian $A \in \Gamma_1$.
 - (i) Let $|Z(G)| = p$. Then G is of maximal class (Remark 5) and, by Theorem 9.5, since $\exp(G) = p$, we must have $m \leq p$. It is easy to check that then indeed $\alpha_1(G) = p^{m-3}$ (see Remark 5). Next we assume that $|Z(G)| > p$.
 - (ii) As in Remark 13, we have $|G : Z(G)| > p^2$. Therefore, there is a nonabelian $H_1 \in \Gamma_1$ containing $Z(G)$ as a subgroup of index $> p$. Take $Z(G) < R \in \Gamma_1(H_1) \cap \Gamma_2$ and set $\Gamma_1^R = \{H_1, \dots, H_{p+1}\}$. One may assume that H_1, \dots, H_p are nonabelian. It follows from $Z(G) < H_i$ and $|Z(G)| > p$ that H_i is not of maximal class so, by induction, $\alpha_1(H_i) > p^{m-4}$. If H_{p+1} is abelian, then R is also abelian, and we have $\alpha_1(G) \geq \sum_{i=1}^p \alpha_1(H_i) > p^{m-4} \cdot p = p^{m-3}$, contrary to the hypothesis. If H_{p+1} is nonabelian, then, by (a), we get

$$\alpha_1(G) \geq \alpha_1(H_1) + \sum_{i=2}^{p+1} \beta_1(H_i, R) > p^{m-4} + p^{m-5}(p-1) \cdot p = p^{m-3},$$

a contradiction. \square

5^o . \mathcal{M}_3 -groups. A p -group G is said to be an \mathcal{M}_3 -group, if all its \mathcal{A}_1 -subgroups have the same order p^3 . The groups of maximal class with abelian subgroup of index p are \mathcal{M}_3 -groups (Remark 5). If an \mathcal{A}_2 -group G is also an \mathcal{M}_3 -group, then $|G| = p^4$ and $\alpha_1(G) \in \{p, p^2\}$.

Theorem C1. *Let G be a nonabelian \mathcal{M}_3 -group of order p^m and exponent p , $m > 3$. Then:*

- (a) *If $H \in \Gamma_1$, then $\beta_1(G, H) \geq p^{m-4}(p-1)$.*
- (b) *$\alpha_1(G) \geq p^{m-3}$.*
- (c) *If, in addition, $\alpha_1(G) = p^{m-3}$, then G is of maximal class with abelian subgroup of index p .*

Theorem C₂. Let G be a nonabelian group of order p^m . Suppose that G has an \mathcal{A}_1 -subgroup of order p^a but has no \mathcal{A}_1 -subgroups of order $> p^a$. Then $\alpha_1(G) \geq p^{m-a}$. If, in addition, $\alpha_1(G) = p^{m-a}$, then all \mathcal{A}_1 -subgroups of G have the same order p^a .

The proofs are omitted since they are repetitions of the proof of Theorem C. For $p = 2$, see §90. See also Problem 155.

6°. *p-groups with few conjugate classes of \mathcal{A}_1 -subgroups.* Given a p -group G , let $\kappa_1(G)$ denote the number of conjugate classes of \mathcal{A}_1 -subgroups in G .

Given $H \in \Gamma_1$, we define (i) $\beta_1(G, H)$ is the number of conjugate G -classes of \mathcal{A}_1 -subgroups not contained in H , (ii) $\bar{\kappa}_1(H)$ is the number of G -classes of \mathcal{A}_1 -subgroups contained in H . We have $\bar{\kappa}_1(H) \leq \kappa_1(H)$ and, as a rule, the strong inequality holds. Obviously, $\bar{\kappa}_1(G) = \kappa_1(G)$.

Theorem 76.17 (compare with Lemma 76.5). *Let G be a p -group and let $H \in \Gamma_1$ be nonabelian. Then $\bar{\beta}_1(G, H) \geq p - 1$. If $\bar{\beta}_1(G, H) = p - 1$, then:*

- (a) $d(G) = 2$ and $\Gamma_1 = \{H_1 = H, \dots, H_p, A\}$, where A is the unique abelian member of the set Γ_1 .
- (b) $H'_1 = \dots = H'_p$, G/H'_1 is an \mathcal{A}_1 -group so $|G'| = p|H'_1|$ and $d(H_i) \leq 3$, $i \leq p$.
- (c) If $|H'_i| = p$ for some $i > 1$, then H_2, \dots, H_p are \mathcal{A}_1 -groups and $\beta_1(G, H) = p - 1$.

Lemma 76.18. *Let G be a p -group and let a nonabelian $H \in \Gamma_1$ be not an \mathcal{A}_1 -subgroup. Suppose that $\bar{\kappa}_1(H) = 1$. Then (a) H has no proper nonabelian G -invariant subgroups and the set $\Gamma_1(H)$ has exactly one abelian member, (b) $d(G) = 2$, (c) $|H'| > p$.*

Proof. Assume that a nonabelian $A \in \Gamma_1(H)$ is G -invariant and let $U \leq A$ be an \mathcal{A}_1 -subgroup. By Proposition 10.28, H has an \mathcal{A}_1 -subgroup V that is not contained in A . Since $U^G \leq A$, U and V are not conjugate in G , a contradiction. This proves the first assertion of (a).

Assume that $|H'| = p$; then $d(H) > 2$ since H is not an \mathcal{A}_1 -group (Lemma 65.2(a)). Let $U < H$ be an \mathcal{A}_1 -subgroup. Then $U' = H'$ so $U \triangleleft H$. It follows that $H = N_G(U)$ so $|G : N_G(U)| = p$. In that case, H contains exactly p subgroups conjugate with U in G so, by hypothesis, $\alpha_1(H) = p$. However, by Theorem B, $\alpha_1(H) \geq p^2$, contrary to what has just been said. Thus, $|H'| > p$, proving (c).

The set $\Gamma_1(H)$ has exactly one abelian member (otherwise, $|H'| = p$), and this completes the proof of (a). Then, since all members of the set $\Gamma_1(H) \cap \Gamma_2$ are abelian, we get $|\Gamma_1(H) \cap \Gamma_2| = 1$ (Lemma 64.1(q)), hence $d(G) = 2$, completing the proof of (b). \square

Proof of Theorem 76.17. Let $N \in \Gamma_2 \cap \Gamma_1(H)$; then $N \not\leq Z(G)$ since H is non-abelian. Set $\Gamma_1^N = \{H_1 = H, \dots, H_{p+1}\}$. Since the set Γ_1^N has at most one abelian member, one may assume that H_1, \dots, H_p are nonabelian. By Proposition 10.28,

there exists an \mathcal{A}_1 -subgroup $B_i \leq H_i$ such that $B_i \not\leq N$, $i = 2, \dots, p$. For $i \neq j$, we have $B_i^G N = H_i \neq H_j = B_j^G N$ so $B_i^G \neq B_j^G$, and we conclude that B_i and B_j are not conjugate in G . Thus, $\bar{\beta}_1(G, H) \geq |\{B_2, \dots, B_p\}| = p - 1$.

Now let $\bar{\beta}_1(G, H) = p - 1$. For $i = 2, \dots, p$, all \mathcal{A}_1 -subgroups of H_i that are not contained in N , are G -conjugate with B_i so H_{p+1} must be abelian (otherwise, $\bar{\beta}_1(G, H) > p - 1$); then N is also abelian. In that case, $\bar{\kappa}_1(H_i) = 1$ for $i = 2, \dots, p$ so, by Lemma 76.18(b), $d(G) = 2$; then $\Gamma_1 = \Gamma_1^N$ and $N = \Phi(G)$. By Lemma 76.2, $H'_1 = \dots = H'_p$ and G/H'_1 is an \mathcal{A}_1 -subgroup so $|G'| = p|H'_1|$ and, since $H'_i \leq \Phi(H_i)$, we get $d(H_i) = d(H_i/H'_i) \leq 3$ for $i = 2, \dots, p$ (Lemma 76.1). Now, (c) follows easily from Lemmas 65.2(a) and 76.18. \square

If G is a group of maximal class and order $p^n > p^3$ with abelian subgroup of index p , then $\kappa_1(G) = p$ and, if $H \in \Gamma_1$ is nonabelian, then $\bar{\beta}(G, H) = p - 1$.

Corollary 76.19 (compare with Lemma 76.6(b)). *Let G be a p -group. If $\kappa_1(G) = p + 1$, then $d(G) = 2$ and $\Phi(G)$ is abelian.*

Proof. Since G is neither abelian nor an \mathcal{A}_1 -group, there exists $R \in \Gamma_2$ such that $R \not\leq Z(G)$ (Lemma 76.3). Set $\Gamma_1^R = \{H_1, \dots, H_{p+1}\}$; then at most one member of the set Γ_1^R is abelian. Suppose that H_1 is nonabelian; then $\bar{\beta}_1(G, H_1) \leq p$, by hypothesis. If $\bar{\beta}_1(G, H_1) = p - 1$, then $d(G) = 2$ and $R = \Phi(G)$ is abelian (Theorem 76.17). Now we assume that $\bar{\beta}_1(G, H_1) = p$; then $\bar{\kappa}_1(H_1) = 1$ (otherwise, $\kappa_1(G) > p + 1$). In that case, $d(G) = 2$ and H_1 has no proper nonabelian G -invariant subgroups (Lemma 76.18(a,b)) so $\Phi(G)$, as a proper G -invariant subgroup of H_1 , is abelian. \square

Proposition 76.20. *Suppose that a p -group G is neither abelian nor an \mathcal{A}_1 -group. Let all proper nonabelian normal subgroups of G be members of the set Γ_1 . Then $d(G) \leq 3$ and one of the following holds:*

- (a) $d(G) = 2$ and either $\text{cl}(G) = 2$ or G/G' has a cyclic subgroup of index p .
- (b) $d(G) = 3$. If R is a G -invariant subgroup of index p in G' , then G/R is an \mathcal{A}_2 -group.

Proof. Suppose that $d(G) > 2$. By hypothesis, all members of the set Γ_2 are abelian so $\Phi(G) \leq Z(G)$ and $d(G) = 3$ (Lemma 76.3). Let R be a G -invariant subgroup of index p in G' . We claim that G/R is an \mathcal{A}_2 -group. Without loss of generality, one may assume that $R = \{1\}$; then $|G'| = p$. It follows from $d(G) = 3$ that G is not an \mathcal{A}_1 -group (Lemma 76.1). Let $B < G$ be an \mathcal{A}_1 -subgroup. In view of $B' = G'$ we get $B \triangleleft G$ so $B \in \Gamma_1$, by hypothesis, and G is an \mathcal{A}_2 -group.

Now suppose that $d(G) = 2$. Let $M/G' < G/G'$ be of index p^2 . Then, by hypothesis, M is abelian. It follows that $M \leq C_G(G')$. If G is not of class 2, then G/G' is not generated by subgroups of index p^2 so it has a cyclic subgroup of index p . \square

Proposition 76.21. *Let G be a nonabelian p -group.*

- (a) (Compare with Theorem 76.9) If $d(G) > 2$, then $\kappa_1(G) \geq p^2$.
(b) If $d(G) > 3$, then $\kappa_1(G) > p^2 + p + 1$.

Proof. (a) Suppose that all members of the set Γ_2 are abelian. Then $d(G) = 3$ and $\Phi(G) \leq Z(G)$ (Lemma 76.3). Let $\{M_1, \dots, M_s\}$ be the set of all nonabelian members of the set Γ_1 ; then $s \geq p^2$ (Exercise 1.6(a)). It remains to show that $\kappa_1(G) \geq s$. Let $A_i \leq M_i$ be an \mathcal{A}_1 -subgroup; then $M_i = A_i \Phi(G)$ is the unique member of the set Γ_1 , containing A_i , $i = 1, \dots, s$. It follows that A_1, \dots, A_s are pairwise not conjugate in G , and we are done in this case.

Now suppose that the set Γ_2 has a nonabelian member N . Take $T \in \Gamma_1(N) \cap \Gamma_3$; then $T \not\leq Z(G)$. Since G/T is generated by any $p+2$ subgroups of order p , it follows that T is contained in at most $p+1$ abelian members of the set Γ_2 . In that case, there are p^2 distinct subgroups $L_1/T, \dots, L_{p^2}/T$ of order p in G/T such that L_1, \dots, L_{p^2} are nonabelian; obviously, $L_i \in \Gamma_2$ for all i . Let $A_i \leq L_i$ be an \mathcal{A}_1 -subgroup not contained in T (Proposition 10.28), $i = 1, \dots, p^2$; then $L_i = A_i T$. Since A_1, \dots, A_{p^2} are pairwise not conjugate in G , we get $\kappa_1(G) \geq p^2$.

(b) Let $d(G) > 3$. Suppose that all members of the set Γ_3 are abelian. Then all members of the set Γ_4 are contained in $Z(G)$ so $d(G) = 4$ (otherwise, $G = \langle H \mid H \in \Gamma_4 \rangle$ is abelian). If $|G : Z(G)| = p^2$, then $G = BZ(G)$ for each \mathcal{A}_1 -subgroup $B < G$ so all \mathcal{A}_1 -subgroups are normal in G . Therefore, $\kappa_1(G) = \alpha_1(G) \geq p^3$ (Theorem B). Since, $p^3 > p^2 + p + 1$, we are done in this case. Thus, $|G : Z(G)| \in \{p^3, p^4\}$. It follows that at least $|\Gamma_3| - 1 = p^3 + p^2 + p$ members of the set Γ_3 are not contained in $Z(G)$. Let T_1, T_2 and T_3 be those distinct members of the set Γ_3 that are not contained in $Z(G)$. Since any $p+2$ distinct subgroups of order p generate G/T_i , it follows that at least p^2 members of the set $\Gamma_2^{T_i}$ are nonabelian, $i = 1, 2, 3$. Let $i \neq j$, $i, j \leq 3$ and $K \in \Gamma_2^{T_i} \cap \Gamma_2^{T_j}$. Then $K = T_i T_j$ is determined uniquely. It follows that the set $\mathfrak{M} = \bigcup_{i=1}^3 \Gamma_2^{T_i}$ contains at least $3p^2 - 3$ distinct nonabelian members. Let $\mathfrak{M}' = \{H_1, \dots, H_k\}$ be the set of all nonabelian members in the set \mathfrak{M} , where $k \geq 3p^2 - 3$, and let $L_s \leq H_s$ be an \mathcal{A}_1 -subgroup, $s \leq k$. Since the intersection of any two distinct members of the set \mathfrak{M}' is abelian, H_s is the unique member of the set \mathfrak{M}' containing L_s , $s \leq k$. It follows that L_1, \dots, L_k are not pairwise G -conjugate so $\kappa_1(G) \geq k \geq 3p^2 - 3 > p^2 + p + 1$.

Now suppose that the set Γ_3 has a nonabelian member T . Set $\Gamma_2^T = \{H_1, \dots, H_k\}$, $k = p^2 + p + 1$. Let $L_i \leq H_i$ be an \mathcal{A}_1 -subgroup not contained in T , $i = 1, \dots, k$ (L_i exists, by Proposition 10.28), and let $L \leq T$ be an \mathcal{A}_1 -subgroup. We have $L_i T = H_i$ for $i \leq k$. Since L, L_1, \dots, L_k are pairwise not conjugate in G , we get $\kappa_1(G) \geq k + 1 > k = p^2 + p + 1$. \square

Let G be a nonabelian p -group. Given $\mathfrak{M} \subseteq \Gamma_1$, let $\kappa_1(\mathfrak{M})$ be the number of conjugate G -classes of \mathcal{A}_1 -subgroups contained in the members of the set \mathfrak{M} (obviously, $\kappa_1(\Gamma_1) = \kappa_1(G)$, unless G is an \mathcal{A}_1 -group).

Remarks. 14. Suppose that every \mathcal{A}_1 -subgroup is contained in the unique maximal subgroup of a nonabelian p -group G . Then $\Phi(G)$ is abelian and one and only one of the following holds: (i) $d(G) = 2$, (ii) $d(G) = 3$ and $\Phi(G) \leq Z(G)$. Indeed, the groups from (i) and (ii) satisfy the hypothesis (if $H < G$ is an \mathcal{A}_1 -subgroup, then, in both cases, $H\Phi(G)$ is the unique maximal subgroup of G containing H). Now let G satisfy the hypothesis. Then all members of the set Γ_2 are abelian. By Lemma 76.3, $d(G) \leq 3$ and, if $d(G) = 3$, then $\Phi(G) \leq Z(G)$.

15. Suppose that G is a nonabelian p -group with $d(G) > 2$. We claim that the following assertions are equivalent: (a) $\kappa_1(\Gamma_1^K) \leq p$ for all $K \in \Gamma_2$, (b) G is an \mathcal{A}_2 -group with $\alpha_1(G) = p^2$. Let (b) holds. Then all nonabelian members of the set Γ_1 are \mathcal{A}_1 -subgroups and $|G : Z(G)| = p^2$ (Lemma 76.4(d)). If $K \in \Gamma_2 - \{Z(G)\}$, then $KZ(G) \in \Gamma_1$ so $\kappa_1(\Gamma_1^K) = p$ and (b) \Rightarrow (a). It remains to prove the reverse implication. Assume that $H_1 \in \Gamma_1$ is neither abelian nor minimal nonabelian. Then there is a nonabelian $K_1 \in \Gamma_1(H_1)$. In that case, $\alpha_1(\Gamma_1^{K_1}) \geq p + 2 > p$, a contradiction. Thus H_1 does not exist so G is \mathcal{A}_2 -group.

Exercise 5. Let G be a p -group and let the set Γ_1 have exactly p nonabelian members. Then: (a) $\Gamma_1 = \{H_1, \dots, H_p, A\}$, where A is abelian. (b) $H'_1 = \dots = H'_p$ has index p in G' .

Exercise 6. Let G be a nonabelian two-generator p -group and $|G : G'| = p^n > p^2$. Prove that if G has only one normal subgroup of index p^n , then G/G' is abelian of type (p^{n-1}, p) and $\exp(G) \geq p^n$. (*Hint.* Consider the quotient group G/R , where R is a G -invariant subgroup of index p in G' . Use Lemma 65.2(a).)

2-groups with a self-centralizing abelian subgroup of type (4, 2)

The results of this section are taken from [Jan9]. Here we classify finite 2-groups G which possess an abelian subgroup $A \cong C_4 \times C_2$ such that $C_G(A) = A$. If A is normal in G , then G/A is isomorphic to a subgroup of $\text{Aut}(A) \cong D_8$. Therefore we may assume in the sequel that such a subgroup A is not normal in G . We investigate first the case where $A \leq \Phi(G)$ and prove the following basic result.

Theorem 77.1. *Let G be a 2-group which possesses a self-centralizing abelian subgroup A of type (4, 2) but G does not possess any self-centralizing abelian normal subgroup of type (4, 2). If $A \leq \Phi(G)$, then G has no normal elementary abelian subgroups of order 8.*

Proof. We assume that $A \leq \Phi(G)$. Let $W_0 = \Omega_1(A)$ so that $W_0 \cong E_4$ and $Z(\Phi(G)) < A$ (the inclusion is strong since A is not normal in G). It follows from $|G : C_G(W_0)| \leq 2$ that $W_0 \leq Z(\Phi(G))$. Since $Z(\Phi(G)) < A$, it follows that $W_0 = Z(\Phi(G))$ so W_0 is a normal four-subgroup in G .

We claim that W_0 is the unique normal four-subgroup of G . Indeed, if W_1 were another normal four-subgroup of G , then A does not centralize W_1 and so $C_G(W_1)$ is a maximal subgroup of G not containing A , contrary to our assumption that $A \leq \Phi(G)$. Since $A < \Phi(G)$ and $|G/\Phi(G)| \geq 4$, we get $|G| \geq 2^6$.

Assume that $W_0 \leq Z(G)$. Let B be a normal subgroup of G such that $W_0 < B \leq \Phi(G)$ and $|B : W_0| = 2$. Then G stabilizes the chain $B > W_0 > \{1\}$ and so $G/C_G(B)$ is elementary abelian. In particular, $\Phi(G) \leq C_G(B)$ which contradicts the fact that $Z(\Phi(G)) = W_0$. Hence $|G : C_G(W_0)| = 2$ and so $Z(G) = \langle z \rangle < W_0$. Set $W_0 = \langle z, u \rangle$ and $T = C_G(W_0)$. For each $x \in G - T$, $u^x = uz$ and for each $a \in A - W_0$, $C_T(a) = C_T(A) = A$ since $A = \langle a, W_0 \rangle$ and $W_0 \leq Z(T)$.

Suppose that A_1 is a normal elementary abelian subgroup of order 16 of $T = C_G(W_0)$. Take an element $a \in A - W_0$. Since $a^2 \in W_0 \leq Z(T)$, the element a induces on A_1 an automorphism of order ≤ 2 and so $|C_{A_1}(a)| \geq 4$ since $\langle a, A_1 \rangle$ is not of maximal class (Proposition 1.8). Since $C_T(a) = A$, we get $C_{A_1}(a) = W_0$ and $A \cap A_1 = W_0$. Set $C = AA_1$ so that $|C| = 2^5$, $Z(C) = W_0$ and $|C : A_1| = 2$.

Set $\langle s \rangle = \Omega_1(A) < W_0$ and we see that all four elements in $A - W_0$ are square roots of s in C . Let aa_1 ($a \in A - W_0, a_1 \in A_1$) be any square root of s in C . Then we have

$s = (aa_1)^2 = aa_1aa_1 = a^2(a^{-1}a_1a)a_1 = sa_1^a a_1$, and so $a_1^a = a_1$ which implies that $a_1 \in W_0$ hence $aa_1 \in A - W_0$. It follows that four elements in $A - W_0$ are the only square roots of s in C and they form a single conjugate class in C (it follows from $C_T(a) = A$ that $C_C(a)$ has index 4 in C). Since T centralizes s , it follows that $A - W_0$ is a conjugacy class in $N_T(C)$ so $\langle A - W_0 \rangle = A$ is normal in $N_T(C)$ which implies $C = T$ (in view of $W_0 \leq Z(T)$ we have $|T : A| = |T : C_T(A)| \leq 4 = |C : A|$) and $|G| = 2|T| = 2|C| = 2^6$. Since $W_0Z(T) < A$, we conclude that $Z(T) = W_0$. It follows that A_1 is the unique abelian subgroup of index 2 in T so A is characteristic in T ; then A_1 is normal in G . It follows from the previous sentence that $T/W_0 \cong E_{2^3}$ (otherwise, T contains an abelian subgroup of index 2 and exponent 4, which is not the case). By Lemma 1.1, $|T'| = 4$ so $T' = W_0 = \Phi(G) = Z(T)$, and T is special.

Let b be any element in $C - A_1 = T - A_1$ so that $b = a_1a$ for an $a \in A - W_0$ and $a_1 \in A_1$ (recall that $A \cap A_1 = W_0$). Hence $C_{A_1}(b) = C_{A_1}(a) = W_0$. In particular, $b^2 \in W_0$ and so four elements in $\langle W_0, b \rangle - W_0$ are either involutions (in case $b^2 = 1$) or square roots of the involution b^2 . Conversely, let bx ($x \in A_1$) be any square root of b^2 or an involution if $b^2 = 1$ in $C - A_1$. Then $b^2 = (bx)^2 = bxbx = b^2(b^{-1}xb)x = b^2x^b x$, which implies $x^b = x$ and so $x \in C_T(b) = W_0$. Hence four elements in $\langle W_0, b \rangle - W_0$ are all possible square roots of b^2 if $\langle W_0, b \rangle \cong C_4 \times C_2$ (or involutions if $\langle W_0, b \rangle \cong E_8$) in $T - A_1$. By Exercises 17–19 in §10 and Theorem 1.17(a), each group of order 2^5 contains at most 19 involutions, unless it is elementary abelian or isomorphic to $D_8 \times E_4$. It follows that $T - A_1$ contains at least 12 elements of order 4 and so, by what has been proved already, the set of squares of these elements is $W_0^\#$. Thus, each involution in W_0 has exactly four square roots in $T - A_1$ and, in addition, there are exactly four involutions in $T - A_1$.

Let $z \in W_0$ be the central involution in G . By the previous paragraph, there are exactly four square roots of z in C and if c is one of them, then $\langle W_0, c \rangle \cong C_4 \times C_2$ and all square roots of z in $C = T$ form the set $\langle W_0, c \rangle - W_0$. Hence $\langle W_0, c \rangle - W_0$ is a normal subset in G and so $\langle W_0, c \rangle$ is normal in G in view of $z \in Z(G)$. Since $Z(T) = W_0$, A_1 is the unique abelian subgroup of index 2 in T so $C_T(c) = \langle W_0, c \rangle$. Thus $\langle W_0, c \rangle$ is a self-centralizing (in G) normal abelian subgroup of G of type (4, 2), contrary to the hypothesis.

We have proved that $T = C_G(W_0)$ has no normal elementary abelian subgroups of order 16.

Let U be a noncyclic abelian normal subgroup of G . Then $W_0 \leq U$ (because of the uniqueness of W_0) so $U \leq C_G(W_0) = T$. By the previous paragraph, $U \not\cong E_{2^4}$ so G has no normal elementary abelian subgroups of order 16.

Suppose that $E_8 \cong E \triangleleft G$. By the previous paragraph, $E \leq T$, and $E > W_0$, and so $A \cap E = W_0$.

Let B be a maximal G -invariant abelian subgroup containing E . Since B is noncyclic, we have $B \leq T$. We know that $C_G(B) = B$.

Suppose that $B = E$. Then G/E , as a subgroup of order $|G : E| = 8$ of $\text{Aut}(E) \cong \text{GL}(3, 2) \cong \text{PSL}(2, 7)$, is isomorphic to D_8 . Set $V_0 = AE$ so that $V_0/E = \Phi(G/E)$

and therefore V_0 is normal in G . Indeed, if M/E is a maximal subgroup of G/E , then $A \leq M$ since $A \leq \Phi(G)$, and so $V_0/E = AE/E < M/E$, proving our claim.

Since T stabilizes the chain $E > W_0 > \{1\}$ and $C_T(E) = E$, it follows that $T/E \cong E_4$. Take an element $a \in A - W_0$ so that four elements in $A - W_0$ are square roots of $a^2 \neq 1$. Let ae' ($e' \in E$) be any square root of a^2 in V_0 . Then we have $a^2 = (ae')^2 = ae'ae' = a^2(e')^a e'$, which gives $(e')^a = e'$ and so $e' \in W_0$ since $C_T(a) = A$. It follows that $A - W_0$ is the set of all square roots of a^2 in V_0 and so $A = \langle A - W_0 \rangle$ is normal in T . Since A is not normal in G , we have for every $x \in G - T$, $A^x \neq A$. Since $A^x \leq V_0$ and $A \cap A^x = W_0$, we have $V_0 - E = Ea = (A - W_0) \cup (A^x - W_0)$ and so x sends four elements in $A - W_0$ onto four elements in $A^x - W_0$. But $G/E \cong D_8$ and so (since $T/E \cong E_4$ and $V_0/E = \Phi(G/E)$) there is $y \in G - T$ with $y^2 \in V_0 - E$. Since V_0 is nonabelian, A , A^x and E are all abelian subgroups of index 2 in V_0 . Since $\langle y^2, W_0 \rangle$ equals either A or A^x , one of these subgroups is normal in G since it is normalized by $\langle y, T \rangle = G$; then both of them are normal in G , and this is a contradiction.

We have proved that $B > E$ and so $|B| \geq 2^4$. Since $\Omega_1(B) = E$ (recall that G has no normal elementary abelian subgroups of order 2^4), B is an abelian group of rank 3. Take an element $a \in A - W_0$. Since $a^2 \in W_0 \leq Z(T)$, a induces an involutory automorphism on B with $C_B(a) = W_0 \leq \Omega_1(B)$ (since $a \notin B$ in view of $C_T(a) = A$). Applying Proposition 51.2, we see that a inverts $\mathfrak{V}_1(B)$ and B/W_0 . Suppose that some $e \in E - W_0$ ($= E - A$) is a square in B . Then a inverts (centralizes) e ($\in \mathfrak{V}_1(B)$) so e centralizes $\langle a, W_0 \rangle = A$, a contradiction. Suppose that each involution in W_0 is a square in B . Then $\Omega_2(B) = \langle b_1 \rangle \times \langle b_2 \rangle \times \langle b_3 \rangle$, where $o(b_1) = o(b_2) = 4$, b_3 is an involution in $E - W_0$, and $\langle b_1^2, b_2^2 \rangle = W_0$. Since a inverts B/W_0 , we get $b_1^a = b_1^{-1}w$ with $w \in W_0$ and so $b_1^a = b_1^{-1}w = b_1(b_1^2 w) = b_1 w_1$, where $w_1 \in W_0$. Similarly, $b_2^a = b_2 w_2$ and $b_3^a = b_3 w_3$ with $w_2, w_3 \in W_0$. Since $C_{\Omega_2(B)}(a) = W_0$, w_1, w_2, w_3 must be three distinct involutions in W_0 (otherwise, if, for example, $w_1 = w_2$, then $(b_1 b_2)^a = b_1 b_2$, which is not the case). But then $(b_1 b_2 b_3)^a = (b_1 b_2 b_3)(w_1 w_2 w_3) = b_1 b_2 b_3 \in \Omega_2(B) - W_0$, a contradiction. Hence we have $B = \langle b \rangle \times \langle w \rangle \times \langle e \rangle$, where

$$o(b) = 2^m, \quad m > 1, \quad b^{2^{m-1}} = z, \quad \langle z \rangle = \mathfrak{V}_{m-1}(B) = Z(G), \quad W_0 = \langle z, w \rangle,$$

and $e \in E - W_0$. Also we set $v = b^{2^{m-2}}$ so that $o(v) = 4$, $v^2 = z$, and $\Omega_2(B) = \langle E, v \rangle$ is abelian of type $(4, 2, 2)$.

Set $V = AB$ and assume that $V < T$ ($V \leq T$ since $A, B < T$). Set $\tilde{V} = N_T(V)$ so that $|\tilde{V} : V| \geq 2$. Since B is normal in G , $V - B = aB$ ($a \in A - W_0$) is a normal subset in $V^* = N_G(V) \geq \tilde{V}$. Set $a^2 = w' \in W_0$ so that four elements in $A - W_0$ are square roots of w' in $V - B$. An element $ab' \in V - B$ ($b' \in B$) is a square root of w' if and only if $w' = (ab')^2 = ab'ab' = a^2(b')^a b' = w'(b')^a b'$ or $(b')^a = (b')^{-1}$. If $(b')^a = (b')^{-1}$ and $(b'')^a = (b'')^{-1}$ ($b', b'' \in B$), then $(b'b'')^a = (b')^a(b'')^a = (b')^{-1}(b'')^{-1} = (b'b'')^{-1}$, and so the set B_0 of elements of B which are inverted by a is a subgroup of B . Therefore, the number of square roots of w' in $V - B$ equals $|B_0|$. It follows from $C_T(a) = A$ that $B_0 \cap E = W_0$. We have $|B| = 2^{m+2}$ ($m > 1$) (recall

that B is abelian of type $(2^m, 2, 2)$) so $|V - B| = 2^{m+2}$ and therefore $|B_0| \leq 2^{m+1}$. All conjugates of a in \tilde{V} lie in $V - B$ and all these conjugates are square roots of w' since $\tilde{V} \leq T$ and T centralizes $w' \in W_0$. Since $C_{\tilde{V}}(a) = A$, we get $|\tilde{V} : A| \leq 2^{m+1}$. But $|V| = 2^{m+3}$ and so $|\tilde{V}| = 2^{m+4}$, $|\tilde{V} : V| = 2$, and $|B_0| = 2^{m+1}$. It follows that B_0 covers B/E and so we may choose $b \in B_0$ such that $B_0 = \langle b \rangle \times \langle w \rangle$, where $w \in W_0 - \langle z \rangle$ (since $b^{2^{m-1}} = z$).

Suppose for a moment that $\tilde{V} = N_T(V) = N_G(V)$. Then looking at G/B , we get, by Proposition 1.8, that G/B is of maximal class and V/B is a noncentral subgroup of order 2 in G/B . Let R/B be a cyclic subgroup of index 2 in G/B . Then R is a maximal subgroup of G and $R \cap V = B$. In particular, $A \not\leq R$, contrary to our assumption $A \leq \Phi(G)$. We have proved that $V^* = N_G(V) > \tilde{V} = N_T(V)$ so that $|V^* : \tilde{V}| = 2$, $G = TV^*$, and $T \cap V^* = T \cap N_G(V) = N_T(V) = \tilde{V}$.

Assume that $C_{V^*}(a) = A = C_{\tilde{V}}(a)$ and take an element $y \in V^* - \tilde{V}$ so that $y \in G - T$. Then all 2^{m+2} elements in $V - B$ form a single conjugate class in V^* . Since w' has exactly 2^{m+1} square roots in $V - B$, it follows that $w' = a^2 \neq z$ (since $\langle z \rangle = Z(G)$) and so $(w')^y = w'z$. Hence y sends 2^{m+1} square roots of w' in $V - B$ onto 2^{m+1} square roots of $w'z$ in $V - B$. Since $e \notin B_0$ ($e \in E - W_0$), we have $(ae)^2 = w'z = aeae = a^2e^a e = w'e^a e$, and so $e^a = ez$. On the other hand, a inverts $B_0 = \langle b, w \rangle$ and so setting $v = b^{2^{m-2}}$, we get $v^2 = z$ and $v^a = v^{-1} = vz$. But then $(ev)^a = ezvz = ev$, contrary to $C_B(a) = W_0$. We have proved that $\tilde{A} = C_{V^*}(a) > A$, where $|\tilde{A} : A| = 2$ and $\tilde{A} \cap T = A$.

Take an element $y \in \tilde{A} - A$ so that y acts non-trivially on W_0 . But y centralizes a and so y centralizes $a^2 = w'$ which gives $w' = z = b^{2^{m-1}}$, where $\langle z \rangle = Z(G)$. Suppose $y^2 \in W_0$ so that $\langle W_0, y \rangle \cong D_8$. In that case there are involutions in $\langle W_0, y \rangle - W_0$ and so we may assume that y is an involution. Act with the involution y on E . Since y acts non-trivially on W_0 and $|C_E(y)| = 4$, there is an involution $e' \in E - W_0$ with $(e')^y = e'$. We have $1 \neq [a, e'] \in W_0$ and so $[a, e']^y = [a^y, (e')^y] = [a, e']$, which gives $[a, e'] = z$ or $(e')^a = e'z$. But a inverts B_0 and so $v^a = v^{-1} = vz$ (where $v = b^{2^{m-2}}$) which gives $(ve')^a = vze'z = ve' \notin W_0$. This is a contradiction since $C_B(a) = W_0$.

We have proved that for each $y \in \tilde{A} - A$, $y^2 \in A - W_0$ and so we may assume that $y^2 = a$. Since $a^2 = z$ centralizes E , it follows that y induces on E an automorphism of order 4 and so $C_E(y) = \langle z \rangle$. Hence for an $e \in E - W_0$, we get $e^y = ew_0$ with $w_0 \in W_0 - \langle z \rangle$ and $w_0^y = w_0z$. This gives $e^a = e^{y^2} = (ew_0)^y = (ew_0)(w_0z) = ez$. On the other hand, a inverts $B_0 = \langle b, w_0 \rangle$ and so $v^a = v^{-1} = vz$. This gives $(ve)^a = vzez = ve \notin W_0$, contrary to $C_B(a) = W_0$.

The contradiction in the previous paragraph shows that we must have $V = AB = T$. We set again $a^2 = w' \in W_0$ ($a \in A - W_0$) and $v = b^{2^{m-2}}$ ($m > 1$) so that $v^2 = z$, where $\langle z \rangle = Z(G)$ and $B = \langle E, b \rangle$. We have $|G/B| = 4$. If $G/B \cong E_4$, then $\Phi(G) \leq B$ and this contradicts our assumption $A \leq \Phi(G)$. Hence $G/B \cong C_4$ and G/B acts faithfully on E (since $T = B\langle a \rangle$ and a acts non-trivially on E). If

$y \in G - T$, then for an element $e \in E - W_0$, we have $e^y = ew$ with $w \in W_0 - \langle z \rangle$ and $w^y = wz$. Then we compute $e^{y^2} = (ew)^y = (ew)(wz) = ez$. But $y^2 \in T - B$ and $T = B\langle a \rangle$ and so a acts in the same way on E as the element y^2 which implies $e^a = ez$. By Proposition 51.2, a inverts $\Omega_1(B)$. If $m > 2$, then $v \in \Omega_1(B)$ and so $v^a = v^{-1} = vz$. We get in that case $(ev)^a = ezvz = ev$ which contradicts to $C_B(a) = W_0$.

We have proved that we must have $m = 2$ and so $b = v$, $|B| = 2^4$, and $|G| = 2^6$. The argument of the previous paragraph shows that a does not invert any element (of order 4) in $B - E$ and so the subgroup B_0 of all elements of B inverted by a is equal $B_0 = W_0$. Indeed, if a inverts an element $s \in B - E$, then $s^a = s^{-1} = sz$ and so $(es)^a = ezs = es$, contrary to $C_B(a) = W_0$. Hence $a^2 = w'$ has exactly $|B_0| = 4$ square roots in $T - B = V - B = (AB) - B$ and they all lie in $A - W_0$. Since $\langle A - W_0 \rangle = A$, A is normal in $T = AB$. For each $x \in T - B$, $x^2 \in W_0$ since $C_B(x) = C_B(a) = W_0$, and x (acting in the same way on B as the element a) inverts on B exactly the elements of W_0 . It follows that x^2 has exactly four square roots in $T - B$. Hence each involution in W_0 has exactly four square roots in $T - B$ and (since $|T - B| = 16$) $T - B$ contains exactly four involutions.

Let $a' \in T - B$ so that $(a')^2 = z$. Set $A^* = W_0\langle a' \rangle \cong C_4 \times C_2$ and A^* is normal in G . Indeed, $\langle z \rangle = Z(G)$ and so G normalizes the subset $\{W_0\langle a' \rangle - W_0\}$ of all square roots of z in $T - B$. We have $C_G(W_0) = T$ and $C_T(a') = \langle a' \rangle C_B(a')$. But $C_B(a') = C_B(a) = W_0$ and so A^* is a self-centralizing abelian normal subgroup of type $(4, 2)$ in G . This is a final contradiction and our theorem is proved. \square

In our next result we shall determine the structure of the groups appearing in Theorem 77.1.

Theorem 77.2. *Let G be a 2-group which possesses a self-centralizing abelian subgroup A of type $(4, 2)$ but G does not possess any self-centralizing abelian normal subgroup of type $(4, 2)$. If $A \leq \Phi(G)$, then G has the following properties:*

- (i) *G has no normal elementary abelian subgroups of order 8.*
- (ii) *G has the unique normal four-subgroup $W_0 = \Omega_1(A)$.*
- (iii) *G has a normal metacyclic subgroup N such that $\Omega_2(N) = W$ is abelian of type $(4, 4)$, $C_G(W) \leq N$, $\Omega_1(W) = W_0$, $C_G(W_0) \geq N$, $|G : C_G(W_0)| = 2$, and $G/N \cong C_4$ or D_8 .*
- (iv) *N is either abelian of type $(2^k, 2^{k+1})$ or $(2^k, 2^k)$, $k \geq 2$, or N is minimal non-abelian and more precisely $N = \langle a, b \mid a^{2^m} = b^{2^n} = 1, a^b = a^{1+2^{m-1}} \rangle$, where either $m = n$ with $n \geq 3$ or $m = n + 1$ with $n \geq 2$.*

Proof. Suppose that our 2-group G satisfies all the assumptions of our theorem together with $A \leq \Phi(G)$. By Theorem 77.1, G has no normal elementary abelian subgroups of order 8. By the first three paragraphs of the proof of Theorem 77.1, we know that $W_0 = Z(\Phi(G)) = \Omega_1(A)$ is the unique normal four-subgroup of G ,

$|G : C_G(W_0)| = 2$, $Z(G)$ is of order 2, and $|G| \geq 2^6$. Set $W_0 = \langle z, u \rangle$, $T = C_G(W_0)$, where $\langle z \rangle = Z(G)$. For each $t \in A - W_0$, $C_T(t) = A$.

We apply now the results of §50, since G is neither abelian nor of maximal class. It follows that G possesses a normal metacyclic subgroup N such that $C_G(\Omega_2(N)) \leq N$, G/N is isomorphic to a subgroup of D_8 and $W = \Omega_2(N)$ is abelian of type (4, 2) or (4, 4). In any case, $W_0 = \Omega_1(W) = \Omega_1(N)$ is the unique normal four-subgroup of G and $W_0 \not\leq Z(G)$. If $A \leq N$, then $A \leq W = \Omega_2(N)$. Since $C_G(A) = A$, we have $A = W$ and then A is normal in G , a contradiction. Hence $A \not\leq N$ and so $A \cap N = W_0$. Since $A \leq \Phi(G)$, G/N is not elementary abelian. Hence G/N is isomorphic to C_4 or D_8 . If $T = C_G(W_0)$ does not contain N , then T covers G/N and G/N acts faithfully on W (since $C_G(W) \leq N$). In that case $C_G(W_0)/C_N(W_0)$ cannot contain elements of order 4 (since that group centralizes $W_0 = \Omega_1(W)$) and so G/N is elementary abelian, a contradiction. Hence $T = C_G(W_0) \geq N$.

Assume that $G/N \cong C_4$. If N is abelian of type $(2^j, 2)$, $j \geq 2$, then G/N acts faithfully on $\Omega_2(N) \cong C_4 \times C_2$. If $N > \Omega_2(N)$, then there is a characteristic cyclic subgroup $Z \cong C_4$ of N so that Z is normal in G . But then $|G : C_G(Z)| \leq 2$ and therefore A (being contained in $\Phi(G)$) centralizes Z , a contradiction. Thus $N = \Omega_2(N)$ is a normal abelian self-centralizing subgroup of type (4, 2) in G , a contradiction. We have proved that $\Omega_2(N) = W$ is abelian of type (4, 4). Suppose that Z^* is a G -invariant cyclic subgroup of order 4 contained in N . But then again A centralizes Z^* , a contradiction. Hence there is no such Z^* and so we may apply Proposition 50.4. It follows that N is either abelian of type $(2^n, 2^n)$ or $(2^{n+1}, 2^n)$ with $n \geq 2$ or N is minimal nonabelian and more precisely $N = \langle a, b \mid a^{2^m} = b^{2^n} = 1, a^b = a^{1+2^{m-1}} \rangle$, where either $m = n$ with $n \geq 3$ or $m = n + 1$ with $n \geq 2$.

Assume that $G/N \cong D_8$. The structure of N in that case is already determined by Theorem 50.1. The minimal case $N \cong C_4 \times C_2$ cannot occur because in that case N would be a self-centralizing normal abelian subgroup of type (4, 2) of G , a contradiction. \square

Finally, we consider the case where $A \not\leq \Phi(G)$.

Theorem 77.3. *Suppose that G is a 2-group that possesses a self-centralizing abelian subgroup A of type (4, 2). If $\Omega_1(A) \not\leq \Phi(G)$, then G possesses an involution t such that $C_G(t) = \langle t \rangle \times D$, where D is isomorphic to one of the following groups: C_4 , D_8 , Q_{2^n} , $n \geq 3$, or SD_{2^m} , $m \geq 4$. Such groups G have been classified in §48, §49, and §51.*

Proof. Suppose that $\Omega_1(A) \not\leq \Phi(G)$. There is a maximal subgroup M of G such that $A - M$ contains an involution t . It follows that $A_0 = A \cap M \cong C_4$ and $C_G(t) = \langle t \rangle \times D$, where $D = C_M(t) \geq A_0$. We have $C_D(A_0) = A_0$ and so (by a well-known result of M. Suzuki) either $D = A_0 \cong C_4$ or D is a 2-group of maximal class. In the second case D is isomorphic to D_8 , Q_{2^n} , $n \geq 3$ or SD_{2^m} , $m \geq 4$. \square

Theorem 77.4. Suppose that G is a 2-group that possesses a self-centralizing abelian subgroup A of type $(4, 2)$. If $W_0 = \Omega_1(A) \leq \Phi(G)$ but $A \not\leq \Phi(G)$, then for any $a \in A - W_0$, $C_G(a) = \langle a \rangle * M_0$, $|\langle a \rangle \cap M_0| = 2$, where $M_0 = W_0$ or M_0 is isomorphic to one of the following groups: D_{2^n} , $n \geq 3$ or SD_{2^m} , $m \geq 4$ and $G > C_G(a)$.

Proof. Suppose that M is a maximal subgroup of G which does not contain A . Then $A \cap M = W_0 = \Omega_1(A)$. Let $a \in A - W_0$ so that $G = M\langle a \rangle$ and $C_G(a) = \langle a \rangle C_M(a)$ with $C_{M_0}(W_0) = W_0$, where $M_0 = C_M(a)$. By a result of M. Suzuki, either $M_0 = W_0$ or M_0 is of maximal class. In the second case, M_0 is isomorphic to one of the following groups: D_{2^n} , $n \geq 3$, or SD_{2^m} , $m \geq 4$. If $G = C_G(a)$, then $\Phi(G) = \Phi(C_G(a)) = \Phi(M_0)$ is cyclic, contrary to our assumption. \square

Exercise. Describe the subgroup structure of the holomorph of the abelian group of type $(4, 2)$.

§78

Minimal nonmodular p -groups

The main results of this section are taken from [Jan10].

1^o . We know that a 2-group is modular if and only if it is D_8 -free (Theorem 44.13). Here we classify minimal nonmodular 2-groups G , i.e., nonmodular 2-groups all of whose proper subgroups are modular. Hence there is $N \triangleleft G$ such that $G/N \cong D_8$ -free but each proper subgroup of G is D_8 -free. We shall use freely all results on modular p -groups from §73 and Appendix 24. In this section a 2-group is said to be *Hamiltonian* if it is nonabelian and all its subgroups are normal. A Dedekindian 2-group is Hamiltonian if it is nonabelian. A metacyclic 2-group H is called *ordinary metacyclic* with respect to A if H possesses a cyclic normal subgroup A such that H/A is cyclic and H centralizes $A/\mathcal{U}_2(A)$, or what is the same, $H/\mathcal{U}_2(A)$ is abelian. In other words, a metacyclic 2-group is ordinary if and only if it is powerful (see §26). Below we use freely the following facts:

(*) If minimal nonmodular 2-group G is of maximal class and order $\geq 2^4$, then $G \cong Q_{24}$. Moreover, a nonabelian 2-group G with cyclic subgroup of index 2 is modular if and only if $G \in \{Q_8, M_{2^n}\}$. It follows that any two involutions of G are permutable so $\Omega_1(G)$ is elementary abelian.

(**) [Wil] Let G be a Q_8 -free modular 2-group. Then $d(\Omega_1(G)) = d(G)$. If, in addition, $d(G) = 2$, then G is ordinary metacyclic.

(***) Let N be a normal subgroup of a 2-group G such that $G/N \cong D_8$. If L/N is the unique cyclic subgroup of index 2 in G/N and $x \in G - L$, then $x^2 \in N$. Indeed, all elements of $(G/N) - (L/N)$ are involutions.

Until the end of this subsection, G is a minimal nonmodular 2-group. In that case, G contains two non-permutable cyclic subgroups A and B . Since the subgroup $\langle A, B \rangle$ is nonmodular, we get $G = \langle A, B \rangle$ so $d(G) = 2$. By hypothesis, G has a normal subgroup N such that $G/N \cong D_8$. It follows from $d(G) = 2 = d(G/N)$ that $N \leq \Phi(G)$. The following proposition clears up the structure of N .

Remark 1. Suppose that G is a modular 2-group of order 16 containing a subgroup $H \cong E_8$. Then, G is Q_8 -free in view of the existence of H . Since G has no subgroups $\cong D_8$, it is either abelian or minimal nonabelian. Assume that G is nonabelian. Then $G = \langle a, b \mid a^4 = b^2 = c^2 = 1, c = [a, b], [a, c] = [b, c] = 1 \rangle$ and $G/\langle a^2 \rangle \cong D_8$, a contradiction. Thus, G is abelian.

Proposition 78.1. *We have $d(N) \leq 2$, so N is metacyclic (Theorem 44.13).*

Proof. Suppose that $d(N) \geq 3$. Then N possesses a G -invariant subgroup R such that $N/R \cong E_8$. The quotient group G/R is also minimal nonmodular. We want to obtain a contradiction. To this end, we may assume that $R = \{1\}$; then $N \cong E_8$. Let S/N be any subgroup of order 2 in G/N . Then S (being modular) is abelian, by Remark 1, so S centralizes N . On the other hand, $G/N \cong D_8$ is generated by its subgroups of order 2, and so $N \leq Z(G)$.

Assume that $Z(G) > N$; then $Z(G)/N = Z(G/N) = \Phi(G/N)$ so $Z(G) = \Phi(G)$. In that case, G is minimal nonabelian. Then $\Omega_1(G) = N$ and $|G'| = 2$ (Lemma 65.1) so $G' < N$, a contradiction since $G/N \cong D_8$ is nonabelian. Thus, $N = Z(G)$.

Let L/N be the unique cyclic subgroup of index 2 in G/N . Then L is abelian since $N = Z(G)$. If $L = N \times L_1$ with $L_1 \cong C_4$, then $\mathfrak{U}_1(L) = \mathfrak{U}_1(L_1)$ is of order 2 and so $\mathfrak{U}_1(L) \leq Z(G)$, a contradiction since $\mathfrak{U}_1(L) \not\leq N = Z(G)$. Hence L does not split over N and so $L = NC$, where $C \cong C_8$ and $C \cap N = C_0$ is of order 2. We have $\Phi(L) = \Phi(C) = C_1 \cong C_4$, where $C_0 < C_1$, and $\Phi(G) = C_1N$ is abelian of type $(4, 2, 2)$. For each $x \in G - L$, $x^2 \in N$, by (**), and so there is $b \in G - L$ with $b^2 \in N - C_0$ (otherwise, $\Phi(G) = \mathfrak{U}_1(G) = C_1$). Since $C_G(C_1) = L$, $\text{Aut}(C_1) \cong C_2$ and C_1 is normal in G , it follows that b inverts C_1 . In that case, $D = \langle C_1, b \rangle$ is (nonabelian) metacyclic of order 2^4 and exponent 2^2 so $D/\langle b^2 \rangle \cong D_8$, a contradiction. \square

Proposition 78.1 is a variant of Theorem 44.13. It follows from Theorem 44.13 that the subgroup N of Proposition 78.1 is metacyclic.

Remark 2. Let, as in the following four propositions, the subgroup N be cyclic. We claim that then $\mathfrak{U}_2(G) = \Phi(N)$. One may assume that $N > \{1\}$. In view of $\mathfrak{U}_2(G) \geq \mathfrak{U}_2(N)$, it suffices to show that $\exp(G/\mathfrak{U}_2(N)) = 8$. Without loss of generality, one may assume that $\mathfrak{U}_2(N) = \{1\}$, i.e., N is cyclic of order 4. Then $\Phi(G)$ is abelian of order 8. One may assume that $\Phi(G)$ is abelian of type $(4, 2)$ (otherwise, G has a cyclic subgroup of index 2, contrary to (*)). Since $\Phi(G) = \mathfrak{U}_1(G)$ is not generated by involutions, there exists $x \in G$ such that $o(x^2) = 4$; then $o(x) = 8$, and we are done. It follows from the obtained result and Lemma 64.1(m) that G is metacyclic if and only if $G/\Phi(N)$ is metacyclic.

Proposition 78.2. *Suppose that N is cyclic and some proper subgroup of G is not Q_8 -free. Then G is isomorphic to Q_{24} or to the uniquely determined group X of order 2^5 with $\Omega_2(X) \cong Q_8 \times C_2$ given in §52.*

Proof. Suppose that N is cyclic and G has a maximal subgroup M which is not Q_8 -free. Since M is modular, it follows that M is Hamiltonian (§73 or Appendix 24), i.e., $M = Q \times E$ with $Q \cong Q_8$ and $\exp(E) \leq 2$. In particular, $\exp(M) = 4$ and $\mathfrak{U}_1(M) = \Phi(M) = \mathfrak{U}_1(Q)$. We have $N < M$ since $N \leq \Phi(G)$ so $|N| \leq 4$; in that case, $|G| = |G/N||N| \leq 8 \cdot 4 = 32$. If $|G'| = 2$, it follows from $d(G) = 2$ that G

is minimal nonabelian (Lemma 65.2(a)), a contradiction since $M < G$ is nonabelian. Hence $|G'| \geq 4$ so G has at most one abelian maximal subgroup (Lemma 65.2(c)).

(i) Suppose that $|N| = 4$; then $|G| = 32$ and $|\Phi(G)| = 8$. Let $L/N \cong C_4$ be the unique cyclic subgroup of index 2 in G/N ($\cong D_8$). By (*), G is not of maximal class. In that case, the metacyclic subgroup L is noncyclic (Lemma 64.1(t)) so $|\mathfrak{U}_1(L)| = \frac{1}{4}|L| = 4$ and therefore L is not Hamiltonian. Suppose that L is abelian. We have $\mathfrak{U}_1(L) > \mathfrak{U}_1(N) = \mathfrak{U}_1(M)$. Let K be the maximal subgroup of G distinct from M and L . We know that K must be nonabelian and, since $G/N \cong D_8$, we get $K/N \cong E_4$. By (*), K is not of maximal class. Since $N \cong C_4$ does not lie in $Z(M)$, we have $C_G(N) = L$. Then $|K : C_K(N)| = 2$ so $K \not\cong M_{16}$ (otherwise, $N = \Phi(K) = Z(K)$), and we conclude (Theorem 1.2) that $\exp(K) = 4$. Take $k \in K - C_K(N)$; then $k^2 \in N$, in view of $K/N \cong E_4$, and therefore $\langle N, k \rangle \cong Q_8$. It follows that K is Hamiltonian (§73 or Appendix 24) and so $\mathfrak{U}_1(K) = \mathfrak{U}_1(N) < \mathfrak{U}_1(L)$. Hence $\Phi(G) = \mathfrak{U}_1(G) = \mathfrak{U}_1(L)$ is of order 4, a contradiction since $|\Phi(G)| = 8$.

We have proved that L is nonabelian. In particular, $N = \langle n \rangle \not\leq Z(L)$ since L/N is cyclic, and if we set $L = \langle N, l \rangle$, then $n^l = n^{-1}$ and $l^4 \in \langle n^2 \rangle$. If $o(l) = 4$, then $L/\langle l^2 \rangle \cong D_8$, a contradiction. Hence $o(l) = 8$ and so $L \cong M_{16}$ with $\langle l^4 \rangle = \langle n^2 \rangle = L'$ and $\Phi(L) = Z(L) = \langle l^2 \rangle \cong C_4$. Note that $\Omega_2(L) = N\Phi(L)$ is abelian of type (4, 2). Set $K = C_G(N)$ so that K is the maximal subgroup of G distinct from M and L and (noting that $\langle l^2 \rangle > \langle n^2 \rangle$) we get (see also Exercise 1.133) $\Phi(G) = \Phi(M)\Phi(L)\Phi(K) = \langle n^2 \rangle \langle l^2 \rangle \Phi(K) = \langle l^2 \rangle \Phi(K)$. Since $K/N \cong E_4$, we have $\Phi(K) \leq N$. But $\Phi(G) > N$ and so we must have $\Phi(K) = N$ (otherwise, $\Phi(G) = \langle l^2 \rangle$ is of order 4). It follows that the modular subgroup K has a cyclic subgroup of index 2 and K is Q_8 -free since K cannot be Hamiltonian (because $|K| = 16$ and $|\mathfrak{U}_1(K)| = 4$; see §73 and Appendix 24). Hence K is either abelian of type (8, 2) or $K \cong M_{16}$. In any case, $\Omega_2(K) = \Phi(L)N = \Phi(G)$ is abelian of type (4, 2). It follows that $\Omega_2(G) = M \cong Q_8 \times C_2$ and consequently G is the uniquely determined group of order 2^5 described in §52.

(ii) Now let $|N| = 2$. In that case, $|G| = 16$ and $|G'| = 4$ so $|G : G'| = 4$. By Taussky's theorem, G is of maximal class so, by (*), $G \cong Q_{16}$. \square

It is easy to check that the group G of Proposition 78.2 of order 2^5 is the group \mathcal{F} from Appendix 24. Indeed, take $u \in G - M$ and put $U = \langle u \rangle$; then $|U| = 8$ since $M = \Omega_2(G)$. Assume that $UQ = QU$. Then UQ is of maximal class (Theorem 1.2), contrary to (*). It follows that $U \cap Q$ is normal in G and $G/(U \cap Q) \cong D_8$. By Appendix 24, $G \cong \mathcal{F}$.

Proposition 78.3. *Suppose that $N > \{1\}$ is cyclic and all proper subgroups of G are Q_8 -free. Then $\Omega_2(G) = \Phi(N)$ and $G/\Phi(N)$ is minimal nonabelian of order 2^4 and exponent 4. Thus $G/\Phi(N)$ is isomorphic to one of the following groups:*

- (a) $\langle x, y \mid x^4 = y^2 = 1, [x, y] = z, z^2 = [x, z] = [y, z] = 1 \rangle$ is nonmetacyclic,
- (b) $\langle x, y \mid x^4 = y^4 = 1, x^y = x^{-1} \rangle$ is metacyclic.

Proof. By Remark 2, $\mathfrak{U}_2(G) = \Phi(N)$ so $G/\mathfrak{U}_2(G)$ is 2-generator nonabelian of exponent 4 and order 2^4 . Therefore, by hypothesis, $G/\mathfrak{U}_2(G)$ is minimal nonabelian. By Lemma 65.1 that $G/\mathfrak{U}_2(G) = G/\Phi(N)$ is isomorphic to the group (a) or (b). \square

In the next two propositions we determine the groups G of Proposition 78.3.

Proposition 78.4. *Suppose that $N > \{1\}$ is cyclic and all proper subgroups of G are Q_8 -free. If $G/\Phi(N)$ is as in Proposition 78.3(a), then G has a normal elementary abelian subgroup $E = \langle n, z, t \rangle$ of order 8 such that G/E is cyclic. We set $G = \langle E, x \rangle$, where $o(x) = 2^{s+1}$, $s \geq 1$, $E \cap \langle x \rangle = \langle n \rangle$, $[t, x] = z$, $[z, x] = n^\epsilon$, $\epsilon = 0, 1$, and $G = \langle x, t \rangle$. We have $G/\langle x^2 \rangle \cong D_8$, $\Phi(G) = \langle x^2 \rangle \times \langle z \rangle$, $\Omega_1(G) = E$, and G is Q_8 -free. If $\epsilon = 0$, then G is minimal nonabelian nonmetacyclic. If $\epsilon = 1$, then $s \geq 2$, $G' = \langle z, n \rangle \cong E_4$ and $Z(G) = \langle x^4 \rangle$.*

Proof. Let $M/\Phi(N) = \Omega_1(G/\Phi(N))(\cong E_8)$; then N is a maximal cyclic subgroup of M . Set $|N| = 2^s$, $s \geq 1$. Let S/N be any subgroup of order 2 in M/N . Since M is D_8 -free and Q_8 -free, S cannot be of maximal class. It follows that S is either abelian of type $(2^s, 2)$ or $S \cong M_{2^{s+1}}$ ($s > 2$). In any case, there exists an involution in $S - N$. Hence $\Omega_1(M)$ covers $M/N \cong E_4$ and, since M is modular, $E = \Omega_1(M)$ is elementary abelian of order 8, by the product formula. It follows that E is normal in G and $E \cap N = \Omega_1(N) = \langle n \rangle \leq Z(G)$. In particular, $\Phi(G) = N\Omega_1(\Phi(G))$ is abelian of type $(2^s, 2)$, $s \geq 1$ since $\Omega_1(\Phi(G)) \cong E_4$ centralizes $\Phi(G)$. Take an involution $t \in E - \Phi(G)$.

Let $K \neq M$ be a maximal subgroup of G such that $K/N \cong E_4$; then $K \cap M = \Phi(G)$ since $d(G) = 2$. Suppose that N is a maximal cyclic subgroup of K . Then, by the argument of the previous paragraph, $\Omega_1(K)$ covers K/N and so there is an involution $r \in K - M$ since $E_8 \cong \Omega_1(K) \neq \Omega_1(M) (= E)$; then $r \notin E$. Since G has no elementary abelian subgroups of order 2^4 , there is in E an involution u such that $ru \neq ur$. Then $\langle r, u \rangle$ is dihedral, a contradiction. We have proved that there is an element $x \in K - M$ such that $\langle x^2 \rangle = N$ and so $o(x) = 2^{s+1}$, $s \geq 1$. Since $\langle x, t \rangle = G$ (indeed, involutions xN and tN lie in different maximal subgroups of $G/N \cong D_8$) and $t \in E - \Phi(G)$, we get $G = E\langle x \rangle$ with $E \cap \langle x \rangle = \Omega_1(N) = \langle n \rangle \cong C_2$ and so G/E is cyclic of order 2^s and $|G| = 2^{s+3}$. In particular, $G' < E$ and so $|G'| \in \{2, 4\}$. Since $d(G) = 2$ and G is not minimal nonabelian, we get $|G'| = 4$ (Lemma 65.2(a)).

We have $[x, t] \neq 1$ since $\langle x, t \rangle = G$ is nonabelian, so $z = [x, t]$ is an involution in $(E \cap \Phi(G)) - \langle n \rangle$ since $\langle x \rangle$ is not normal in G . Indeed, if $\langle x \rangle$ were normal in G , then $G/\Phi(N) = \langle t\Phi(N) \rangle \cdot \langle x \rangle / \Phi(N)$ is metacyclic, which is not the case. It follows that $E = \langle n, z, t \rangle$, where $z \in \Phi(G)$, and $\langle x \rangle$ is not normal in G . Thus $N_G(\langle x \rangle)$ is a maximal subgroup of G and so $z \in \Phi(G) \leq N_G(\langle x \rangle)$ and therefore z normalizes $\langle x \rangle$. Since $\langle x, z \rangle$ cannot be of maximal class, by (*), we have either $[x, z] = 1$ or $[x, z] = n$ (in which case $\langle x, z \rangle \cong M_{2^{s+1}}$, $s > 1$). Let us consider the first possibility. We have $C_G(z) \geq \langle E, x \rangle = G$ so $z \in Z(G) \cap G'$. Then $G/\langle z \rangle$ has a cyclic subgroup $\langle x, z \rangle / \langle z \rangle$ of index 2. It follows that then $G/\langle z \rangle$ is neither abelian nor isomorphic to

$M_{2^{s+1}}$ (otherwise, $G/\langle z \rangle$ has two distinct cyclic subgroups of index 2 so G has two distinct abelian maximal subgroups, and we get $|G'| < 4$, a contradiction). It follows (Lemma 64.1(t)) that $G/\langle z \rangle$ is of maximal class so it is isomorphic to Q_{16} , by (*), contrary to the existence of E . Now let $\langle x, z \rangle \cong M_{2^{s+1}}$, $s > 1$. Then $\langle x \rangle$ induces an automorphism of order 4 on E .

Let u be an involution in $G - E$. Then, by Remark 1, $F = E\langle u \rangle \cong E_8$. But G/E is cyclic and so $F/E = (E\langle x^{2^{s-1}} \rangle)/E$ and so $x^{2^{s-1}}$ is an element of order 4 contained in $F - E$, a contradiction. We have proved that $\Omega_1(G) = E$. \square

Proposition 78.5. Suppose that $N > \{1\}$ is cyclic and all proper subgroups of G are Q_8 -free. If $G/\Phi(N)$ is metacyclic, then G is also metacyclic and we have one of the following possibilities:

- (i) $G = \langle x, y \mid x^4 = y^{2^{s+1}} = 1, s \geq 1, x^y = x^{-1} \rangle$, where G is minimal non-abelian and $N = \langle y^2 \rangle$.
- (ii) $G = \langle x, a \mid x^{2^{s+1}} = a^8 = 1, s \geq 2, x^{2^s} = a^4, a^x = a^{-1} \rangle$, where G is an A_2 -group with $N = \langle x^2 \rangle$, $Z(G) = N$ (see §65), $G' = \langle a^2 \rangle \cong C_4$ and G is of class 3.

In both cases (i) and (ii), G is a minimal non- Q_8 -free 2-group.

Proof. By Remark 2, $\Phi(N) = \mathfrak{U}_2(G)$ and G is also metacyclic. Set $|N| = 2^s$, $s \geq 1$. If $s = 1$, then G is isomorphic to the group (b) of Proposition 78.3 and we are done. Now we assume that $s \geq 2$.

Let S/N be a subgroup of order 2 in G/N . By (*), S is not of maximal class so S is either cyclic of order 2^{s+1} or S is abelian of type $(2^s, 2)$ or $s > 2$ and $S \cong M_{2^{s+1}}$. If $\Phi(G)$ is cyclic, then G has a cyclic subgroup of index 2, contrary to (*). Also, $M_{2^{s+1}}, s > 2$, having cyclic center, cannot be the Frattini subgroup (Burnside). Taking $S = \Phi(G)$, we see that $\Phi(G)$ is abelian of type $(2^s, 2)$, $s \geq 2$.

Let $\Omega_1(N) = \langle n \rangle$ so that $\langle n \rangle \leq \Phi(N) \cap Z(G)$. For any subgroup S/N of order 2 in G/N , by the previous paragraph, $S/\langle n \rangle$ is abelian so centralizes $N/\langle n \rangle$. Since G/N is generated by its subgroups of order 2, we get $N/\langle n \rangle \leq Z(G/\langle n \rangle)$.

Suppose for a moment that G is minimal nonabelian. Since $\Phi(G)$ is abelian of type $(2^s, 2)$, we get at once (Lemma 65.1): $G = \langle x, y \mid x^4 = y^{2^{s+1}} = 1, s \geq 1, x^y = x^{-1} \rangle$, where $N = \langle y^2 \rangle$; this is a group of part (i). In what follows we assume that G is not minimal nonabelian. In particular, $|G'| \geq 4$ (Lemma 65.2(a)).

We will determine the structure of all three maximal subgroups of G . Let M be a maximal subgroup of G such that $M/N \cong E_8$. If N is a maximal cyclic subgroup of M , then for each subgroup S/N of order 2 of M/N , there is an involution in $S - N$. Hence $\Omega_1(M)$ covers M/N and, since M is D_8 -free and Q_8 -free, $\Omega_1(M)$ is elementary abelian and $\Omega_1(M) \cap N = \langle n \rangle$ so that $\Omega_1(M) \cong E_8$, by the product formula. This is a contradiction since G is metacyclic. It follows that N is not a maximal cyclic subgroup of M . Let M_0 be a maximal cyclic subgroup of M containing N so that $M_0 \cong C_{2^{s+1}}$ is of index 2 in M . By (*), M is not of maximal class and

so M is either abelian of type $(2^{s+1}, 2)$ or $M \cong M_{2^{s+2}}$, $s \geq 2$ (Lemma 64.1(t)). In any case, $N \leq Z(M)$ and $M/\langle n \rangle$ is abelian since $M' \leq \langle n \rangle$. Let K ($\neq M$) be another maximal subgroup of G with $K/N \cong E_4$. Then K is either abelian of type $(2^{s+1}, 2)$ or $K \cong M_{2^{s+2}}$, $s \geq 2$, and again $N \leq Z(K)$ and $K/\langle n \rangle$ is abelian. We get $C_G(N) \geq MK = G$ so $N \leq Z(G)$. Since G is not minimal nonabelian, we get $\Phi(G) \neq Z(G)$. We have proved that $N = Z(G)$.

Let L/N be the unique cyclic subgroup of index 2 in G . Then L is abelian and using Lemma 64.1(q), we get $|G'| = 4$. By Lemma 64.1(u), L is the unique abelian maximal subgroup of G and so $M \cong K \cong M_{2^{s+2}}$ with $M' = K' = \langle n \rangle$. In particular, G is an \mathcal{A}_2 -group (since $|G'| = 4$, this also follows from Corollary 65.3).

We have $G' > \langle n \rangle$ and, since $G' \not\leq N = Z(G)$ and $|\Phi(G)/N| = 2$, we get $\Phi(G) = NG'$, $N \cap G' = \langle n \rangle = \Omega_1(N)$ and $\text{cl}(G) = 3$.

Since G is metacyclic, there exists a cyclic normal subgroup Z of order 8 such that $Z > G'$. But $N \cap Z = N \cap G' = \langle n \rangle$ and so $NZ = L$ which determines the structure of the maximal subgroup L and shows that L does not split over N . It follows that L is abelian of type $(2^s, 2)$.

Set $Z = \langle a \rangle$. By (***)¹, we get $\langle x^2 \rangle = N$ for each $x \in G - L$. Hence $G = Z\langle x \rangle$ with $Z \cap \langle x \rangle = \langle n \rangle$ for a fixed $x \in G - L$ (since $\Omega_1(G) = \Omega_1(L)$, x is not an involution). In view of $|G'| = 4$ and $G' < Z$, we get either $a^x = a^{-1}$ or $a^x = a^{-1}n$, where $n = a^4$. However, if $a^x = a^{-1}n$, then we replace $Z = \langle a \rangle$ with $Z^* = \langle au \rangle$, where $u \in N$ is such that $u^2 = n$. Then we have $(au)^x = a^{-1}nu = a^{-1}u^{-1} = (au)^{-1}$. Since $\langle (au)^2 \rangle = \langle a^2 \rangle = G'$, we may assume from the start that $a^x = a^{-1}$ and so the structure of G is completely determined. \square

Remark 3. Let G be a 2-group and let N be a G -invariant metacyclic subgroup of $\Phi(G)$. We claim that N is ordinary metacyclic. One may assume that N is nonabelian; then N has no cyclic subgroups of index 2 since $Z(N)$ must be noncyclic. There exists a maximal cyclic subgroup A of N such that $N' < A$ and N/A is cyclic. We have to prove that $N/\mathfrak{U}_2(A)$ is abelian. This is the case if $|A : N'| > 2$. Now we assume that $|A : N'| = 2$ and obtain a contradiction. Under our assumption, N/N' is abelian with cyclic subgroup of index 2 (indeed, by the choice of A and Frobenius–Stickelberger theorem on abelian groups, A/N is a direct factor of N/N'). In particular, N has no epimorphic images which is abelian of type $(4, 4)$. Now consider the quotient group $\bar{N} = N/\mathfrak{U}_2(N)$. Since N has no cyclic subgroups of index 2, we get $|\bar{N}| = 16$. By assumption, \bar{N} is nonabelian so $\bar{N} = \langle x, y \mid x^4 = y^4 = 1, x^y = x^{-1} \rangle$. In that case, $\bar{N}/\langle y^2 \rangle \cong D_8$ has a cyclic center, a contradiction since $N/\mathfrak{U}_2(N) \leq \Phi(G/\mathfrak{U}_2(N))$.

In the rest of this subsection we consider the case $d(N) = 2$.

Proposition 78.6. *Suppose that $d(N) = 2$. Then $G/\Phi(N)$ is the minimal nonabelian nonmetacyclic group of order 2^5 and exponent 4. In particular, $G/\Phi(N)$ has the unique epimorphic image isomorphic to Q_8 . Each maximal subgroup of G is Q_8 -free and N is ordinary metacyclic.*

Proof. We want to determine the structure of $G/\Phi(N)$. Since $G/\Phi(N)$ is also minimal nonmodular, we may assume for a moment that $\Phi(N) = \{1\}$ so that $N \cong E_4$ and $|G| = 2^5$. Let S/N be any subgroup of order 2 in G/N . Since $S \not\cong D_8$, S is abelian and so $N \leq Z(G)$ since such subgroups S generate G .

Suppose that $Z(G) = N$. Let L/N be the unique cyclic subgroup of index 2 in G/N ; then L is abelian. If $L = N \times R$ with $R \cong C_4$, then $\Omega_1(L) = \Omega_1(R) \not\leq N$ and $\Omega_1(L) \leq Z(G)$, contrary to our assumption. Hence $L = NL_1$ with $L_1 \cong C_8$ and $L_0 = L_1 \cap N \cong C_2$; thus, L is abelian of type (8, 2). We have $\Phi(L) = \Phi(L_1) \cong C_4$, where $\Phi(L) > L_0$. For each $x \in G - L$, $x^2 \in N$, by (**), and $\Phi(G) = \Omega_1(G) = \Phi(L)N$. This implies that there exists $b \in G - L$ such that $b^2 \in N - L_0$. Assume that this is false. Then all elements in $(G/L_0) - (L/L_0)$ are involutions so G/L_0 is generated by involutions and, since G/L_0 is not dihedral, it is not generated by two involutions. Since G/L_0 is minimal nonmodular, all its involutions commute so G/L_0 is elementary abelian; then $d(G) \geq 4$, a contradiction. Since $\Phi(L) \not\leq Z(G)$, we get $C_G(\Phi(L)) = L$ so b inverts $\Phi(L)$. But then $D = \langle \Phi(L), b \rangle$ is nonabelian metacyclic of order 2^4 and exponent 4; in that case, $D/\langle b^2 \rangle \cong D_8$, a contradiction.

We have proved that $Z(G) > N$ and so $Z(G) = \Phi(G)$. It follows that each maximal subgroup of G is abelian and so G is minimal nonabelian. In particular, $|G'| = 2$ and since G' covers $Z(G)/N = (G/N)'$, we have $Z(G) = N \times G'$ is elementary abelian of order 8. It follows that G is the uniquely determined minimal nonabelian nonmetacyclic group of order 2^5 and exponent 4: $G = \langle a, b \mid a^4 = b^4 = 1, [a, b] = c, c^2 = [a, c] = [b, c] = 1 \rangle$, where $Z(G) = \langle a^2, b^2, c \rangle$, $G' = \langle c \rangle$, and $G/\langle a^2c, b^2c \rangle$ is the unique quotient group of G which is isomorphic to Q_8 . In particular, G is not Q_8 -free.

We return now to the remaining case $\Phi(N) > \{1\}$. Assume that N is not Q_8 -free. Then N (being modular) is Hamiltonian (see §73 and Appendix 24). But $d(N) = 2$ and so $N \cong Q_8$. This is a contradiction since $Z(N)$ is cyclic and $N < \Phi(G)$ (Burnside). We have proved that N is Q_8 -free and so $N/\Omega_2(N)$ must be abelian.

By Remark 3, N is ordinary metacyclic.

Suppose that a maximal subgroup M of G is not Q_8 -free. Then M (being modular) is Hamiltonian and so $M = Q \times E$, $Q \cong Q_8$, $\exp(E) \leq 2$. In particular, $\Phi(M)$ is of order 2 and $\exp(M) = 4$. In view of $N < \Phi(G) < M$, we get $\exp(N) = 4$ and N is abelian of type (4, 2) since N is metacyclic. In that case, $|G| = 2^6$. We get $\Phi(M) = \Omega_1(M) = \Omega_1(N) = \Phi(N)$ and so $M/\Phi(N)$ is an elementary abelian subgroup of order 16 in the minimal nonabelian group $G/\Phi(N)$, contrary to Lemma 65.1. Thus, all maximal subgroups of G are Q_8 -free. \square

Proposition 78.7. Suppose that $d(N) = 2$. Then for each maximal subgroup M of G we have $d(M) = 3$. Also, $\Phi(N) = \Omega_2(G)$, $E = \Omega_1(G) = \Omega_1(\Phi(G)) \cong E_8$, $E \leq Z(\Phi(G))$, and either $G/E \cong Q_8$ with $\Omega_2(G) = \Phi(G)$ being abelian of type (4, 2, 2) or G/E is noncyclic and ordinary metacyclic.

Proof. By (*), $\Omega_1(G)$ is elementary abelian.

Set $F = \Phi(G)$ so we have $F/\Phi(N) = \Phi(G/\Phi(N)) = \Omega_1(G/\Phi(N)) \cong E_8$ (Proposition 78.6). Since $\Phi(N) \leq \Phi(F)$, we get $\Phi(N) = \Phi(F)$. Thus $d(F) = 3$ and F is D_8 -free and, by Proposition 78.6, Q_8 -free, $E = \Omega_1(F) \cong E_8$ (by (**)) is normal in G . Let M be any maximal subgroup of G so that $M/\Phi(N)$ is abelian of type $(4, 2, 2)$, $\Phi(N) \leq \Phi(M)$ and so $d(M) = 3$. But M is also D_8 -free and Q_8 -free and therefore, by (***) $\Omega_1(M) \cong E_8$ which implies $\Omega_1(M) = \Omega_1(F) = \Omega_1(G)$ since $\Omega_1(G) \leq \Omega_1(M)$ in view of $\Omega_1(G/N) = \Omega_1(M/N)$ (Lemma 65.3).

We have $\Phi(N) \geq \mathcal{U}_2(G)$ (Proposition 78.6). On the other hand, $\exp(G/\mathcal{U}_2(G)) = 4$ and so each maximal subgroup of $G/\mathcal{U}_2(G)$, being modular and Q_8 -free, is abelian. Thus $G/\mathcal{U}_2(G)$ is minimal nonabelian of exponent 4 and so $|G/\mathcal{U}_2(G)| \leq 2^5$. It follows $\mathcal{U}_2(G) = \Phi(N)$.

If G/E is not D_8 -free, then there is a normal subgroup N^* of G such that $E \leq N^*$ and $G/N^* \cong D_8$. By Proposition 78.1, N^* must be metacyclic, a contradiction. Hence G/E is D_8 -free so it is modular.

Suppose that G/E is not Q_8 -free. Then G/E is Hamiltonian (§73 or Appendix 24; by the previous paragraph, G/E is modular). Since $d(G/E) = 2$, we get $G/E \cong Q_8$ so $\Omega_2(G) = \Phi(G)$ since $E = \Omega_1(G)$. On the other hand, G/E cannot act faithfully on E since $\text{Aut}(E)$ has no subgroups $\cong Q_8$, and so $C_G(E) \geq \Phi(G)$. In particular, $\Phi(G)$ is abelian of type $(4, 2, 2)$.

We assume that G/E is Q_8 -free. In that case, by (**), G/E is ordinary metacyclic but noncyclic since $\Phi(G) \geq E$. There is a cyclic normal subgroup S/E of G/E with the cyclic factor-group G/S . Let $s \in S$ be such that $S = \langle E, s \rangle$ and let $r \in G - S$ be such that $G = \langle S, r \rangle$. Since $E \leq \Phi(G)$, we have $G = \langle r, s \rangle$.

Since $S = \langle E, s \rangle$ is a proper subgroup of G , it follows that S is D_8 -free and, by Proposition 78.6, Q_8 -free. Since $S/\langle s \rangle_S$ is a subgroup of the symmetric group $S_{|S|/\langle s \rangle} = S_4$, whose Sylow 2-subgroup is isomorphic to D_8 , that quotient group is abelian and contains a subgroup isomorphic $S/\langle S\langle s \rangle \cong E_4$ so $\langle s \rangle$ is normal in S and s induces an automorphism of order ≤ 2 on E which implies that s^2 centralizes E .

Since $\langle E, r \rangle < G$, we get (as in the previous paragraph) that r^2 centralizes E . On the other hand, $\Phi(G) = \langle E, r^2, s^2 \rangle$ and so we get again $E \leq Z(\Phi(G))$. \square

We summarize our results in a somewhat different form.

Theorem 78.8 (Janko). *Let G be a minimal nonmodular 2-group of order $> 2^5$. Then each proper subgroup of G is Q_8 -free and $G/\mathcal{U}_2(G)$ is minimal nonabelian of order 2^4 or 2^5 .*

(a) Suppose that $|G/\mathcal{U}_2(G)| = 2^4$. If N is any normal subgroup of G such that $G/N \cong D_8$, then N is cyclic. If $G/\mathcal{U}_2(G)$ is nonmetacyclic, then G is Q_8 -free and $\Omega_1(G) \cong E_8$ with $G/\Omega_1(G)$ cyclic. If $G/\mathcal{U}_2(G)$ is metacyclic, then G is also metacyclic and G is either minimal nonabelian or an A_2 -group.

(b) Suppose that $|G/\mathcal{U}_2(G)| = 2^5$. Then $G/\mathcal{U}_2(G)$ is nonmetacyclic, G is not Q_8 -free and $\Omega_1(G) \cong E_8$ with $G/\Omega_1(G) \cong Q_8$ or $G/\Omega_1(G)$ is ordinary meta-

cyclic (but not cyclic). Moreover, if N is any normal subgroup of G such that $G/N \cong D_8$, then N is ordinary metacyclic but noncyclic.

Remark 4. Let us change the last paragraph of the proof of Proposition 78.1 by the following argument. Let A be a minimal nonabelian subgroup of G . Let $|A| > 8$. If $Z(A)$ is cyclic, setting $N = (N \cap A) \times N_1$, we get $G = A \times N_1$, $d(G) = 4$, a contradiction. Let $Z(A) \cong E_4$. Then A is metacyclic without cyclic subgroup of index 2. Since A is D_8 -free, $|A| = 2^5$ and $G = A \times N_1$, where $N < N_1$ is of order 2. In that case, G is modular, a contradiction. If $Z(A) \cong E_8$, then A is D_8 -free so $A = G$. In that case, $G' < N$, which is a contradiction. Now let $|A| = 8$; then $A \cong Q_8$. By Lemma 1.1, $|G'| = 4$. If L is as in the last paragraph of the proof of Proposition 78.1, then $G' < L$ and $G' \not\leq N = \Omega_1(L)$ so $G' \cong C_4$. Then $A' = \Omega_1(G')$ and $AN/A' \cong E_{16}$, a contradiction since G/A' is minimal nonabelian in view of $(G/A)' = G'/A' \cong C_2$ (Lemma 65.2(a)) so must be $|\Omega_1(G/A')| \leq 8$ (Lemma 65.1).

2^o . We recall that a p -group G is modular if and only if any subgroups X and Y of G are permutable, i.e., $XY = YX$. We turn now to the case $p > 2$.

Proposition 78.9. *Let G be a modular p -group with $p > 2$ and $d(G) = 2$. Then G is metacyclic.*

Proposition 78.10. *Let G be a minimal nonmodular p -group, $p > 2$, which is generated by two subgroups A and B of order p . Then $G \cong S(p^3)$ (the nonabelian group of order p^3 and exponent p).*

Proof. Since G is a p -group, $G_1 = \langle A^G \rangle$ and $G_2 = \langle B^G \rangle$ are proper normal subgroups of G and so G_1 and G_2 are modular. It follows that G_1 and G_2 are elementary abelian. But $\langle G_1, B \rangle = \langle A, B \rangle = \langle G_2, A \rangle = G$, and so G_1 and G_2 are two distinct maximal subgroups of G . By Lemma 64.1(u), we have $|G'| = p$ and $G' \leq G_1 \cap G_2$. Thus G/G' is abelian and G/G' is generated by elementary abelian subgroups G_1/G' and G_2/G' . Hence G/G' is elementary abelian and $d(G) = 2$ implies that $G/G' \cong E_{p^2}$. Thus, $G \cong S(p^3)$ since the metacyclic nonabelian group of order p^3 is modular. \square

Proposition 78.11 (see Theorem 44.13). *Let G be a minimal nonmodular p -group. Then G possesses a normal subgroup N such that $d(N) \leq 2$, $N \leq \Omega_1(G)$, and G/N is a nonmodular group of order p^3 . If $p = 2$, then $G/N \cong D_8$ and if $p > 2$, then $G/N \cong S(p^3)$, $N = \Omega_1(G)$, and N is metacyclic. The subgroup N is metacyclic. In particular, if $p > 2$, then G is nonmetacyclic.*

Proof. There are non-permutable cyclic subgroups $\langle a \rangle$ and $\langle b \rangle$. It follows $G = \langle a, b \rangle$ and so $d(G) = 2$. Since $\langle a^p, b^p \rangle \leq \Phi(G)$, the subgroups $E = \langle a^p, b \rangle$ and $F = \langle a, b^p \rangle$ are proper subgroups of G . Hence E and F are modular and so $E = \langle a^p \rangle \langle b \rangle$, $F = \langle a \rangle \langle b^p \rangle$, and $G = \langle E, F \rangle$. Set $N = \langle a^p \rangle \langle b^p \rangle$ so that $|E : N| = |F : N| = p$. It follows that N is normal in G , $N \leq \Omega_1(G)$, and $d(N) \leq 2$. It remains to determine

the structure of $\bar{G} = G/N = \langle \bar{a}, \bar{b} \rangle$, where \bar{G} is a minimal nonmodular p -group generated by elements \bar{a} and \bar{b} of order p . If $p = 2$, then \bar{G} is dihedral, and, by $(*)$, $\bar{G} \cong D_8$. If $p > 2$, then Proposition 78.10 implies that $\bar{G} \cong S(p^3)$. In that case we have $N = \mathfrak{V}_1(G)$ and Proposition 78.9 implies that N is metacyclic. \square

Proposition 78.12. *Let G be a minimal nonmodular p -group, $p > 2$, with $|G| > p^4$. Then $\Omega_1(G)$ is elementary abelian of order $\geq p^3$.*

Proof. Let A and B be subgroups of order p in G such that $AB \neq BA$. Then $G = \langle A, B \rangle$ and so Proposition 78.10 implies that $G \cong S(p^3)$, a contradiction. We have proved that $AB = BA$ and so $\langle A, B \rangle$ is abelian. Hence $\Omega_1(G)$ is elementary abelian.

Assume that each proper subgroup of G is metacyclic. By Proposition 78.11, G is nonmetacyclic and so $|G| \leq p^4$ (Theorem 69.1 for $p > 2$), a contradiction.

Let M be a nonmetacyclic maximal subgroup of G . Since M is modular, Proposition 78.9 implies that $d(M) \geq 3$. By Proposition 78.11, G is not a 3-group of maximal class (since it has a maximal subgroup H which satisfies $H/\mathfrak{V}_1(H) \cong S(3^3)$, so non-modular. Therefore, if $|\Omega_1(G)| < p^3$, then, by Theorem 13.7, G must be metacyclic so modular (Proposition 78.11), a contradiction. Thus, $|\Omega_1(G)| \geq p^3$. \square

Remark 5. Minimal nonmodular p -group of exponent p is isomorphic to $S(p^3)$. Indeed, $p > 2$. All proper subgroups of G are elementary abelian so $G \cong S(p^3)$, by Lemma 65.3.

Theorem 78.13. *Let G be a minimal nonmodular p -group, $p > 2$, with $|G| > p^4$. If $\mathfrak{V}_1(G)$ is cyclic, then $\Omega_1(G) \cong E_{p^3}$ and $G/\mathfrak{V}_1(G)$ is cyclic of order $\geq p^2$ (i.e. G is an L_3 -group; see §§17, 18).*

Proof. By Proposition 78.11, $G/\mathfrak{V}_1(G) \cong S(p^3)$. By assumption, $N = \mathfrak{V}_1(G)$ is cyclic. By Proposition 78.12, $E = \Omega_1(G)$ is elementary abelian of order $\geq p^3$. But $|E \cap N| = p$ and E does not cover G/N , and so $E \cong E_{p^3}$, by the product formula. On the other hand, there is $a \in G - N$ with $\langle a^p \rangle = N$. Since $|G : \langle a \rangle| = p^2$ and $|\langle a \rangle \cap E| = p$, we get $G = \langle E, a \rangle$, by the product formula, and we are done. \square

Proposition 78.14. *Let G be a minimal nonmodular p -group, $p > 2$, with $|G| > p^4$. Suppose that $d(\mathfrak{V}_1(G)) = 2$ and let M be any maximal subgroup of G . Then $d(M) \leq 3$.*

Proof. Suppose that this is false. Let M be a maximal subgroup of G with $d(M) \geq 4$. Set $N = \mathfrak{V}_1(G)$ so that $M/N \cong E_{p^2}$ and $N/\Phi(N) \cong E_{p^2}$. Since $\Phi(N) \leq \Phi(M)$, we must have $\Phi(M) = \Phi(N)$ so that $M/\Phi(N) \cong E_{p^4}$. We shall study the structure of $G/\Phi(N)$ (which is also minimal nonmodular of order $> p^4$ and exponent p^2) and so we may assume $\Phi(N) = \{1\}$ which implies $M \cong E_{p^4}$. Since $\Omega_1(G)$ is elementary abelian, we have $M = \Omega_1(G)$. If $x \in G - M$, then $x^p \in Z(G)^\#$. There is $y \in G - M$ such that $y^p \in N - \langle x^p \rangle$ since $N = \mathfrak{V}_1(G)$; then again $y^p \in Z(G)^\#$. Since $N \cong E_{p^2}$, we get $N \leq Z(G)$. If $Z(G) > N$, then $Z(G)/N = Z(G/N) = \Phi(G/N)$ and

so $Z(G) = \Phi(G)$. But then G is minimal nonabelian. By Lemma 65.1, we get $|\Omega_1(G)| \leq p^3$, a contradiction.

We have proved that $Z(G) = N$. By Lemma 1.1, $|G| = p^5 = p|Z(G)||G'|$ and so $|G'| = p^2$. Since $G/N \cong S(p^3)$, $G' \neq N (= Z(G))$, $G' \cap Z(G) \cong C_p$ and $G' < M$ so that $C_G(G') = M$. Since $N = \mathfrak{V}_1(G)$, where is $v \in G - M$ such that $v^p \in N - G'$. It follows that the subgroup $H = \langle G', v \rangle$ is nonabelian. We claim that $H/\langle v \rangle \cong S(p^3)$. Assume that this is false. Then that quotient group is elementary abelian. Set $\bar{G} = G/\langle v \rangle$; then $C_{\bar{G}}(\bar{G}') \geq \langle \bar{M}, \bar{v} \rangle = \bar{G}$ so $\bar{G} = Z(\bar{G})$. Since $\bar{G}/Z(\bar{G}) \cong E_{p^2}$, the group \bar{G} is minimal nonabelian so $|\bar{G}'| = p$ (Lemma 65.1), a contradiction. We have proved that each maximal subgroup of G is generated by three elements. \square

Theorem 78.15 (Janko). *Let G be a minimal nonmodular p -group, $p > 2$, with $|G| > p^4$. Then $\mathfrak{V}_1(G)$ is metacyclic and $G/\mathfrak{V}_1(G) \cong S(p^3)$ (nonabelian group of order p^3 and exponent p). If $\mathfrak{V}_1(G)$ is noncyclic, then $\Phi(G) = \mathfrak{V}_1(G) \times C_p$, $\Omega_1(\Phi(G)) = \Omega_1(G) \cong E_{p^3}$, $G/\Omega_1(G)$ is metacyclic and for each maximal subgroup M of G we have $d(M) = 3$.*

Proof. Set $N = \mathfrak{V}_1(G) (< \Phi(G))$ and suppose that $d(N) = 2$. By Proposition 78.12, $\Omega_1(G)$ is elementary abelian of order $\geq p^3$ and $\Omega_1(G) \cap N \cong E_{p^2}$. Since $\Omega_1(G)$ does not cover $G/N \cong S(p^3)$, $N\Omega_1(G)$ is contained in a maximal subgroup M of G . By Proposition 78.14, $d(M) \leq 3$ and the modularity of M implies $d(M) = d(\Omega_1(M))$ [Suz1]. This implies $\Omega_1(G) \cong E_{p^3}$ and $(N\Omega_1(G))/N = \Phi(G/N)$. Thus $\Phi(G) = N\Omega_1(G)$ and so for each maximal subgroup X of G , we have $d(X) = 3$ since $X \geq \Phi(G)$ and $d(X) = d(\Omega_1(X)) = d(\Omega_1(G))$.

We know that $\text{Aut}(\Omega_1(G))$ does not possess an automorphism of order p^2 (see, for example, §33). There are elements $a, b \in G$ such that $N = \langle a^p \rangle \langle b^p \rangle$ and a^p and b^p centralize $\Omega_1(G)$. Hence $\Phi(G) = N \times Z$ with $|Z| = p$.

If $G/\Omega_1(G)$ is nonmodular, then (Proposition 78.11) there is a normal subgroup K of G with $K \geq \Omega_1(G)$, $G/K \cong S(p^3)$, and $d(K) \leq 2$. This is a contradiction since $d(K) = d(\Omega_1(K)) = 3$. Hence $G/\Omega_1(G)$ is modular and since $d(G/\Omega_1(G)) \leq 2$, $G/\Omega_1(G)$ is metacyclic and our theorem is proved. \square

Nonmodular quaternion-free 2-groups

Modular Q_8 -free 2-groups are classified in [Iwa] (see §73). Here we classify nonmodular Q_8 -free 2-groups. The original proof of the corresponding classification theorem, given in [Wil2], depends on the structure theory of powerful 2-groups. In addition, in the proof of Lemma 10 and 13 in [Wil2] there are some gaps. Our new proof of the classification theorem is completely elementary and does not involve powerful 2-groups. Nevertheless, the proof is very involved and reaches probably a deepest result ever proved in the finite 2-group theory.

We first prove some easy preliminary results. Then we state the Main Theorem 79.7 and afterwards we describe in great detail the groups appearing in the Main Theorem. Propositions 79.8 to 79.11, describing these groups, are also of independent interest since they are needed by applying the Main Theorem in future investigations. After that the proof of the Main Theorem follows.

Lemma 79.1. *In a Q_8 -free 2-group X there are no elements x, y with $o(x) = 2^k > 2$ and $o(y) = 4$ so that $x^y = x^{-1}$. If $D \leq X$ and $D \cong D_8$, then $C_X(D)$ is elementary abelian.*

Proof. If $y^2 = x^{2^{k-1}}$, then $\langle x, y \rangle \cong Q_{2^{k+1}}$. If $\langle x \rangle \cap \langle y \rangle = \{1\}$, then we have $\langle x, y \rangle / \langle x^{2^{k-1}} y^2 \rangle \cong Q_{2^{k+1}}$. Suppose that $D \leq X$, where $D = \langle a, t \mid a^4 = t^2 = 1, a^t = a^{-1} \rangle \cong D_8$. If v is an element of order 4 in $C_X(D)$, then $o(tv) = 4$ and tv inverts a , a contradiction. Hence $C_X(D)$ must be elementary abelian. \square

Lemma 79.2. *Let X be a Q_8 -free 2-group with elements a and b of order 4 such that $[a, b^2] = [a^2, b] = 1$. If $[a, b] \neq 1$, then $\langle a, b \rangle$ is minimal nonabelian nonmetacyclic of order 2^4 and therefore $[a, b] = a^2b^2$ and ab is an involution.*

Proof. Without loss of generality, one may assume that $X = \langle a, b \rangle$ holds. We have $\langle a^2, b^2 \rangle \leq Z(X)$. Set $[a, b] = c$; then $c \neq 1$. We compute

$$1 = [a^2, b] = [a, b]^a [a, b] = c^a c \quad \text{and} \quad 1 = [a, b^2] = [a, b][a, b]^b = c c^b.$$

By Lemma 79.1, c must be an involution and, by the displayed equalities, $[c, a] = [c, b] = 1$. Hence $\langle c \rangle$ is normal in X and $X/\langle c \rangle$ is abelian. It follows that $X' = \langle c \rangle$ and so X , by Lemma 65(a), is minimal nonabelian (and so of class 2) and therefore $\exp(X) = 4$. By assumption, $X \not\cong Q_8$, and $X \not\cong D_8$ since D_8 has only one cyclic

subgroup of order 4. We have proved that $|X| \geq 2^4$. Considering $X/\langle c \rangle$, we conclude that $|\langle a, b \rangle| \leq 2^5$.

On the other hand, $c = [a, b]$, a^2 , and b^2 are central involutions in X . Set $V = \langle a^2c, b^2c \rangle$ so that $V \leq Z(\langle a, b \rangle)$ and $|V| = 4$. We consider X/V and compute

$$a^b = a[a, b] = ac = a^{-1}(a^2c), \quad b^a = b[b, a] = bc = b^{-1}(b^2c).$$

Since X/V is Q_8 -free, Lemma 79.1 implies that at least one of a^2 or b^2 is contained in V . Hence $a^2 = b^2c$ or $b^2 = a^2c$ and so in any case $c = a^2b^2 \in V$ since $a^2c \cdot b^2c = a^2b^2$. It follows from the displayed equalities that $X/V \cong E_4$ so $|X| = |V||E_4| = 2^4$. \square

Lemma 79.3 (see §78 and especially Proposition 78.4). *Let G be a Q_8 -free minimal nonmodular 2-group of order > 8 . Then G has a normal elementary abelian subgroup $E = \Omega_1(G) = \langle n, z, t \rangle$ of order 8 with G/E cyclic. There is an element $x \in G - E$ of order 2^{s+1} , $s \geq 1$, such that $G = \langle E, x \rangle$, $E \cap \langle x \rangle = \langle n \rangle$, and $t^x = tz$, $z^x = zn^\epsilon$, $\epsilon = 0, 1$, where in case $\epsilon = 1$ we must have $s > 1$ and we have in that case $G' = \langle n, z \rangle \cong E_4$ and $Z(G) = \langle x^4 \rangle$. If $\epsilon = 0$, then G is a minimal nonabelian nonmetacyclic group so $E \cong E_8$. In any case, $\langle x^2 \rangle$ is normal in G , $G/\langle x^2 \rangle \cong D_8$, and $\Phi(G) = \langle x^2, z \rangle$ is abelian of type $(2^s, 2)$.*

Lemma 79.4. *Let V be a minimal non-quaternion-free 2-group. Then there is a normal subgroup U of V such that $V/U \cong Q_8$ and $U < \Phi(V)$ so that $d(V) = 2$. We have $\Phi(V)/U = Z(V/U)$ so that for each $x \in V - \Phi(V)$, $x^2 \in \Phi(V) - U$. In particular, there are no involutions in $V - \Phi(V)$.*

We use very often the following

Lemma 79.5 (= Lemma 64.1(u)). *If A and B are two distinct maximal subgroups of a p -group G , then $|G' : (A'B')| \leq p$.*

For the sake completeness we also state the Iwasawa's result in a suitable form.

Proposition 79.6 ([Iwa] and §73). *A 2-group G is modular if and only if G is D_8 -free. A 2-group G is modular and Q_8 -free if and only if G possesses a normal abelian subgroup A with cyclic G/A and there is an element $g \in G$ and an integer $s \geq 2$ such that $G = \langle A, g \rangle$ and $a^g = a^{1+2^s}$ for all $a \in A$ (and so, if $\exp(G) \leq 4$, then G is abelian).*

Main Theorem 79.7 (B. Wilkens). *A finite 2-group G is nonmodular and quaternion-free if and only if G is one of the following groups:*

- (a) (*Wilkens group of type (a) with respect to N*) G is a semidirect product $\langle x \rangle \cdot N$, where N is a maximal abelian normal subgroup of G with $\exp(N) > 2$ and, if t is the involution in $\langle x \rangle$, then every element in N is inverted by t .
- (b) (*Wilkens group of type (b) with respect to N*) $G = N\langle x \rangle$, where N is a maximal elementary abelian normal subgroup of G and $\langle x \rangle$ is not normal in G .

- (c) (Wilkins group of type (c) with respect to N, x, t) $G = \langle N, x, t \rangle$, where N is an elementary abelian normal subgroup of G and t is an involution with $[N, t] = 1$. If $o(xN) = 2^k$, then $G/N \cong M_{2^{k+1}}$, $k \geq 3$, and $x^{2^k} \neq 1$; furthermore $[x^{2^{k-1}}, N] = 1$ and $\langle t, x^{2^{k-1}} \rangle \cong D_8$.

We analyze now in great detail the above Wilkins groups of types (a), (b), and (c). In what follows we call these groups W_x -groups, where $x \in \{a, b, c\}$ so, for example, W_b -group is a Wilkins group of type (b).

Remark 1. A nonabelian 2-group $G = \langle t \rangle \cdot N$ is said to be *generalized dihedral* with base N , if t is an involution and N is an (abelian) subgroup of index 2 in G such that t inverts N . We claim that if also $G = \langle t_1 \rangle \cdot N_1$ is generalized dihedral with base N_1 , then $N_1 = N$. Assume that this is false. We have $N \cap N_1 = Z(G)$ and $|G : (N \cap N_1)| = 4$, $G = N \cup Nt$ is a partition and all elements of the coset Nt are involutions and invert N . Therefore, if $x \in N_1 \cap Nt$, then x centralizes and inverts $N \cap N^\alpha$ so $\exp(N \cap N_1) = 2$. It follows that $N_1 = \langle x, N \cap N_1 \rangle$ is elementary abelian, which is a contradiction since $\exp(N_1) > 2$. In particular, the base of G is characteristic in G .

Proposition 79.8. *Let G be a W_a -group with respect to N . Then $\Omega_1(G) = N\langle t \rangle$, where t is an involution in $G - N$ inverting N and N is characteristic in $\Omega_1(G)$ and so in G . If G is a W_a -group with respect to N_1 , then $N = N_1$. Also, G is not D_8 -free but G is Q_8 -free. If $z \in \Omega_1(Z(G))$, then $G/\langle z \rangle$ is either abelian or a W_a - or W_b -group.*

Proof. By hypothesis, G is a semidirect product $\langle x \rangle \cdot N$, where N is a maximal abelian normal subgroup of G with $\exp(N) > 2$ and, if t is the involution in $\langle x \rangle$, then every element in N is inverted by t . Since G/N is cyclic, we have $\Omega_1(G) \leq N\langle t \rangle$. The coset Nt consist of involutions and so $\Omega_1(G) = N\langle t \rangle$. It follows that $\Omega_1(G)$ is a generalized dihedral group with respect N . By Remark 1, N is the unique base of $\Omega_1(G)$ so it is characteristic in $\Omega_1(G)$ and in G . Thus, if G is also a W_a -group with respect to N_1 , then $N_1 = N$.

Since t inverts N and $\exp(N) > 2$, G is not D_8 -free. Suppose that G is not Q_8 -free. Let V be a minimal non- Q_8 -free subgroup of G so that V has a normal subgroup U with $V/U \cong Q_8$ and $\Phi(V) > U$; it follows that $d(V) = 2$. Since $V \not\leq N$ and G/N is cyclic, we see that $V/(V \cap N) > \{1\}$ is cyclic. Let t' be an element in $V - N$ such that $(t')^2 \in N$. Then Nt' is the involution in G/N and so all elements in Nt' are involutions. In particular, all elements in the set $S = (V \cap N)t'$ are involutions. By Lemma 79.4, $S \leq \Phi(V)$ and so also $\langle S \rangle = (V \cap N)\langle t' \rangle \leq \Phi(V)$. But then $V/\Phi(V)$, as an epimorphic image of $V/(V \cap N)$, is cyclic, a contradiction.

Let $z \in Z(G)$ be an involution. We want to determine the structure of $G/\langle z \rangle$. We know that $G = \langle x \rangle \cdot N$ is a semidirect product. Let t be the involution in $\langle x \rangle$. We have $z \in N$ and t inverts N and so t inverts $N/\langle z \rangle$. If $\exp(N/\langle z \rangle) > 2$, then $G/\langle z \rangle$ is a W_a -group.

Let $\exp(N/\langle z \rangle) = 2$. Set $E = \langle t \rangle N$. Then $E/\langle z \rangle = \Omega_1(G/\langle z \rangle)$ is a maximal elementary abelian normal subgroup of $G/\langle z \rangle$. If $\langle x, z \rangle = \langle x \rangle \times \langle z \rangle$ is not normal in G , then $G/\langle z \rangle$ is a W_b -group. Suppose that $\langle x, z \rangle$ is normal in G . Then $G' \leq \langle x, z \rangle \cap N = \langle z \rangle$ so $G' = \langle z \rangle$. In that case, $G/\langle z \rangle$ is abelian, and we are done. \square

Remark 2. Let a 2-group G of exponent > 2 have two distinct elementary abelian subgroups E and E_1 of index 2. Then $G = D \times L$, where $D \cong D_8$ and $\exp(L)$ divides 2. Since $\exp(G) > 2$, G is nonabelian. It follows that $E \cap E_1 = Z(G)$ has index 4 in G . Let A be a minimal abelian subgroup of G ; then $|A : (A \cap Z(G))| > 2$ so $G = AZ(G)$, by the product formula. In that case, $A \cap Z(G) = Z(A)$. If $Z(G) = Z(A) \times L$, then $G = A \times L$ and $\exp(L)$ divides 2. Since A has two distinct elementary abelian subgroup of index 2, then $A \cong D_8$ (Lemma 65.1).

Proposition 79.9. (i) A 2-group G is a W_b -group with respect to E if and only if E is a maximal normal elementary abelian subgroup E such that G/E is cyclic and G is not D_8 -free.

(ii) Let G be a W_b -group with respect to E . Then G is Q_8 -free. We have $|\Omega_1(G) : E| \leq 2$. If $|\Omega_1(G) : E| = 2$, then G has exactly two maximal normal elementary abelian subgroups E and E_1 and we have $\Omega_1(G) = EE_1$. In that case, if G is also a W_b -group with respect to E_1 , then $|\Omega_1(G) : E_1| = 2$ and $\Omega_1(G) \cong D_8 \times E_{2^s}$. Let $z \in \Omega_1(Z(G))$. Then $G/\langle z \rangle$ is either abelian or a W_b -group or $G/\langle z \rangle \cong D \times F$, where $\exp(F) \leq 2$ and either $D \cong D_8$ or $D \cong M_{2^n}$, $n \geq 4$ (in which case $G/\langle z \rangle$ is modular and nonabelian). Finally, if G is any 2-group with an elementary abelian normal subgroup E_0 such that $G = \langle E_0, y \rangle$ (and so G/E_0 is cyclic) and $\langle y \rangle$ is not normal in G , then G is a W_b -group with respect to any maximal elementary abelian normal subgroup E of G containing E_0 .

Proof. (i) Let G be a nonmodular 2-group possessing a maximal elementary abelian normal subgroup E such that G/E is cyclic. We have $G = \langle E, x \rangle$ for some $x \in G$ and if $\langle x \rangle \not\leq G$, then G is a W_b -group.

Assume that $\langle x \rangle$ is normal in G . In that case, $G' \leq \langle x \rangle \cap E$ and, since G is nonmodular (and so nonabelian), $G' = \langle x \rangle \cap E = \langle z \rangle \cong C_2$. We have $|G : C_G(x)| = 2$ since $|G : C_G(x)| \leq |G'|$ for each $x \in G$. We set $E_1 = C_E(x)$ so that $|E : E_1| = 2$ and $E_1 \leq Z(G)$. Let t be an involution in $E - E_1$ and let V be a complement of $\langle z \rangle$ in E_1 so that $G = V \times \langle x, t \rangle$, by the product formula. If $|G/E| = 2^s > 2$, then $\langle x, t \rangle \cong M_{2^{s+2}}$, $s \geq 2$ since a 2-group of maximal class has no cyclic epimorphic images of order $2^s > 2$, and so for each $a \in A = \langle x \rangle \times V$, $a^t = a^{1+2^s}$ since $\exp(V)$ divides 2. But Proposition 79.6 implies that G is modular, a contradiction. Hence $|G/E| = 2$ and $\langle x, t \rangle \cong D_8$. In that case $\tilde{x} = xt$ is an involution in $G - E$, $G = E\langle \tilde{x} \rangle, \langle \tilde{x} \rangle$ is not normal in G , and so G is a W_b -group.

(ii) Conversely, let G be a W_b -group with respect to E so that $G = \langle E, g \rangle$, where E is a maximal normal elementary abelian subgroup of G and $\langle g \rangle$ is not normal in G .

Set $Z = \langle g \rangle \cap E$ so that $|Z| \leq 2$ and $Z \leq Z(G)$. Set $S = N_G(\langle g \rangle)$ so that $S \neq G$ and $S \cap E < E$. Since $G = \langle g \rangle S$, we get $N_G(S) = \langle g \rangle N_E(S)$, by the modular law, so, in view of $N_E(S) > E \cap S$, there is an involution $n \in E - S$ normalizing S . Since $[n, g] \in [n, S] \leq$ and $[n, g] \in [E, g] \leq E$, we get $[n, g] \in S \cap E$ and $1 \neq u = [n, g] \notin \langle g \rangle$ since $n \notin S = N_G(\langle g \rangle)$. We have $[n, g] = ng^{-1}ng = nn^g = u$. On the other hand, $\Phi(S) = \langle g^2 \rangle$ and so $\langle g^2 \rangle$ is normal in $\langle S, n \rangle$ so that $n^{g^2} = nz$ with $z \in Z$. Hence $\langle g \rangle$ normalizes $\langle n, n^g, Z \rangle$ and acts nontrivially on the four-group $\langle n, n^g, Z \rangle / Z$, where $\langle g^2 \rangle \geq Z$. It follows that $\langle n, g \rangle / \langle g^2 \rangle \cong D_8$ and so G is not D_8 -free.

We claim that G is Q_8 -free. Indeed, if V is a minimal non- Q_8 -free subgroup of G , then, by Lemma 79.4, there are no involutions in $V - \Phi(V)$ so that $\Phi(V) \geq V \cap E$. But then $V/\Phi(V)$ is cyclic since $V/(V \cap E)$ is, a contradiction.

Set $W/E = \Omega_1(G/E)$ so that $\Omega_1(G) \leq W$ and $|\Omega_1(G) : E| \leq |W : E| = 2$. Suppose that $|\Omega_1(G) : E| = 2$ so that $\Omega_1(G) = W$ and there is an involution $t \in W - E$. Since E is a maximal normal elementary abelian subgroup of G , W is not elementary abelian so $\langle t \rangle$ is not normal in W , and we conclude that W is a W_b -group with respect to E . Let $t_1 \in W - E$ be an involution, $t_1 \neq t$. Then $tE = t_1E$ since $|W : E| = 2$. In that case $tt_1 \in E$ is involution so all involutions in $W - E$ commute with t . Set $E_1 = C_W(t)$ so that $E_1 - E$ is the set of all involutions in $W - E$, by what has just been proved. Since $\langle E_1 - E \rangle = E_1$, E_1 is normal in G and E and E_1 are the only maximal normal elementary abelian subgroups of G . If G is also a W_b -group with respect to E_1 , then G/E_1 must be cyclic and so $|W : E_1| = 2$ and in that case $W = \Omega_1(G) \cong D_8 \times E_{2^s}$, by Remark 2.

Let z be a central involution in G , where $G = \langle E, x \rangle$ and $\langle x \rangle$ is not normal in G ; then $z \in E$ since E is a maximal elementary abelian subgroup of G . If $z \in \langle x \rangle$, then $\langle x \rangle / \langle z \rangle$ is not normal in $G / \langle z \rangle$ so $G / \langle z \rangle$ is a W_b -group with respect to $E / \langle z \rangle$. Suppose that $z \notin \langle x \rangle$. If $\langle x, z \rangle$ is not normal in G , then again $G / \langle z \rangle$ is a W_b -group. Assume that $\langle x, z \rangle = \langle x \rangle \times \langle z \rangle$ is normal in G . If $\langle x \rangle \cap E = \{1\}$, then $\langle x, z \rangle \cap E = \langle z \rangle$ and $G' \leq \langle x, z \rangle \cap E = \langle z \rangle$ and so $G / \langle z \rangle$ is abelian. Assume that $\langle x \rangle \cap E \neq \{1\}$ so that $\langle x, z \rangle \cap E = \Omega_1(\langle x \rangle) \times \langle z \rangle \cong E_4$ and suppose that $G / \langle z \rangle = \bar{G}$ is nonabelian. Then $\bar{G} = \langle \bar{x} \rangle \bar{E}$ with $\langle \bar{x} \rangle \cap \bar{E} \cong C_2$ and both $\langle \bar{x} \rangle$ and \bar{E} are normal in \bar{G} so that $\bar{G}' = \langle \bar{x} \rangle \cap \bar{E}$. Let \bar{t} be an involution in \bar{E} which does not centralize $\langle \bar{x} \rangle$. If $o(\bar{x}) = 4$, then $\langle \bar{x}, \bar{t} \rangle \cong D_8$ and if $o(\bar{x}) > 4$, then $\langle \bar{x}, \bar{t} \rangle \cong M_{2^n}$, $n \geq 4$ since $\langle \bar{x}, \bar{t} \rangle \cap \bar{E} \cong E_4$ (see Theorem 1.2). We have $\bar{E} = (\langle \bar{x} \rangle \cap \bar{E}) \times \langle \bar{t} \rangle \times \bar{V}$, where $(\langle \bar{x} \rangle \cap \bar{E}) \times \bar{V} = C_{\bar{E}}(\bar{x})$ so that $\bar{G} = \bar{V} \times \langle \bar{x}, \bar{t} \rangle$ and we are done. \square

Proposition 79.10. *Let G be a W_c -group with respect to N, x, t . Then G is Q_8 -free but is not D_8 -free. We have $\Omega_1(G) = \langle x^{2^{k-1}}, t \rangle N \cong D_8 \times E_{2^s}$ ($k \geq 3$) and $G = \Omega_1(G)\langle x \rangle$ so that $G / \Omega_1(G)$ is cyclic of order ≥ 4 . Also, N is the unique maximal normal elementary abelian subgroup of G . No subgroup of order ≥ 8 in $\langle x \rangle$ is normal in G . The involution $z = x^{2^k}$ lies in $G' \cap Z(G)$ and $G / \langle z \rangle$ is a W_b -group. If $z' \in \Omega_1(Z(G))$ and $z' \neq z$, then $z' \in N$ and $G / \langle z' \rangle$ is a W_c -group.*

Proof. By hypothesis, $G = \langle N, x, t \rangle$, where N is an elementary abelian normal subgroup of G and t is an involution with $[N, t] = 1$. If $\phi(xN) = 2^k$, then $G/N \cong M_{2^{k+1}}$, $k \geq 3$, and $x^{2^k} \neq 1$; furthermore $[x^{2^{k-1}}, N] = 1$ and $\langle t, x^{2^{k-1}} \rangle \cong D_8$ so that G is not D_8 -free. We set $a = x^{2^{k-1}}$ and $z = a^2$. We have

$$(G/N)' = \Omega_1(Z(G/N)) = (\langle a \rangle N)/N \quad \text{and} \quad \Omega_1(G/N) = (\langle t, a \rangle N)/N = W/N,$$

where $W = \langle t, a \rangle N$ and $Z(W) = N$. Each involution in G is contained in W and $W = \Omega_1(W)$ and so $\Omega_1(G) = W \cong D_8 \times E_{2^s}$ (Remark 2) and $G = \Omega_1(G)\langle x \rangle$ so that $G/\Omega_1(G)$ is cyclic of order ≥ 4 . By the structure of G/N , if X is a normal subgroup of G with $N \leq X \leq W$, then $X \in \{N, W, \langle a \rangle N\}$, where $\langle a \rangle N$ is abelian of type $(4, 2, \dots, 2)$ so that N is a maximal normal elementary abelian subgroup of G . Let N_1 be any maximal normal elementary abelian subgroup of G ; then $N_1 < \Omega_1(G) = W$. Assume that $N_1 \neq N$. Since N_1 does not cover W/N (since all elements in $(\langle a \rangle N) - N$ are of order 4), we get $|NN_1 : N| = 2$, $NN_1 \triangleleft G$ and so (by the above) $NN_1 = \langle a \rangle N$, a contradiction. Thus, N is the unique maximal normal elementary abelian subgroup of G so it is characteristic in G .

Let $Y \leq \langle x \rangle$ with $|Y| \geq 8$ and assume that t normalizes Y . Since t inverts $\langle a \rangle$ and $\langle a \rangle < Y$, it follows that $Y\langle t \rangle$ is of maximal class and order 2^m , $m \geq 4$, and so $(Y\langle t \rangle)/\langle z \rangle \cong D_{2^{m-1}}$ is isomorphic to a proper subgroup of $G/N \cong M_{2^n}$, $n \geq 4$, which is not the case. Thus, Y is not normal in G .

Let G be not Q_8 -free and let $V \leq G$ be minimal non- Q_8 -free. By Lemma 79.4, there are no involutions in $V - \Phi(V)$ and so $\Phi(V) \geq V \cap N$. On the other hand, $\Phi(V)$ is contained in the maximal subgroup $\langle x \rangle N$ of G and note that $\Omega_1(\langle x \rangle N) = N$ (since $N \cap \langle x \rangle = \langle z \rangle$ and a centralizes N). It follows that $\Omega_1(\Phi(V)) = V \cap N$. Note that G/N has exactly three involutions: Na , Nt , and $N(at)$, where all elements in the coset Na are of order 4 and all elements in cosets Nt and $N(at)$ are involutions. Let $(V \cap N)s$ ($s \in V$) be an involution in $V/(V \cap N)$. Then Ns is an involution in G/N . If all elements in the coset Ns are involutions, then $s \in \Phi(V)$, contrary to the above fact that $\Omega_1(\Phi(V)) = V \cap N$. It follows that $Ns = Na$ and so $(V \cap N)s = (Na) \cap V$ is the unique involution in $V/(V \cap N)$. Since G/N is Q_8 -free, we get that $V/(V \cap N)$ is cyclic. But then $V/\Phi(V)$ is also cyclic, a contradiction.

We shall determine the structure of $G/\langle z \rangle = \bar{G}$. Since $\overline{\Omega_1(G)} = \Omega_1(G)/\langle z \rangle$ is an elementary abelian normal subgroup of \bar{G} , $\bar{G} = \overline{\Omega_1(G)}\langle \bar{x} \rangle$, and $\langle \bar{x} \rangle$ is not normal in \bar{G} (noting that $z \in \langle x \rangle$ and $\langle x \rangle$ is not normal in G), \bar{G} is a W_b -group. Let z' be an involution in $Z(G)$ and $z' \neq z$. Then $z' \in N$ and $\langle z' \rangle \cap \langle a, t \rangle = \{1\}$ so that $G/\langle z' \rangle$ is not D_8 -free. Obviously, $G/\langle z' \rangle$ is a W_c -group. \square

Proposition 79.11. *Let G be one of the Wilkins groups. Suppose that there is an involution $z \in Z(G)$ such that $G/\langle z \rangle$ is modular (i.e., D_8 -free).*

- (i) *If $G/\langle z \rangle$ is abelian, then G is a W_b -group and more precisely: $G = D \times E$ where $\exp(E) \leq 2$ and $D = \langle x, t \mid x^{2^n} = t^2 = 1, n \geq 1, [x, t] = z, z^2 =$*

$[x, z] = [t, z] = 1$. (If $n = 1$, then $D \cong D_8$, and if $n > 1$, then D is minimal nonabelian nonmetacyclic with $\Omega_1(D) \not\leq Z(D)$.)

- (ii) If $G/\langle z \rangle$ is nonabelian, then there is another involution $z' \in Z(G)$ such that $\langle z' \rangle$ is a characteristic subgroup of G and $G/\langle z' \rangle$ is a W_b -group.

Proof. (i) Suppose that $G/\langle z \rangle$ is abelian. Then $G' = \langle z \rangle$ and by Propositions 79.8, 79.9, and 79.10, G is either a W_a - or W_b -group.

Suppose that G is a W_a -group. Then $G = \langle x \rangle \cdot N$ (a semidirect product), where N is a maximal normal abelian subgroup of G with $\exp(N) > 2$ and if t is the involution in $\langle x \rangle$, then t inverts each element of N . Suppose $n \in N$ with $o(n) > 2$. Then $\langle n, t \rangle$ is dihedral and so $n^2 \in \langle n, t \rangle'$. It follows that $n^2 \in \langle z \rangle$ and therefore $N/\langle z \rangle$ is elementary abelian with $\Omega_1(N) = \langle z \rangle$ and $|N : \Omega_1(N)| = 2$. Suppose $\langle x \rangle > \langle t \rangle$ and let $v \in \langle x \rangle$ with $v^2 = t$. Let $n \in N$ with $o(n) = 4$. We have $[n, v] \neq 1$ and so $[n, v] = z$ which gives $n^v = nz$. But then $n^t = n^{v^2} = (nz)^v = n^v z^v = nzz = n$ since $z \in Z(G)$. This is a contradiction and so $\langle x \rangle = \langle t \rangle$. If $n \in N$ with $o(n) = 4$, then $D = \langle n, t \rangle \cong D_8$. Let E be a complement of $\langle z \rangle$ in $\Omega_1(N)$, where t centralizes $\Omega_1(N)$. We get $G = \langle t \rangle \cdot N = D \times E$, where $D \cong D_8$ and $\exp(E) \leq 2$.

Suppose that G is a W_b -group. Then $G = \langle N, x \rangle$, where N is a maximal normal elementary abelian subgroup of G and $\langle x \rangle$ is not normal in G . We have $z \in N$ and $G' = \langle z \rangle$. If $z \in \langle x \rangle \cap N$, then $\langle x \rangle$ is normal in G , a contradiction. Hence $z \notin \langle x \rangle$ and $\langle x, z \rangle = \langle x \rangle \times \langle z \rangle$ is normal in G . Since $\langle x, z \rangle$ contains exactly two cyclic subgroups $\langle x \rangle$ and $\langle xz \rangle$ of index 2 not containing $\langle z \rangle$, we have $|G : N_G(\langle x \rangle)| = 2$. There is $t \in N - N_G(\langle x \rangle)$ such that $x^t = xz$. Also note that $N_G(\langle x \rangle)$ centralizes $\langle x \rangle$ (since $G' = \langle z \rangle$). Let E be a complement of $\langle z, \langle x \rangle \cap N \rangle$ in $N_N(\langle x \rangle)$. Then $G = D \times E$, where $D = \langle x, t | x^{2^n} = t^2 = 1, n \geq 1, [x, t] = z, z^2 = [x, z] = [t, z] = 1 \rangle$.

(ii) Suppose that $G/\langle z \rangle$ is nonabelian. By Propositions 79.8, 79.9, and 79.10, G is a W_b -group. Then $G = \langle N, x \rangle$, where N is a maximal normal elementary abelian subgroup of G and $\langle x \rangle$ is not normal in G . If $z \in \langle x \rangle \cap N$, then the fact that $\langle x \rangle$ is not normal in G gives that $\langle x \rangle/\langle z \rangle$ is not normal in $G/\langle z \rangle$ and so $G/\langle z \rangle$ is a W_b -group, a contradiction. Hence $z \notin \langle x \rangle$. If $\langle x, z \rangle$ is not normal in G , then again $G/\langle z \rangle$ is a W_b -group, a contradiction. Hence $\langle x, z \rangle = \langle x \rangle \times \langle z \rangle$ is normal in G . Assume first that $\langle x \rangle \cap N = \{1\}$. Then $\langle x, z \rangle \cap N = \langle z \rangle$ and $G' \leq \langle x, z \rangle \cap N = \langle z \rangle$ and so $G/\langle z \rangle$ is abelian, a contradiction. Hence $\langle x \rangle \cap N > \{1\}$ and so $\langle x, z \rangle \cap N = \Omega_1(\langle x \rangle) \times \langle z \rangle$. Since $G' \leq \langle x, z \rangle \cap N$ and $G/\langle z \rangle$ is nonabelian (by assumption), we get $1 \neq |G'| \leq 4$ and $G' \not\leq \langle z \rangle$. We have $\Omega_1(\langle x \rangle) \leq Z(G)$. Set $\Omega_1(\langle x \rangle) = \langle x_0 \rangle$ and $S = N_G(\langle x \rangle)$ so that $\langle x_0, z \rangle \leq Z(G)$, $|G : S| = 2$ and $|N : (S \cap N)| = 2$ because $\langle x \rangle$ is not normal in G and the abelian normal subgroup $\langle x, z \rangle$ has exactly two cyclic subgroups $\langle x \rangle$ and $\langle xz \rangle$ of index 2. Therefore, we have $[x, s] = z$ or $[x, s] = x_0z$ for an $s \in N - S$ and so $\Phi(G) = \langle x^2, [\langle x \rangle, N] \rangle = \langle x^2 \rangle \times \langle z \rangle$.

Suppose $o(x) \geq 8$ so that $\Phi(\Phi(G)) = \langle x^4 \rangle \geq \langle x_0 \rangle$ and $\langle x_0 \rangle$ is a characteristic subgroup of G . But $\langle x \rangle/\langle x_0 \rangle$ is not normal in $G/\langle x_0 \rangle$ (since $\langle x \rangle$ is not normal in G) and so $G/\langle x_0 \rangle$ is a W_b -group, and we are done in this case.

Suppose $o(x) = 4$ so that $x^2 = x_0$. If $\langle x \rangle \not\leq Z(S)$, then there is an involution t in $S \cap N$ which inverts $\langle x \rangle$ and so $\langle x, t \rangle \cong D_8$. But then $G/\langle z \rangle$ is not D_8 -free, a contradiction: $G/\langle z \rangle$ is modular. Hence $\langle x \rangle$ is central in S and so $G' = \langle [x, s] \rangle = \langle x_0z \rangle$ (since in case $G' = \langle [x, s] \rangle = \langle z \rangle$, $G/\langle z \rangle$ would be abelian). But then $\langle x, s \rangle$ is the minimal nonabelian nonmetacyclic group of order 2^4 with $\langle x, s \rangle' = \langle x_0z \rangle$ and $\langle x, s \rangle/\langle z \rangle \cong D_8$, contrary to our assumption that $G/\langle z \rangle$ is modular. \square

Lemma 79.12. *Let G be a W_b -group with respect to N . Suppose in addition that $\Omega_1(G) = N$. Then for each element $g \in G$ such that $G = \langle N, g \rangle$, $N \cap \langle g \rangle = \langle g_0 \rangle$ is of order 2 and $G/\langle g_0 \rangle$ is also a W_b -group (and so $G/\langle g_0 \rangle$ is nonmodular).*

Proof. It is enough to show that $\langle g \rangle$ is not normal in G (because then $\langle g \rangle/\langle g_0 \rangle$ is also not normal in $G/\langle g_0 \rangle$). Suppose false. Then $G' \leq N \cap \langle g \rangle = \langle g_0 \rangle$ and so $G' = \langle g_0 \rangle$. We have $|G : C_G(g)| = 2$ and let t be an involution in $N - C_N(g)$. If $o(g) = 4$, then $\langle g, t \rangle \cong D_8$ and so gt is an involution in $G - N$, a contradiction. Hence $o(g) > 4$ and $\langle g, t \rangle \cong M_{2^n}$, $n \geq 4$. If V is a complement of $\langle g_0 \rangle$ in $C_N(g)$, then $G = V \times \langle g, t \rangle$. But then G is modular (see Proposition 79.6), a contradiction. \square

Proof of the Main Theorem

Let G be a nonmodular quaternion-free 2-group of a smallest possible order which is not isomorphic to any Wilkens group. Hence any proper nonmodular subgroup and any proper nonmodular factor group is isomorphic to a Wilkens group. We shall study such a minimal counter-example G and our purpose is to show that such a group G does not exist.

(i) There is a central involution z of G such that $G/\langle z \rangle$ is nonmodular (and so $G/\langle z \rangle$ is isomorphic to a Wilkens group).

Suppose that this is false. Then for each $z \in \Omega_1(Z(G))$, $G/\langle z \rangle$ is modular. Suppose that $z_0 \in \Omega_1(Z(G))$ is such that $G/\langle z_0 \rangle$ is modular. Since G is nonmodular, there is a minimal nonmodular subgroup K of G which is isomorphic to a group of Lemma 79.3. Obviously, K is a W_b -group and so $K \neq G$. Since $G/\langle z_0 \rangle$ is modular, we have $z_0 \in K$. If $K \cong D_8$, then $\langle z_0 \rangle = \Omega_1(Z(G)) = K'$. Suppose that K has a normal elementary abelian subgroup $E = \langle n, z, t \rangle$ of order 8 such that $K = \langle E, x \rangle$, $o(x) = 2^{s+1}$, $s \geq 1$, $E \cap \langle x \rangle = \langle n \rangle$, $t^x = tz$, $z^x = zn^\epsilon$, $\epsilon = 0, 1$, $\Omega_1(K) = E$, and in case $\epsilon = 1$ we have $s > 1$ and $Z(K) = \langle x^4 \rangle$. If $\epsilon = 1$, then we must have $z_0 = n$. But then $K/\langle z_0 \rangle$ is nonmodular since $K/\langle x^2 \rangle \cong D_8$. Hence we have $\epsilon = 0$ in which case K is minimal nonabelian nonmetacyclic with $Z(K) = \langle x^2, z \rangle = \Phi(K)$ and $K' = \langle z \rangle$. Since $K/\langle z_0 \rangle$ is modular (and $K/\langle n \rangle$ is nonmodular), we have either $z_0 = z$ (and then $K/\langle z_0 \rangle$ is abelian) or $z_0 = zn$ (in which case $s > 1$ and $K/\langle zn \rangle \cong M_{2^{s+2}}$).

Let H be a maximal subgroup of G containing K . Since H is nonmodular and $H \neq G$, H is a Wilkens group. Since $H/\langle z_0 \rangle$ is modular, we may use Proposition 79.11. If $H/\langle z_0 \rangle$ is nonabelian, then there is another involution z'_0 in $Z(H)$ such that $\langle z'_0 \rangle$ is a characteristic subgroup in H and $H/\langle z'_0 \rangle$ is nonmodular. But then $z'_0 \in Z(G)$

and $G/\langle z'_0 \rangle$ is nonmodular, contrary to our assumption. Hence $H/\langle z_0 \rangle$ must be abelian and so $K/\langle z_0 \rangle$ is also abelian. In particular, $z_0 = z$, where $\langle z \rangle = K'$. In any case $\Omega_1(Z(G)) = \langle z \rangle$ is of order 2. By Proposition 79.11(a), we have $H = D \times E_0$, where $\exp(E_0) \leq 2$ and

$$D = \langle y, t \mid y^{2^m} = t^2 = 1, m \geq 1, [y, t] = z, z^2 = [z, y] = [z, t] = 1 \rangle.$$

If $m = 1$, then $D \cong D_8$ and if $m > 1$, then D is minimal nonabelian nonmetacyclic with $E_8 \cong \Omega_1(D) \not\leq Z(D)$ and $z = z_0$, where $\langle z \rangle = D' = H' = \Omega_1(Z(G))$.

Suppose $m = 1$. Then $Z(H) = \langle z \rangle \times E_0$ is elementary abelian. If $|E_0| \geq 4$, then acting with an element $x \in G - H$ on $Z(H)$, we see that $|C_{Z(H)}(x)| \geq 4$ and $C_{Z(H)}(x) \leq Z(G)$, contrary to the fact that $\Omega_1(Z(G))$ is of order 2. Hence $|E_0| \leq 2$. If $D = H \cong D_8$, then $C_G(D) \leq D$ would imply that G is of maximal class and then $G/\langle z \rangle \cong D_8$, a contradiction. If $D = H \cong D_8$ and $C_G(D) \not\leq D$, then Lemma 79.1 implies that $G \cong D_8 \times C_2$, contrary to $|\Omega_1(Z(G))| = 2$. Hence we must have $H = D \times \langle t \rangle$, where t is an involution with $C_G(t) = H$. Since $H/\langle z \rangle$ is elementary abelian, $\exp(G/\langle z \rangle) \leq 4$ and therefore $G/\langle z \rangle$ is abelian since $G/\langle z \rangle$ is modular (and Q_8 -free) of exponent ≤ 4 . In particular, D is normal in G . We have $C_H(D) = \langle z, t \rangle$. If $C_G(D) > \langle z, t \rangle$, then $C_G(t) = G$, a contradiction. Hence $C_G(D) = \langle z, t \rangle$ and $\text{Aut}(D_8) \cong D_8$ implies that $G/\langle z, t \rangle \cong D_8$, a contradiction: $G/\langle z \rangle$ is modular.

Suppose $m > 1$. Here $Z(D) = \Phi(D) = \langle y^2, z \rangle$ is abelian of type $(2^{m-1}, 2)$ and $Z(H) = \langle y^2, z \rangle \times E_0$ so that $\Omega_1(Z(H)) = \langle y^4 \rangle$. If $m > 2$, then $\Omega_1(\langle y^4 \rangle)$ is of order 2 and $\Omega_1(\langle y^4 \rangle) \leq Z(G)$, contrary to the fact that $\Omega_1(Z(G)) = \langle z \rangle$. Thus we have $m = 2$, $|D| = 2^4$, and $Z(H) = \langle y^2, z \rangle \times E_0$ is elementary abelian. Suppose that $E_0 \neq \{1\}$. Then acting with an element $x \in G - H$ on $Z(H)$, we get $|C_{Z(H)}(x)| \geq 4$ and $C_{Z(H)}(x) \leq Z(G)$, a contradiction. It follows $D = H$ and so $|G| = 2^5$.

If $x \in G - H$ is of order 8, then $x^4 \in Z(H) - \langle z \rangle$ (with $\langle z \rangle = H'$) since $\Phi(H) = Z(H)$ and z is not a square in H . But then $Z(H) \leq Z(G)$, a contradiction. Hence $\exp(G) = 4$ and the fact that $G/\langle z \rangle$ is modular gives that $G/\langle z \rangle$ is abelian. It follows $G' = H' = \langle z \rangle$. Since $H = D = \langle y, t \rangle$ and $|G : C_G(y)| = |G : C_G(t)| = 2$, we get $|G : C_G(H)| \leq 4$. But $|H : C_H(H)| = |H : Z(H)| = 4$ and so $C_G(H)$ must cover G/H . But then $E_4 \cong Z(H) \leq Z(G)$, a final contradiction.

(ii) The factor group $G/\langle z \rangle$ ($z \in \Omega_1(Z(G))$) is not isomorphic to a W_a -group.

Suppose that this is false. Then $G/\langle z \rangle$ has a maximal normal abelian subgroup $N/\langle z \rangle$ of exponent > 2 such that G/N is cyclic of order ≥ 2 and if $L/N = \Omega_1(G/N)$, then for each element $x \in L - N$, $x^2 \in \langle z \rangle$, and x inverts each element of $N/\langle z \rangle$.

If all elements in $L - N$ are involutions, then each $y \in L - N$ inverts each element in N which implies that N is abelian of exponent > 2 , N is a maximal normal abelian subgroup of G and if $G = \langle N, g \rangle$, then G is a semidirect product of N and $\langle g \rangle$ and the involution in $\langle g \rangle$ inverts N . Thus, G is a W_a -group, a contradiction. Hence, there is $v \in L - N$ with $v^2 = z$.

Let $n \in N$ be of order 8. Then $n^v = n^{-1}z^\epsilon$ ($\epsilon = 0, 1$) and therefore $(n^2)^v = (n^{-1}z^\epsilon)^2 = n^{-2}$, contrary to Lemma 79.1. Thus, $\exp(N) = \exp(N/\langle z \rangle) = 4$.

Suppose that N is abelian. Let s and l be elements of order 4 in N such that $\langle s \rangle \cap \langle l \rangle = \{1\}$. In that case $o(sl) = 4$ and using Lemma 79.1, we get $s^v = s^{-1}z$, $l^v = l^{-1}z$ and consequently $(sl)^v = s^{-1}zl^{-1}z = (sl)^{-1}$, a contradiction. Hence N is abelian of type $(4, 2, \dots, 2)$ and since $\exp(N/\langle z \rangle) = 4$, $z \notin \Omega_1(N)$. We set $\Omega_1(N) = \langle t \rangle$ with $t \neq z$ and so $|N : \Omega_1(N)| = 2$, where each element in $N - \Omega_1(N)$ is of order 4 and has square equal to t . Also, $\langle t \rangle = \Omega_1(N)$ is central in G . Suppose that $a \in N - \Omega_1(N)$ is such that $a^2 = t$ and (by Lemma 79.1) $a^v = a^{-1}z = a(zt)$. By Lemma 79.2, $\langle v, a \rangle$ is minimal nonabelian nonmetacyclic of order 2^4 with $[v, a] = zt$ and va is an involution. Suppose that v does not commute with an involution $u \in \Omega_1(N)$. Then $u^v = uz$, $o(au) = 4$, and $(au)^v = a^{-1}zuz = (au)^{-1}$, contrary to Lemma 79.1. It follows that $C_N(v) = \Omega_1(N)$, $[\langle v \rangle, N] = \langle tz \rangle$, $L' = \langle tz \rangle$, $\Omega_1(N) = Z(L)$, $\Phi(L) = \langle z, t \rangle$, where $\langle t \rangle = \Omega_1(N)$. We have $L - N = v\Omega_1(N) \cup (va)\Omega_1(N)$, where all elements in $v\Omega_1(N)$ are of order 4 and their squares are equal z and all elements in $(va)\Omega_1(N)$ are involutions. Thus $E = \langle va \rangle \Omega_1(N) = \Omega_1(L)$ is elementary abelian of index 2 in L and also $E = \Omega_1(G)$ (since G/N is cyclic) is the unique maximal normal elementary abelian subgroup of G . Now, L/E is a normal subgroup of order 2 in G/E with cyclic factor group G/L . Thus G/E is abelian. If G/E were cyclic, then the fact that G is not D_8 -free gives that G is a W_b -group, a contradiction. Thus G/E is abelian of type $(2^s, 2)$, $s \geq 1$. If $s > 1$, then we set $K/E = \Omega_1(G/E) \cong E_4$. Since $K \geq L$, K is not D_8 -free and so $K < G$ implies that K must be a Wilkens group. But $E = \Omega_1(K)$ and K/E is noncyclic, a contradiction (see Propositions 79.8 to 79.10). Hence $s = 1$, $G/E \cong E_4$, and so $\exp(G) = 4$. We have $G/N \cong C_4$ and so for each $x \in G - L$, $x^2 \in L - N$ and so $x^2 \in E - N$. Since the square of each element in G is contained in $\langle z \rangle$ or $\langle t \rangle$ or in $E - N$, it follows that tz is not a square in G . Hence $\Omega_1(G/\langle tz \rangle) = E/\langle tz \rangle$. If $G/\langle tz \rangle$ were nonmodular, then $G/\langle tz \rangle$ must be a Wilkens group and then $(G/\langle tz \rangle)/(E/\langle tz \rangle) \cong G/E$ must be cyclic, a contradiction. It follows that $G/\langle tz \rangle$ is modular and since $\exp(G) = 4$, $G/\langle tz \rangle$ is abelian and so $G' = \langle tz \rangle$. Suppose that $x \in G - L$ is such that $x^2 = E - N$. Then $[v, x] \in \langle tz \rangle$ and so $[v, x^2] = [v, x]^2 = 1$. But then v centralizes E and since $L = \langle E, v \rangle$, we get that L is abelian, a contradiction. Thus, N is nonabelian and so $N' = \langle z \rangle$.

The subgroup N is nonmodular because a Q_8 -free modular 2-group of exponent 4 is abelian. Let S be a minimal nonabelian subgroup of N . Then $S' = \langle z \rangle$ and S is normal in N . Since v inverts $N/\langle z \rangle$, v normalizes S and so S is normal in $L = \langle N, v \rangle$. Since $\exp(S) = 4$ and S is Q_8 -free, it follows that either $S \cong D_8$ or S is minimal nonabelian nonmetacyclic of order 2^4 . If $S \cong D_8$, then $\Omega_1(S) = \langle z \rangle$ and $N' = \langle z \rangle$ implies that $C_N(S)$ covers N/S . In that case, Lemma 79.1 implies that $C_N(S)$ is elementary abelian and so $\Omega_1(N) = \langle z \rangle$, contrary to $\exp(N/\langle z \rangle) > 2$. It follows that we have the second possibility:

$$S = \langle a, t \mid a^4 = t^2 = 1, [a, t] = z, z^2 = [a, z] = [t, z] = 1 \rangle.$$

We put $b = at$ and compute $b^2 = a^2t^2[t, a] = a^2z$, so that $S' = \langle z \rangle$, $o(b) = 4$,

$\langle a \rangle \cap \langle b \rangle = \{1\}$, and $S = \langle a, b \rangle$ with $[a, b] = a^2b^2 = z$. Again, since $N' = S' = \langle z \rangle$, we get that $C_N(S)$ covers N/S and $C_N(S) \cap S = Z(S) = \Phi(S) = \langle z, a^2 \rangle$. Suppose that $y \in C_N(S)$ is of order 4. Since $\langle a \rangle \cap \langle b \rangle = \{1\}$, there is an $s \in \langle a, b \rangle$ so that $\langle s \rangle \cap \langle y \rangle = \{1\}$ and $o(sy) = 4$. We get $(sy)^v = s^{-1}zy^{-1}z = s^{-1}y^{-1} = (sy)^{-1}$, contrary to Lemma 79.1. Thus, $C_N(S)$ is elementary abelian and $N = SC_N(S)$, $S \cap C_N(S) = Z(S)$ and so the structure of N is completely determined.

We act with $\langle v \rangle$ on $S = \langle a, b \rangle$ and get (using Lemma 79.1) $a^v = a^{-1}z = a(a^2z)$, $b^v = b^{-1}z = ba^2$, which together with $v^2 = z$ determines uniquely the structure of $T = S\langle v \rangle$.

Suppose that v does not centralize $C_N(S) = Z(N)$. Then there is an involution $s \in C_N(S) - S$ such that $s^v = sz$. Then $o(as) = 4$ and $(as)^v = a^{-1}zs = (as)^{-1}$, contrary to Lemma 79.1. Hence $C_N(S) = C_N(T)$ and $L = TC_L(T)$ with $T \cap C_L(T) = Z(T) = \langle z, a^2 \rangle$.

We have $\Omega_1(S) = \langle z, a^2, ab \rangle \cong E_8$, $\langle z, a^2 \rangle = Z(T)$,

$$\begin{aligned} (av)^2 &= avav = av^2v^{-1}av =aza^{-1}z = 1, \\ (ab)^{av} &= (abz)^v = a^{-1}zb^{-1}zz = a^{-1}b^{-1}z = aa^2bb^2z \\ &= aba^2(a^2z)z = ab. \end{aligned}$$

Hence $F = \langle z, a^2, ab, av \rangle \cong E_{24}$ is an elementary abelian maximal subgroup of T and so from $T' \geq \langle z, a^2 \rangle$ and $|T| = 2^5 = 2|T'||Z(T)|$ follows that $T' = Z(T) = \langle z, a^2 \rangle$. Finally, $T/\langle z, a^2 \rangle$ is elementary abelian and therefore $Z(T) = T' = \Phi(T) \cong E_4$ and so T is a special group of order 2^5 . For each $x \in T - F$, $C_F(x) = Z(T)$ and so the set $T_0 = T - F$ has exactly four square roots of z , four square roots of a^2 , four square roots of za^2 and so T_0 must contain exactly four involutions in $T - S$. If t_0 is one of them, then $C_F(t_0) = Z(T)$, and F and $\langle z, a^2, t_0 \rangle \cong E_8$ are the only maximal normal elementary abelian subgroups of T (containing all involutions of T).

We have $C_N(S) = C_N(T) = Z(L)$ and so if we set $U = FZ(L)$ and $V = \langle z, a^2, t_0 \rangle Z(L)$, then $L = UV$, $U \cap V = Z(L)$, U and V are the only maximal normal elementary abelian subgroup of L and they are of distinct orders and so U and V are normal in G and $|U : Z(L)| = 4$, $|V : Z(L)| = 2$, $L' = \Phi(L) = \langle z, a^2 \rangle$. For each $t_0 \in V - Z(L)$, $C_U(t_0) = Z(L)$ and so both U and V are self-centralizing in L . Also, U is the unique abelian maximal subgroup of L (otherwise, by a result of A. Mann, $|L'| \leq 2$). Now, G/N is cyclic, $L/N = \Omega_1(G/N)$, and so $\Omega_1(G) = L$, which is a W_b -group with respect to U . In particular, $L < G$.

If G/U is cyclic, then (since G is not D_8 -free) G is a W_b -group, a contradiction. Hence G/U is noncyclic. But $L/U \leq Z(G/U)$ and G/L is cyclic (since $L \geq N$ and G/N is cyclic) and so G/U is abelian of type $(2^n, 2)$. Set $K/U = \Omega_1(G/U) \cong E_4$. If $G \neq K$, then K is a Wilkens group with $\Omega_1(K) = L$. By the structure of L , L has no abelian maximal subgroups of exponent > 2 and so K is not a W_a -group. Also, $|K : \Omega_1(K)| = 2$ and so K is not a W_c -group. Hence K must be a W_b -group with respect to U . But $K/U \cong E_4$, a contradiction. Hence $G = K$ and so $G/U \cong E_4$

implies $\exp(G) = 4$. Since $\Omega_1(G) = L$, all elements in $G - L$ are of order 4 and if $x \in G - L$, then $x^2 \in U - N$, where $N = \langle Z(L), ab, a \rangle$ and $U \cap N = Z(L) \times \langle ab \rangle$.

If $C_G(V) > V$, then $C_L(V) = V$ implies that there is $y \in G - L$ with $y^2 \in V$, contrary to $y^2 \in U - N$. We have proved that $C_G(V) = V$ and so G/V acts faithfully on V . We have $G/V \cong (U\langle x \rangle)/Z(L)$, where $U/Z(L) \cong E_4$ and $\langle x \rangle Z(L)/(Z(L) \cong C_4)$ with $x \in G - L$. Thus $G/V \cong D_8$ or $G/V \cong C_4 \times C_2$. But $L/V \cong U/Z(L) \cong E_4$ is a four-subgroup in G/V and for each $x \in G - L$, $x^2 \in U - N$ so that $\langle x \rangle \cap V = \{1\}$. Hence all elements in $(G/V) - (L/V)$ are of order 4 and so $G/V \cong C_4 \times C_2$.

If $L' = \langle z, a^2 \rangle = Z(L)$, then $V \cong E_8$. But $G/V \cong C_4 \times C_2$ cannot act faithfully on $V \cong E_8$. We have proved that $Z(L) > L'$ and so $|Z(L)| \geq 8$.

We act with $\langle x \rangle$ on $Z(L)$, where $x \in G - L$. Since $x^2 \in L$, $\langle x \rangle$ induces an automorphism of order ≤ 2 on $Z(L)$. Since $|Z(L)| \geq 8$, it follows that $|C_{Z(L)}(x)| \geq 4$. Suppose that x centralizes an involution $u \in Z(L) - L'$ so that $u \in Z(G)$. Since $G/\langle u \rangle$ is nonabelian and of exponent 4, $G/\langle u \rangle$ must be nonmodular. Thus $G/\langle u \rangle$ is a Wilkens group with $\Omega_1(G/\langle u \rangle) = L/\langle u \rangle$ because $\Omega_1(G) = L$ and u is not a square in G . Then $U/\langle u \rangle$ and $V/\langle u \rangle$ are the only maximal normal elementary abelian subgroups of $G/\langle u \rangle$ and both G/U and G/V are noncyclic and so $G/\langle u \rangle$ cannot be a W_b -group. Also, $G/\langle u \rangle$ cannot be a W_a -group since $\Omega_1(G/\langle u \rangle) = L/\langle u \rangle$ and $|G/L| = 2$. If $G/\langle u \rangle$ is a W_a -group, then (by the first part of the proof of (ii)) L must possess a nonabelian maximal subgroup N_0 containing $\langle u \rangle$ such that $N'_0 = \langle u \rangle$. This is a contradiction since $u \in Z(L) - L'$. We have proved that for each $x \in G - L$, $C_{Z(L)}(x) \leq L'$. Since $|C_{Z(L)}(x)| \geq 4$, we must have $C_{Z(L)}(x) = L' = Z(G) = \langle z, a^2 \rangle$.

Suppose that $x \in G - L$ is such that $x^2 \in U - N$. We have $U = \langle z, a^2, ab, av \rangle Z(L)$ and so $(ab)^{x^2} = ab$. On the other hand, $x^2 \in L - N$ and x^2 inverts $N/\langle z \rangle$. Thus $a^{x^2} = a^{-1}z^\epsilon$, $b^{x^2} = b^{-1}z^\eta$ ($\epsilon, \eta = 0, 1$), and so, noting that $b^2 = a^2z$ we get

$$ab = (ab)^{x^2} = a^{-1}z^\epsilon b^{-1}z^\eta = a^{-1}b^{-1}z^{\epsilon+\eta} = aa^2bb^2z^{\epsilon+\eta} = abz^{1+\epsilon+\eta},$$

which gives $\epsilon + \eta \equiv 1 \pmod{2}$ and so $\epsilon = 1$ or $\eta = 1$.

Suppose $\epsilon = 1$. Then $a^{x^2} = a^{-1}z = a(a^2z)$ and we apply Lemma 79.2 in the group $G/\langle a^2z \rangle = \bar{G}$. We have (using bar convention) $o(\bar{x}) = o(\bar{a}) = 4$ and $[\bar{x}^2, \bar{a}] = 1 = [\bar{x}, \bar{a}^2]$. If $[\bar{x}, \bar{a}] = 1$, then $[x, a] \in \langle a^2z \rangle$ (and $\langle x, a \rangle$ is of class ≤ 2 since $\langle x, a \rangle' \leq \langle a^2z \rangle$) and so $[x^2, a] = [x, a]^2 = 1$, a contradiction. Thus $[\bar{x}, \bar{a}] \neq 1$ and so (by Lemma 79.2) $o(\bar{x}\bar{a}) = 2$. Hence $(xa)^2 \in \langle a^2z \rangle$, contrary to the fact that $xa \in G - L$ and $(xa)^2 \in U - N$.

Let $\eta = 1$. Then $b^{x^2} = b^{-1}z = b(a^2)$ and we apply Lemma 79.2 to $G/\langle a^2 \rangle = \bar{G}$. We have $o(\bar{x}) = o(\bar{b}) = 4$ and $[\bar{x}^2, \bar{b}] = 1 = [\bar{x}, \bar{b}^2]$. If $[\bar{x}, \bar{b}] = 1$, then $[x, b] \in \langle a^2 \rangle$ (and $\langle x, b \rangle$ is of class ≤ 2 since $\langle x, b \rangle' \leq \langle a^2 \rangle$) and so $[x^2, b] = [x, b]^2 = 1$, a contradiction. Thus $[\bar{x}, \bar{b}] \neq 1$ and so (by Lemma 79.2) $o(xb) = 2$. Hence $(xb)^2 \in \langle a^2 \rangle$, contrary to the fact that $xb \in G - L$ and $(xb)^2 \in U - N$. Our claim (ii) is proved.

(iii) $G/\langle z \rangle$ ($z \in \Omega_1(Z(G))$) is not isomorphic to a W_b -group.

Suppose this is false. Then $G/\langle z \rangle$ has a maximal normal elementary abelian subgroup $N/\langle z \rangle$ so that G/N is cyclic and $G/\langle z \rangle$ is not D_8 -free. If N is elementary abelian, then G is a W_b -group with respect to N , a contradiction. Hence N is not elementary abelian and so $\Omega_1(N) = \langle z \rangle$ and $G \neq N$. Set $L/N = \Omega_1(G/N)$.

(α) Let N be abelian. Then $|N : \Omega_1(N)| = 2$ and for each $a \in N - \Omega_1(N)$, $a^2 = z$. Also, $\langle N - \Omega_1(N) \rangle = N$, $\Omega_1(G) \leq L$, and $\Omega_1(G/\langle z \rangle) \leq L/\langle z \rangle$. Let $v \in L - N$ with $v^2 = z$ and let $x \in N - \Omega_1(N)$. By Lemma 79.2, $[v, x] = 1$ and so v centralizes N . But then L is abelian with $\Omega_1(L) = \langle z \rangle$ and $L \triangleleft G$, a contradiction: $N/\langle z \rangle$ is a maximal normal elementary abelian subgroup of $G/\langle z \rangle$. Thus, for each $v \in L - N$, $v^2 \neq z$.

Suppose that for each $x \in L - N$, $x^2 \in N - \Omega_1(N)$. If $G = \langle N, g \rangle$, then $\langle g \rangle$ covers $G/\Omega_1(N)$. But then $G/\Omega_1(N)$ is cyclic and (since G is not D_8 -free) G is a W_b -group, a contradiction. We have proved that there is $x \in L - N$ with $x^2 \in \Omega_1(N)$.

Suppose that there are no involutions in $L - N$. There is $x \in L - N$ such that $x^2 \in \Omega_1(N) - \langle z \rangle$. Suppose that x does not commute with an $a \in N - \Omega_1(N)$. By Lemma 79.2, xa is an involution, a contradiction. Hence x commutes with all elements in $N - \Omega_1(N)$ and therefore L is abelian of type $(4, 4, 2, \dots, 2)$. We have $\Omega_1(L) = \Omega_1(N) = \Omega_1(G)$ and $L/\Omega_1(L) \cong E_4$. Since G is nonabelian, we have $L < G$. Because $N/\Omega_1(N)$ is a normal subgroup of order 2 in $G/\Omega_1(N)$ and G/N is cyclic, $G/\Omega_1(N)$ is abelian of type $(2^s, 2)$, $s \geq 2$. For each $y \in L - N$, $y^2 = x^2$ or $y^2 = x^2z$. Hence, if $g \in G$ is such that $G = \langle N, g \rangle$, then $\Omega_1(\langle g \rangle) = \langle x^2 \rangle$ or $\Omega_1(\langle g \rangle) = \langle x^2z \rangle$ and so $\Omega_1(L) = \langle z, x^2 \rangle \leq Z(G)$. We may assume (by a suitable notation) that $\langle g \rangle \geq \langle x \rangle$. Set $M = \langle g \rangle\Omega_1(N)$ so that M is a maximal subgroup of G . Suppose that $G/\langle x^2 \rangle$ is nonmodular so that it is a Wilkens group. But $\Omega_1(G/\langle x^2 \rangle) = S_0/\langle x^2 \rangle$, where $S_0 = \Omega_1(N)\langle x \rangle$. On the other hand, G/S_0 is noncyclic (since L/S_0 and M/S_0 are two nontrivial cyclic subgroups of G/S_0 with $(L/S_0) \cap (M/S_0) = \{1\}$). This is a contradiction and so $G/\langle x^2 \rangle$ is modular. Since $\Omega_1(G/\langle z \rangle) = N/\langle z \rangle$, we may use Lemma 79.12 and we see that $G/\langle x^2, z \rangle$ is nonmodular. This is not possible since $G/\langle x^2 \rangle$ is modular. Thus, there are involutions in $L - N$.

Let t be an involution in $L - N$. If t centralizes an element $a \in N - \Omega_1(N)$, then $ta \in L - N$ and $(ta)^2 = z$, a contradiction. Thus, $C_N(t) \leq \Omega_1(N)$. For any $x \in L - N$, $C_N(x) = C_N(t)$ and so $x^2 \in \Omega_1(N)$. It follows that $\exp(L) = 4$.

Suppose that t does not centralize $\Omega_1(N)$. Let w be a fixed involution in $\Omega_1(N) - C_N(t)$ and let a be a fixed element in $N - \Omega_1(N)$. We have $w^t = wu$ with $1 \neq u \in C_N(t)$ and $(tw)^2 = (twt)w = wuw = u$ and so $u \in C_N(t) - \langle z \rangle$ (since $tw \in L - N$). Since $C_N(tw) = C_N(t) < \Omega_1(N)$, we have $[tw, a] \neq 1$. By Lemma 79.2, $(tw)a$ is an involution. We get $1 = (twa)^2 = twatwa = w^ta^tw = wua^tw = uaa^t$, and so $a^t = a^{-1}u = aa^2u = a(uz)$. We consider the factor group $L/\langle uz \rangle = \bar{L}$ and we see that $o(\bar{a}) = 4$, $o(\bar{t}) = 2$, $[\bar{a}, \bar{t}] = 1$, $\bar{a}^2 = \bar{z}$. Also, $w^t = wu = wz(uz)$ gives $\bar{w}^{\bar{t}} = \bar{w}\bar{z}$ so that $\langle \bar{w}, \bar{t} \rangle \cong D_8$ with $Z(\langle \bar{w}, \bar{t} \rangle) = \langle \bar{z} \rangle$. Hence $\langle \bar{w}, \bar{t} \rangle \langle \bar{a} \rangle$ is the central product $D_8 * C_4$, contrary to Lemma 79.1 (applied in \bar{L}). We have proved

that t centralizes $\Omega_1(N)$ so that $S = \langle t \rangle \times \Omega_1(N)$ is an elementary abelian maximal subgroup of L . Since L is nonabelian and $\exp(L) = 4$, L is nonmodular.

Let $a \in N - \Omega_1(N)$. Then by Proposition 51.2, $a^t = a^{-1}s$, $s \in \Omega_1(N)$. If $s = 1$, then t inverts N , G/N is cyclic and so G would be a W_a -group, a contradiction. Thus, $s \neq 1$ and $(ta)^2 = (tat)a = a^{-1}sa = s$ and so $s \in \Omega_1(N) - \langle z \rangle$. Set $ta = y$ so that $y^2 = s$ and since $C_N(y) = C_N(t)$, we have for each $n \in C_N(t) = \Omega_1(N)$, $(ny)^2 = n^2y^2 = s$ and $[t, N] = \langle zs \rangle = L'$. The group L has exactly three abelian maximal subgroups: $S = \Omega_1(G)$, N , and $\Omega_1(N)\langle y \rangle$, where only S is elementary abelian and all three are normal in G with $\mathfrak{V}_1(\Omega_1(N)\langle y \rangle) = \langle s \rangle$, $s \in \Omega_1(N) - \langle z \rangle$. We have $\Omega_1(N) = Z(L)$ and z, s and zs are central involutions in G .

If $G = L$, then G would be a W_b -group, a contradiction. Thus $L < G$. Since G/N is cyclic of order 2^s , $s \geq 2$, we have $G = \langle N, g \rangle$ with $g^{2^{s-1}} \in L - N$. If $g^{2^{s-1}} \in L - N - S$, then $\langle g \rangle$ covers G/S , G/S is cyclic and so G would be a W_b -group with respect to S , a contradiction. It follows that $g^{2^{s-1}} \in S - \Omega_1(N)$. If L is not maximal in G , then there is a subgroup $K > L$ with $|K : L| = 2$ and so K is a Wilkens group. Since $S = \Omega_1(K)$ and $K/S \cong E_4$, we have a contradiction. Indeed, $(S\langle g^{2^{s-2}} \rangle)/S$ and L/S are two distinct subgroups of order 2 in K/S . Hence $|G : L| = 2$ and for each $g \in G - L$, $g^2 \in S - \Omega_1(N)$.

We apply now Lemma 79.2 in the group $G/\langle zs \rangle = \bar{G}$, where $\langle zs \rangle = L'$. We have for some elements $g \in G - L$ and $a \in N - \Omega_1(N)$, $o(\bar{g}) = o(\bar{a}) = 4$ and since $a^{g^2} = a(zs)$, we get $[\bar{a}, \bar{g}^2] = 1 = [\bar{a}^2, \bar{g}]$. If $[\bar{g}, \bar{a}] = 1$, then $[g, a] \in \langle zs \rangle$ and so $[g^2, a] = [g, a]^2 = 1$, a contradiction. Hence $[\bar{g}, \bar{a}] \neq 1$ and so (by Lemma 79.2) $o(\bar{g}\bar{a}) = 2$ which gives $(ga)^2 \in \langle zs \rangle$, contrary to $ga \in G - L$ and (by the above) $(ga)^2 \in S - \Omega_1(N)$. We have proved that N must be nonabelian.

(β) Let N be nonabelian.

This case is very difficult. We have $\mathfrak{V}_1(N) = N' = \langle z \rangle$. Let D be a minimal nonabelian subgroup of N so that $D' = \langle z \rangle$. Since $d(D) = 2$ and $D/\langle z \rangle$ is elementary abelian, we have $D/\langle z \rangle \cong E_4$ and therefore $D \cong D_8$. The subgroup D is normal in N and since $D' = N'$, $C_N(D)$ covers N/D . By Lemma 79.1, $C_N(D)$ is elementary abelian. We have $C_N(D) = Z(N)$, $N = DZ(N)$ with $D \cap Z(N) = Z(D) = \langle z \rangle$ so that $Z(N)$ is normal in G . Set $D = \langle a, u \mid a^4 = u^2 = 1, a^2 = z, a^u = a^{-1} \rangle$ so that $A = \langle a, Z(N) \rangle$, $E_1 = \langle u, Z(N) \rangle$, and $E_2 = \langle au, Z(N) \rangle$ are all abelian maximal subgroups of N , where A is of exponent 4 (all elements in $A - Z(N)$ are of order 4, $\mathfrak{V}_1(A) = \langle z \rangle$), and E_1 and E_2 are both elementary abelian. Thus A is normal in G . All elements in $N - A$ are involutions, $Z(N) = \Omega_1(A)$, N is a W_a -group with respect to A and also a W_b -group with respect to E_1 and E_2 .

Since N/A is a normal subgroup of order 2 in G/A and G/N is cyclic, it follows that G/A is abelian. If G/A were cyclic, then we have $G = \langle A, g \rangle$ with some $g \in G$ and since $\Omega_1(\langle g \rangle)$ is of order 2 and inverts A (of exponent > 2), G is a W_a -group, a contradiction. It follows that G/A is abelian of type $(2^m, 2)$, $m \geq 1$, and $L/A \cong E_4$, where $L/N = \Omega_1(G/N)$. Also note that $N/Z(N) \cong E_4$.

Suppose that for each $l \in L - N$, $l^2 \in A - Z(N)$. This is equivalent to assuming that $L/Z(N) \cong C_4 \times C_2$ which also implies that both E_1 and E_2 are normal in L . If $G = \langle N, g \rangle$, then either $E_1^g = E_2$ (in which case $G > L$ and $G/Z(N) \cong M_{2^n}$, $n \geq 4$, and G is a W_c -group) or $E_1^g = E_1$, E_1 is normal in G , $\langle g \rangle$ covers G/E_1 and since G is not D_8 -free, G is a W_b -group. In both cases we have a contradiction.

Thus, $L/Z(N)$ is not isomorphic to $C_4 \times C_2$ and so $L/Z(N)$ is either elementary abelian or $L/Z(N) \cong D_8$. In any case, there is $l \in L - N$ with $l^2 \in Z(N)$.

(β1) Let $L/Z(N) \cong D_8$. Then $E_1^x = E_2$ for $x \in L - N$, and so $G = L$. Indeed, G/N acts on the set $\{E_1, E_2\}$ and so, if $G > L$, then L would normalize E_1 .

Suppose in addition that there are no involutions in $L - N$. Let $l \in L - N$ with $l^2 \in Z(N)$ so that $l^2 \neq 1$ and $o(l) = 4$. Let a_0 be any element in $A - Z(N)$ so that $a_0^2 = z$. If $[l, a_0] \neq 1$, then la_0 is an involution in $L - N$, a contradiction. Thus l centralizes each element in $A - Z(N)$ and since $\langle A - Z(N) \rangle = A$, $A\langle l \rangle$ is an abelian maximal subgroup of $G = L$. Also, $Z(N) = Z(G)$ (since $Z(L/Z(N)) = A/Z(N)$) and so we may use the relation $|G| = 2|G'||Z(G)|$ which gives $|G'| = 4$. But G' covers $A/Z(N) = (G/Z(N))'$ and so $G' \cong C_4$ is a cyclic subgroup of order 4 in A inverted by u (since u inverts A) and so we have $G'\langle u \rangle \cong D_8$. We may assume $G' = \langle a \rangle < D \cong D_8$ so that D is normal in G . By Lemma 79.1, $C_G(D)$ is elementary abelian and so $C_G(D)$ cannot cover G/N (since there are no involutions in $G - N$). Hence $C_G(D) = Z(N)$ and so $l \in G - N$ induces an outer automorphism on D . Hence $a^l = a^{-1}$, contrary to Lemma 79.1.

We have proved that there are involutions in $G - N$ and let t be one of them so that $\Omega_1(G) = G$. Since $G/Z(N) \cong D_8$, there is $k \in G - N$ such that $k^2 \in A - Z(N)$. Our ultimate goal is to show that $Z(N) = Z(G)$. Suppose $Z(N) \neq Z(G)$.

Assume there is $s \in G - N$ with $s^2 = z$ and let $a_0 \in A - Z(N)$. If $[s, a_0] \neq 1$, then (Lemma 79.2) $[s, a_0] = s^2 a_0^2 = zz = 1$, a contradiction. Thus s centralizes $A - Z(N)$ and $\langle A - Z(N) \rangle = A$ and so $Z(N) \leq Z(G)$. Since $Z(G/Z(N)) = A/Z(N)$, we have $Z(N) = Z(G)$. This is a contradiction and so there is no $s \in G - N$ with $s^2 = z$. In particular, the involution t does not centralize any element in $A - Z(N)$.

Now, $A\langle t \rangle < G$ maximal. If $x \in At$ is of order 8, then $o(x^2) = 4$ and $x^2 \in A - Z(N)$. But then t centralizes x^2 (noting that $C_A(t) = C_A(x)$), a contradiction. Hence $\exp(A\langle t \rangle) = 4$ and since $A\langle t \rangle$ is nonabelian, $A\langle t \rangle$ is nonmodular and therefore $A\langle t \rangle$ must be a Wilkins group. If X is an abelian maximal subgroup of $A\langle t \rangle$ distinct from A , then $X \cap A \leq Z(N)$ (recalling that t does not commute with any element in $A - Z(N)$) and since $|A : (X \cap A)| = 2$, we get $X \geq Z(N)$ and so $Z(N) = Z(G)$, a contradiction. Hence A is the unique abelian maximal subgroup of $A\langle t \rangle$.

If all elements in $(A\langle t \rangle) - A$ are involutions, then t inverts each element of A and so t centralizes $Z(N)$ and then $Z(N) = Z(G)$, a contradiction. It follows that there is an element c of order 4 in At such that $c^2 \in Z(N) - \{z\}$. But $[c, a] \neq 1$ (since t does not centralize a) and so (by Lemma 79.2) ac is an involution for each $a \in A - Z(N)$. Since t does not centralize $Z(N)$ (otherwise $Z(N) = Z(G)$), $Z(N)\langle t \rangle$ contains less than $2|Z(N)| - 1$ involutions. All $|Z(N)|$ elements ca ($a \in A - Z(N)$) are involutions and

so $A\langle t \rangle$ contains at least $2|Z(N)| - 1$ involutions. This shows that $\Omega_1(A\langle t \rangle) = A\langle t \rangle$. Since A (of exponent > 2) is the unique abelian maximal subgroup of $A\langle t \rangle$, $A\langle t \rangle$ must be a W_a -group. In that case t inverts A and so t centralizes $Z(N)$ and $Z(N) = Z(G)$, a contradiction.

We have proved that $Z(N) = Z(G)$ and so $Z(N)\langle k \rangle = A\langle k \rangle$ is an abelian maximal subgroup of G (noting that $k^2 \in A - Z(N)$ and so $Z(N)\langle k \rangle/Z(N)$ is cyclic). Using the relation $|G| = 2|G'||Z(G)|$ we get $|G'| = 4$ and so $G' \cong C_4$ (since G' covers $A/Z(N)$). We may assume (as before) that $G' \leq D$ and so D is normal in G with $C_G(D) = Z(N)$ (since $C_G(D)$ is elementary abelian and $|G : Z(G)| = 8$). The involution t induces an outer automorphism on D and so $D\langle t \rangle \cong D_{2^4}$. It follows that $G = (D\langle t \rangle) \times E_{2^m}$ for some $m \geq 1$, which is a W_a -group, a contradiction.

($\beta 2$) We have proved that we must have $L/Z(N) \cong E_8$ and so $\exp(L) = 4$.

In that case we prove first that there are involutions in $L - N$. Suppose false. If v is any element in $L - N$ and $a_0 \in A - Z(N)$, then $1 \neq v^2 \in Z(N)$ and $a_0^2 = z$ so that we may apply Lemma 79.2. If $[v, a_0] \neq 1$, then va_0 is an involution, a contradiction. Hence $L = \langle L - N \rangle$ centralizes $A = \langle A - Z(N) \rangle$. In particular, $A \leq Z(N)$ which contradicts the fact that $Z(N) < A$. We have proved that there are involutions in $L - N$ and so $L = \Omega_1(L) = \Omega_1(G)$ (noting that G/N is cyclic and $L/N = \Omega_1(G/N)$).

Assume $C_G(D) > Z(N)$ so that $C_G(D)$ covers L/N and (Lemma 79.1) $C_G(D)$ is elementary abelian. In that case, $L \cong D_8 \times E_{2^m}$ and $\Omega_1(L) = \langle z \rangle$ which contradicts our assumption that $N/\langle z \rangle$ is a maximal normal elementary abelian subgroup of $G/\langle z \rangle$. Hence $C_G(D) = Z(N)$. If D were normal in L , then $L/Z(N) \cong D_8$ since $\text{Aut}(D) \cong D_8$. This is a contradiction and so $N_G(D) = N$. In particular, $Z(L) \leq Z(N)$ and $Z(N) > \langle z \rangle$.

($\beta 2a$) We assume that $G > L$. Then $L = \Omega_1(L)$ (being nonmodular) is a W_a - or W_b -group. In particular, L has an abelian maximal subgroup B . Since $B \cap N$ is an abelian maximal subgroup of N , we get $B \cap N \in \{A, E_1, E_2\}$. Hence $B \cap N \geq Z(N)$ and so $Z(N) \leq Z(L)$. By the result in the previous paragraph, we get $Z(N) = Z(L)$. Since $|L : Z(L)| = 8$, B is the unique abelian maximal subgroup of L and so B is normal in G . Using the relation $|L| = 2|L'||Z(L)|$, we get $|L'| = 4$. Since $L' \leq Z(L)$, $L' \cong E_4$ and $L' > \langle z \rangle$.

It is easy to see that $|G : L| = 2$. Suppose that this is false. Let $K < G$ be such that $|K : L| = 2$. Since $L = \Omega_1(K)$, K must be a W_a - or W_b -group. By the uniqueness of B in L , follows that K/B is a cyclic group (of order 4). Since $N < L$ and G/N is cyclic, G/L is cyclic. But L/B is a normal subgroup of order 2 in G/B and so G/B is abelian. We have $L/B \leq \Omega_1(G/B)$. On the other hand, G/L is cyclic and $K/L = \Omega_1(G/L)$ so that $\Omega_1(G/B) \leq K/B$. Since $K/B \cong C_4$, we get $\Omega_1(G/B) \leq L/B$ and so $\Omega_1(G/B) = L/B$. Hence G/B is cyclic. If L is of type (a) (in the case $\exp(B) > 2$), then all elements in $L - B$ are involutions and so G is also a W_a -group, a contradiction. If L is of type (b), then B must be elementary abelian and (since G is not D_8 -free) G is also a W_b -group, a contradiction. We have proved that $|G : L| = 2$ and $G/B \cong E_4$ (because in case $G/B \cong C_4$,

G would be a W_a - or W_b -group). But $G/N \cong C_4$ and so for each $x \in G - L$, $x^2 \in B - N$.

We assume first that $\exp(B) > 2$. Then L is a W_a -group. In that case $B/Z(N) \cong E_4$, all elements in $L - B$ are involutions and $\Omega_1(B) = Z(N)$. Indeed, if $|B : \Omega_1(B)| = 2$, then acting by conjugation with an involution in $L - B$ on B , we see that $|L'| = 2$, a contradiction. Hence we must have $\Omega_1(B) = Z(N)$ so that B is abelian of type $(4, 4, 2, \dots, 2)$, $B \cap N = A$, u inverts B , each element in $B - N$ is of order 4, and if $k \in B - N$, then $k^2 = z_0 \in L' - \langle z \rangle$ (noting that $k^u = k^{-1}$ and so $k^2 \in L'$) and $L'\langle a, k \rangle = \langle a, k \rangle \cong C_4 \times C_4$ (if $k^2 = z$, then ak would be an involution in $B - N$, contrary to $\Omega_1(B) = Z(N)$). Let $x \in G - L$ so that $x^2 \in B - N$ and we may assume that $x^2 = k$, where $k^2 = z_0 \in L' - \langle z \rangle$. In particular, $C_G(z_0) \geq \langle L, x \rangle = G$ and so $L' \leq Z(G)$. Let x' be an arbitrary element in $G - L$ so that $(x')^2 = k' \in B - N$ and $(k')^2 = z' \in L' - \langle z \rangle$. Consider the factor group $\tilde{G} = G/\langle z' \rangle$. We have $o(\bar{a}) = o(\bar{x}') = 4$ and $[\bar{a}^2, \bar{x}'] = 1 = [\bar{a}, (\bar{x}')^2]$ and so we may use Lemma 79.2. If $[\bar{a}, \bar{x}'] \neq 1$, then $o(\bar{a}\bar{x}') = 2$ and so $(ax')^2 \in \langle z' \rangle \leq N$, a contradiction. Hence we must have $[\bar{a}, \bar{x}'] = 1$ and so $[a, x'] \in \langle (x')^4 \rangle$. It follows that $[a, x] = z_0^\epsilon$ ($\epsilon = 0, 1$). Consider the element $y = xu \in G - L$; then $[a, y] = [a, xu] = [a, u][a, x]^u = zz_0^\epsilon \neq 1$. On the other hand, $[a, y] \in \langle y^4 \rangle$, $y^4 \in L' - \langle z \rangle$. Thus $\epsilon = 1$ and $y^4 = zz_0$. Finally, consider the factor group $\tilde{G} = G/\langle zz_0 \rangle$ so that $o(\tilde{y}) = o(\tilde{k}) = 4$ and $[\tilde{y}, \tilde{k}^2] = 1 = [\tilde{y}^2, \tilde{k}]$ and apply again Lemma 79.2. Since $[k, x] = 1$, we get $[k, y] = [k, xu] = [k, u][k, x]^u = k^2 = z_0$, and so $[\tilde{k}, \tilde{y}] \neq 1$. Thus $o(\tilde{k}\tilde{y}) = 2$ and so $(ky)^2 \in \langle zz_0 \rangle \leq N$. This is a contradiction since $ky \in G - L$.

We study now the case $\exp(B) = 2$ and L is a W_b -group. We may assume that $B \cap N = E_1$. Since $G/B \cong E_4$, $\exp(G) = 4$. Let t be an involution in $B - N$. Since $B \geq E_1 = Z(N)\langle u \rangle$, t centralizes $u \in D$. But $N_L(D) = N$ and so $[a, t] \in L' - \langle z \rangle$. Suppose that $L' \leq Z(G)$. Let $x \in G - L$ so that $x^2 \in B - N$ and (by the above) $[a, x^2] = z_0 \in L' - \langle z \rangle$. Consider the factor group $G/\langle z_0 \rangle = \tilde{G}$ so that $o(\bar{a}) = o(\bar{x}) = 4$. If $[\bar{x}, \bar{a}] = 1$, then $[x, a] \in \langle z_0 \rangle$. But $\langle x, a \rangle' = \langle z_0 \rangle$ and so $\langle x, a \rangle$ is of class 2. Thus $[x^2, a] = [x, a]^2 = 1$, a contradiction. Hence $[\bar{x}, \bar{a}] \neq 1$ and so (by Lemma 79.2) $o(\bar{x}\bar{a}) = 2$, which gives $(xa)^2 \in \langle z_0 \rangle$, contrary to $xa \in G - L$ and $(xa)^2 \in B - N$. We have proved that $L' \not\leq Z(G)$. Again, let $x \in G - L$ so that $\langle x \rangle$ induces an involutory automorphism on $Z(L) = Z(N)$. Suppose $Z(N) > L'$. Then there is an involution $z' \in Z(L) - L'$ centralized by x and so $z' \in Z(G)$. Since $G/\langle z' \rangle$ is nonmodular (noting that $D \cap \langle z' \rangle = \{1\}$), $G/\langle z' \rangle$ is a Wilkins group. All squares of elements of G lie either in $B - N$ or in L' . Indeed, let as ($s \in B$) be any element in $L - B$. Then $(as)^2 = a^2(a^{-1}sas) = z[a, s] \in L'$. Therefore z' is not a square of any element in G which implies $L/\langle z' \rangle = \Omega_1(G/\langle z' \rangle)$. Let $y \in L$ be such that $[y, L] \leq \langle z' \rangle$. But $\langle z' \rangle \cap L' = \{1\}$ and so $[y, L] = \{1\}$ and therefore $y \in Z(L)$. Hence $Z(L/\langle z' \rangle) = Z(L)/\langle z' \rangle$. Since $|L : Z(L)| = 8$, the elementary abelian group $B/\langle z' \rangle$ is the unique abelian maximal subgroup of $L/\langle z' \rangle$. It follows that $G/\langle z' \rangle$ must be a W_b -group with respect to $B/\langle z' \rangle$. But then G/B must be cyclic, a contradiction. We have proved that $L' = Z(L)$ and so $|G| = 2^6$. Now,

$A = \langle a \rangle \times \langle z_0 \rangle = \langle a \rangle L' \cong C_4 \times C_2$ is normal in G and is self-centralizing in L (since B is the unique abelian maximal subgroup of L). If $C_G(A) \not\leq L$, then there is $g \in C_G(A) - L$ such that $g^2 \in A \leq N$, contrary to $g^2 \in B - N$. Thus A is self-centralizing in G and so $G/A \cong D_8$ since $\text{Aut}(A) \cong D_8$. On the other hand, N/A is a normal subgroup of order 2 in G/A and $G/N \cong C_4$ so that G/A is abelian. This is a contradiction. We have proved that the case $G > L$ is not possible.

($\beta 2b$) It remains to study the case $G = L = \Omega_1(G)$. Since $G/Z(N) \cong E_8$, $\exp(G) = 4$. If for each $x \in G - N$, $x^2 \in \langle z \rangle$, then $G/\langle z \rangle$ is elementary abelian, contrary to our assumption that $N/\langle z \rangle$ is a maximal normal elementary abelian subgroup of $G/\langle z \rangle$. Hence there is $k \in G - N$ such that $k^2 \in Z(N) - \langle z \rangle$. It follows that $k^2 \in Z(G)$ and so $\langle z \rangle < Z(G) \leq Z(N)$.

Let $z' \in Z(G) - \langle z \rangle$. Since $G/\langle z' \rangle$ is nonmodular (noting that $D \cap \langle z' \rangle = \{1\}$ with $D \cong D_8$), it follows that $G/\langle z' \rangle$ is a Wilkens group with $\Omega_1(G/\langle z' \rangle) = G/\langle z' \rangle$ and so $G/\langle z' \rangle$ cannot be a W_c -group. Hence $G/\langle z' \rangle$ must be a W_b -group by our previous result (ii). Thus, G has a maximal subgroup N_1 containing z' such that $N_1/\langle z' \rangle$ is a maximal normal elementary abelian subgroup of $G/\langle z' \rangle$. By our previous result (iii)(α), $\langle z' \rangle = \mathfrak{U}_1(N_1) = N'_1$ (since N_1 must be nonabelian). In particular, z' is a square of an element in $G - N$ and z' is a commutator in G . Conversely, if $k \in G - N$, then $k^2 \in Z(G)$ so that $\Phi(G) \leq Z(G)$. Hence $Z(G) = G' = \Phi(G)$ and so G is a special group. Now, $N \cap N_1$ is a maximal subgroup of N and since $\mathfrak{U}_1(N \cap N_1) \leq \langle z \rangle \cap \langle z' \rangle = \{1\}$, $N \cap N_1$ is elementary abelian and so $N \cap N_1 = E_1$ (or E_2) containing $Z(N)$ and (by the structure of $N_1 \cong N$) $Z(N_1)$ is a subgroup of index 2 in $N \cap N_1$. But $Z(N) \cap Z(N_1) \leq Z(G)$ and so $|Z(N) : Z(G)| \leq 2$.

Let $|Z(N) : Z(G)| = 2$ and let s be an involution in $Z(N) - Z(G)$. Let t be an involution in $G - N$. We have $[t, s] = s_0$ with $s_0 \in Z(G)$ and $s_0 \neq 1$ since $Z(N) \neq Z(G)$. If $n \in N$, then $[tn, s] = [t, s][n, s] = [t, s] = s_0 \in Z(G)$. Hence, for each $x \in G - N$, $[x, s] = s_0$, where s_0 is a fixed involution in $Z(G)$. Take an involution $z' \in Z(G) - \langle z \rangle$. Let N_1 be a maximal subgroup of G such that $\langle z' \rangle = \mathfrak{U}_1(N_1) = N'_1$. Then $N \cap N_1$ is an elementary abelian maximal subgroup of N containing $Z(N)$. If $f_1 \in N_1 - N$, then $[f_1, s] = z' = s_0$. Let N_2 ($\neq N_1$) be a maximal subgroup of G such that $\langle zz' \rangle = \mathfrak{U}_1(N_2) = N'_2$. Then again, $N \cap N_2 \geq Z(N)$ and if $f_2 \in N_2 - N$, then $[f_2, s] = zz' = s_0$. Hence $zz' = z'$ and so $z = 1$, a contradiction.

We have proved that $Z(N) = Z(G)$. Suppose that $Z(G)$ possesses a four-subgroup $\langle z_1, z_2 \rangle$ such that $\langle z_1, z_2 \rangle \cap \langle z \rangle = \{1\}$ (which is equivalent with the assumption $|Z(G)| \geq 8$). Let $k_1, k_2 \in G - N$ be such that $k_1^2 = z_1$ and $k_2^2 = z_2$. Suppose that k_1 centralizes all elements (of order 4) in $A - Z(N)$. Then k_1 centralizes $A = Z(N)\langle a \rangle = \langle A - Z(N) \rangle$ and so $A\langle k_1 \rangle$ is an abelian maximal subgroup of G . Using a result of A. Mann (Lemma 79.5 with respect to maximal subgroups $A\langle k_1 \rangle$ and N), we get $|G'| \leq 4$. But $G' = Z(G)$ is of order ≥ 8 , a contradiction. We may assume that $[a, k_1] \neq 1$ and so (Lemma 79.2) $[a, k_1] = a^2 k_1^2 = zz_1$. We have either $[a, k_2] = 1$ or $[a, k_2] \neq 1$ in which case (Lemma 79.2) $[a, k_2] = a^2 k_2^2 = zz_2$. We have $[a, k_1 k_2] = [a, k_1][a, k_2] = zz_1[a, k_2]$, and so either $[a, k_1 k_2] = zz_1$

or $[a, k_1 k_2] = z z_1 z z_2 = z_1 z_2$. But the element $k_1 k_2$ is contained in N and so $[a, k_1 k_2] \in \langle z \rangle$, a contradiction.

We have proved that we must have $Z(N) = Z(G) \cong E_4$ and so $|G| = 2^5$. Let $z' \in Z(G) - \langle z \rangle$ and let $k_1, k_2 \in G - N$ be such that $k_1^2 = z'$ and $k_2^2 = z z'$. Suppose $[k_1, k_2] = 1$ so that $\langle k_1, k_2 \rangle \cong C_4 \times C_4$, $k_1 k_2 \in N$ and $(k_1 k_2)^2 = k_1^2 k_2^2 = z$ and therefore we may assume that $k_1 k_2 = a$. Hence $\langle k_1, k_2 \rangle$ is an abelian maximal subgroup of G normalized by u , where u inverts each element in

$$\langle k_1, k_2 \rangle \cap N = \langle a \rangle \times \langle z' \rangle \cong C_4 \times C_2 \quad \text{and} \quad G = \langle k_1, k_2 \rangle \langle u \rangle.$$

We know that there are involutions in $G - N$ and so there is an element $k \in \langle k_1, k_2 \rangle - N$ such that uk is an involution. This gives $(uk)^2 = ukuk = 1$, $k^u = k^{-1}$ and so u inverts each element of the abelian group $\langle k_1, k_2 \rangle$. In this case G is a W_a -group, a contradiction. Hence $[k_1, k_2] \neq 1$ and using Lemma 79.2 we get $[k_1, k_2] = k_1^2 k_2^2 = z'(zz') = z$, $o(k_1 k_2) = 2$, $k_1 k_2 \in N$. Because $k_1 k_2 \notin Z(\langle k_1, k_2 \rangle)$, we may assume $k_1 k_2 = u$ (an involution in $N - A$). Since $[k_1, u] = [k_1, k_1 k_2] = [k_1, k_2] = z$ (which gives $u^{k_1} = uz$) and $D = \langle a, u \rangle \cong D_8$ is not normal in G , we have $[a, k_1] \neq 1$. By Lemma 79.2, $[a, k_1] = a^2 k_1^2 = zz'$ and $k_1 a$ is an involution in $G - N$. We have $u^{k_1 a} = (uz)^a = (uz)z = u$. Hence $\langle u, k_1 a \rangle \cong E_4$ with $\langle u, k_1 a \rangle \cap Z(G) = \{1\}$ and so $\langle u, k_1 a, Z(G) \rangle \cong E_{16}$. Since G is not D_8 -free, it follows that G is a W_b -group. This is our final contradiction and so our statement (iii) is completely proved.

(iv) The factor group $G/\langle z \rangle$ ($z \in \Omega_1(Z(G))$) is not isomorphic to a W_c -group.

Suppose that the assertion (iv) is false. Then $G/\langle z \rangle$ is a W_c -group. Hence we may set $\Omega_1(G/\langle z \rangle) = H/\langle z \rangle$ (implying that $\Omega_1(G) \leq H$) so that $H = H_1 H_2$, where H_1 and H_2 are normal subgroups in H with $H_1 \cap H_2 = \langle z \rangle$, $H_1/\langle z \rangle \cong D_8$, $H_2/\langle z \rangle$ is elementary abelian and G/H is cyclic of order ≥ 4 . Let $Z/\langle z \rangle$ be the unique cyclic subgroup of index 2 in $H_1/\langle z \rangle$ and set $Z(H_1/\langle z \rangle) = Z_0/\langle z \rangle$ so that $|Z : Z_0| = 2$ and $|Z_0 : \langle z \rangle| = 2$. Let $Z_0 H_2 = N$, $Z H_2 = A$, so that $Z(H/\langle z \rangle) = N/\langle z \rangle$ and $N/\langle z \rangle$ is the unique maximal normal elementary abelian subgroup of $G/\langle z \rangle$, $G/N \cong M_{2^n}$, $n \geq 4$, $A/N = (G/N)'$, $H/N = \Omega_1(G/N) \cong E_4$. If E_1/N and E_2/N are other two subgroups of order 2 in H/N (distinct from A/N), then $E_1^G = E_2$, $E_1/\langle z \rangle$ and $E_2/\langle z \rangle$ are elementary abelian and $A/\langle z \rangle$ is abelian of type $(4, 2, \dots, 2)$. Also, $N_G(E_1) = N_G(E_2) > H$ and $|G : N_G(E_1)| = 2$. Finally, G possesses a subgroup S such that $G = HS$, $H \cap S = Z$, and $S/\langle z \rangle$ is cyclic so that S is abelian. In fact, S is either cyclic or abelian of type $(2^n, 2)$, $n \geq 4$. Also, S is cyclic if and only if Z_0 is cyclic (since $Z_0/\langle z \rangle = \Omega_1(S/\langle z \rangle)$). We have $H' \leq Z_0$ and H' covers $Z_0/\langle z \rangle$.

(α) Suppose Z_0 (and so also S) is cyclic.

We have $H_1/\langle z \rangle \cong D_8$ and $(H_1/\langle z \rangle)' = Z_0/\langle z \rangle$. Since H'_1 covers $Z_0/\langle z \rangle$ and Z_0 is cyclic, we get that $H'_1 = Z_0$ is of index 4 in H_1 . By a very well-known result of O. Taussky, H_1 is of maximal class. Since H_1 is Q_8 -free, we get $H_1 \cong D_{2^4}$. An involution $t \in H_1 - Z$ inverts Z and so $H_3 = \langle Z_0, t \rangle \cong D_8$. The subgroup H_3 is normal in H_1 and $[H_3, H_2] \leq H_1 \cap H_2 = \langle z \rangle$ implies that H_3 is normal in H .

Since $C_{H_1}(H_3) = \langle z \rangle$ and $H_1/\langle z \rangle \cong D_8 \cong \text{Aut}(H_3)$, we get that $C_H(H_3)$ covers H/H_1 . By Lemma 79.1, $C_H(H_3)$ is elementary abelian. In particular, $\Omega_1(H) = H = \Omega_1(G)$. Since H is nonmodular, H is a Wilkens group with $\Omega_1(H) = H$ and so H is either a W_a - or W_b -group. It follows that H has an abelian maximal subgroup \tilde{A} which is unique (by a result of A. Mann) since $H' \geq H'_1$ and $|H'_1| = 4$ (see Lemma 79.5). In particular, \tilde{A} is normal in G . Also, $\tilde{A} \cap H_1 = Z \cong C_8$ since Z is the unique abelian maximal subgroup of $H_1 \cong D_{2^4}$ and so $\exp(\tilde{A}) > 2$. If $t \in H_1 - Z$, then H must be a W_a -group and the involution t inverts on \tilde{A} . Let $\tilde{N} = \Omega_2(\tilde{A}) = Z_0\Omega_1(\tilde{A})$ (since \tilde{A}/Z is elementary abelian) so that \tilde{N} is normal in G , and $\tilde{N}/\langle z \rangle$ is a normal elementary abelian subgroup of $G/\langle z \rangle$. By the uniqueness of $N/\langle z \rangle$, $\tilde{N} \leq N$ and so $\tilde{A} = Z\tilde{N} \leq ZN = A$ and therefore $\tilde{A} = A$ is abelian of type $(8, 2, \dots, 2)$. Let $G_1 > H$ be such that $|G_1 : H| = 2$. Hence $G_1 \neq G$ and $G = HS_1$, where $S_1 = S \cap G_1$. It follows that G_1 is also a Wilkens group with $\Omega_1(G_1) = H$. Since $|G_1 : H| < 4$, G_1 is of type (a) or (b). But $A = \tilde{A}$ is the unique abelian maximal subgroup of H and $\exp(A) > 2$. Thus G_1 must be a W_a -group with respect to A and so $G_1/A \cong C_4$. On the other hand, we know that $S_1 \cap H = Z$. Hence, if $x \in S_1 - H$, then $x^2 \in Z \leq A$. This is a contradiction since $G_1/A \cong C_4$ and therefore $x^2 \in H - A$.

(β) We have $Z_0 \cong E_4$ and so S splits over $\langle z \rangle$.

We set $Z = \langle a \rangle \times \langle z \rangle$ so that $Z_0 = \langle a^2 \rangle \times \langle z \rangle$ and replacing a with az (if necessary), we may put $S = \langle s \rangle \times \langle z \rangle$ with $\Omega_2(\langle s \rangle) = \langle a \rangle = S \cap H$. If $|H'_1| = 4$, then $|H_1 : H'_1| = 4$, $H'_1 = Z_0$, and (by a result of O. Taussky) H_1 is of maximal class. In that case Z_0 would be cyclic, a contradiction.

We have proved that $|H'_1| = 2$ and so $Z_0 = H'_1 \times \langle z \rangle$. We set $H'_1 = \langle z_0 \rangle$ so that z_0 is a central element in H . But S is abelian, $G = HS$, and $S \cap H = Z > Z_0 = \langle z, z_0 \rangle$. It follows $C_G(\langle z, z_0 \rangle) \geq \langle H, S \rangle = G$ and so $\langle z, z_0 \rangle \leq Z(G)$.

We show that there are exactly two possibilities for the structure of H_1 . Since $H_1/Z_0 \cong E_4$, we have $\exp(H_1) = 4$. Suppose that H_1 is minimal nonabelian. If H_1 is metacyclic (of exponent 4), then we know that H_1 is not Q_8 -free. Thus H_1 must be nonmetacyclic and we know that there is only one such minimal nonabelian group of order 2^4 and exponent 4. In particular, there is an element $b \in H_1 - Z$ such that $b^2 = z$, $[a, b] = a^2b^2 = a^2z = z_0$, where $H'_1 = \langle z_0 \rangle$, z_0 is not a square in H_1 , and ab is an involution so that $\Omega_1(H_1) = \langle z, z_0, ab \rangle$. Suppose now that H_1 is not minimal nonabelian. Then there is a subgroup $D \cong D_8$ in H_1 which covers $H_1/\langle z \rangle$. Thus $H_1 = D \times \langle z \rangle$ and $H'_1 = D' = \langle z_0 \rangle$. We have $D \cap Z = \langle a \rangle$ or $D \cap Z = \langle az \rangle$ and all elements in $H_1 - Z$ are involutions inverting $\langle a, z \rangle$. Replacing a with az (if necessary), we may assume that $D \cap Z = \langle a \rangle$. If t is an involution in $D - Z$, then $D = \langle a, t \rangle$, where $z_0 = a^2$ is a square in H_1 .

Suppose that H_2 is nonabelian. Then $H'_2 = \langle z \rangle$ since $H_2/\langle z \rangle$ is elementary abelian. Let H_4 be a minimal nonabelian subgroup of H_2 so that $H'_4 = \langle z \rangle$, $H_4/\langle z \rangle$ is elementary abelian and $d(H_4) = 2$. Thus $H_4/\langle z \rangle \cong E_4$ and so $H_4 \cong D_8$. The subgroup H_4 is normal in H_2 and H_2 centralizes $H_4/\langle z \rangle$. We have $[H_1, H_4] \leq H_1 \cap H_2 = \langle z \rangle$

and so H_1 also centralizes $H_4/\langle z \rangle$ and H_4 is normal in H . Thus, H centralizes $H_4/\langle z \rangle$ and therefore there is no $h \in H$ inducing an outer automorphism on H_4 (because otherwise such an element h would act nontrivially on $H_4/\langle z \rangle$). It follows that $C_H(H_4)$ covers H/H_4 . But H/H_4 is nonabelian since $H_4 \leq H_2$ and $H/H_2 \cong H_1/\langle z \rangle \cong D_8$. This contradicts Lemma 79.1. We have proved that H_2 must be abelian and so H_2 is either abelian of type $(4, 2, \dots, 2)$ or elementary abelian. In any case, $N = Z_0 H_2 = \langle z_0 \rangle \times H_2$ since $z_0 \in Z(G)$.

($\beta 1$) Suppose that H_2 is abelian of type $(4, 2, \dots, 2)$, where $\Omega_1(N) = \Omega_1(H_2) = \langle z \rangle$. Set $E = \Omega_1(H_2)$ so that $\Omega_1(N) = \langle z_0 \rangle \times E$ and all elements in $H_2 - E$ are of order 4. Let h be an arbitrary element in $H_2 - E$ so that $h^2 = z$.

We consider first the possibility that H_1 is minimal nonabelian nonmetacyclic. Let x be any element of order 4 in H_1 so that $x^2 = z$ or $x^2 = zz_0$, where $\langle z_0 \rangle = H'_1$. Suppose that $[x, h] \neq 1$. By Lemma 79.2, $[x, h] = x^2 h^2 = x^2 z$. On the other hand, $[x, h] \leq H_1 \cap H_2 = \langle z \rangle$ and so $[x, h] = z$ which gives $x^2 = 1$, a contradiction. Hence $[x, h] = 1$ and since H_1 is generated by its elements of order 4 (noting that $\Omega_1(H_1) \cong E_8$) and $H_2 = \langle H_2 - E \rangle$, we get $[H_1, H_2] = \{1\}$. We apply Lemma 79.1 in the factor group $\bar{H} = H/\langle zz_0 \rangle$. We have $\bar{H}_1 \cong D_8$ and $\langle H_1, h \rangle = \bar{H}_1 * \langle \bar{h} \rangle$ is the central product of \bar{H}_1 with $\langle \bar{h} \rangle \cong C_4$, where $\bar{H}_1 \cap \langle \bar{h} \rangle = Z(\bar{H}_1)$, a contradiction.

We consider now the possibility, where $H_1 = D \times \langle z \rangle$ with

$$D = \langle a, t \mid a^4 = t^2 = 1, a^t = a^{-1} \rangle, \quad a^2 = z_0, \quad \text{and} \quad \langle z_0 \rangle = D'.$$

If $[a, h] \neq 1$, then $[a, h] \in H_1 \cap H_2 = \langle z \rangle$ and so $[a, h] = z$. On the other hand, Lemma 79.2 implies $[a, h] = a^2 h^2 = z_0 z$, a contradiction. Hence $[a, h] = 1$ and so a centralizes $H_2 = \langle H_2 - E \rangle$. It follows that $A = ZH_2 = \langle a \rangle \times H_2$ is an abelian maximal subgroup of H with $\exp(A) = 4$ and A is normal in G . We have $\Omega_1(H_1) = H_1$ and so $\Omega_1(H)$ contains the maximal subgroup $H_1 E$ of H , where $E = \Omega_1(H_2)$ with $|H_2 : E| = 2$. If $[t, h] = 1$, then $D = \langle a, t \rangle \cong D_8$ centralizes $\langle h \rangle \cong C_4$, contrary to Lemma 79.1. Hence $[t, h] \neq 1$ and since $[t, h] \in H_1 \cap H_2 = \langle z \rangle$, we get $[t, h] = z$ with $z = h^2$. Thus, $\langle t, h \rangle \cong D_8$ and so th is an involution in $H - (H_1 E)$. We have proved that $\Omega_1(H) = H$ and since $\Omega_1(G) \leq H$, we get also $\Omega_1(G) = H$. Also, $H' = \langle z, z_0 \rangle \cong E_4$ and therefore, by a result of A. Mann (Lemma 79.5), A is the unique abelian maximal subgroup of H . Take a subgroup G_1 of G with $H < G_1 < G$ and $|G_1 : H| = 2$. It follows that G_1 must be a W_α -group with $\Omega_1(G_1) = H$ since $|G_1 : H| = 2$ and A is the unique abelian maximal subgroup of H (with $\exp(A) > 2$). In that case G_1/A is cyclic. On the other hand, setting $S_1 = S \cap G_1$, we have $G_1 = HS_1$ and $S_1 \cap H = Z$. Thus, if $g \in S_1 - H$, then $g^2 \in Z \leq A$. This contradicts the fact that $G_1/A \cong C_4$.

($\beta 2$) We have proved that H_2 (and so also $N = \langle z_0 \rangle \times H_2$) is elementary abelian. Suppose first that H_1 is minimal nonabelian nonmetacyclic. In this case z_0 is not a square in H_1 , where $\langle z_0 \rangle = H'_1$. There is $b \in H_1 - Z$ with $b^2 = z$, $t = ab$ is an involution, and $a^2 = zz_0$. Now, $A = ZN = \langle a \rangle N$ is normal in G and $(\langle t \rangle N)^s =$

$\langle b \rangle N$ (recalling that $S = \langle s \rangle \times \langle z \rangle$) since $G/N \cong M_{2^n}$, $n \geq 4$, and so G acts nontrivially on the four-group H/N . The subgroup $\Omega_1(H)$ contains the maximal subgroup $\langle t \rangle N$ of H , where $\Omega_1(H_1) = \langle z, z_0, t \rangle \cong E_8$ and $N \cap H_1 = \langle z, z_0 \rangle$. If t centralizes H_2 , then $\langle t \rangle N$ is elementary abelian. But $(\langle t \rangle N)^s = \langle b \rangle N$ and $\langle b \rangle N$ is not elementary abelian, a contradiction. Hence t does not centralize H_2 and so $[H_2, t] = \langle z \rangle$ since $[H_2, t] \leq H_1 \cap H_2 = \langle z \rangle$. It follows that $\langle t \rangle N$ is nonabelian and so $\langle b \rangle N$ is also nonabelian. In particular, $H' = \langle z, z_0 \rangle \cong E_4$, $[H_2, b] = \langle z \rangle$, and so $\langle b \rangle$ is normal in $H_2\langle b \rangle$. Let u be an involution in H_2 with $[b, u] = z$ so that $\langle b, u \rangle \cong D_8$ and therefore bu is an involution. But $bu \in H - (\langle t \rangle N)$ and so $\Omega_1(H) = H$. It follows that H must be a W_a - or W_b -group. In that case H must possess an abelian maximal subgroup M which is also unique (by a result of A. Mann since $|H'| = 4$). We have $M \geq H' = \langle z, z_0 \rangle$. If M does not contain H_2 , then M covers H/H_2 which is nonabelian (since $H/H_2 \cong H_1/\langle z \rangle \cong D_8$), a contradiction. Hence $M \geq H_2$ and so $M \geq \langle H', H_2 \rangle = N$. Since $\langle t \rangle N$ and $\langle b \rangle N$ are nonabelian, we get that $M = A = \langle a \rangle N$ is abelian (of exponent 4). Thus H is a W_a -group with respect to A and so the involution t must invert each element in A . In particular, $a^t = a^{-1} = aa^2 = a(zz_0)$. This is a contradiction since $H'_1 = \langle z_0 \rangle$.

It remains to investigate the case, where $H_1 = D \times \langle z \rangle$ with

$$D = \langle a, t \mid a^4 = t^2 = 1, a^t = a^{-1} \rangle, \quad a^2 = z_0, \quad \langle z_0 \rangle = D'$$

and

$$S = \langle s \rangle \times \langle z \rangle, \quad \langle s \rangle \cap H = \langle a \rangle, \quad (\langle t \rangle N)^s = \langle at \rangle N$$

since $G/N \cong M_{2^n}$, $n \geq 4$. Obviously, in this case $\Omega_1(H) = H = \Omega_1(G)$. Suppose that t does not centralize H_2 . Then $[t, H_2] \leq H_1 \cap H_2 = \langle z \rangle$ and so $[t, H_2] = \langle z \rangle$ and $H' = \langle z, z_0 \rangle \cong E_4$. Then $\langle t \rangle N$ and $\langle at \rangle N = (\langle t \rangle N)^s$ are nonabelian. But H is a Wilkens group with $\Omega_1(H) = H$ and so H must have an abelian maximal subgroup U which is unique (by a result of A. Mann). If U does not contain H_2 , U covers H/H_2 and this is a contradiction since $H/H_2 \cong D_8$. Hence $U \geq \langle H', H_2 \rangle = N$ and so $U = A = \langle a \rangle N$ is abelian of exponent 4. Thus, H is a W_a -group with respect to A . In particular, the involution t inverts each element in A and so t centralizes H_2 , a contradiction. Hence t centralizes H_2 and so $\langle t \rangle N$ is elementary abelian. In that case $\langle at \rangle N = (\langle t \rangle N)^s$ is also elementary abelian. In particular, $D = \langle t, at \rangle \cong D_8$ centralizes H_2 and so $H = D \times H_2$. It follows that G is a W_c -group, a contradiction. Our statement (iv) is proved.

We have proved that the nonmodular factor group $G/\langle z \rangle$ ($z \in \Omega_1(Z(G))$) (according to our statement (i)) is not isomorphic to any Wilkens group (according to (ii), (iii), and (iv)). This is a final contradiction and so the Main Theorem is proved.

Minimal non-quaternion-free 2-groups

Here we classify minimal non-quaternion-free 2-groups. A 2-group G is minimal non-quaternion-free if G is not quaternion-free but each proper subgroup of G is quaternion-free. Recall that a 2-group G is modular if and only if G is D_8 -free.

The main theorem is a consequence of results of the previous section.

Theorem 80.1. *Let G be a minimal non-quaternion-free 2-group. Then G possesses a unique normal subgroup N such that $G/N \cong Q_8$. We have $N < \Phi(G)$ and so $G/\Phi(G) \cong E_4$ and $\Omega_1(G) \leq \Phi(G)$. If R is any G -invariant subgroup of index 2 in N , then $\mathcal{H}_2 = G/R$ is the minimal nonabelian metacyclic group of order 2^4 and exponent 4: $\mathcal{H}_2 = \langle a, b \mid a^4 = b^4 = 1, a^b = a^{-1} \rangle$, where $\mathcal{H}_2/\langle a^2b^2 \rangle \cong Q_8$, $X/\langle b^2 \rangle \cong D_8$, and $X/\langle a^2 \rangle \cong C_4 \times C_2$. In particular, if $|G| > 8$, then G has a normal subgroup S such that $G/S \cong D_8$ and so G is nonmodular.*

Proof. The group G possesses a normal subgroup N such that $G/N \cong Q_8$. Suppose that A is a maximal subgroup of G not containing N . Then $AN = G$ so $A/(A \cap N) \cong G/N \cong Q_8$, a contradiction. Thus, $N < \Phi(G)$ so $d(G) = 2$. It follows from $\Omega_1(G/N) = \Phi(G/N)$ that $\Omega_1(G) \leq \Phi(G)$. We may assume $|G| > 8$.

Let R be any G -invariant subgroup of index 2 in N .

We shall determine the structure of G/R . For that purpose we may assume $R = \{1\}$ so that $|N| = 2$, $N < \Phi(G)$, $N \leq Z(G)$, $|\Phi(G)| = 4$, $|G| = 2^4$ and $\Phi(G)/N = Z(G/N) = (G/N)'$, where $G/N \cong Q_8$. By Theorem 1.2, G has no cyclic subgroups of index 2 so $\Phi(G)$ is a four-subgroup. In that case, $N < Z(G)$ since G is not of maximal class so $\Phi(G) = Z(G)$ and G is minimal nonabelian. Since $\Omega_1(G) = \Phi(G)$ is a four-subgroup, G is metacyclic (of exponent 4). Since $\mathcal{H}_2 = \langle a, b \mid a^4 = b^4 = 1, a^b = a^{-1} \rangle$ is the unique nonabelian metacyclic group of order 16 and exponent 4, we get $G \cong \mathcal{H}_2$.

Next we do not assume that $R = \{1\}$. Let $M \neq N$ be a G -invariant subgroup of index 2 in $\Phi(G)$; then $L = M \cap N$ is of index 2 in N , by the product formula. By the previous paragraph, $G/L \cong \mathcal{H}_2$ so $G/M \in \{C_4 \times C_2, D_8\}$. In particular, G is nonmodular. This argument shows that N is the unique G -invariant subgroup of index 8 in G such that $G/N \cong Q_8$. \square

Let G be a minimal non- Q_8 -free 2-group of order > 8 such that each proper subgroup of G is modular. Then G is a minimal nonmodular 2-group and such groups

have been classified in §78. Therefore, we may assume in the sequel that G has a maximal subgroup H which is nonmodular. Since H is Q_8 -free, we are in a position to apply Theorem 79.7 classifying nonmodular Q_8 -free 2-groups. Also, we assume that the reader is familiar with Propositions 79.8, 79.9 and 79.10 describing the Wilkens groups of types (a), (b), and (c), which appear in Theorem 79.7.

Theorem 80.2. *Let G be a minimal non-quaternion-free 2-group which has a nonmodular proper subgroup. Then G has one of the following properties:*

- (i) $\Omega_1(G) = \Phi(G) = A\langle t \rangle$, where A is a maximal normal abelian subgroup of G with $\exp(A) > 2$, t is an involution inverting each element in A , and $G/A \cong Q_8, D_8$, or $C_4 \times C_2$. If $G/A \cong D_8$ or $C_4 \times C_2$, then A is abelian of type $(4, 2, \dots, 2)$.
- (ii) $\Omega_1(G) = EE_1$, where $E \neq E_1$ are the only maximal normal elementary abelian subgroups of $\Omega_1(G)$ and $|\Omega_1(G) : E| = 2$, $|\Omega_1(G) : E_1| \geq 2$. We have either $\Omega_1(G) = \Phi(G)$ (and then $G/\Omega_1(G) \cong E_4$) or $G/\Omega_1(G) \cong Q_8$. If $G/\Omega_1(G) \cong Q_8$, then also $|\Omega_1(G) : E_1| = 2$ which implies $\Omega_1(G) \cong D_8 \times E_{2^s}$.
- (iii) $\Omega_1(G) = E$ is elementary abelian and G/E is isomorphic to Q_8, M_{2^n} , $n \geq 4$, or $C_{2^m} \times C_2$, $m \geq 1$. If $G/E \cong M_{2^n}$ or $C_{2^m} \times C_2$ with $m \geq 2$, then $\Omega_2(G)$ is abelian of type $(4, 4, 2, \dots, 2)$.

Proof. Let G be a minimal non-quaternion-free 2-group possessing a maximal subgroup H which is nonmodular. It follows that H is a Wilkens group of type (a), (b), or (c). In particular, $H/\Omega_1(H)$ is cyclic, where $\Omega_1(H) = \Omega_1(G)$ since $\Omega_1(G) \leq \Phi(G)$. If $\Omega_1(G)$ is not elementary abelian, then we know (by the structure of the Wilkens group H) that $\Omega_1(G)$ is nonmodular and so in that case each maximal subgroup M of G is a Wilkens group. It follows that $M/\Omega_1(G)$ is cyclic, where $\Omega_1(M) = \Omega_1(G)$. In that case, $X = G/\Omega_1(G) \cong E_4$ or Q_8 . Here we have used a trivial fact that noncyclic 2-group X , all of whose maximal subgroups are cyclic, must be isomorphic to E_4 or Q_8 .

(i) Suppose that H is a Wilkens group of type (a). Then H is a semidirect product $H = \langle x \rangle \cdot A$, where A is a maximal normal abelian subgroup of H with $\exp(A) > 2$ and if t is the involution in $\langle x \rangle$, then t inverts each element of A . We have $\Omega_1(H) = \Omega_1(G) = A\langle t \rangle$ and A is a characteristic subgroup in H (Proposition 79.8) and so A is normal in G . By the previous paragraph, $G/\Omega_1(G) \cong E_4$ or Q_8 . However, if $G/\Omega_1(G) \cong Q_8$, then G/A (having a cyclic subgroup H/A of index 2) is of maximal class. But such a group does not have a proper factor group isomorphic to Q_8 . Hence $G/\Omega_1(G) \cong E_4$ and so $\Omega_1(G) = \Phi(G)$. Since $d(G/A) = 2$, we get $G/A \cong Q_8, D_8$ or $C_4 \times C_2$.

Suppose that A is not a maximal normal abelian subgroup of G . Let B be a maximal normal abelian subgroup of G containing A so that $B \cap H = A$, $|B : A| = 2$, and $G = \langle x \rangle \cdot B$ with $\langle x \rangle \cap B = \{1\}$. Let $b \in B - A$ and we compute $(bb^t)^t = b^t b =$

$bb^t \in A$, since $b^t \in B - A$ so that $bb^t = s \in \Omega_1(A)$. If $s = 1$, $b^t = b^{-1}$ and so t inverts each element of the abelian group B . It follows that $G = \langle x \rangle \cdot B$ is a Wilkens group of type (a). In that case G would be Q_8 -free (Proposition 79.8), a contradiction. Hence $s \neq 1$ and $(bt)^2 = btbt = bb^t = s$ shows that $o(bt) = 4$. Let a be an element of order 4 in A . We have $a^{bt} = a^{-1}$ and $\langle a, bt \rangle \neq G$ (since $a \in \Phi(G)$) and so $\langle a, bt \rangle$ is Q_8 -free, contrary to Lemma 79.1. We have proved that A is a maximal normal abelian subgroup of G .

Suppose that $G/A \cong D_8$ or $C_4 \times C_2$. In that case there is a maximal subgroup K of G such that $K/A \cong E_4$ and $\Omega_1(K) = \Omega_1(G)$. Then K is a Wilkens group of type (a) or (b) since $|K : \Omega_1(K)| = 2$ (and so K cannot be a Wilkens group of type (c)). Suppose that K is a Wilkens group of type (a) with respect to a maximal normal abelian subgroup A_1 of K with $\exp(A_1) > 2$. We know that $A_1 \leq \Omega_1(K) = \Omega_1(G)$, $|\Omega_1(G) : A_1| = 2$ and K/A_1 is cyclic. Since K/A is noncyclic, we have $A_1 \neq A$. All elements in $A_1 - A$ are involutions and if $t_0 \in A_1 - A$, then t_0 inverts and centralizes each element in $A \cap A_1$ and so $A \cap A_1$ is elementary abelian. It follows that $\exp(A_1) = 2$, a contradiction. We have proved that K is a Wilkens group of type (b) with respect to a maximal normal elementary abelian subgroup E of K . We know that $|\Omega_1(K) : E| = 2$ (Proposition 79.9). Since $\Omega_1(K) = \Omega_1(G)$, we have $|A : A \cap E| = 2$ and so A is abelian of type $(4, 2, \dots, 2)$.

(ii) Assume that H is a Wilkens group of type (b) with respect to E and $|\Omega_1(H) : E| = 2$, where H/E is cyclic. We have $\Omega_1(H) = \Omega_1(G)$ and $\Omega_1(G) \leq \Phi(G)$ so that $\Omega_1(G)$ is nonmodular. Indeed, $\Omega_1(G)$ has exactly two maximal normal elementary abelian subgroups E and E_1 , where $\Omega_1(G) = EE_1$ and so $\Omega_1(G)$ is a Wilkens group of type (b) (and so nonmodular). By the first paragraph of the proof, $G/\Omega_1(G) \cong E_4$ or Q_8 .

Suppose that $G/\Omega_1(G) \cong Q_8$. It is easy to see that E is not normal in G . Suppose false. Since G/E has a cyclic subgroup H/E of index 2 and $G/\Omega_1(G) \cong Q_8$, we get that G/E must be of maximal class. But there is no 2-group of maximal class having Q_8 as a proper homomorphic image. Hence E is not normal in G and so for each $x \in G - H$, $E^x = E_1$. In particular, $|\Omega_1(G) : E_1| = 2$ and $F = E \cap E_1 = Z(\Omega_1(G))$. Take $e \in E - F$, $e_1 \in E_1 - F$ so that $D = \langle e, e_1 \rangle \cong D_8$ and if V is a complement of $\langle [e, e_1] \rangle$ in F , then $\Omega_1(G) = D \times V \cong D_8 \times E_2^s$.

(iii) Suppose that H is a Wilkens group of type (b) with respect to E and $E = \Omega_1(H)$ so that $E = \Omega_1(G)$ (since $E \leq \Phi(G)$), E is normal in G and G/E is noncyclic with the cyclic subgroup H/E of index 2.

Let F/E be a proper subgroup of G/E such that $F/E \cong E_4$. Then F is abelian. Indeed, since $F \neq G$, F is Q_8 -free. If F is not D_8 -free, then F must be a Wilkens group. But then $F/\Omega_1(F)$ must be cyclic. This is a contradiction since $\Omega_1(F) = E$. It follows that F is D_8 -free. Since $\exp(F) \leq 4$, F must be abelian (Proposition 79.6).

Since each proper subgroup of G/E is Q_8 -free, G/E cannot be semidihedral or Q_{2m} with $m \geq 4$. Suppose that $G/E \cong D_{2n}$, $n \geq 3$. In that case G/E is generated by its four-subgroups and so $E \leq Z(G)$. This is a contradiction because in that case H

would be abelian (noting that H/E is cyclic). We have proved that G/E is isomorphic to Q_8 , M_{2^n} , $n \geq 4$, or $C_{2^m} \times C_2$, $m \geq 1$.

Suppose that G/E is not isomorphic to Q_8 or $C_2 \times C_2$. Set $F/E = \Omega_1(G/E)$ so that $F/E \cong E_4$. By the above, F is abelian. Obviously, $F = \Omega_2(G)$ is abelian of type $(4, 4, 2, \dots, 2)$.

(iv) Finally, assume that H is a Wilkens group of type (c). We have $\Omega_1(H) = \Omega_1(G) \cong D_8 \times E_2$ and $H/\Omega_1(G)$ is cyclic of order ≥ 4 (Proposition 79.10). The subgroup $\Omega_1(G)$ has exactly three abelian maximal subgroups E_1, E_2, A , where E_1 and E_2 are elementary abelian and A is abelian of type $(4, 2, \dots, 2)$. By the structure of H , E_1 and E_2 are not normal in H and $H/E_1 \cap E_2 \cong M_{2^n}$, $n \geq 4$. By the first paragraph of the proof, $G/\Omega_1(G) \cong Q_8$ since $|H/\Omega_1(G)| \geq 4$. Thus $H/E_1 \cap E_2 \cong M_{2^4}$.

On the other hand, $\Omega_1(G)$ is normal in G and so $N_G(E_1) = N_G(E_2) = K$ is a maximal subgroup of G distinct from H . Since $K \geq \Omega_1(G)$, K is nonmodular and therefore K is a Wilkens group. But K cannot be a Wilkens group of type (c) since E_1 and E_2 are normal in K . Hence K is either a Wilkens group of type (a) with respect to A or K is a Wilkens group of type (b) with respect to E_1 or E_2 . The group G with such a maximal subgroup K has been considered in (i) and (ii) and so we do not get here new possibilities for the structure of G . Our theorem is proved. \square

Let

$$\mathcal{H}_2 = \langle a, b \mid a^4 = b^4 = 1, a^b = a^{-1} \rangle,$$

$$\mathcal{H}_1 = \langle a, b \mid a^4 = b^4 = 1, c = [a, b], c^2 = 1, [a, c] = [b, c] = 1 \rangle.$$

Exercise 1. Let $G = \mathcal{H}_1$. Then $1, a^2, b^2$ are only squares in G . In particular, a^2b^2 is not a square.

Solution. Let $g = a^i b^j c^k \in G$. Then $g^2 = (a^i b^j)^2$. If i is even, then $g^2 = b^{2j} \in \{1, b^2\}$. If j is even, then $g^2 = a^{2i} \in \{1, a^2\}$. If i and j are odd, then $g^2 = (ab)^2 = ab^2 a^b = ab^2 ac = a^2 b^2 c$.

Exercise 2. If $G = \mathcal{H}_1$, then $G/\langle a^2b^2 \rangle \cong \mathcal{H}_2$.

Solution. Since $G/\langle a^2b^2 \rangle$ is nonabelian of exponent 4, it suffices to show that it is metacyclic. Note that $a^2b^2 \in \Phi(G)$. Let A_i , $i = 1, 2, 3$, be all maximal subgroups of G ; then these subgroups are abelian of type $(4, 2, 2)$. It follows that $\langle a^2b^2 \rangle$ is a direct factor of A_i , $i = 1, 2, 3$, so all maximal subgroups of $G/\langle a^2b^2 \rangle$ are abelian of type $(4, 2)$. Then, by Lemma 65.1, $G/\langle a^2b^2 \rangle$ is metacyclic, as was to be shown.

Exercise 3. Classify Q_8 -free minimal nonabelian 2-groups. (*Hint.* G is Q_8 -free if and only if $G/\mathcal{O}_2(G)$ is metacyclic.)

Exercise 4. (a) A direct product of two Q_8 -free 2-groups is not necessarily Q_8 -free.

(*Hint.* (a) The group $D_8 \times C_4$ has an epimorphic image isomorphic to $Q_8 * C_4$.)

- (b) A direct product of two D_8 -free 2-groups is not necessarily D_8 -free. (*Hint.* The group $Q_8 \times C_4$ has an epimorphic image isomorphic to $D_8 * C_4$.)
- (c) Suppose that G is Q_8 -free. If $D_8 \cong D \leq G$, then $C_G(D)$ is elementary abelian.
- (d) Suppose that G is D_8 -free. If $Q_8 \cong Q \leq G$, then $C_G(Q)$ is elementary abelian.

Problem 1. Study the structure of nonabelian \mathcal{H}_2 -free 2-groups.

Problem 2. Study the structure of minimal non- \mathcal{H}_2 -free 2-groups.

Let $S(p^3)$ be a nonabelian group of order p^3 and exponent p ; then $p > 2$. Obviously, $S(p^3)$ -free p -groups are metacyclic (see Theorem 9.11). It is easy to check that if G is a minimal non- $S(p^3)$ -free p -group, then $p = 3$ and G is a minimal nonmetacyclic group of order 3^4 (see Theorem 69.1).

Maximal abelian subgroups in 2-groups

Abelian subgroups in 2-groups G play an important role. Therefore, it is not very surprising that our assumption that every two distinct maximal abelian subgroups have cyclic intersection determines completely the structure of G . We obtain five classes of 2-groups with this property. More precisely, we prove here the following result.

Theorem 81.1. *Let G be a nonabelian 2-group in which any two distinct maximal abelian subgroups have cyclic intersection. Then $Z(G)$ is cyclic, each abelian subgroup of G is of rank at most 2, the intersection of any two distinct maximal abelian subgroups is equal $Z(G)$, and G has (at least) one abelian subgroup of index 2. Moreover, G is isomorphic to one of the following groups.*

- (a) *Group of maximal class (dihedral, semidihedral or generalized quaternion).*
- (b) $M_{2^n} = \langle a, t \mid a^{2^{n-1}} = t^2 = 1, n \geq 4, a^t = a^{1+2^{n-2}} \rangle$.
- (c) $G = D * C$ (*central product*), where $D \cong D_{2^n}$, $n \geq 3$, is dihedral of order 2^n , $C \cong C_{2^m}$, $m \geq 2$, is cyclic of order 2^m and $D \cap C = Z(D)$.
- (d) $G = \langle x, t \mid (xt)^2 = a, a^{2^m} = t^2 = 1, m \geq 2, x^2 = ab, b^{2^{n-1}} = 1, n \geq 3, b^t = b^{-1}, [a, x] = [a, t] = 1, t^x = tb, a^{2^{m-1}} = b^{2^{n-2}} \rangle$, where $|G| = 2^{m+n}$, $m \geq 2, n \geq 3$, $Z(G) = \langle a \rangle \cong C_{2^m}$, $G' = \langle b \rangle \cong C_{2^{n-1}}$, and $M = \langle x, a \rangle$ is a unique abelian maximal subgroup of G . We have $C_G(t) = \langle t \rangle \times \langle a \rangle \cong C_2 \times C_{2^m}$ and $\langle b, t \rangle \cong D_{2^n}$.
- (e) $G = \langle g, h \mid g^{2^n} = h^{2^m} = 1, m \geq 3, n \geq 3, g^{2^{n-1}} = h^{2^{m-1}}, hg = h^{-1} \rangle$, where G is metacyclic, $|G| = 2^{m+n-1}$ since $\langle g \rangle \cap \langle h \rangle = \langle g^{2^{n-1}} \rangle \cong C_2$. Also, $Z(G) = \langle g^2 \rangle \cong C_{2^{n-1}}$, $G' = \langle h^2 \rangle \cong C_{2^{m-1}}$ and $M = \langle h, g^2 \rangle$ is a unique abelian maximal subgroup of G .

The more general problem to determine the structure of a nonabelian p -group G such that $A \cap B = Z(G)$ for any two distinct maximal abelian subgroups A and B is very difficult. First we show that a p -group G has this property if and only if $C_G(x)$ is abelian for each $x \in G - Z(G)$ (Theorem 81.2). Then we show that such a 2-group G has either an abelian subgroup of index 2 or G is of class 2 and G' is elementary abelian (Theorem 81.3). In Corollary 81.5 we get a new result for an arbitrary finite 2-group.

We also classify 2-groups G such that $A/Z(G)$ is cyclic for each maximal abelian subgroup A of G (a problem of Heineken–Mann). It is surprising that such groups

have the property that $C_G(x)$ is abelian for each element $x \in G - Z(G)$. Then we may use our Theorems 81.2 and 81.3 to classify such groups (Theorem 81.4). In this classification we distinguish the cases, where G has an abelian subgroup of index 2 and the case where $|G : A| > 2$ for each maximal abelian subgroup A of G .

Proof of Theorem 81.1. Let G be a nonabelian 2-group in which any two distinct maximal abelian subgroups have cyclic intersection. Since $Z(G)$ is contained in each maximal abelian subgroup of G , it follows that $Z(G)$ is cyclic.

Suppose that G possesses an elementary abelian subgroup E of order 8. Let A be a maximal abelian subgroup containing E and set $F = \Omega_1(A)$ so that $E \leq F$. Let $B \leq G$ be such that $A < B$ and $|B : A| = 2$ and let $x \in B - A$. Then $x^2 \in A$ and therefore x induces on F an automorphism of order ≤ 2 . It follows that $|C_F(x)| \geq 4$ and the abelian subgroup $C_F(x)\langle x \rangle$ is contained in a maximal abelian subgroup C which is distinct from A since $x \notin A$. But $A \cap C \geq C_F(x)$ and so $A \cap C$ is noncyclic, a contradiction. We have proved that each abelian subgroup of G is of rank at most 2.

We may assume that G is not of maximal class (case (a) of Theorem 81.1) and so G possesses a normal four-subgroup U . Set $M = C_G(U)$ so that $|G : M| = 2$ since $Z(G)$ is cyclic. Let A be a maximal abelian subgroup of G which contains U so that $A \leq M$. Suppose that $A \neq M$ and let $y \in M - A$ be such that $y^2 \in A$. Let B be a maximal abelian subgroup of G containing the abelian subgroup $U\langle y \rangle$. Then $B \neq A$ (since $y \notin A$) and $A \cap B \geq U$, a contradiction. We have proved that whenever U is a normal four-subgroup of G , then $M = C_G(U)$ is an abelian maximal subgroup of G .

If x is any element in $G - M$, then $C_M(x) = Z(G)$ and $Z(G)\langle x \rangle$ is a maximal abelian subgroup of G . Thus, the intersection of any two distinct maximal abelian subgroups of G is equal to $Z(G)$ and this statement also holds for 2-groups of maximal class.

Suppose that G has more than one normal four-subgroup. By Theorem 50.2, $G = D * C$ with $D \cong D_8$, $D \cap C = Z(D)$ and C is either cyclic of order ≥ 4 or C is of maximal class (distinct from D_8). Let U be a four-subgroup in D so that U is normal in G . By the above, $C_G(U)$ is abelian and so C must be cyclic. We have obtained a group stated in part (c) of Theorem 81.1. In the sequel we assume that G has a unique normal four-subgroup U and set $M = C_G(U)$ so that M is an abelian maximal subgroup of rank 2 with $\Omega_1(M) = U$.

(i) First assume $\Omega_2(G) \not\leq M$. Then there is an element $y \in G - M$ of order ≤ 4 so that $y^2 \in U$. We have $U\langle y \rangle \cong D_8$ and so there is an involution $t \in G - M$. Since t does not centralize U and M is abelian of rank 2, we get $C_G(t) = \langle t \rangle \times C_M(t)$, where $C_M(t)$ is cyclic of order 2^m , $m \geq 2$. Indeed, if $m = 1$, then G is of maximal class. Also, we have $t \notin \Phi(G)$, G has no elementary abelian subgroups of order 8 and G is not isomorphic to M_{2^s} , $s \geq 4$, since M_{2^s} has only three involutions. We are now in a position to use Theorem 48.1. It follows that G has a subgroup S of index ≤ 2 , where $S = AL$, L is normal in G , $L = \langle b, t | b^{2^{n-1}} = t^2 = 1, b^t = b^{-1} \rangle \cong D_{2^n}$, $n \geq 3$, $A = \langle a \rangle \cong C_{2^m}$, $m \geq 2$, $A \cap L = Z(L) = \langle z \rangle$, $[a, t] = 1$, $C_G(t) = \langle t \rangle \times \langle a \rangle$,

$\Omega_1(G) = \Omega_1(S) = \Omega_2(A) * L$, $\Omega_2(A) \cap L = Z(L)$ and if $|G : S| = 2$, then there is an element $x \in G - S$ such that $t^x = tb$.

Since $\langle b \rangle$ is a unique cyclic subgroup of index 2 in L , $\langle b \rangle$ is normal in G . Set $B = \Omega_2(A) * L = \Omega_1(G)$, $\Omega_2(A) = \langle l \rangle$, $l^2 = z$, and $\langle v \rangle = \Omega_2(\langle b \rangle)$ so that $\langle v \rangle$ and $\langle l \rangle = Z(B)$ are normal in G . Hence $\langle l, v \rangle \cong C_4 \times C_2$ is normal in G . Set $u = lv$ so that $U = \langle z, u \rangle = \Omega_1(\langle l, v \rangle) \cong E_4$ is a unique normal four-subgroup in G . We know that $M = C_G(U)$ is abelian and $|G : M| = 2$. Note that b centralizes U and $u^t = (lv)^t = lv^{-1} = lvz = uz$. If $v^a = v^{-1} = vz$, then $A = \langle a \rangle > \Omega_2(A) = \langle l \rangle$ and we replace a with $a' = at$. In that case $o(a') = o(a)$, $\Omega_2(\langle a' \rangle) = \langle l \rangle$ and

$$u^{a'} = (lv)^{at} = (avz)^t = av^{-1}z = lv = u,$$

so that $\langle a' \rangle$ centralizes U and $S = \langle a' \rangle L$. Writing again a instead of a' , we may assume from the start that $A = \langle a \rangle$ centralizes U . Hence $C_S(U) = \langle a, b \rangle$ is of index 2 in S and therefore $M = C_G(U)$ covers G/S and $G = M\langle t \rangle$. But M is abelian and t centralizes $\langle a \rangle$ and so $\langle a \rangle \leq Z(G)$. On the other hand, $C_G(t) = \langle t \rangle \times \langle a \rangle$ and $C_M(t) = \langle a \rangle$ so that $A = \langle a \rangle = Z(G)$.

If $G = S$, then $G = L * A$, where $L \cong D_{2^n}$, $n \geq 3$, $A \cong C_{2^m}$, $m \geq 2$, and $L \cap A = Z(L)$. We have obtained groups stated in part (c) of Theorem 81.1. In what follows we assume that $|G : S| = 2$ and we know that in that case there is an element $x \in G - S$ such that $t^x = tb$. We may assume that $x \in M - S$. Indeed, if $x = tx'$ with $x' \in M - S$, then $tb = t^x = t^{tx'} = t^{x'}$.

Since M is abelian and $C_M(t) = \langle a \rangle = Z(G)$, it follows that $C_M(xt) = \langle a \rangle$ and so $(xt)^2 \in \langle a \rangle$. Set $(xt)^2 = a'$ and assume that $\langle a' \rangle \neq \langle a \rangle$. This implies that there is an element $a'' \in \langle a \rangle - \langle a' \rangle$ such that $(a'')^2 = (a')^{-1}$. We get $(xt \cdot a'')^2 = (xt)^2 (a'')^2 = 1$ and so $x(ta'')$ (with $ta'' \in S$) is an involution in $G - S$, contrary to $\Omega_1(G) = \Omega_1(S)$. It follows that $\langle a' \rangle = \langle a \rangle$ and so replacing a with a' (and writing again a instead of a'), we may assume from the start that $(xt)^2 = a$. From the last relation and $t^x = tb$ we get:

$$a = (xt)^2 = xt \cdot xt = x^2(x^{-1}tx)t = x^2tbt = x^2b^{-1}$$

and so $x^2 = ab$. The structure of G is uniquely determined and we have obtained the group stated in part (d) of Theorem 81.1.

(ii) Finally, assume that $\Omega_2(G) \leq M$. Note that M is abelian of rank 2 and so M is metacyclic. Hence G is also metacyclic. If G has a cyclic subgroup of index 2, then G is either of maximal class or $G \cong M_{2^n}$, $n \geq 4$, and these are the groups stated in parts (a) and (b) of Theorem 81.1. In what follows we assume that G has no cyclic subgroups of index 2. We have $U = \Omega_1(M) = \Omega_1(G) \cong E_4$, where $M = C_G(U)$ is an abelian maximal subgroup of G .

Let H be a normal cyclic subgroup with cyclic G/H so that $|H| \geq 4$ and $|G/H| \geq 4$. We have $U \cap H = \langle z \rangle \cong C_2$ and $z \in Z(G)$ so that if $u \in U - \langle z \rangle = U - H$, then $M = C_G(u)$, where $|G : M| = 2$ and M is abelian. Suppose that u does not centralize H . Then $|H : (H \cap M)| = 2$ and therefore M covers G/H . Let $m \in M$ be

such that $\langle m \rangle$ covers $M/M \cap H$ and note that $C_G(H) = H$ since u does not centralize H . Let $h \in H - M$ so that $H = \langle h \rangle$ and $h^m = hz$. Then $h^{m^2} = (hz)^m = hz \cdot z = h$. This is a contradiction since $|G/H| \geq 4$ and so $m^2 \notin H$.

We have proved that u centralizes H and so $M > H$. Let $g \in G - M$ so that $\langle g \rangle$ covers G/H , $g^2 \in M$ and g^2 centralizes H and therefore g induces on $H = \langle h \rangle$ an involutory automorphism. Also, $u^g = uz$ since $Z(G)$ is cyclic. If $h^g = hz$, then $G' = \langle z \rangle$ and G is minimal nonabelian. In that case G is splitting metacyclic, i.e., there is $g' \in G - M$ such that $\langle g' \rangle$ covers G/H and $\langle g' \rangle \cap H = \{1\}$. It follows that $\Omega_1(\langle g' \rangle) \leq Z(G)$ and so $Z(G) \geq \langle z, \Omega_1(\langle g' \rangle) \rangle \cong E_4$, a contradiction. We have proved that $h^g = h^{-1}z^\epsilon$, $\epsilon = 0, 1$ and $|H| \geq 8$. (Indeed, if $|H| = 4$, then $h^g = h^{-1} = hz$ and we have again $G' = \langle z \rangle$, as above.) In particular, $C_H(g) = \langle z \rangle$ and so $\langle g \rangle \cap H \leq \langle z \rangle$. However, if $\langle g \rangle \cap H = \{1\}$, then $C_G(\Omega_1(\langle g \rangle)) \geq \langle M, g \rangle = G$ and so $E_4 \cong \langle z, \Omega_1(\langle g \rangle) \rangle \leq Z(G)$, a contradiction.

We have proved that $\langle g \rangle \cap H = \langle z \rangle$ and so $o(g) \geq 8$ and $Z(G) = \langle g^2 \rangle$. If $h^g = h^{-1}z$, then we replace h with $h' = hu$, where $[h, u] = 1$ and so $o(h') = o(h)$ and

$$(h')^g = (hu)^g = h^{-1}z \cdot uz = h^{-1}u = (hu)^{-1} = (h')^{-1}$$

and $\langle h', g \rangle = \langle hu, g \rangle = \langle h, g \rangle = G$ since $u \in U \leq \Phi(G)$. (Indeed, $\Phi(G) \leq M$ is abelian and so if $\Phi(G) = \Omega_1(G)$ were cyclic, then $|G : \Phi(G)| = 4$ implies that G would have a cyclic subgroup of index 2.) Writing h instead of h' , we see that we may assume from the start that $h^g = h^{-1}$. We have obtained the group stated in part (e) of Theorem 81.1. \square

Theorem 81.2. $A \cap B = Z(G)$ for any two distinct maximal abelian subgroups A, B if and only if $C_G(x)$ is abelian for each $x \in G - Z(G)$. \square

Proof. Let $x \in G - Z(G)$ and suppose that $C_G(x)$ is nonabelian. Let A be a maximal abelian subgroup of $C_G(x)$ so that $A \neq C_G(x)$ and $A \geq Z(G)\langle x \rangle > Z(G)$. Let $b \in C_G(x) - A$ and let B be a maximal abelian subgroup of $C_G(x)$ containing $\langle b \rangle$ so that $A \neq B$ and B also contains the abelian subgroup $Z(G)\langle x \rangle$. Obviously, A and B are also maximal abelian subgroups of G but $A \cap B \geq Z(G)\langle x \rangle > Z(G)$.

Conversely, let $C \neq D$ be maximal abelian subgroups of G such that $C \cap D > Z(G)$. Let $y \in (C \cap D) - Z(G)$ so that $C_G(y) \geq \langle C, D \rangle$, where $\langle C, D \rangle$ is non-abelian. \square

Theorem 81.3. Let G be a nonabelian 2-group such that $A \cap B = Z(G)$ for every two distinct maximal abelian subgroups A and B . Then one of the following holds:

- (a) G has an abelian subgroup of index 2.
- (b) G is of class 2, G' is elementary abelian and $\Phi(G) \leq Z(G)$.

Proof. Let A be a maximal normal abelian subgroup of G . Then $G/A \neq \{1\}$ acts faithfully on A and $\{1\} \neq Z(G) < A$. Let K be a G -invariant subgroup such that $Z(G) < K \leq A$ and $|K : Z(G)| = 2$. Let x be any element in $G - A$. Then

$C_A(x) = Z(G)$ and so $\langle x \rangle \cap A \leq Z(G)$. Indeed, let B be a maximal abelian subgroup containing the abelian subgroup $C_A(x)\langle x \rangle$. Then $A \neq B$ and $A \cap B \geq C_A(x) = Z(G)$. Let $k \in K - Z(G)$ so that $k^2 \in Z(G)$ and $k^x = kl$ with some $l \in Z(G)$. We get

$$k^2 = (k^2)^x = (k^x)^2 = (kl)^2 = k^2l^2,$$

and so $l^2 = 1$ and therefore l is an involution in $Z(G)$. This gives

$$k^{x^2} = (k^x)^x = (kl)^x = k^x l = (kl)l = kl^2 = k,$$

and so (by the above) $x^2 \in A$ and (since $\langle x \rangle \cap A \leq Z(G)$) $x^2 \in Z(G)$. In particular, G/A is elementary abelian. Let $a \in A - Z(G)$ and set $a^x = a' \in A - Z(G)$ so that $(a')^x = (a^x)^x = a^{x^2} = a$ (since $x^2 \in Z(G)$). Therefore, $(aa')^x = a'a = aa'$ which implies that $aa' = z \in Z(G)$ and $a' = a^x = a^{-1}z$ and so x inverts $A/Z(G)$.

Suppose that $|G/A| \geq 4$. Then there are elements $x, y \in G - A$ such that $xy \in G - A$. In this case x and y both invert $A/Z(G)$ and so xy centralizes $A/Z(G)$. But xy also must invert $A/Z(G)$ which implies that $A/Z(G)$ is elementary abelian. Hence $\Phi(G) \leq Z(G)$ (noting that for each $x \in G - A$, $x^2 \in Z(G)$) and so G is of class 2. For each $g, h \in G$, $[g, h]^2 = [g^2, h] = 1$ and so G' is elementary abelian. \square

Theorem 81.4. *Let G be a nonabelian 2-group such that $A/Z(G)$ is cyclic for each maximal abelian subgroup A of G . Then one of the following holds:*

- (a) *G has an abelian subgroup M of index 2 and we have either $G = HZ(G)$ with H minimal nonabelian or $G/Z(G) \cong D_{2^n}$, $n \geq 3$, is dihedral of order 2^n with G' cyclic of order ≥ 4 , $G' \cap Z(G) \cong C_2$, and if $x \in G - M$, then $x^2 \in Z(G)$ and x inverts G' .*
- (b) *G is of class 2, G' is elementary abelian of order ≥ 8 , $\Phi(G) \leq Z(G)$ and whenever A is a maximal abelian subgroup of G , then $|A : Z(G)| = 2$.*

Proof. Suppose that there is an element $a \in G - Z(G)$ such that $H = C_G(a)$ is nonabelian. Let A be a maximal abelian subgroup of G containing $\langle a \rangle$. Then $Z(G)\langle a \rangle \leq A < H < G$. By our assumption, $A/Z(G) \neq \{1\}$ is cyclic. Assume that $H/Z(G)$ contains a subgroup of order 2 distinct from $\Omega_1(A/Z(G))$. In that case there is $x \in H - A$ such that $x^2 \in Z(G)$. Since $[a, x] = 1$, $\langle a, x \rangle$ is abelian but $\langle a, x \rangle Z(G)/Z(G)$ is noncyclic, a contradiction. We have proved that $H/Z(G)$ has only one subgroup of order 2 and so $H/Z(G) \cong Q_{2^n}$, $n \geq 3$, is generalized quaternion of order 2^n . Indeed, if $H/Z(G)$ were cyclic, then H is abelian, a contradiction. Since $H/Z(G) \cong Q_{2^n}$, it follows that $a^2 \in Z(G)$, $Z(H) = Z(G)\langle a \rangle$, $|Z(H) : Z(G)| = 2$ and for each $y \in Z(H) - Z(G)$, $C_G(y) = H = C_G(a)$. Set $|Z(G)| = 2^m$, $m \geq 1$, so that $|H| = 2^{m+n}$. Let $A_0/Z(G)$ be a cyclic subgroup of index 2 in $H/Z(G)$ so that A_0 is abelian and $Z(H) < A_0$. Let $A_1/Z(G) = (H/Z(G))'$ so that $Z(H) \leq A_1 < A_0$ and $|H : A_1| = 4$ and therefore $|A_1| = 2^{m+n-2}$. Since $A_1 = H'Z(G)$, H' covers $A_1/Z(G)$ and so $|H'| \geq 2^{n-2} = |A_1/Z(G)|$.

By Lemma 1.1, we get $|H| = 2|\text{Z}(H)||H'|$ and so $2^{m+n} = 2 \cdot 2^{m+1}|H'|$ and therefore $|H'| = 2^{n-2}$. This gives $H' \cap \text{Z}(G) = \{1\}$ and so H' is cyclic with $H' \cap \text{Z}(H) = \langle y \rangle \cong \text{C}_2$. It follows that $\langle y \rangle$ is characteristic in H and so if T is a subgroup of G such that $H < T \leq G$ and $|T : H| = 2$, then $\langle y \rangle$ is central in T , contrary to the above fact that $\text{C}_G(y) = H$, where $y \in \text{Z}(H) - \text{Z}(G)$. We have proved that for each $a \in G - \text{Z}(G)$, $\text{C}_G(a)$ is abelian.

By Theorem 81.2, $A \cap B = \text{Z}(G)$ for any two distinct maximal abelian subgroups A and B of G . We may use Theorem 81.3 and so either G has an abelian subgroup of index 2 or $G' \leq \text{Z}(G)$, $\phi(G) \leq \text{Z}(G)$ and G' is elementary abelian.

(i) First we consider the case, where G has an abelian subgroup M of index 2. Then $\text{Z}(G) < M$ and for each $x \in G - M$, $\text{C}_M(x) = \text{Z}(G)$ and so $x^2 \in \text{Z}(G)$. By our assumption, $M/\text{Z}(G) \neq \{1\}$ is cyclic. If G has another abelian maximal subgroup N , then $M \cap N = \text{Z}(G)$ and this implies that $|M : \text{Z}(G)| = 2$. Conversely, suppose that $M/\text{Z}(G) = 2$. In that case $G/\text{Z}(G) \cong \text{E}_4$ (because $G/\text{Z}(G) \cong \text{C}_4$ would imply that G is abelian) and so G has more than one abelian maximal subgroup. We analyze this case further. Let H be a minimal nonabelian subgroup of G . Then $|H : (H \cap \text{Z}(G))| = 4$, H covers $G/\text{Z}(G)$ and so $G = H\text{Z}(G)$ and $G' \cong \text{C}_2$. We have obtained the first possibility stated in part (a) of our theorem.

It remains to consider the case, where $M/\text{Z}(G) \cong \text{C}_{2^n}$, $n \geq 2$, where M is a unique abelian maximal subgroup of G . We know that for each $x \in G - M$, $x^2 \in \text{Z}(G)$. It follows that x inverts the cyclic group $M/\text{Z}(G)$ of order ≥ 4 and so $G/\text{Z}(G) \cong \text{D}_{2^{n+1}}$ is dihedral of order 2^{n+1} . Set $|\text{Z}(G)| = 2^m$, $m \geq 1$, and $(G/\text{Z}(G))' = L/\text{Z}(G)$ so that $G/L \cong \text{E}_4$ and $L = G'\text{Z}(G)$. Since G has an abelian maximal subgroup, we may use Lemma 1.1 and we get $|G| = 2^{m+n+1} = 2 \cdot 2^m|G'|$ and so $|G'| = 2^n$. Hence $G' \cap \text{Z}(G) = \langle z \rangle \cong \text{C}_2$, $G'/\langle z \rangle$ is cyclic of order 2^{n-1} and G' is abelian.

Suppose that G' is not cyclic. Then G' splits over $\langle z \rangle = G' \cap \text{Z}(G)$. Since $\mathfrak{U}_1(G')$ is normal in G and $\mathfrak{U}_1(G') \cap \text{Z}(G) = \{1\}$, it follows that $\mathfrak{U}_1(G') = \{1\}$ and so $G' \cong \text{E}_4$ and $G/\text{Z}(G) \cong \text{D}_8$. Let $a \in M - (\text{Z}(G)G')$ so that $\langle a \rangle$ covers $M/\text{Z}(G) \cong \text{C}_4$ and so $a^2 \notin \text{Z}(G)$. For an $x \in G - M$, we have $[a, x] = t \in G' - \langle z \rangle$. Then we get

$$[a^2, x] = [a, x]^a[a, x] = t^a t = t^2 = 1.$$

But then $\text{C}_G(a^2) = \langle M, x \rangle = G$ and so $a^2 \in \text{Z}(G)$, a contradiction. We have proved that G' is cyclic of order ≥ 4 .

For any $x \in G - M$ and any $m \in M - L$ (where $L = G'\text{Z}(G)$), we have $x^2 \in \text{Z}(G)$ and $[m, x] = g$ with $\langle g \rangle = G' \cong \text{C}_{2^n}$. This gives $m^x = mg$ and so $m = m^{x^2} = (mg)^x = mgg^x$ and this implies $g^x = g^{-1}$ and therefore x inverts G' . We have obtained the second possibility in part (a) of our theorem.

(ii) Now we consider the case, where G has no abelian subgroups of index 2, $G' \leq \text{Z}(G)$, $\Phi(G) \leq \text{Z}(G)$ and G' is elementary abelian. It follows that $|A : \text{Z}(G)| = 2$ for each maximal abelian subgroup A of G . If $|G : \text{Z}(G)| = 4$, then G would have an abelian subgroup of index 2, a contradiction. Hence, $G/\text{Z}(G) \cong \text{E}_{2^m}$, $m \geq 3$, and so

there exist elements $g, h, i \in G - Z(G)$ such that $\langle g, h, i \rangle Z(G)/Z(G) \cong E_8$. We have $[g, h] \neq 1$, $[g, i] \neq 1$, and $[h, i] \neq 1$.

Suppose that $|G'| = 2$. Then $[g, h] = [g, i]$ and so $[g, hi] = [g, h][g, i] = 1$ and therefore $\langle g, hi \rangle Z(G)/Z(G) \cong E_4$, a contradiction.

Suppose that $G' \cong E_4$. In that case $[g, h] = t_1$, $[g, i] = t_2$ and $[h, i] = t_3$, where t_1, t_2, t_3 are pairwise distinct involutions in G' . In this case,

$$[gh, gi] = [g, i][h, g][h, i] = t_2t_1t_3 = 1,$$

and so $\langle gh, gi \rangle Z(G)/Z(G) \cong E_4$, a contradiction. We have proved that $|G'| \geq 8$. \square

Corollary 81.5. *Let G be an arbitrary nonabelian 2-group. Let A and B be any two distinct maximal abelian subgroups in G with and intersection $A \cap B$ of maximal possible order. Then the nonabelian subgroup $H = \langle A, B \rangle$ either possesses an abelian subgroup of index 2 or H is of class 2 and H' is elementary abelian.*

Proof. Obviously, $A \cap B = Z(H)$. If C and D are any two distinct maximal abelian subgroups in H , then $C \cap D \geq Z(H)$ and the maximality of $|A \cap B|$ forces $C \cap D = Z(H)$. Then our result follows from Theorem 81.3. \square

A classification of 2-groups with exactly three involutions

This section is written by the second author. The first author inserted in proofs of theorems a number of explanations and added a few exercises.

According to Sylow–Frobenius, the number of involutions in a 2-group (also in any finite group of even order) is odd. The 2-groups with exactly one involution are classified (Proposition 1.3). Therefore, it is natural to classify the 2-groups with exactly three involutions. It appears that this problem is enormously difficult.

We finish here a classification of 2-groups with exactly three involutions (Theorems 82.1, 82.2, 82.8, 82.16, and 82.18). A. D. Ustjuzaninov [Ust2] has proved that if a 2-group G has exactly three involutions and $Z(G)$ is noncyclic, then G has a normal metacyclic subgroup M of index at most 4 and G/M is elementary abelian. M. Konvisser [Kon2] goes one step further and proves that if a 2-group G has exactly three involutions and $Z(G)$ is cyclic, then G has a metacyclic subgroup M of index at most 4 and “ M is normal in G in most of the cases”. But he is not very precise in which cases M is not normal in G and what is the structure of G in these cases. Here we clear up this remaining difficult situation and determine completely the structure of G in terms of two generators and relations.

Of course, if a 2-group G has exactly three involutions, it has no normal elementary abelian subgroups of order 8. However, it is impossible to deduce the classification of such groups as G from results of §50 where the groups without normal elementary abelian subgroups of order 8 are treated. It follows from §50 that our group G has a normal metacyclic subgroup M such that G/M is isomorphic to a subgroup of D_8 .

Now we describe the obtained results in some detail.

Let a 2-group G has exactly three involutions and $|G| > 4$. Then it possesses a normal abelian subgroup W which is either of type $(4, 2)$ or $(4, 4)$. Set $C = C_G(W)$; then C is metacyclic since $\Omega_2(C) = W$. (i) Suppose that G has no normal abelian subgroups of type $(4, 4)$. Then C is abelian of type $(2^n, 2)$, $n \geq 2$ and $|G/C| \leq 4$. If $n > 2$ and $|G/C| > 2$, then $G/C \cong E_4$. If $G/C \cong C_4$, then $n = 2$, $C = W$ and G is uniquely determined. (ii) Now let W be abelian of type $(4, 4)$. (ii1) Suppose that $\Omega_1(W) \leq Z(G)$. In that case G/C is elementary abelian of order ≤ 8 and $C \leq M \leq G$, where M is metacyclic with $|G : M| \leq 4$. (ii2) Next assume that $\Omega_1(W) \not\leq Z(G)$, i.e., $Z(G)$ is cyclic. (ii2.1) If $|G/C| > 2^3$, then $C = W$ and G is

one of eight two-generator groups of order 2^8 . (ii2.2) Now let $|G/C| = 8$. Then G possesses a metacyclic subgroup which is normal in G except in two cases described in detail; in both these cases $G/C \cong D_8$, $C < \Phi(G)$, $|\text{Z}(G)| = 2$ and G is given in terms of generators and defining relations.

Theorem 82.1. *Let G be a metacyclic 2-group. Then:*

- (i) *G contains exactly one involution if and only if G is either cyclic or generalized quaternion.*
- (ii) *G contains more than three involutions if and only if G is either dihedral or semidihedral.*
- (iii) *All other metacyclic 2-groups contain exactly three involutions.*

Proof. If G is cyclic or of maximal class, then the number of involutions in G is $\equiv 1 \pmod{4}$.

Suppose that G is metacyclic but neither cyclic nor of maximal class. Let $\{1\} \neq Z = \langle b \rangle \neq G$ be a cyclic normal subgroup of G , where G/Z is cyclic. Let H/Z be the subgroup of order 2 in G/Z . Then all involutions in G lie in H and H is not cyclic (otherwise, $Z \leq \Phi(H) \leq \Phi(G)$ so $G/\Phi(G)$ is cyclic and G is cyclic). If H is abelian or isomorphic to M_{2^n} , $n \geq 4$, then $\Omega_1(H) \cong E_4$ and G has exactly three involutions. If H is of maximal class, then $o(b) \geq 4$ and taking an element $x \in H - Z$, we have $b^x = b^{-1}$ or $b^x = b^{-1+2^{n-1}}$, where $o(b) = 2^n$, $n \geq 3$. But such an automorphism of order 2 induced with x on $\langle b \rangle$ is not a square in $\text{Aut}(\langle b \rangle)$ and so we have $G = H$ is of maximal class, a contradiction. \square

For another proof of Theorem 82.1, one can use Proposition 10.19(a).

Theorem 82.2. *Let G be a nonmetacyclic 2-group with exactly three involutions. If W is a maximal normal abelian noncyclic subgroup of exponent ≤ 4 in G , then $W \cong C_4 \times C_2$ or $W \cong C_4 \times C_4$, $W = \Omega_2(C_G(W))$ and $C_G(W)$ is metacyclic.*

Suppose that G has no normal subgroups isomorphic to $C_4 \times C_4$. Then G has a normal subgroup $W \cong C_4 \times C_2$, $C = C_G(W)$ is abelian of type $(2^n, 2)$, $n \geq 2$, and G/C is isomorphic to a proper (!) nontrivial subgroup of D_8 . If $n > 2$, then $G/C \cong C_2$ or E_4 . If $G/C \cong C_4$, then $n = 2$ and G is the unique 2-group of order 2^5 with $\Omega_2(G) \cong C_2 \times Q_8$ (see §52):

$$G = \langle g, v \mid g^8 = v^4 = 1, g^4 = v^2 = z, [v, g] = u, u^2 = [u, v] = 1, [u, g] = z \rangle.$$

Here $\text{Z}(G) = \langle z \rangle$ is of order 2, $W = \langle v, u \rangle \cong C_4 \times C_2$ is a maximal normal abelian subgroup of G , $G/W \cong C_4$, $\Omega_1(G) = \Omega_1(W) = \langle z, u \rangle \cong E_4$, $\Phi(G) = \langle g^2, u \rangle \cong C_4 \times C_2$, $G' = \langle z, u \rangle$, and $\Omega_2(G) = \langle W, g^2 \rangle \cong C_2 \times Q_8$.

Proof. Suppose that G is a nonmetacyclic 2-group with exactly three involutions. Let W be a noncyclic maximal abelian normal subgroup of exponent ≤ 4 in G . Since $|G| > 8$, we get $W \not\cong E_4$ (otherwise, $C_G(W) = W$ so $|G| = 8$). Therefore we

have either $W \cong C_4 \times C_2$ or $W \cong C_4 \times C_4$. By a result of Alperin (Corollary 10.2), $W = \Omega_2(C)$, where $C = C_G(W)$, and a result of N. Blackburn (Theorem 41.1, Remark 2) implies that C is metacyclic.

(See Exercise 49.1.) Suppose that $W \cong C_4 \times C_2$. Then Theorem 42.1 (noting that $|\Omega_2(C)| = 8$ and $Z(C)$ is noncyclic) implies that $C \cong C_{2^n} \times C_2$ with $n \geq 2$. If $n > 2$, then W contains a cyclic subgroup Z of order 4 which is characteristic in C and so Z is normal in G . Each $y \in G$ acts on Z and on $W_0 = \Omega_1(W) \cong E_4$ and so (noting that $\text{Aut}(Z) \cong C_2$ and a Sylow 2-subgroup of $\text{Aut}(W_0) \cong C_2$) $G/C \cong C_2$ or $G/C \cong E_4$ (take into account that $C = C_G(Z) \cap C_G(\Omega_1(W))$). We know that $\text{Aut}(W) \cong D_8$ and therefore if $G/C \cong C_4$ or $G/C \cong D_8$, then $n = 2$ so $C = W$.

It remains to treat the cases $G/W \cong C_4$ or D_8 , where $W = C = C_G(W)$. We shall show (as a surprise!) that $G/W \cong D_8$ actually cannot occur. We set $W = \langle v, u \mid v^4 = u^2 = [v, u] = 1 \rangle$ and $z = v^2$ so that $\langle z \rangle = \Omega_1(W) \leq Z(G)$. In any case, there is an element $g \in G$ inducing on W the following automorphism of order 4:

$$(1) \quad v^g = vu, \quad u^g = uz, \quad (v^{g^{-1}} = vu^{g^{-1}} = vu),$$

which implies

$$(1a) \quad \begin{aligned} v^{g^2} &= (vu)^g = (vu)(uz) = vz = v^{-1}, \\ u^{g^2} &= (uz)^g = (uz)z = u = u^{-1}, \end{aligned}$$

so that g^2 inverts each element of W so $g^4 \in C_G(W) = W$, and $C_W(g) = \langle z \rangle$. Hence

$$(2) \quad g^4 = z,$$

since $\Omega_1(G) = \Omega_1(W) = W_0 = \langle z, u \rangle$; in particular, $o(g) = 8$.

We compute for each $w \in W$:

$$(g^2w)^2 = g^2wg^2w = g^4w^{g^2}w = zw^{-1}w = z,$$

and so all elements in g^2W are of order 4 and therefore all elements in $\langle W, g \rangle - \langle W, g^2 \rangle$ are of order 8 (it is easy to check, using the previous displayed formula, that $(gw)^4 = (g^3w)^2 = z$). We get $\Omega_2(\langle W, g \rangle) = \langle W, g^2 \rangle = \langle u \rangle \times \langle v, g^2 \rangle \cong C_2 \times Q_8$, and so $\langle W, g \rangle$ is the unique group of order 25 with $\Omega_2(\langle W, g \rangle) \cong C_2 \times Q_8$ according to the results in §52. If $\langle W, g \rangle = G$, we are done.

We assume, by the way of contradiction, that $\langle W, g \rangle \neq G$. Then, by the above, $G/W \cong D_8$ so all elements in $G/W - (\langle g, W \rangle / W)$ are involutions. Therefore, there is $h \in G - \langle W, g \rangle$ such that h induces on W the following involutory automorphism:

$$(3) \quad u^h = uz, \quad v^h = v,$$

and so $C_W(h) = \langle v \rangle$ which together with $h^2 \in W$ forces $h^2 \in \langle v \rangle$. Indeed, since W has exactly two cyclic subgroups of order 4 and $\langle v \rangle$ is not normal in G , by (1), it

follows that $|G : N_G(\langle v \rangle)| = 2$, so each $h \in C_G(\langle v \rangle) - W$ satisfies (3). We also have $G = \langle W, g, h \rangle$. If $h^2 \in \langle z \rangle$, then $\langle W_0, h \rangle \cong D_8$ has $5 > 3$ involutions, a contradiction. Thus, replacing v with v^{-1} (if necessary, and noting that (1) remains valid), we may assume from the start:

$$(4) \quad h^2 = v.$$

Indeed, from what has just been said and (3), $o(h^2) > 2$ and $h^2 \in W$. From (3) follows $h^u = hz = hh^4 = h^{1+4}$ and so $\langle W, h \rangle \cong M_{24}$ is a metacyclic nonnormal subgroup of index 4 in G with $\Omega_1(\langle W, h \rangle) = \langle u, z \rangle$ and $\Omega_2(\langle W, h \rangle) = W$.

If $\Omega_2(G) = \Omega_2(\langle W, g \rangle) = \langle W, g^2 \rangle \cong C_2 \times Q_8$, then by the results in §52 (and the fact that $G > \Omega_2(G)$) we get $|G| = 2^5$, contrary to our assumption that $\langle W, g \rangle \neq G$. It follows that $G - \langle W, g \rangle$ must contain elements of order 4 and they must lie in the coset $(hg)W$ of the group $G/W \cong D_8$ (note that $(hg)W$ is a noncentral involution in G/W). By (3) and (4), we have

$$(4a) \quad u^{hg} = (uz)^g = (uz)z = u, \quad v^{hg} = v^g = vu,$$

and so $C_W(hg) = W_0$ which implies:

$$(5) \quad (hg)^2 = w_0 \in W_0 \quad \text{and} \quad w_0 \neq 1.$$

From (5) and (4) follows $hg hg = w_0, h^2 g^h g = w_0, vg^h = w_0 g^{-1}$, and so we obtain:

$$(6) \quad g^h = (v^{-1} w_0) g^{-1}.$$

For each $u^i v^j \in W$ we compute (take into account that all elements in the set $G - W$ are not involutions)

$$1 \neq ((hg)u^i v^j)^2 = (hg)^2(u^i v^j)^{hg} u^i v^j = w_0 u^i (vu)^j u^i v^j = w_0 (uz)^j$$

which implies, if we take $j = 1$ in the displayed formula, that $w_0 = (hg)^2 \neq uz$. Thus, $(hg)^2 = u$ or z . However, if $(hg)^2 = u$, then (by the above) $(h(gv))^2 = ((hg)v)^2 = u(uz) = z$ and so replacing g with gv (if necessary), we may assume from the start:

$$(7) \quad (hg)^2 = w_0 = z \quad \text{and} \quad g^h = (v^{-1} w_0) g^{-1} = (v^{-1} v^2) g^{-1} = vg^{-1}$$

(in the second formula we used (6)). Here we note that replacing g with gv , the previous relations (1) and (2) remain unaltered.

We observe that

$$\begin{aligned} L &= \langle W, g^2, hg \rangle = \Omega_2(G), & \langle L, h \rangle &= G, & L' &= \langle u, z \rangle = W_0, \\ Z(L) &= L', & \Phi(L) &= L' \end{aligned}$$

so that L is a special 2-group of order 2^5 . From (a4) and (a1) follows $[v, hg] = u$ and $[v, g^2] = z$, respectively. We compute using (1), (2), (4), and (7):

$$(g^2)^h = (vg^{-1})^2 = vv^g g^{-2} = v(vu)g^2z = v^2ug^2z = g^2u,$$

(since g^2 centralizes $W_0 = \langle u, z \rangle$ and $v^2 = z$) and so $[g^2, h] = u$. This implies that $[g^2, hg] = [g^2, g][g^2, h]^g = u^g = uz$.

We claim that $S = \langle g^2(hg), v(hg) \rangle \cong C_4 \times C_4$ is normal in G . This gives us our final contradiction since we have assumed that G has no normal subgroup isomorphic to $C_4 \times C_4$. Indeed,

$$\begin{aligned} [g^2(hg), v(hg)] &= [g^2, v][g^2, hg][hg, v] = z(uz)u = 1, \\ (g^2(hg))^2 &= g^4(hg)^2[hg, g^2] = zzuz = uz, \\ (v(hg))^2 &= v^2(hg)^2[hg, v] = zzu = u, \end{aligned}$$

and so $S \cong C_4 \times C_4$ and S is normal in L (since $S \geq W_0 = L'$). Finally, using (1), we get (recall that $g^4 = z$, by (2))

$$\begin{aligned} (hg)^h &= hv g^{-1} = (hg)(g^{-1}vg^{-1}) = (hg)g^{-2}(vgv^{-1}) = (hg)g^2zv^{g^{-1}} \\ &= (hg)g^2z(vuz) = (hg)g^2vu, \end{aligned}$$

so that, using the facts that $(hg)g^2 = g^2(hg)uz$ and $(hg)v = v(hg)u$, we get

$$\begin{aligned} (g^2(hg))^h &= (g^2u)(hg)g^2vu = g^4(hg)uzv = (hg)uv = v(hg), \\ (vg^2)^h &= (vg^2)u, \end{aligned}$$

which shows that S is normal in G since $v(hg) \cdot g^2(hg) \equiv vg^2 \pmod{W_0}$. \square

If, in Theorem 82.2, $|G : C| = 2$, then G possesses a cyclic subgroup of index 4 so its structure is described in §74. Next, one may assume, in this case, that $G - C$ has an element of order 4 (otherwise, G has exactly two cyclic subgroups of order 4, i.e., belongs to the groups classified early in this book; see §43). This fact can help to write out the defining relations for G .

In what follows G will denote a nonmetacyclic 2-group containing exactly three involutions and let W be a maximal normal abelian noncyclic subgroup of exponent ≤ 4 in G and assume that $W \cong C_4 \times C_4$. By Theorem 82.2, $\Omega_2(C) = W$, where $C = C_G(W)$ is metacyclic. We set $W_0 = \Omega_1(W) = \Omega_1(G)$ and denote with $A_G(W) \cong G/C$ the automorphism group of W induced by G .

Lemma 82.3. *Let v be an element of order 4 in $G - W$. Then v centralizes W_0 and W/W_0 and v inverts some element of order 4 in W .*

Proof. We have $v^2 \neq 1$ is an involution in W_0 . If v does not centralize W_0 , then $\langle W_0, v \rangle \cong D_8$ has exactly $5 > 3$ involutions, a contradiction. Thus v centralizes W_0 . Let us prove that v also centralizes W/W_0 . The subgroup $H = \langle v, W \rangle$ is nonabelian and $Z(H) < W$. It suffices to show that H/W_0 is abelian. Assuming that this is false, we get $H/W_0 \cong D_8$. If L/W_0 is a cyclic subgroup of order 4 in H/W_0 , then H has two distinct abelian maximal subgroups W and L so $Z(H) = W \cap L$ has index 4 in H . It follows that $|H'| = 2$ (Lemma 1.1) so $H' < W_0$. Then H/W_0 is abelian, contrary to the assumption. For each $w \in W$, $vw \in H - W$ so $1 \neq (vw)^2 = v^2 w^2 s$ with $s \in W_0$ (since v commutes with $w \bmod W_0$). Note that if $x \in vW$, then each of the four elements in xW_0 have the same square $x^2 \neq 1 \in W_0$ since $\langle x, W_0 \rangle$ is abelian of type (4, 2) and $o(x) = 4$. Since $|vW| = 16$ and W_0 has exactly three involutions, it follows that there is $x \in vW$ and $w \in W - W_0$ such that $x^2 = (xw)^2$. Hence $x^2 = (xw)^2 = xwxw = x^2 w^x w$, which gives $w^x = w^{-1}$. But then also $w^v = w^{-1}$, where w is some element of order 4 in W (since $x \in vW$ and v act the same way on the abelian group W). \square

Lemma 82.4. Suppose that G contains an element g which induces an automorphism γ of order 2 on W and for each element w of order 4 in W , $w^\gamma \neq w$. Then $o(g) = 4$.

Proof. Clearly, $g \in G - W$ so $o(g) > 2$. Since $o(\gamma) = 2$, $g^2 \in C$. If $o(g) > 4$, then $\Omega_2(\langle g \rangle) \leq \Omega_2(C) = W$ hence the group $\langle g_0 \rangle = \langle g \rangle \cap W$ is cyclic of order 4, so $g_0^\gamma = g_0$, a contradiction. Thus $o(g) = 4$. \square

Lemma 82.5. Suppose that $g \in G - C$ with $g^2 \in C$ and the automorphism γ induced by g on W inverts no element of order 4 in W . Then $\langle g, C \rangle$ is metacyclic (and so g centralizes some element of order 4 in W).

Proof. Each element in gC induces the involutory automorphism γ on W . By Lemma 82.3, no element in gC is of order 4. Thus $\Omega_2(\langle g, C \rangle) = W$ and so $\langle g, C \rangle$ is metacyclic (§41, Remark 2). The last assertion holds since $o(g) > 4$ and $\Omega_2(\langle g \rangle) \leq \Omega_2(C) = W$. \square

Lemma 82.6. The automorphism group $\text{Aut}(W)$ of $W = \langle u, y \mid u^4 = y^4 = [u, y] = 1 \rangle \cong C_4 \times C_4$ is of order $2^5 \cdot 3$. The subgroup A of $\text{Aut}(W)$ of all automorphisms normalizing the subgroup $Y = \langle u^2, y \rangle \cong C_2 \times C_4$ is of order 2^5 and so is a Sylow 2-subgroup of $\text{Aut}(W)$. We have $A' = Z(A) = \Phi(A) \cong E_4$ and so A is a special 2-group. Set $W_0 = \Omega_1(W) = \langle u^2, y^2 \rangle$. Then the stabilizer A_0 of the chain $W > W_0 > \{1\}$ is elementary abelian of order 2^4 . The subgroup A_0 contains the “special” subset $S = \{\sigma^2, \xi, \zeta, \mu, \nu\}$ of five automorphisms defined by:

$$\begin{aligned} u^\sigma &= uy, & y^\sigma &= y; & u^\xi &= u, & y^\xi &= yu^2; \\ u^\xi &= uu^2y^2, & y^\xi &= yu^2y^2; & u^\mu &= uu^2y^2, & y^\mu &= yu^2; \\ u^\nu &= uy^2, & y^\nu &= yu^2y^2. \end{aligned}$$

Each $\tau \in S$ has the property that τ does not invert any element of order 4 in W . If X is any maximal subgroup of A_0 , then $X \cap S$ is nonempty. In addition, the “superspecial” automorphisms μ and ν have also the property that they do not centralize any element of order 4 in W .

Finally, A is Q_8 -free but is not D_8 -free.

Proof. See Proposition 50.5. According to the Main Theorem 79.7, A is a Wilkins group of type (b) ($= W_b$ -group) and so A is Q_8 -free but is not D_8 -free. \square

Remark. The group A of Lemma 82.6 has class number 14. Indeed, if χ is an irreducible character of A , then $\chi(1)^2 \leq |A : Z(A)| = 8$ so $\chi(1) \in \{1, 2\}$. Since $|A : A'| = 8$, A has exactly 8 distinct linear characters and $\frac{1}{4}(|A| - |A : A'|) = 6$ distinct nonlinear characters. It follows that the class number of A equals $8 + 6 = 14$, as was to be shown. Since each element of $A_0 - Z(A)$ has exactly two A -conjugates, A_0 is the union of $|Z(A)| + \frac{1}{2}(|A - Z(A)|) = 10$ A -classes. It follows from $|Z(A)| = 4$ that four A -classes contained in $A - A_0$, have size 4.

Lemma 82.7. *No element of G can induce either of the “superspecial” automorphisms μ or ν on $W = \langle u, y \rangle$ (from Lemma 82.6).*

Proof. Suppose that $g \in G$ induces μ or ν on W . Then $g^2 \in C$ and g neither inverts nor centralizes any element of order 4 in W . By Lemma 82.3, $o(g) > 4$ and by Lemma 82.4, $o(g) = 4$, a contradiction. \square

Theorem 82.8 ([Ust2]). *Let G be a 2-group containing exactly three involutions and a normal subgroup $W \cong C_4 \times C_4$. If $\Omega_1(W) \leq Z(G)$, then G contains a normal metacyclic subgroup M of index at most 4 and $\exp(G/M)$ divides 2.*

Proof. Since $\Omega_1(W) = W_0 \leq Z(G)$, G/C stabilizes the chain $W > W_0 > \{1\}$ (see Lemma 82.6) and so G/C is elementary abelian of order $\leq 2^4$. By Lemma 82.7, $|G/C| \leq 2^3$. Suppose that $|G/C| = 2^3$. Then Lemma 82.6 implies that there is $g \in G - C$ inducing a “special” automorphism on W (which does not invert any element of order 4 in W). By Lemma 82.5, the subgroup $M = \langle g, C \rangle$ is metacyclic with $|G : M| = 4$ and M is normal in G and G/M is elementary abelian. \square

In what follows we assume, in addition, that $W_0 = \Omega_1(W) \not\leq Z(G)$.

Lemma 82.9. *If $\Omega_1(W) \not\leq Z(G)$, then with the appropriate choice of generators u and y of W , one of the following four automorphisms is contained in $A_G(W) = G/C$: $\lambda(i, j) : u \rightarrow uy, y \rightarrow u^{2i}y^j$, where $i = 0, 1$ and $j = 1, -1$. These automorphisms lie in four distinct conjugate classes in A (recall that $A = N_{\text{Aut}(W)}(\langle u^2, y \rangle) \in \text{Syl}_2(\text{Aut}(W))$; see Lemma 82.6), where each one is of length 4. We have $Z(A) = \Phi(A) = A' = \langle \lambda^2(0, 1), \lambda^2(1, 1) \rangle = \langle \lambda^2(0, 1), \lambda^2(1, -1) \rangle$ and no two of the elements of order 4 in $\{\lambda(0, 1), \lambda(1, 1), \lambda(1, -1)\}$ are permutable and $\lambda(0, -1)$ is of order 2.*

Proof. Let λ be an element of $A_G(W)$ which does not centralize $\Omega_1(W)$. Each element in $\Omega_1(W)$ is a square in W . Let $u^2 \in \Omega_1(W)$ be such that $(u^2)^\lambda \neq u^2$ ($u \in W$). Set $y = u^{-1}u^\lambda$; then $y^2 = u^2(u^2)^\lambda \notin \{1, u^2\}$ and $o(y) = 4$ so that $u^\lambda = uy$, $W = \langle u \rangle \times \langle y \rangle$ and $y^\lambda = u^{2i}y^j$, $i = 0, 1$, $j = 1, -1$.

Recall that A_0 is the stabilizer of the chain $\{1\} < W_0 < W$; then A_0 is elementary abelian of order 2^4 (Lemma 82.6). For each $\lambda \in A - A_0$, $C_A(\lambda) = \langle \lambda \rangle A'$ (since $A' = Z(A)$ is of order 4) and so the conjugacy class of λ has exactly four elements lying in $\{\lambda A'\}$. Also, $\lambda^2(0, 1)$, $\lambda^2(1, 1)$, and $\lambda^2(1, -1)$ are three distinct involutions in A' . In particular, $\lambda(0, 1)$ (order 4), $\lambda(1, 1)$ (order 4), $\lambda(1, -1)$ (order 4), and $\lambda(0, -1)$ (order 2) lie in four distinct conjugacy classes in A . Since $C_4 \times C_4$ is not a subgroup of A (because $|Z(A)| = 4$), no two elements in $\{\lambda(0, 1), \lambda(1, 1), \lambda(1, -1)\}$ are permutable (recall that, by the above, any two cyclic subgroups, generated by these automorphisms, have trivial intersection). \square

Lemma 82.10. *In the notation of Lemma 82.9, we have $\lambda(1, 1) \notin A_G(W)$.*

Proof. If $g \in G$ induces the automorphism $\lambda(1, 1)$ (of order 4) on W given by $u^g = uy$, $y^g = u^2y$, then $g^4 \in C = C_G(W)$ and $C_W(\langle g \rangle) = \langle y^2 \rangle$. Hence $g^4 = y^2$ since g^2 cannot be an involution. But then $(g^2u)^2 = g^4u^{g^2}u = y^2u^{-1}y^2u = 1$, which is a contradiction since G has only three involutions. \square

Lemma 82.11. *If $\lambda(0, -1) \in A_G(W)$, then $C_G(W) > W$, and if $g \in G$ induces $\lambda(0, -1)$ on W , then $g^2 \in C_G(W) - W$ and $\langle g^2 \rangle > \langle u^2y \rangle$.*

Proof. Let $g \in G$ induce $\lambda(0, -1)$ on W so that $u^g = uy$, $y^g = y^{-1}$. Then $u^{g^2} = uyy^{-1} = u$, $y^{g^2} = y$ so $g^2 \in C = C_G(W)$. Next, it follows from $u^i y^j = (u^i y^j)g = (uy)^i y^{-j} = u^i y^{i-j}$ that $2j \equiv i \pmod{4}$, and so $C_W(g) = \langle u^2y \rangle$. If $g^2 = (u^2y)^i$, then $(gu^{-i})^2 = gu^{-i}gu^{-i} = g^2(u^{-i})^g u^{-i} = (u^2y)^i (uy)^{-i} u^{-i} = 1$, a contradiction. So $g^2 \notin W$ and therefore $\langle g^2 \rangle > \langle u^2y \rangle$ and $C > W$. \square

Lemma 82.12. *Setting $C = C_G(W)$, we have either $|\Omega_3(C)| \leq 2^5$ in which case $C \cong C_4 \times C_{2^n}$, $n \geq 2$, or $|\Omega_3(C)| = 2^6$ in which case C/W is metacyclic with exactly three involutions.*

Proof. We have $W = \Omega_2(C)$ and C is metacyclic so that C/W is also metacyclic. Suppose that C/W is of maximal class. Let D/W be a cyclic maximal subgroup of C/W . Then D is an abelian maximal subgroup of C . Set $R/W = (C/W)'$ so that $R > W$, $|D/R| = 2$, and $C/R \cong E_4$. Now, C' covers R/W and C' is cyclic since C is metacyclic, and so $C' \cap W \cong C_4$. Indeed, $C' \cap W \geq 2$, and, assuming that there we have equality, we see that a metacyclic group $C/(C' \cap W)$ contains a nonmetacyclic subgroup $C'/(C' \cap W) \times W/(C' \cap W)$, which is a contradiction. This implies $|R : C'| = 4$ and so $|C : C'| = |C : R||R : C'| = 2^4$. Noting that C is nonabelian but possesses an abelian maximal subgroup, we get, by Lemma 1.1, $|Z(C)| = \frac{1}{2}|C : C'| = 2^3$. This is a contradiction since $W \leq Z(C)$ and $|W| = 2^4$.

We have proved that C/W is not of maximal class. If C/W is cyclic, then, since $\Omega_2(C) = W$, C is abelian of type $(2^2, 2^n)$, $n \geq 2$, and $2^4 \leq |\Omega_3(C)| \leq 2^5$. If C/W is noncyclic, then C/W is metacyclic with exactly three involutions (Theorem 82.1) and so $\Omega_1(C/W) \cong E_4$ which implies $|\Omega_3(C)| = 2^6$. \square

Lemma 82.13. *If $|\Omega_3(C)| = 2^6$, then $|A_G(W)| \leq 8$.*

Proof. Here $C = C_G(W)$, $W_0 = \Omega_1(W)$, and $D = \Omega_3(C)$. If X is any subgroup of D such that $W < X < D$, then $X \cong C_8 \times C_4$ is abelian since $\Omega_2(C) = W \leq Z(C)$. But $D/W \cong E_4$ (Lemma 82.12) and D is metacyclic and so $\Phi(D) = W$. It follows that D is either abelian or minimal nonabelian. Since $\exp(D) = 8$, we have $D = \langle a, d \mid a^8 = d^8 = 1, a^d = a^{1+4\epsilon}, \epsilon = 0, 1 \rangle$, where $W = \langle a^2, d^2 \rangle$.

Suppose that $|G/C| > 8$ (recall that $A_G(W) = G/C$). We identify G/C with a subgroup S of the group A of all 2^5 automorphisms of $W = \langle u, y \rangle$ keeping $\langle y, u^2 \rangle$ fixed (see Lemma 82.6 and 82.9). In particular, S contains the involutory automorphism $\beta = \lambda^2(1, 1)$ (since $S \geq \Phi(A)$), where $u^\beta = u^{-1}y^2$, $y^\beta = y^{-1}$ and we note that β centralizes W_0 (and W/W_0) and $w^\beta \neq w$ for each $w \in W - W_0$. Let $g \in G$ induce the automorphism β on W . Then $g^2 \in C$ and since g fixes no element in $W - W_0$, we have $g^2 \in W_0$ implying that $g^2 \in Z(C)$ and $o(g) = 4$. It follows that g induces an involutory automorphism on $D = \Omega_3(C) = \langle a, d \rangle$. We claim that g fixes each of the three maximal subgroups $S_1 = \langle a, W \rangle$, $S_2 = \langle d, W \rangle$, $S_3 = \langle ad, W \rangle$ of D each of which is abelian of type $(8, 4)$. If, for example, $S_1^g = S_2$, then $(\Omega_1(S_1))^g = \Omega_1(S_2)$ and so $\langle a^2, W_0 \rangle^g = \langle d^2, W_0 \rangle$ which contradicts the fact that β centralizes W/W_0 . Hence g induces an involutory automorphism on each of three abelian subgroups S_1 , S_2 , S_3 and $C_{S_i}(g) = W_0$ for each $i = 1, 2, 3$. By Proposition 51.2, g inverts each of three subgroups $\Omega_1(S_1)$, $\Omega_1(S_2)$, and $\Omega_1(S_3)$ (which are three maximal subgroups of W) and so g inverts W , contrary to the fact that $u^\beta = u^{-1}y^2 \neq u^{-1}$. \square

Lemma 82.14. *Suppose there is an element $s \in G$ which induces the automorphism $\gamma = \lambda^2(0, 1)$ on W and $|\Omega_3(C)| = 2^5$, where $C = C_G(W)$. Then $C = \langle s^2 \rangle \times \langle u \rangle \cong C_{2^n} \times C_4$, where $n \geq 3$ and the element $u \in W$ is as in Lemma 82.9. If $S = \langle s, C \rangle$, then $\Omega_2(S) = \langle s^4 \rangle$ and S is minimal nonabelian metacyclic.*

Proof. Set again $W_0 = \Omega_1(W)$, where $W = \langle u, y \rangle$, $u^\gamma = uy^2$, $y^\gamma = y$ and note that γ is “special” in the sense of Lemma 82.6. Also set $S = \langle s, C \rangle$ so that $|S : C| = 2$ since $s^2 \in C$. Each element in sC induces the “special” automorphism γ on W and since γ does not invert any element in $W - W_0$, Lemma 82.3 implies that there are no elements of order 4 in $S - C$. Hence $\Omega_2(S) = W$, and Remark 2 following Theorem 41.1 shows that S is metacyclic.

We know from Lemma 82.12 that C is abelian of type $(2^n, 2^2)$, $n \geq 3$, so that $\Omega_3(C)$ is abelian of type $(8, 4)$ and $C/W \neq \{1\}$ is cyclic.

Suppose that there is $x \in S - C$ with $x^2 \in W$ (in which case $x^2 \in W - W_0$ since $\Omega_2(S) = W$). Set $T = \langle \Omega_3(C), x \rangle$, where $|\Omega_3(C) : W| = 2$, by hypothesis, $T/W \cong E_4$, and all elements in $T - W$ are of order 8 (noting that $W \leq \Omega_2(T) \leq$

$\Omega_2(S) = W$ so $\Omega_2(T) = W$. Since T is metacyclic as a subgroup of S and $T/W \cong E_4$, we get $\Phi(T) = W$. Also x , the element of T , induces on W the involutory automorphism γ (indeed, $x^{-1}s \in C$ in view of $|S : C| = 2$) and so T is nonabelian. If $|T'| = 2$, then this fact together with $d(T) = 2$ implies that T is minimal nonabelian which forces $W = \Phi(T) = Z(T)$, a contradiction since, by the choice, x does not centralizes W . Hence $|T'| > 2$. On the other hand, $\exp(T) = 8$, $|T| = 2^6$, and T is metacyclic. Thus T possesses a cyclic normal subgroup Z of order 8 such that $T/Z \cong C_8$. Since $T' < Z$, we get $T' \cong C_4$. But $\text{Aut}(Z) \cong E_4$ and so $|T : C_T(Z)| = 2$ and if $t \in T - C_T(Z)$, then t induces an involutory automorphism on Z . Next, $C_T(Z)$ is abelian of type $(8, 4)$, $t^2 \in Z(T)$. Assume that $T' < Z(T)$. Then $|T : Z(T)| = 4$ so $|T'| = 2$ (Lemma 1.1), a contradiction. Then t does not centralize T' so t inverts T' (in view of $T' \cong C_4$, the unique nonidentity automorphism inverts T'). Since t induces on W the “special” automorphism γ which does not invert any element of order 4 in W , we get a contradiction since $T' < W$.

We have proved that for each $x \in S - C$, $x^2 \in C - W$. In particular, $\Omega_3(C)/W$ is the unique subgroup of order 2 in S/W , and so S/W is either cyclic or generalized quaternion.

Suppose that S/W is generalized quaternion. Set $C_0/W = (S/W)'$ so that $|S : C_0| = 4$, $S' < C_0$ ($<$, by Taussky's theorem, since S is not of maximal class in view of $W < S$), S' covers C_0/W , S' is cyclic since S is metacyclic and $\Omega_2(S') < \Omega_2(S) = W$. Hence $S' \cap W \cong C_4$ which implies $|C_0 : S'| = 4$ and $|S : S'| = |S : C_0||C_0 : S'| = 16$. Noting that S has the abelian maximal subgroup $C \cong C_{2^n} \times C_4$, we get, by Lemma 1.1, $|Z(S)| = \frac{1}{2}|S : S'| = 2^3$. On the other hand, $W_0 \leq Z(S)$ and if $x \in S - C$, then $x^2 \in \Omega_3(C) - W$ and so $o(x^2) = 8$. We get $C_S(x^2) \geq \langle C, x \rangle = S$ and so $x^2 \in Z(S)$. Hence $Z(S) \geq \langle W_0, x^2 \rangle$ and so $|Z(S)| \geq 2^4$, a contradiction.

We have proved that S/W is cyclic and so, if $s \in S - C$, then $\langle s \rangle$ covers S/W and $\langle s \rangle \cap W \cong C_4$. Since $C_W(s) = \langle W_0, y \rangle$, we have $\langle s \rangle \cap W = \langle y \rangle$ or $\langle s \rangle \cap W = \langle yu^2 \rangle$ and so in any case $C = \langle s^2 \rangle \times \langle u \rangle$. Also, $\langle s \rangle W_0$ is another abelian maximal subgroup of S (distinct from C) and so $|S'| = 2$ (Lemma 1.1). It follows that S (being metacyclic) is minimal nonabelian (see also Lemma 65.2(a)). For each $s^i u^j \in S$, we get $(s^i u^j)^4 = (s^4)^i (u^4)^j [u^j, s^i]^6 = (s^4)^i$, which implies $\Omega_2(S) = \langle s^4 \rangle$, and we are done. \square

Recall that the unique minimal nonabelian nonmetacyclic group of order 2^4 is isomorphic to $\langle x, y \mid x^4 = y^2 = z^2 = 1, z = [x, y], [x, z] = [y, z] = 1 \rangle$ (Lemma 65.1). Recall also that $A_G(W)$ is the group of automorphisms induced by G on its normal abelian subgroup $W = \langle u \rangle \times \langle y \rangle$ of type $(4, 4)$.

Lemma 82.15. *If $|A_G(W)| > 2^3$, then $|A_G(W)| = 2^4$, $W = C_G(W)$ and $A_G(W) = \langle \lambda(0, 1), \lambda(1, -1) \rangle$ which is the minimal nonabelian nonmetacyclic group of order 2^4 .*

Proof. The “superspecial” automorphisms μ and ν and $\lambda(1, 1)$ cannot be contained in $A_G(W)$ (Lemma 82.7 and 82.10) and so $|A_G(W)| = 2^4$ and $A_G(W)$ is a maximal subgroup in the automorphism group A (of order 2^5) of all automorphisms of

W fixing the subgroup $\langle W_0, y \rangle$, where $W_0 = \Omega_1(W)$. This implies that $\mu\nu$ and $v\lambda(1, 1)$ are contained in $A_G(W)$. We check that $\lambda^{-1}(0, 1) = v\lambda(1, 1)$ and so $\langle \mu\nu, \lambda(0, 1) \rangle \leq A_G(W)$, where we also see that $\mu\nu = \lambda^2(1, -1)$ and $Z(A) = \Phi(A) = \langle \lambda^2(0, 1), \lambda^2(1, -1) \rangle$ (see Lemma 82.6 and Lemma 82.9).

There are exactly three maximal subgroups of A containing $\langle \mu\nu, \lambda(0, 1) \rangle$ (which is abelian of type $(4, 2)$ and contains $\Phi(A)$) and they are candidates for $A_G(W)$:

$$\langle \lambda(0, 1), \lambda(1, 1) \rangle, \quad \langle \lambda(0, 1), \lambda(0, -1), \lambda^2(1, 1) \rangle, \quad \langle \lambda(0, 1), \lambda(1, -1) \rangle.$$

We claim that the last subgroup coincides with $A_G(W)$. Since $\lambda(1, 1) \notin A_G(W)$, it will suffice to show that $A_G(W) \neq \langle \lambda(0, 1), \lambda(0, -1), \lambda^2(1, 1) \rangle$.

Suppose, by the way of contradiction, that $A_G(W) = \langle \lambda(0, 1), \lambda(0, -1), \lambda^2(1, 1) \rangle$. Then using Lemmas 82.11, 82.12, and 82.13, we see that $|\Omega_3(C)| = 2^5$ and $C \cong C_{2^n} \times C_4$, $n \geq 3$. Let $t \in G$ induce $\lambda(0, 1)$ on W so that $u^t = uy$, $y^t = y$ and $C_W(t) = \langle y \rangle$. Using Lemma 82.14, we get $\langle t \rangle \cap W \cong C_4$ and $\langle t \rangle \cap W = [t, W] = \langle [t, u] \rangle = \langle t^{2^n} \rangle$ for some $n \geq 3$. We have $C = C_G(W) = \langle t^4 \rangle \times \langle u \rangle$ and setting $T = \langle t, C \rangle$ we get $T' = [t, W] = \langle y \rangle \leq Z(T)$ and so T is of class 2. Consider the element $\rho = \mu\nu \cdot \lambda(0, 1)\lambda(0, -1) \in A_G(W)$ and check that $u^\rho = u^{-1}$ and $y^\rho = y$ so that $(t^{2^n})^\rho = t^{2^n}$. On the other hand, $\rho^{-1}\lambda(0, 1)\rho = \lambda^{-1}(0, 1)$ (which is verified by direct application of both sides on u and y) and so, if $r \in G$ induces ρ on W , then $t^r \equiv t^{-1} \pmod{C}$ which gives $t^r = t^{-1+4i}u^j$ for some $i, j \in \mathbb{Z}$. Thus $(t^{2^n})^r = (t^{-1+4i}u^j)^{2^n} = t^{-2^n}$, where we have used the fact that T is of class 2 and $n \geq 3$. But this contradicts the above result $(t^{2^n})^r = t^{2^n}$.

We have proved that $A_G(W) = \langle \lambda(0, 1), \lambda(1, -1) \rangle$. Hence $A_G(W)$ is generated by two elements $\lambda(0, 1)$ and $\lambda(1, -1)$ of order 4 and we have

$$[\lambda^2(0, 1), \lambda(1, -1)] = [\lambda(0, 1), \lambda^2(1, -1)] = 1, \quad [\lambda(0, 1), \lambda(1, -1)] \neq 1,$$

and $A_G(W)$ is Q_8 -free (Lemma 82.6 and 82.9). This implies that $A_G(W)$ is the uniquely determined minimal nonabelian nonmetacyclic group of order 2^4 (Lemma 79.2).

Suppose $C > W$ so that C is abelian of type $(2^m, 2^2)$, $m \geq 3$ (Lemma 82.12, 82.13, and 82.14). Set $S = \langle t^2, C \rangle$, where $t \in G$ induces $\lambda(0, 1)$ on W . By the structure of $G/C \cong A_G(W)$, S is normal in G and by Lemma 82.14, $\mathfrak{U}_2(S) = \langle s^4 \rangle$ (with $s = t^2$) is a cyclic characteristic subgroup of S of order at least 4. Hence W contains a cyclic subgroup of order 4 which is normal in G . However, $\lambda(1, -1)$ does not normalize any of the six cyclic subgroups of order 4 in W . Hence $C = W$. \square

Recall that automorphisms $\lambda(i, j)$ of W are defined in Lemma 82.9 as follows:

$$\lambda(i, j) : u \rightarrow uy, \quad y \rightarrow u^{2i}y^j, \quad \text{where } i = 0, 1 \text{ and } j = 1, -1.$$

Theorem 82.16. *Let G be a 2-group containing exactly three involutions and a normal subgroup $W \cong C_4 \times C_4$. Suppose that $|G/C_G(W)| > 2^3$. Then $C_G(W) = W$,*

$\Omega_1(W) \not\leq Z(G)$ so that $Z(G)$ is cyclic, G/W is the unique minimal nonabelian nonmetacyclic group of order 2^4 , and G is isomorphic to one of the following eight groups of order 2^8 :

$$(*) \quad \begin{aligned} G = \langle g, h \mid g^{16} = 1, & g^4 = y, h^4 = y^2, (h^2g)^2 = u^i y^{2\eta} g^2, \\ & u^4 = [u, y] = 1, (gh)^2 = u^{2\epsilon} y^2, u^g = uy, y^g = y, \\ & u^h = uy, y^h = u^2 y^{-1} \rangle, i = \pm 1, \epsilon, \eta = 0, 1. \end{aligned}$$

Here we have $\langle u, y \rangle = W$, $Z(G) = \langle y^2 \rangle \cong C_2$, $\Phi(G) = \langle W, g^2, h^2 \rangle$, $T = \langle W, g \rangle$ is a nonnormal metacyclic subgroup of class 2 with $|G : T| = 4$, $S = \langle W, g^2 \rangle$ is normal in G and $G/S \cong D_8$.

Conversely, each of the eight groups of order 2^8 given with $(*)$ has exactly three involutions and satisfies the assumptions of our theorem.

Proof. (i) Using Lemma 82.15, we have $W = C_G(W)$ and $G/W \cong A_G(W) = \langle \lambda(0, 1), \lambda(1, -1) \rangle$ is the minimal nonabelian nonmetacyclic group of order 2^4 so that $\Phi(A_G(W)) = Z(A_G(W)) = \langle \lambda^2(0, 1), \lambda^2(1, -1) \rangle$, $\lambda(0, 1) \cdot \lambda(1, -1)$ is an involution not contained in $Z(A_G(W))$, and $(A_G(W))' = \langle \lambda^2(0, 1) \cdot \lambda^2(1, -1) \rangle$, where

$$u^{\lambda(0, 1)} = uy, \quad y^{\lambda(0, 1)} = y, \quad u^{\lambda(1, -1)} = uy, \quad y^{\lambda(1, -1)} = u^2 y^{-1}.$$

Let $g \in G$ be an element inducing $\lambda(0, 1)$ on $W = \langle u, y \rangle$ so that

$$u^g = uy, \quad y^g = y, \quad u^{g^2} = uy^2, \quad y^{g^2} = y, \quad u^{g^{-1}} = uy^{-1}, \quad y^{g^{-1}} = y.$$

Since $C_W(g) = \langle y \rangle$, we have $g^4 \in \langle y \rangle$. Also, $[W, g] = \langle y \rangle$ and since g^2 does not invert any element in $W - W_0$, g^2W does not contain any element of order 4 (Lemma 82.3). Hence $\Omega_2(\langle W, g \rangle) = W$ and so $T = \langle W, g \rangle$ is metacyclic, $\langle g^4 \rangle = \langle y \rangle$, and $o(g) = 16$. We have $T' = \langle y \rangle = \langle g^4 \rangle \leq Z(T)$ and so T is of class 2, $\langle g \rangle$ is normal in T and $|G : T| = 4$. Set $S = \langle W, g^2 \rangle$. By the structure of G/W , T is a non-normal metacyclic subgroup of index 4 in G and S is normal in G with $G/S \cong D_8$. If $g^4 = y^{-1}$, then we replace u, y with $u' = u^{-1}, y' = y^{-1}$ so that (noting that T is of class 2):

$$\begin{aligned} [u', g] &= [u^{-1}, g] = [u, g]^{-1} = y^{-1} = y', \\ g^4 &= y', \quad (u')^g = u'y', \quad (y')^g = y^{-1} = y', \\ (u')^{\lambda(1, -1)} &= u^{-1}y^{-1} = u'y', \quad (y')^{\lambda(1, -1)} = u^2y = (u')^2(y')^{-1}. \end{aligned}$$

Thus, writing again u, y instead of u', y' , we may assume from the start that $[u, g] = y = g^4$.

For each $u^i y^j \in W$, we compute:

$$(g^2 u^i y^j)^2 = g^4 (u^{g^2})^i (y^{g^2})^j u^i y^j = y u^i y^{2i} y^j u^i y^j = y^{1+2(i+j)} u^{2i},$$

which shows that $o(g^2 u^i y^j) = 8$ and so indeed $\Omega_1(\langle W, g \rangle) = \langle u^2, y^2 \rangle = W_0$.

Let $h \in G$ be an element such that h induces $\lambda(1, -1)$ on W so that $G = \langle W, g, h \rangle$ and

$$\begin{aligned} u^h &= uy, & y^h &= u^2y^{-1}, & u^{h^2} &= u^{-1}, \\ y^{h^2} &= y^{-1}, & u^{h^{-1}} &= u^{-1}y^{-1}, & y^{h^{-1}} &= u^2y, \end{aligned}$$

which implies $C_W(h) = \langle y^2 \rangle$ and therefore $h^4 = y^2$. Since h^2 inverts W , we have, for each $w \in W$. $(h^2w)^2 = h^4(w)^{h^2}w = y^2w^{-1}w = y^2$, and so $\Omega_1(\langle W, h \rangle) = W_0 = \langle y^2, u^2 \rangle$.

Since $\lambda(0, 1) \cdot \lambda(1, -1)$ is an involution in $A_G(W)$, we have $(gh)^2 \in W$ and

$$u^{gh} = u^{-1}, \quad y^{gh} = y(u^2y^2), \quad (uy)^{gh} = (uy)y^2,$$

so that $C_W(gh) = W_0$ and $(gh)^2 = w_0 \in W_0$, $w_0 \neq 1$. All elements in ghW must be of order 4. For each $u^i y^j \in W$, we get

$$((gh)u^i y^j)^2 = (gh)^2(u^{gh})^i(y^{gh})^j u^i y^j = w_0 u^{-i} y^j u^{2j} y^{2j} u^i y^j = w_0 u^{2j},$$

and so $w_0 \neq u^2$ which implies:

$$(8) \quad (gh)^2 = u^{2\epsilon} y^2, \quad \epsilon = 0, 1.$$

As result, we have obtained the group G satisfying (*).

(ii) It remains to show that any group given by (*), has exactly three involutions.

We have $\Omega_1(G/W) = \langle gh, g^2, h^2 \rangle W/W \cong E_8$ and so we must show that there are no involutions in $(\langle gh, g^2, h^2 \rangle W) - W$. We have already shown that there are no involutions in cosets g^2W, h^2W , and $(gh)W$. Since $(G/W)' = \langle g^2h^2 \rangle W/W$ and

$$\begin{aligned} (gh)^g &\equiv gh^g \equiv gh(g^2h^2) \pmod{W}, \\ ((gh)h^2)^g &\equiv gh^g h^2 \equiv gh(g^2h^2)h^2 \equiv (gh)g^2 \pmod{W}, \end{aligned}$$

it follows that we still have to require (and show) that there are no involutions in cosets $(gh)h^2W$ and g^2h^2W .

From (8) follows:

$$\begin{aligned} (hg)^2 &= hghg = g^{-1}(ghgh)g = ((gh)^2)^g = (u^{2\epsilon} y^2)^g \\ &= u^{2\epsilon} y^{2\epsilon} y^2 = u^{2\epsilon} y^{2(\epsilon+1)}, \end{aligned}$$

and so we get:

$$(9) \quad (hg)^2 = u^{2\epsilon} y^{2(\epsilon+1)}.$$

From (8) and (9) (since g commutes with y) follows:

$$\begin{aligned} (ghgh)(hghg) &= u^{2\epsilon} y^2 \cdot u^{2\epsilon} y^{2(\epsilon+1)} = y^{2\epsilon}, \\ gh^{-1}(h^2gh^2g)hg &= y^{2\epsilon}, \quad h^{-1}(h^2g)^2h = y^{2\epsilon}g^{-2} = y^{2\epsilon}g^{-4}g^2 = y^{2\epsilon-1}g^2, \end{aligned}$$

and so

$$(10) \quad (h^2g)^2 = (y^{2\epsilon-1})^{h^{-1}}(g^2)^{h^{-1}} = u^2y^{2\epsilon-1}(g^2)^{h^{-1}}.$$

Again from (8) and (9) follows: $(hghg)(ghgh) = y^{2\epsilon}$, $hg(hg^2h^{-1})(h^2g)h = y^{2\epsilon}$, and so multiplying the last relation with h from the left and with h^{-1} from the right we get:

$$(h^2g)(g^2)^{h^{-1}}(h^2g) = hy^{2\epsilon}h^{-1} = (y^{h^{-1}})^{2\epsilon} = (u^2y)^{2\epsilon} = y^{2\epsilon},$$

and so

$$(g^2)^{h^{-1}} = (h^2g)^{-1}y^{2\epsilon}(h^2g)^{-1} = (y^{2\epsilon})^{h^2g}(h^2g)^{-2} = y^{-2\epsilon}(h^2g)^{-2},$$

which together with (10) gives $(h^2g)^2 = u^2y^{2\epsilon-1} \cdot y^{-2\epsilon}(h^2g)^{-2}$, and so we obtain finally,

$$(11) \quad (h^2g)^4 = u^2y^{-1}.$$

Since $W\langle h^2, g \rangle / W$ is abelian of type $(4, 2)$, we get $(h^2g)^2 = u^i y^j g^2$ for some $i, j \in \mathbb{Z}$. This gives together with (11):

$$\begin{aligned} (h^2g)^4 &= u^2y^{-1} = u^i y^j g^2 \cdot u^i y^j g^2 = u^i y^j g^4 (u^i y^j)^{g^2} \\ &= u^i y^j y u^i y^{2i} y^j = u^{2i} y^{2(i+j)+1}, \end{aligned}$$

which implies that i is odd and $j = 2\eta$ is even and so we get the fundamental relation:

$$(12) \quad (h^2g)^2 = u^i y^{2\eta} g^2, \quad i = \pm 1, \quad \eta = 0, 1.$$

Since $(h^2g)^2 \in \mathfrak{V}_1(G)$, $y^{2\eta} g^2 \in \mathfrak{V}_1(G)$, (12) gives that $u \in \mathfrak{V}_1(G)$. This fact together with $g^4 = y$ shows that $\mathfrak{V}_1(G) \geq W$ and so $d(G) = 2$ (since $d(G/W) = 2$).

From (12) follows at once $h^2gh^2g = u^i y^{2\eta} g^2$, $h^2(gh^2g^{-1}) = u^i y^{2\eta}$, which together with $h^4 = y^2$ gives:

$$(13) \quad (h^2)^{g^{-1}} = h^2 u^i y^{2(\eta+1)}.$$

From (13), we get directly the following two relations which we shall need:

$$(14) \quad (h^2)^g = h^2 u^{-i} y^{-i-2(\eta+1)},$$

$$(15) \quad (h^2)^{g^{-2}} = h^2 u^{2i} y^{-i} = h^2 u^2 y^{-i}.$$

Using (8) and (14), we get (since $h^4 = y^2$)

$$\begin{aligned} ((gh)h^2)^2 &= ghh^2 \cdot ghh^2 = ghg(g^{-1}h^2g)h^3 = ghg \cdot h^2u^{-i}y^{-i-2\eta-2}h^3 \\ &= (ghg)u^i y^{i+2\eta+2}h^5 = (ghgh)(h^{-1}u^i y^{i+2\eta+2}y^2h) \\ &= (gh)^2 u^i y^i (u^2 y^{-1})^{i+2\eta} = u^{2\epsilon-i} y^{2(\eta+1)}, \end{aligned}$$

and so for each $u^r y^s \in W$ ($r, s \in \mathbb{Z}$), we get

$$((gh)h^2 u^r y^s)^2 = ((gh)h^2)^2 (u^{gh^3})^r (y^{gh^3})^s u^r y^s = u^{2\epsilon-i+2r+2s} y^{2(\eta+1)+2s},$$

which is an element of order 4 in W (since $i = \pm 1$) and so we have shown that there are no involutions in $(gh)h^2 W$.

Using (15), we get (since $g^4 = y$)

$$\begin{aligned} (g^2 h^2)^2 &= g^2 h^2 g^2 h^2 = (g^2 h^2 g^{-2}) g^4 h^2 = (h^2)^{g^{-2}} y h^2 \\ &= h^2 u^2 y^{-i} y h^2 = h^4 (h^{-2} (u^2 y^{-i+1}) h^2) = y^2 u^2 y^{i-1} = u^2 y^{i+1}, \end{aligned}$$

and so for each $u^r y^s \in W$ ($r, s \in \mathbb{Z}$), we get

$$(g^2 h^2 u^r y^s)^2 = (g^2 h^2)^2 (u^{g^2 h^2})^r (y^{g^2 h^2})^s u^r y^s = u^2 y^{2r+i+1},$$

which is an involution in W_0 and so we have also shown that there are no involutions in $g^2 h^2 W$. The proof is complete. \square

Lemma 82.17. *Let G be a 2-group with exactly three involutions and a normal subgroup $W \cong C_4 \times C_4$ so that $W_0 = \Omega_1(W) \not\leq Z(G)$. Suppose that $A_G(W) \cong G/C_G(W)$ is of order 8. Then G contains a metacyclic subgroup M of index ≤ 4 and M is normal in G except in the case, where $A_G(W) = \langle \lambda(1, -1), \lambda(0, -1) \rangle \cong D_8$.*

Proof. We consider $X = A_G(W)$ as a subgroup of the group A (of order 2^5) of all automorphisms of $W = \langle u, y \rangle$ normalizing $\langle W_0, y \rangle$ (see Lemmas 82.6 and 82.9). Let A_0 be the stabilizer of the chain $W > W_0 > \{1\}$ so that $A_0 \cong E_{24}$ and $X \not\leq A_0$. Then we can choose a basis $\{u, y\}$ of W so that X contains one of the elements of order 4: $\lambda(0, 1)$, $\lambda(1, 1)$, $\lambda(1, -1)$, or the involution $\tau = \lambda(0, -1)$ (Lemma 82.9), where all these elements lie in $A - A_0$.

Set $C = C_G(W)$. If $\lambda(0, 1) \in X$ and $g \in G$ induces $\lambda(0, 1)$ on W , then $|G : \langle C, g \rangle| = 2$ and $\langle C, g \rangle$ is metacyclic (of index 4 in G) since $\Omega_2(\langle C, g \rangle) = \Omega_2(\langle C, g^2 \rangle) = W$ noting that g^2 (inducing $\lambda^2(0, 1)$ on W) does not invert any element in $W - W_0$ and so there are no elements of order 4 in $g^2 C$ (Lemma 82.3). Hence we may assume that $\lambda(0, 1) \notin X$.

Since $\lambda(1, 1) \notin X$ (Lemma 82.10), it follows that $\lambda(1, -1) \in X$ or $\tau \in X$. Note that for each $x \in A - A_0$, $|C_A(x)| = 8$ and $C_A(x) = \langle x \rangle A'$, where $A' = Z(A) = \Phi(A) = \langle \lambda^2(0, 1), \lambda^2(1, 1) \rangle \cong E_4$. If X is abelian, we have in any case $\lambda^2(0, 1) \in X$. But in that case, if $t \in G$ induces $\lambda^2(0, 1)$ on W , then $|G : \langle C, t \rangle| = 4$, $\langle C, t \rangle$ is normal in G , and $\langle C, t \rangle$ is metacyclic (by the previous paragraph).

Suppose that X is nonabelian so that $X \cong D_8$ (since A is Q_8 -free). Since $X \cap A_0 \cong E_4$, there are elements of order 4 in $X - A_0$ and so we may assume that $\lambda(1, -1) \in X$. But there are also involutions in $X - A_0$ and so either $\tau \in X$ or $\tau \lambda^2(1, 1) \in X$. (We recall that τ has exactly four A -conjugates which lie in the set $\tau A'$.) But, if $\tau \lambda^2(1, 1) \in X$, then $\gamma = \lambda(1, -1) \tau \lambda^2(1, 1) \in X$. We check that $u^\gamma = uu^2 y^2$, $y^\gamma = yu^2$, so

that $\gamma = \mu$ is “superspecial” (Lemma 82.6). According to Lemma 82.7, $\mu \notin A_G(W)$ and so this case cannot occur. Hence $X = \langle \lambda(1, -1), \lambda(0, -1) = \tau \rangle \cong D_8$, where the involution $\lambda(0, -1)$ inverts the element $\lambda(1, -1)$ of order 4.

Suppose that $t \in G$ induces $\lambda(0, -1)$ on W . By Lemma 82.3 (noting that $t^2 \in C$), there are no elements of order 4 in tC and since tC cannot contain involutions, we have $\Omega_2(\langle C, t \rangle) = W$ and so $\langle C, t \rangle$ is a nonnormal metacyclic subgroup of index 4 in G and we are done. \square

Theorem 82.18. *Let G be a 2-group with exactly three involutions and a normal subgroup $W \cong C_4 \times C_4$ so that $W_0 = \Omega_1(W) \not\leq Z(G)$. Set $C = C_G(W)$ and assume that $|G/C| = 8$. Then G contains a metacyclic subgroup M of index at most 4 in G and M is normal in G except in the following cases (α) and (β) , where $G/C \cong D_8$, $|C| = 2^{2n+1}$, $n \geq 2$, $C = \langle a, b \mid a^{2^{n+1}} = b^{2^n} = 1, [a, b] = a^{2^n\epsilon}, \epsilon = 0, 1 \rangle$ with $\epsilon = 0$ if $n = 2$, $Z(G)$ is of order 2, $\Phi(G) > C$, and the structure of G is determined with two generators and relations:*

(α) $n = 2$, $|G| = 2^8$, and $G = \langle g, t \mid g^8 = t^{16} = 1, g^4 = t^8 = z, t^2 = a, ag = au^{-1}, u^4 = [a, u] = 1, ug = u^{-1}a^2, u^t = u^{-1}a^2, (gt)^2 = zu^i, i = 0, 1, 2, 3 \rangle$ with $Z(G) = \langle z \rangle \cong C_2$, $C = \langle a \rangle \times \langle u \rangle \cong C_8 \times C_4$, $W = \langle a^2, u \rangle \cong C_4 \times C_4$, $\phi(G) = \langle g^2 \rangle C$, where g^2 inverts each element in C , and $\Omega_1(G) = \Omega_1(W) = \langle z, u^2 \rangle \cong E_4$. Finally, $\langle C, t \rangle$ is a non-normal metacyclic subgroup of index 4 in G .

(β) $n > 2$, $|G| = 2^{2n+4}$, and $G = \langle g, t \rangle$, where

$$\begin{aligned} g^8 &= t^{2^{n+2}} = 1, & g^4 &= t^{2^{n+1}} = z, & t^2 &= a, \\ a^g &= ab, & b^{2^n} &= 1, & [a, b] &= z^\epsilon, \quad \epsilon = 0, 1. \end{aligned}$$

(β_1) If $\epsilon = 0$, then $C = \langle a, b \rangle$ is abelian of type $(2^{n+1}, 2^n)$ and

$$b^g = b^{-1}a^{-2}, \quad b^t = b^{-1}a^{-2}, \quad (tg)^2 = z(a^2b)^s \quad \text{with } s \in \mathbb{Z} \text{ (any integer).}$$

(β_2) If $\epsilon = 1$, then $C = \langle a, b \rangle$ is a minimal nonabelian metacyclic group, $b^g = b^{-1}a^{-2}z^\eta b^{2^{n-1}}$, $\eta = 0, 1$, and either:

(β_{21}) $(tg)^2 = z^r(a^2b)^s$ with $b^t = b^{-1}a^{-2}z^{1+\eta}b^{2^{n-1}}$, where s is any odd integer and if $s \equiv 1 \pmod{4}$, then $r = 1$ and if $s \equiv -1 \pmod{4}$, then $r = 0$; or

(β_{22}) $(tg)^2 = z^r(a^4b^2)^s$ with $b^t = b^{-1}a^{-2}z^\eta b^{2^{n-1}}$, where in case that s is odd, then $r = 0$ and in case that s is even, then $r = 1$.

In all these cases $Z(G) = \langle z \rangle \cong C_2$, $\Phi(G) = \langle C, g^2 \rangle$, $W = \langle a^{2^{n-1}}, b^{2^{n-2}} \rangle = \Omega_2(C) \cong C_4 \times C_4$, $\langle C, t \rangle$ is a nonnormal metacyclic subgroup of index 4 in G , and in all above groups $\Omega_1(G) = \Omega_1(W) = \langle z, b^{2^{n-1}} \rangle \cong E_4$.

Proof. We continue with the situation in Lemma 82.17, where $A_G(W) = \langle \lambda(1, -1), \lambda(0, -1) \rangle \cong D_8$ and

$$u^{\lambda(1, -1)} = uy, \quad y^{\lambda(1, -1)} = u^2y^{-1}, \quad u^{\lambda(0, -1)} = uy, \quad y^{\lambda(0, -1)} = y^{-1}.$$

We recall that $\lambda(1, -1)$ (of order 4) does not fix any of the six cyclic subgroups of order 4 in W and $\lambda(0, -1)$ is an involution inverting $\lambda(1, -1)$.

Let g be an element in G which induces $\lambda(1, -1)$ (of order 4) on W so that $u^g = uy$, $y^g = u^2y^{-1}$, and $C_W(g) = \langle y^2 \rangle$. This implies that $C_C(g) = \langle y^2 \rangle$, where $C = C_G(W)$ since $\Omega_2(C) = W = \langle u, y \rangle$. There are no involutions in g^2C and so $g^4 = y^2$ and we set $y^2 = z$. We have $Z(G) \leq C$ which together with $C_C(g) = \langle z \rangle$ implies $Z(G) = \langle z \rangle$.

Let t be an element in G which induces the involution $\lambda(0, -1)$ on W so that $u^t = uy$, $y^t = y^{-1}$. By Lemma 82.11, $t^2 \in C - W$ and therefore $C > W$.

Replace y with $y' = yu^2$. Then $(y')^2 = y^2 = z$, $y = y'u^2$, and so

$$\begin{aligned} u^g &= uy = uy'u^2 = u^{-1}y', & (y')^g &= (yu^2)^g = u^2y^{-1}u^2y^2 = y = u^2y', \\ u^t &= uy = uy'u^2 = u^{-1}y', & (y')^t &= (yu^2)^t = y^{-1}u^2y^2 = u^2y = u^2y'u^2 = y'. \end{aligned}$$

Since $g^4 = y^2 = z = (y')^2$ and $W = \langle u, y' \rangle$, we may write again y instead of y' so that we get from the start the following fundamental relations:

$$(**) \quad u^g = u^{-1}y, \quad y^g = u^2y, \quad u^t = u^{-1}y, \quad y^t = y, \quad g^4 = y^2 = z,$$

and so we see that $C_W(t) = \langle y \rangle$ which implies $\langle t^2 \rangle > \langle y \rangle$ since $t^2 \in C - W$. Also note that $u^{g^2} = u^{-1}$, $y^{g^2} = y^{-1}$ and so g^2 inverts each element in W .

Since g does not normalize any cyclic subgroup of order 4 in C , Proposition 50.4 implies (together with the facts that $W_0 \notin Z(G)$, $C > W$, and $W \leq Z(C)$) that we have the following cases for the structure of C :

$$(16) \quad |C| = 2^5, C = \langle a, b \mid a^8 = b^4 = [a, b] = 1 \rangle,$$

$$(17) \quad |C| = 2^{2n}, n \geq 3, C = \langle a, b \mid a^{2^n} = b^{2^n} = 1, [a, b] = a^{2^{n-1}\epsilon}, \epsilon = 0, 1 \rangle,$$

$$(18) \quad |C| = 2^{2n+1}, n \geq 3, C = \langle a, b \mid a^{2^{n+1}} = b^{2^n} = 1, [a, b] = a^{2^n\epsilon}, \epsilon = 0, 1 \rangle.$$

Case (a). In this case C is given in (16). Since $t^2 \in C - W$ and $\langle t^2 \rangle > \langle y \rangle$, we may set $C = \langle a \rangle \times \langle u \rangle$, where $a^2 = y$ and $t^2 \in \langle a \rangle - \langle y \rangle$. Replacing t with ta^i for a suitable $i \in \mathbb{Z}$, we may assume from the start that $t^2 = a$ and we know that $u^t = u^{-1}y = u^{-1}a^2$. Also, we know from $(**)$ that $u^g = u^{-1}y$, $y^g = u^2y$, and $g^4 = y^2 = a^4 = z$.

We have $u^{gt} = u$, $y^{gt} = y(u^2y^2)$ so that $C_W(gt) = \langle W_0, u \rangle$, where $W_0 = \langle z, u^2 \rangle$. Since g^2 induces an involutory automorphism on C and g^2 inverts each element in W , we get $C_C(g^2) = W_0$ and so g^2 inverts C/W_0 (Proposition 51.2) which gives $a^{g^2} = a^{-1}w_0$ with some $w_0 \in W_0$.

For each $a^i u^j \in C$, we compute

$$(ta^i u^j)^2 = ta^i u^j ta^i u^j = t^2(a^i u^j)^t a^i u^j = aa^i u^{-j} a^{2j} a^i u^j = a^{1+2(i+j)},$$

which is an element of order 8. Thus $\Omega_2(\langle C, t \rangle) = W$ and so $\langle C, t \rangle$ is a non-normal metacyclic subgroup of index 4 in G .

We set $a^g = a^i u^j$ for some $i, j \in \mathbb{Z}$, where i is odd since a^g must be also an element of order 8 in C . We have

$$y^g = u^2 y = u^2 a^2 = (a^2)^g = (a^g)^2 = a^{2i} u^{2j} = u^{2j} y^i,$$

which implies $i \equiv 1 \pmod{4}$, $j \equiv 1 \pmod{2}$. Since $o(a) = 8$ and $o(u) = 4$, we may set $i = 1 + 4\epsilon$, $j = 1 + 2\eta$, where $\epsilon, \eta = 0, 1$.

By the above result $a^{g^2} = a^{-1} w_0$ with $w_0 \in W_0$, we get (also using the expressions for i, j):

$$a^{g^2} = a^{-1} w_0 = (a^i u^j)^g = (a^i u^j)^i u^{-j} y^j = a^{i^2+2j} u^{j(i-1)} = a^{1+2j},$$

which gives $a^{2(j+1)} = w_0$ and so $w_0 = a^{4(1+\eta)} = z^{1+\eta}$. If $\eta = 0$, then $a^{g^2} = a^{-1} z$ and so $\langle a, g^2 \rangle$ is semidihedral of order 16, contrary to our assumption that G has exactly three involutions. Thus, $\eta = 1$, $w_0 = 1$, $a^{g^2} = a^{-1}$, g^2 inverts C and $a^g = a^{1+4\epsilon} u^3$ with $\epsilon = 0, 1$. For each $c \in C$, we have $(g^2 c)^2 = g^4 c^{g^2} c = z c^{-1} c = z$, and so all elements in $g^2 C$ are of order 4.

Suppose that $\epsilon = 1$ so that $a^g = a a^4 u^{-1} = a z u^{-1} = a(z u)^{-1}$. Set $u' = z u$ so that $u = z u'$ and $a^g = a(u')^{-1}$. We see that all the previous relations remain unchanged if we replace u with u' . Indeed,

$$\begin{aligned} y^g &= (a^2)^g = a^2 (u')^2 = y(u')^2, \\ (u')^g &= (z u)^g = z u^{-1} y = (u')^{-1} y, \\ (u')^t &= (z u)^t = z u^{-1} y = (u')^{-1} y. \end{aligned}$$

Writing again u instead of u' , we see that we may assume from the start that $\epsilon = 0$ and so we get $a^g = a u^{-1}$. Since $t^2 = a$ and $[a, g] = u^{-1}$, we get $C = \langle a, u \rangle \leq \Phi(G)$ and so $\Phi(G) = \langle g^2, C \rangle$, $d(G) = 2$ and $G = \langle g, t \rangle$. We also get $a^{gt} = (a u^{-1})^t = a u y^{-1} = a^{-1} u$, $u^{gt} = u$.

We compute for each $a^r u^s \in C$,

$$a^r u^s = (a^r u^s)^{gt} = a^{-r} u^r u^s \text{ if and only if } a^{2r} = u^r, \quad y^r = u^r, \quad r \equiv 0 \pmod{4},$$

and so $C_C(gt) = \langle z, u \rangle = C_W(gt)$ which forces $(gt)^2 = w_1 \in \langle z, u \rangle$.

For each $a^p u^q \in C$, we compute

$$(gt)(a^p u^q))^2 = (gt)^2 (a^p u^q)^{gt} a^p u^q = w_1 a^{-p} u^p u^q a^p u^q = w_1 u^{p+2q},$$

and so we must have $w_1 u^{p+2q} \neq 1$ for all $p, q \in \mathbb{Z}$. This forces $w_1 = z u^i$ and

so $(gt)^2 = zu^i$ with $i = 0, 1, 2, 3$. The structure of G is determined and we have obtained the groups (α) of our theorem.

Cases (b) and (c), where $C = C_G(W)$ is abelian or minimal nonabelian with $n \geq 3$, given in (17) and (18). Since $\langle t^2 \rangle > \langle y \rangle > \langle z \rangle = Z(G)$, $t^2 \in C$, and $C' \leq \langle z \rangle$, we have $\mathfrak{U}_2(C) \geq C'$ and so C is a powerful 2-group. Obviously, C is D_8 -free and Q_8 -free since C is “ordinary metacyclic” (Proposition 26.27). In particular, C is modular.

By Proposition 26.24, $\mathfrak{U}_1(C) = \langle a^2, b^2 \rangle \leq Z(C)$ and $W = \langle u, y \rangle = \Omega_2(C)$. By Proposition 26.23, for each $x \in \mathfrak{U}_1(C)$, there is $r \in C$ with $x = r^2$. If $r \in \mathfrak{U}_1(C)$, then there is $s \in C$ so that $s^2 = r$ and so $x = s^4$ and so on. Hence for each $c \in C$, there is a generator $l \in C - \mathfrak{U}_1(C)$ such that $\langle c \rangle \leq \langle l \rangle$. Obviously, all the above results could be also obtained directly (without quoting the results about powerful 2-groups) from the structure of C .

It is possible to prove the crucial result that $t^2 \in C - \mathfrak{U}_1(C)$ is a generator of C . Suppose that this is false. Then there is $s \in C$ with $s^2 = t^2$. If $\langle t \rangle$ normalizes $\langle s \rangle$, then $\langle t, s \rangle$ has two distinct cyclic subgroups $\langle t \rangle$ and $\langle s \rangle$ of index 2, where $2^l = o(t) = o(s)$, $l \geq 4$. Thus $\langle t, s \rangle$ is noncyclic and so $\langle t, s \rangle$ is either abelian of type $(2^l, 2)$ or $\langle t, s \rangle \cong M_{2^l+1}$. In any case, there is an involution in $\langle t, s \rangle - \langle s \rangle$, where $\langle t, s \rangle \cap C = \langle s \rangle$, a contradiction. Hence t does not normalize $\langle s \rangle = S$, where $|S| = 2^l$, $l \geq 4$, and $|S : \langle t^2 \rangle| = 2$. Set $S_0 = S^t = \langle s^t \rangle$, where $S_0 \leq C$, $S_0 \geq \langle t^2 \rangle$, $|S_0 : \langle t^2 \rangle| = 2$ since t normalizes (centralizes) $\langle t^2 \rangle$. Since S is normal in C (noting that $S \geq \langle z \rangle$ and $C' \leq \langle z \rangle$), $T = SS_0$ is of order 2^{l+1} and $(s^t)^t = s^{t^2} = s$ implies that t normalizes T and therefore $|\langle T, t \rangle| = 2^{l+2}$ with $\langle T, t \rangle \cap C = T$. Also, S and S_0 are two distinct cyclic subgroups of index 2 in T and so T is not cyclic. We have $o(t^2) \geq 8$ and $\langle t^2 \rangle \leq Z(T)$ so that T cannot be generalized quaternion. Hence T has more than one involution and so $T \geq \Omega_1(C) = W_0$. But $W_0 \in Z(C)$ and $W_0 \cap S = \langle z \rangle$ so that $T = \langle s \rangle \times \langle u^2 \rangle$ is abelian of type $(2^l, 2)$.

Since $o(s^t) = o(s) = 2^l$, we may set $s^t = st^{2i}u^2$ for some integer i . We have $s = s^{t^2} = (st^{2i}u^2)^t = st^{2i}u^2t^{2i}u^2z$, which gives $t^{4i} = z$ and $t^{8i} = 1$. Since $o(t) = 2^l$ ($l \geq 4$), we get $i \equiv 0 \pmod{2^{l-3}}$ and we may set $i = 2^{l-3}i'$. On the other hand, $z = t^{4i} = t^{2^{l-1}i'} = z^{i'}$ and so i' is odd. We get $[s, t] = t^{2i}u^2 = t^{2^{l-2}i'}u^2 = y^ju^2$, where $j = \pm 1$. In particular, $[s, t]$ is of order 4.

Since t acts non-trivially on $T/\langle t^2 \rangle \cong E_4$, we have $\langle t, s \rangle/\langle t^2 \rangle \cong D_8$, where $\langle t, s \rangle = \langle T, t \rangle$. Let $A/\langle t^2 \rangle$ be the cyclic subgroup of index 2 in $\langle t, s \rangle/\langle t^2 \rangle$ so that A is abelian since $\langle t^2 \rangle \leq Z(\langle t, s \rangle)$. But then $\langle t, s \rangle$ possesses two distinct abelian maximal subgroups T and A . By a well-known result of A. Mann (Lemma 64.1 (u)), $(\langle t, s \rangle)'$ is of order 2, contrary to the above result that $o([s, t]) = 4$. We have proved that $t^2 \in C - \mathfrak{U}_1(C)$.

Let $x \in C - \mathfrak{U}_1(C)$. Since x is a generator of C , there is $v \in C - \mathfrak{U}_1(C)$ so that $\langle x, v \rangle = C$. Since C is modular, we have $\langle x \rangle \langle v \rangle = C$ and so $|C| = (o(x)o(v)) : (|\langle x \rangle \cap \langle v \rangle|)$. If $|C| = 2^{2n}$, then $\exp(C) = 2^n$ and in that case $o(x) = o(v) = 2^n$ and $\langle x \rangle \cap \langle v \rangle = \{1\}$ so that $\langle x \rangle$ has a complement in C . If $|C| = 2^{2n+1}$, then $\exp(C) = 2^{n+1}$ and in that case $o(x) = 2^n$ or $o(x) = 2^{n+1}$.

Case (b), where $|C| = 2^{2n}$, $\exp(C) = 2^n$, $n \geq 3$, is given in (17). As a surprise, we shall show that this case cannot occur at all! Set $\langle t^2 \rangle = \langle a \rangle$ so that $o(a) = 2^n$ since we have proved that $t^2 \in C - \mathfrak{U}_1(C)$. We choose the generator a of $\langle a \rangle$ so that $a^{2^{n-2}} = y$, where $y^2 = z$ with $\langle z \rangle = Z(G)$. We have $t^2 = aa^{2i}$ ($i \in \mathbb{Z}$) and replacing t with $t' = ta^{-i}$ we get $(t')^2 = t^2a^{-2i} = aa^{2i}a^{-2i} = a$. Note that t' operates the same way on W as t does (since $W \leq Z(C)$) and so writing again t instead of t' , we may assume from the start that $t^2 = a$.

Let $\langle b \rangle$ be a cyclic subgroup of order 2^n of C which contains $\langle u \rangle$ so that $\langle a \rangle \cap \langle b \rangle = \{1\}$ and we may choose the generator b of $\langle b \rangle$ so that $b^{2^{n-2}} = u$. Hence $|\langle a, b \rangle| = o(a)o(b) = 2^{2n}$ so that $\langle a, b \rangle = C$. If C is nonabelian, then $|C'| = 2$ and so $C' \leq Z(G)$ which implies $C' = \langle z \rangle$. Hence, we have in any case, $a^b = az^\epsilon$, where $\epsilon = 0, 1$.

We consider first the special case $n = 3$, $\epsilon = 1$ so that $o(a) = o(b) = 8$ and $a^b = az$. Set $b^t = a^m b^v$ (for some $m, v \in \mathbb{Z}$) and so

$$\begin{aligned} u^t &= u^{-1}y = (b^2)^t = (a^m b^v)^2 = a^{2m} b^{2v} [b, a]^{mv} = y^m u^v z^{mv} \\ &= y^m u^v y^{2mv} = u^v y^{m(1+2v)}, \end{aligned}$$

which gives $v \equiv -1 \pmod{4}$, $m(1+2v) \equiv 1 \pmod{4}$, $m \equiv -1 \pmod{4}$. We may set $m = -1 + 4m'$, $v = -1 + 4v'$ so that $b^t = a^{-1}z^{m'}b^{-1}u^{2v'} = a^{-1}b^{-1}w_1$ with $w_1 \in W_0$. However,

$$b^{t^2} = b^a = bz = (a^{-1}b^{-1}w_1)^t = a^{-1}w_1^{-1}ba w_1^t = a^{-1}abz w_1^{-1}w_1^t = bz w_1^{-1}w_1^t,$$

and so $w_1^t = w_1$, which gives $w_1 = z^\xi$, $\xi = 0, 1$. We get $(tb)^2 = t^2b^t b = aa^{-1}b^{-1}z^\xi b = z^\xi$, so that $\langle tb, W_0 \rangle \cong D_8$ since tb acts non-trivially on W_0 . But then G has more than three involutions, a contradiction.

We have proved that the case $n = 3$, $\epsilon = 1$ cannot happen. In general, we set again $b^t = a^m b^v$ (for some $m, v \in \mathbb{Z}$) and so:

$$u^t = u^{-1}y = (b^{2^{n-2}})^t = (a^m b^v)^{2^{n-2}} = (a^{2^{n-2}})^m (b^{2^{n-2}})^v = u^v y^m,$$

since either $n > 3$ or $n = 3$, $\epsilon = 0$. This gives $v \equiv -1 \pmod{4}$, $m \equiv 1 \pmod{4}$ and so setting $m = 1 + 4m'$, $v = -1 + 4v'$, we get $b^t = (ab^{-1})a^{4m'}b^{4v'}$.

We compute:

$$\begin{aligned} b^{t^2} &= b^a = bz^\epsilon = (a^{1+4m'}b^{-1+4v'})^t = a^{1+4m'}(a^{1+4m'}b^{-1+4v'})^{-1+4v'} \\ &= a^{1+4m'}b^{1-4v'}a^{-1-4m'}a^{4v'+16m'v'}b^{-4v'+16(v')^2} \\ &= a^{4v'(1+4m')}bz^\epsilon b^{8v'(-1+2v')}, \end{aligned}$$

and so $a^{4v'(1+4m')}b^{8v'(-1+2v')} = 1$, which implies $v' \equiv 0 \pmod{2^{n-2}}$ and $b^t = a^{1+4m'}b^{-1}$.

Now, we get $a^{tb} = a^b = az^\epsilon = aa^{2^{n-1}\epsilon} = a^{1+2^{n-1}\epsilon}$, and so tb normalizes $\langle a \rangle$ and $(tb)^2 = t^2b^t b = aa^{1+4m'}b^{-1}b = a^{2(1+2m')}$ is of order 2^{n-1} . Set $R = \langle a, tb \rangle$ so that $\langle a \rangle$ and $\langle tb \rangle$ are two distinct cyclic maximal subgroups (of order 2^n , $n \geq 3$) of R . It follows that R is either abelian of type $(2^n, 2)$ or $R \cong M_{2n+1}$. In any case, there are involutions in $R - \langle a \rangle = R - C$, a contradiction. We have proved that the Case (b) cannot occur.

Case (c), where $|C| = 2^{2n+1}$, $\exp(C) = 2^{n+1}$, $n \geq 3$ is given in (18). We know that $t^2 \in C - \mathfrak{V}_1(C)$ is a generator of C and, since $\langle t^2 \rangle > \langle y \rangle > \langle z \rangle = Z(G)$, we may set $\langle a \rangle = \langle t^2 \rangle$ so that $\langle a \rangle$ is normal in C (since $C' \leq \langle z \rangle$). Let $d \in C$ be another generator for C so that $\langle a, d \rangle = C$. By Proposition 26.24, $\mathfrak{V}_n(C) = \langle a^{2^n}, d^{2^n} \rangle$ and by the structure of C (in Case (c)), $|\mathfrak{V}_n(C)| = 2$. If a is of order 2^n , then $\mathfrak{V}_n(C) = \langle d^{2^n} \rangle \cong C_2$ is normal in G with $o(d) = 2^{n+1}$ and $\langle a \rangle \cap \langle d \rangle = \{1\}$ (since $|C| = 2^{2n+1}$), contrary to the fact that $Z(G) = \langle z \rangle \leq \langle a \rangle$. Hence a is of order 2^{n+1} and we may choose a generator a of $\langle a \rangle$ so that $a^{2^{n-1}} = y$. We have $t^2 = aa^{2i}$ (for some $i \in \mathbb{Z}$) and replacing t with $t' = ta^{-i}$, we get $(t')^2 = t^2a^{-2i} = aa^{2i-2i} = a$. Note that t' acts the same way on $W = \Omega_2(C) = \langle u, y \rangle$ as t does since $W \leq Z(C)$ and so we may assume from the start that $t^2 = a$, where $o(t) = 2^{n+2}$, $n \geq 3$.

Let $\langle b \rangle$ be a cyclic subgroup of C containing $\langle u \rangle$ such that $b \in C - \mathfrak{V}_1(C)$. We know that $o(b) = 2^n$ or $o(b) = 2^{n+1}$. But $\langle a \rangle \cap \langle b \rangle = \{1\}$ since $\langle y \rangle = \Omega_2(\langle a \rangle)$ and $\langle u \rangle = \Omega_2(\langle b \rangle)$ and $\langle y \rangle \cap \langle u \rangle = \{1\}$. We get $\langle a, b \rangle = \langle a \rangle \langle b \rangle$ is of order $o(a)o(b)$ and so $o(b) = 2^n$, $|\langle a, b \rangle| = 2^{2n+1}$ and $\langle a, b \rangle = C$ with $a^b = az^\epsilon$. We may choose a generator b of $\langle b \rangle$ so that $b^{2^{n-2}} = u$.

We recall (from (**)) that $u^g = u^{-1}y$, $y^g = yu^2$, g^2 inverts W , $u^t = u^{-1}y$, $a^t = a$ (since $t^2 = a$), and $g^4 = z$. We have $S = \Omega_n(C) = \langle a^2, b \rangle$ is abelian (of type $(2^n, 2^n)$) g^2 -invariant maximal subgroup of C and g^2 induces an involutory automorphism on S . Since $C_S(g^2) = C_W(g^2) = W_0$, g^2 inverts each element in $\mathfrak{V}_1(S) = \langle a^4, b^2 \rangle$ (Proposition 51.2). This fact will be used often in the sequel.

It is now easy to determine the action of t on C by lifting up the action of t on W . We set $b^t = a^{2i}b^j$ ($i, j \in \mathbb{Z}$) since $b^t \in S$ and compute (noting that $a^{2i} \in Z(C)$):

$$u^{-1}y = u^t = (b^{2^{n-2}})^t = (a^{2i}b^j)^{2^{n-2}} = a^{2^{n-1}i}b^{2^{n-2}j} = y^i u^j,$$

which implies $i \equiv 1 \pmod{4}$, $j \equiv -1 \pmod{4}$ so that we may set $i = 1 + 4i'$, $j = -1 + 4j'$, and $b^t = a^2a^{8i'}b^{-1}b^{4j'}$. Since $t^2 = a$, we get:

$$\begin{aligned} b^{t^2} &= b^a = bz^\epsilon = (a^2a^{8i'}b^{-1}b^{4j'})^t \\ &= a^2a^{8i'}a^{-2}a^{-8i'}bb^{-4j'}a^{8j'}a^{32i'j'}b^{-4j'}b^{16(j')^2} = a^{8j'(1+4i')}b^{1-8j'(1-2j')}, \end{aligned}$$

and so $j' \equiv 0 \pmod{2^{n-3}}$. We may set $j' = 2^{n-3}j''$ and so $z^\epsilon = a^{2^n j''(1+4i')} = z^{j''}$ and $j'' \equiv \epsilon \pmod{2}$. We obtain $b^t = a^{2(1+4i')}b^{-1}b^{2^{n-1}j''} = a^{2(1+4i')}b^{-1}u^{2\epsilon}$.

We consider new elements $t' = a^{2i'}t$ and $a' = a^{1+4i'}$ and see that $\langle a', b \rangle = C$, a' is of order 2^{n+1} , $(a')^{2^{n-1}} = a^{(1+4i')2^{n-1}} = a^{2^{n-1}}a^{2^{n+1}i'} = a^{2^{n-1}} = y$, $(a')^b =$

$a'z^\epsilon$, $(t')^2 = a^{4i'}t^2 = a^{1+4i'} = a'$, and, finally, $b^{t'} = b^{a^{2i'}t} = b^t = (a')^2b^{-1}u^{2\epsilon}$. Hence, writing again a and t instead of a' and t' , respectively, we get $b^t = a^2b^{-1}u^{2\epsilon}$.

We check that all elements $ta^i b^j \in tC$ are of order 2^{n+2} :

$$(ta^i b^j)^2 = t^2(a^i b^j)^t a^i b^j = aa^i a^{2j} b^{-j} u^{2j\epsilon} a^i b^j = a^{1+2i+2j} u^{2j\epsilon} z^{ij\epsilon},$$

and so $\Omega_2(\langle t, C \rangle) = \Omega_2(C) = W$, which implies that $\langle t, C \rangle$ is a non-normal metacyclic subgroup of index 4 in G .

It is very difficult to lift up the action of g from the action on W to the action on C . We set $a^g = a^m b^v$, $b^g = a^{2p} b^q$ for some integers m, v, p, q , where we have used the fact that $b \in \Omega_n(C) = \langle a^2, b \rangle$. We get (since $n \geq 3$):

$$y^g = yu^2 = (a^{2^{n-1}})^g = (a^m b^v)^{2^{n-1}} = (a^{2^{n-1}})^m (b^{2^{n-1}})^v = y^m u^{2v},$$

so that $m \equiv 1 \pmod{4}$, $v \equiv 1 \pmod{2}$. Further (since $a^2 \in Z(C)$):

$$u^g = u^{-1}y = (b^{2^{n-2}})^g = (a^{2p} b^q)^{2^{n-2}} = y^p u^q,$$

so that $p \equiv 1 \pmod{4}$, $q \equiv -1 \pmod{4}$. Therefore we may set:

$$m = 1 + 4\alpha, \quad v = 1 + 2\beta, \quad p = 1 + 4\gamma, \quad q = -1 + 4\delta, \quad \alpha, \beta, \gamma, \delta \in \mathbb{Z},$$

and obtain:

$$a^g = a^{1+4\alpha} b^{1+2\beta}, \quad b^g = a^{2(1+4\gamma)} b^{-1+4\delta}.$$

We set $b' = a^{4\alpha} b^{1+2\beta}$ so that we get a simple relation $a^g = ab'$, where $o(b') = 2^n$, $\langle a, b' \rangle = C$, $(b')^{2^{n-2}} = z^\alpha uu^{2\beta} = z^\alpha u^{\pm 1} = u'$, $(u')^2 = u^2$, $(b')^{2^{n-1}} = u^2$,

$$\begin{aligned} (b')^g &= (a^{4\alpha} b^{1+2\beta})^g = (ab')^{4\alpha} (a^{2(1+4\gamma)} b^{-1+4\delta})^{1+2\beta} \\ &= a^{4\alpha} (b')^{4\alpha} a^{2(1+2\beta)(1+4\gamma)} b^{(1+2\beta)(-1+4\delta)} \\ &= a^{4\alpha(-1+4\delta)} a^{4\alpha(1-4\delta)} a^{4\alpha} (b')^{4\alpha} a^{2(1+2\beta)(1+4\gamma)} b^{(1+2\beta)(-1+4\delta)} \\ &= (b')^{-1+4\delta} (b')^{4\alpha} a^{2(2\alpha+(1+2\beta)(1+4\gamma)+2\alpha(1-4\delta))} = (b')^{-1+4\xi} a^{2\xi}, \end{aligned}$$

where $\xi, \xi \in \mathbb{Z}$ and ξ is odd,

$$\begin{aligned} (b')^t &= (a^{4\alpha} b^{1+2\beta})^t = a^{4\alpha} (a^2 b^{-1} u^{2\epsilon})^{1+2\beta} = a^{4\alpha} a^{2(1+2\beta)} b^{-(1+2\beta)} u^{2\epsilon} \\ &= a^{8\alpha} a^{2(1+2\beta)} (a^{-4\alpha} b^{-(1+2\beta)}) u^{2\epsilon} = (b')^{-1} a^{2(1+2\beta+4\alpha)} u^{2\epsilon} \\ &= (b')^{-1} a^{2\theta} u^{2\epsilon}, \end{aligned}$$

where θ is an odd integer. We write again b instead of b' and also write $\xi = i$,

$\xi = 1 + 2j$, $\theta = 1 + 2k$ (with $i, j, k \in \mathbb{Z}$) so that we obtain the important relations:

$$(19) \quad \begin{aligned} o(b) &= 2^n, & b^{2^{n-1}} &= u^2, & b^{2^{n-2}} &= z^\alpha u^{\pm 1}, \\ t^2 &= a, & g^4 &= z, & a^{2^{n-1}} &= y, \\ y^2 &= z, & a^g &= ab, & b^g &= b^{-1+4i} a^{2+4j}, \\ b^t &= b^{-1} a^{2+4k} u^{2\epsilon}, \end{aligned}$$

where $\alpha, \epsilon = 0, 1$ and $i, j, k \in \mathbb{Z}$.

The fact that $g^4 = z$ gives us more information about the action of g on C . Indeed,

$$\begin{aligned} a^{g^2} &= (ab)^g = abb^{-1+4i} a^{2+4j} = a^{1+2+4j} b^{4i} = a^{-1+4+4j} b^{4i} \\ &= a^{-1+4(1+j)} b^{4i}, \end{aligned}$$

and so (noting that g^2 inverts each element in $\langle a^4, b^2 \rangle$)

$$\begin{aligned} a &= a^{g^4} = (a^{-1+4(1+j)} b^{4i})^{g^2} = (a^{g^2})^{-1} a^{-4(1+j)} b^{-4i} \\ &= a^{1-4(1+j)} b^{-4i} a^{-4(1+j)} b^{-4i} = a^{1-8(1+j)} b^{-8i}, \end{aligned}$$

which gives $1 + j \equiv 0 \pmod{2^{n-2}}$ and $i \equiv 0 \pmod{2^{n-3}}$, and so we may set $i = 2^{n-3}i'$, $j = -1 + 2^{n-2}j'$, which gives us a simple expression for b^g :

$$b^g = b^{-1} b^{2^{n-1}i'} a^{2-4+2^n j'} = b^{-1} u^{2i'} a^{-2} z^{j'} = b^{-1} a^{-2} w_0,$$

where $w_0 = u^{2i'} z^{j'} \in W_0$. We have obtained:

$$(20) \quad b^g = b^{-1} a^{-2} w_0, \quad \text{with } w_0 \in W_0 = \langle a^{2^n} = z, b^{2^{n-1}} = u^2 \rangle.$$

From (19) and (20) we get the action of g^2 on C :

$$\begin{aligned} a^{g^2} &= (ab)^g = abb^{-1} a^{-2} w_0 = a^{-1} w_0, \\ b^{g^2} &= (b^{-1} a^{-2} w_0)^g = ba^2 w_0 a^{-2} b^{-2} z^\epsilon w_0^g = b^{-1} z^\epsilon w_0 w_0^g, \end{aligned}$$

and the fact that there are no involutions in $g^2 C$ gives us some information about w_0 :

$$\begin{aligned} (g^2 a)^2 &= g^4 a^{g^2} a = za^{-1} w_0 a = zw_0 \quad \text{and so } w_0 \neq z, \\ (g^2 b)^2 &= g^4 b^{g^2} b = zb^{-1} z^\epsilon w_0 w_0^g b = zz^\epsilon w_0 w_0^g \neq 1. \end{aligned}$$

This gives us the following information about $w_0 \in W_0$.

- (21) If $\epsilon = 0$, then C is abelian, $w_0 = 1$ and g^2 inverts each element in C ;
- (22) If $\epsilon = 1$, then C is minimal nonabelian, $w_0 \in W_0 - \langle z \rangle$

and so we may set $w_0 = u^2 z^\eta$, $\eta = 0, 1$.

Using the above results, it is easy to check that each element g^2c ($c = a^i b^j \in C$) is of order 4. Indeed, if $\epsilon = 0$, then $(g^2c)^2 = g^4 c^{g^2} c = z c^{-1} c = z$ and, if $\epsilon = 1$, then (noting that $a^i b^j = b^j a^i z^{ij}$ and $w_0 = u^2 z^\eta$, $w_0^g = u^2 z^{\eta+1}$)

$$\begin{aligned} (g^2 a^i b^j)^2 &= g^4 (a^{g^2})^i (b^{g^2})^j a^i b^j = z a^{-i} w_0^i b^{-j} z^j w_0^j (w_0^g)^j a^i b^j \\ &= z^{1+i(j+\eta)} u^{2i}, \end{aligned}$$

and so if i is even, then $(g^2 a^i b^j)^2 = z$ and if i is odd, then

$$(g^2 a^i b^j)^2 = z^{1+i(j+\eta)} u^2 \neq 1.$$

It remains to determine $(tg)^2 \in C$, where $(tg)C$ is an involution in $G/C \cong D_8$ and we require that there are no involutions in $(tg)C$ and note that $(tg)^2 \in C_C(tg)$. Using (19) and (20), we obtain the action of tg on C :

$$\begin{aligned} a^{tg} &= a^g = ab, \\ b^{tg} &= (b^{-1} a^{2+4k} u^{2\epsilon})^g = a^2 b w_0 (ab)^{2+4k} u^{2\epsilon} z^\epsilon \\ &= a^2 b w_0 a^{2+4k} b^{2+4k} z^\epsilon u^{2\epsilon} z^\epsilon = a^{4(1+k)} b^{-1+4(1+k)} w_0 u^{2\epsilon}. \end{aligned}$$

All elements in $C - S$ (where $S = \Omega_n(C) = \langle a^2, b \rangle$) are of order 2^{n+1} and suppose that an element as ($s \in S$) is centralized by tg . Then $(as)^{2^{n-1}} = a^{2^{n-1}} s^{2^{n-1}} = y x_0$ with $x_0 \in W_0$ is also centralized by tg . But tg centralizes W_0 and so $y^{tg} = y$, contrary to the relations in $(**)$ which give $y^{tg} = y u^2$. Thus, $C_C(tg) \leq \langle a^2, b \rangle$ and so $(tg)^2 \in \langle a^2, b \rangle$ which is an abelian group and therefore $b^{(tg)^2} = b$.

This gives

$$\begin{aligned} b = b^{(tg)^2} &= (a^{4(1+k)} b^{-1+4(1+k)} w_0 u^{2\epsilon})^{tg} \\ &= (ab)^{4(1+k)} (a^{4(1+k)} b^{-1+4(1+k)} w_0 u^{2\epsilon})^{-1+4(1+k)} w_0 u^{2\epsilon} \\ &= a^{4(1+k)} b^{4(1+k)} a^{-4(1+k)} b^{1-4(1+k)} w_0 u^{2\epsilon} a^{16(1+k)^2} b^{-4(1+k)+16(1+k)^2} w_0 u^{2\epsilon} \\ &= a^{16(1+k)^2} b^{1+4(1+k)(-1+4(1+k))}, \end{aligned}$$

and so $1+k \equiv 0 \pmod{2^{n-2}}$ and we may set $1+k = 2^{n-2}k'$ for some $k' \in \mathbb{Z}$. Hence, from the above and using (19), we get

$$\begin{aligned} b^{tg} &= a^{2^n k'} b^{-1} b^{2^n k'} w_0 u^{2\epsilon} = b^{-1} w_0 z^{k'} u^{2\epsilon}, \\ b^t &= b^{-1} a^{2+4k} u^{2\epsilon} = b^{-1} a^{-2} a^{4(1+k)} u^{2\epsilon} = b^{-1} a^{-2} z^{k'} u^{2\epsilon}, \end{aligned}$$

and so

$$\begin{aligned} (23) \quad a^{tg} &= ab, & b^{tg} &= b^{-1} w_0 z^{k'} u^{2\epsilon}, \\ b^t &= b^{-1} a^{-2} z^{k'} u^{2\epsilon}, & (tg)^2 \in \langle a^2, b \rangle, & k' = 0, 1. \end{aligned}$$

Assume at the moment that $\epsilon = 0$. Then (21) implies that $C = \langle a, b \rangle$ is abelian, $w_0 = 1$, and g^2 inverts each element in C . Since $(tg)^2 \in C$, we get from (23): $a = a^{(tg)^2} = (ab)^{tg} = ab \cdot b^{-1}z^{k'} = az^{k'}$ and so $k' = 0$. We obtain from (23), $b^{tg} = b^{-1}$, $b^t = b^{-1}a^{-2}$ and compute, using (19):

$$(a^2b)^{tg} = (ab)^2b^{-1} = a^2b, \quad (a^2b)^{2^{n-1}} = a^{2^n}b^{2^{n-1}} = zu^2,$$

so that $C_C(tg) = W_0\langle a^2b \rangle = \langle z \rangle \times \langle a^2b \rangle$ and $(tg)^2 = z^r(a^2b)^s$ with $r = 0, 1$ and some $s \in \mathbb{Z}$. For each $a^i b^j \in C$, we compute

$$\begin{aligned} ((tg)a^i b^j)^2 &= (tg)^2(a^{tg})^i(b^{tg})^j a^i b^j = (tg)^2 a^{2i} b^i \\ &= z^r(a^2b)^s a^{2i} b^i = a^{2(i+s+r2^{n-1})} b^{i+s} = x. \end{aligned}$$

We see that $x = 1$ if and only if $i \equiv -s \pmod{2^n}$ and $r = 0$. Hence we must have $r = 1$ and so $(tg)^2 = z(a^2b)^s$, $s \in \mathbb{Z}$, in which case no element in $(tg)C$ is an involution. Also, from (20) we get $b^g = b^{-1}a^{-2}$. We have obtained the groups stated in parts (β) and (β_1) of our theorem.

In what follows, we always assume $\epsilon = 1$. Then (22) implies that $C = \langle a, b \rangle$ is minimal nonabelian, $a^b = az^\epsilon$, and $w_0 = u^2z^\eta$ with $\eta = 0, 1$. Note that (19), (20), and (23) imply

$$\begin{aligned} u^2 &= b^{2^{n-1}}, & b^g &= b^{-1}a^{-2}z^\eta u^2, & a^{tg} &= ab, \\ b^{tg} &= b^{-1}z^{k'+\eta}, & b^t &= b^{-1}a^{-2}z^{k'}u^2, & k', \eta &= 0, 1. \end{aligned}$$

We compute $C_C(tg) \leq \langle a^2, b \rangle$ (noting that $(ab)^{2i} = (a)^{2i}(b)^{2i}z^i$)

$$\begin{aligned} a^{2i}b^j &= (a^{2i}b^j)^{tg} = (ab)^{2i}b^{-j}z^{(k'+\eta)j} \\ &= (a)^{2i}(b)^{2i}z^i b^{-j}z^{(k'+\eta)j} = a^{2i}b^{2i-j}z^{i+(k'+\eta)j}, \end{aligned}$$

and so $a^{2i}b^j \in C_C(tg)$ if and only if $b^{2(i-j)}z^{i+(k'+\eta)j} = 1$ and this is satisfied if and only if $i - j \equiv 0 \pmod{2^{n-1}}$ and $i + (k' + \eta)j \equiv 0 \pmod{2}$. We may set $j = i + 2^{n-1}\alpha$ ($\alpha \in \mathbb{Z}$) and then

$$a^{2i}b^j = a^{2i}b^{i+2^{n-1}\alpha} = a^{2i}b^i u^{2\alpha}, \quad \text{and } i(1+k'+\eta) \equiv 0 \pmod{2}.$$

Since $u^{2\alpha} \in W_0 \leq C_C(tg)$, we get $C_C(tg) = \{W_0, (a^2b)^i\}$, where $i(1+k'+\eta) \equiv 0 \pmod{2}$. It follows that we have exactly two possibilities for the structure of $C_C(tg)$ (noting that $(a^2b)^{2^{n-1}} = zu^2$):

- (i) If $1+k'+\eta \equiv 0 \pmod{2}$, then $C_C(tg) = \langle z \rangle \times \langle a^2b \rangle$;
- (ii) If $1+k'+\eta \equiv 1 \pmod{2}$, then $C_C(tg) = \langle z \rangle \times \langle a^4b^2 \rangle$.

Suppose that (i) holds. In that case we get $k' \equiv 1 + \eta \pmod{2}$ and so

$$b^{tg} = b^{-1}z, \quad b^t = b^{-1}a^{-2}z^{1+\eta}b^{2^{n-1}}, \quad (tg)^2 = z^r(a^2b)^s, \quad r = 0, 1, \quad s \in \mathbb{Z}.$$

If s is even, then $a^{(tg)^2} = a^{z^r(a^2b)^s} = a = (ab)^{tg} = ab \cdot b^{-1}z = az$, a contradiction. Hence s must be odd and we show that if $s \equiv 1 \pmod{4}$, then $r = 1$ and if $s \equiv -1 \pmod{4}$, then $r = 0$. Indeed, we require that $((tg)a^i b^j)^2 \neq 1$ for all $i, j \in \mathbb{Z}$. Suppose that for some i, j , $((tg)a^i b^j)^2 = 1$. Then

$$1 = ((tg)a^i b^j)^2 = (tg)^2(a^{tg})^i(b^{tg})^j a^i b^j = z^r a^{2s} b^s (ab)^i b^{-j} z^j a^i b^j,$$

which gives at once

$$(iii) \quad b^{i+s} = 1 \text{ and so } i + s \equiv 0 \pmod{2^n}, \quad n \geq 3.$$

If $s \equiv 1 \pmod{4}$, then (iii) gives $i \equiv -1 \pmod{4}$ and $i = -1 + 4i'$, so that

$$(ab)^i = (ab)^{-1+4i'} = b^{-1}a^{-1}a^{4i'}b^{4i'} = b^{-1+4i'}a^{-1+4i'} = b^i a^i$$

and (noting that $z^{ij} = z^j$ since i is odd), we get $1 = z^r a^{2s} b^s b^i a^i b^{-j} z^j b^j a^i z^{ij} = z^r$, and so $r = 0$. Thus, $((tg)a^i b^j)^2 \neq 1$ for all $i, j \in \mathbb{Z}$ if and only if $r = 1$. If $s \equiv -1 \pmod{4}$, then (iii) gives $i \equiv 1 \pmod{4}$ and $i = 1 + 4i'$, so that

$$(ab)^i = (ab)^{1+4i'} = aba^{4i'}b^{4i'} = a^{1+4i'}b^{1+4i'} = a^i b^i$$

and (noting again that $z^{ij} = z^j$)

$$1 = z^r a^{2s} b^s a^i b^i b^{-j} z^j b^j a^i z^{ij} = z^{r+1}$$

and so $r = 1$. Thus, $((tg)a^i b^j)^2 \neq 1$ for all $i, j \in \mathbb{Z}$ if and only if $r = 0$. We have obtained the groups stated in parts (β) , (β_2) , and (β_{21}) of our theorem.

Suppose that (ii) holds. In that case we get $k' \equiv \eta \pmod{2}$ and so

$$b^{tg} = b^{-1}, \quad b^t = b^{-1}a^{-2}z^\eta b^{2^{n-1}}, \quad (tg)^2 = z^r(a^4b^2)^s, \quad r = 0, 1 \text{ and } s \in \mathbb{Z}.$$

We show that if s is odd, then $r = 0$ and if s is even, then $r = 1$. Indeed, we require that $((tg)a^i b^j)^2 \neq 1$ for all $i, j \in \mathbb{Z}$. Suppose that for some i, j , $((tg)a^i b^j)^2 = 1$. Then

$$1 = ((tg)a^i b^j)^2 = (tg)^2(a^{tg})^i(b^{tg})^j a^i b^j = z^r a^{4s} b^{2s} (ab)^i b^{-j} a^i b^j,$$

which gives at once $b^{i+2s} = 1$ and so $i + 2s \equiv 0 \pmod{2^n}$, $n \geq 3$, and this implies that $i = 2i'$ must be even and

$$(ab)^i = (ab)^{2i'} = ((ab)^2)^{i'} = ((a^2b^2z))^{i'} = (a)^{2i'}(b)^{2i'}z^{i'} = a^i b^i z^{i'},$$

which together with $a^i \in Z(C)$ gives

$$1 = z^r a^{4s} b^{2s} a^i b^i z^{i'} b^{-j} b^j a^i = z^r a^{4s+2i} z^{i'} b^{2s+i} = z^{r+i'}$$

and $r + i' \equiv 0 \pmod{2}$. Since $i + 2s \equiv 0 \pmod{2^n}$, we get $2i' + 2s \equiv 0 \pmod{2^n}$ and so $i' + s \equiv 0 \pmod{2^{n-1}}$. Since $((tg)a^i b^j)^2$ must be $\neq 1$ for all $i, j \in \mathbb{Z}$, from the above we get that if s is odd, then i' is odd and so $r = 0$ and if s is even, then i' is even and so we must have $r = 1$. We have obtained the groups stated in parts (β) , (β_2) , and (β_{22}) of our theorem which is now completely proved. \square

Exercise 1. The following conditions for a nonmetacyclic 2-group G are equivalent:
(a) G has exactly three involutions, (b) every minimal nonmetacyclic subgroup of G has exactly three involutions.

Solution. It suffices to prove that $(b) \Rightarrow (a)$. Assume that G has more than three involutions. Clearly, G is not of maximal class. There is $E_4 \cong R \triangleleft G$. Since R has exactly three involutions, there exists an involution $x \in G - R$ and we have $H = \langle x, R \rangle \cong D_8$. Since G is not of maximal class, $C_G(H) \not\leq H$ (Proposition 10.17). Let $y \in C_G(H) - H$ has the minimal possible order. Since G has no elementary abelian subgroups of order 8, we get $o(y) > 2$. It follows that $\exp(C_G(H)) > 2$ so we must have $o(y) = 4$. In that case, $\langle H, y \rangle = H * \langle y \rangle$ of order 16 is minimal nonmetacyclic with exactly $7 > 3$ involutions (see Appendix 16), a contradiction.

It follows from Exercise 1 and Theorem 66.1 that if a nonmetacyclic 2-group G has exactly three involutions and has no subgroups $\cong Q_8$, then all its minimal nonmetacyclic subgroups have order 2^5 . Hence, in any case, G has a section $\cong Q_8$.

Exercise 2. If G has exactly three involutions, then all its minimal nonabelian subgroups are metacyclic.

It follows from Exercise 2 that if G of that exercise has no subgroups $\cong Q_8$, it involves $M_{2^n}, n > 3$.

Exercise 3. Suppose that G is a 2-group with exactly three involutions and $\mu \in \text{Aut}(G)$ has an odd prime order p . Find all possible values of p .

Hint. Since $d(G) \leq 4$ (see §50), we get $p \in \{3, 5, 7\}$ since $o(\mu)$ divides the number $(2^4 - 1)(2^4 - 2)(2^4 - 2^2)(2^4 - 2^3) = 2^6 \cdot 3^2 \cdot 5 \cdot 7$. We claim that $p \neq 7$. Assume that this is false. Let $W = \langle \mu \rangle \cdot G$ be the natural semidirect product. Without loss of generality one may assume that W is a minimal nonnilpotent group. Since G has exactly three involutions, it is nonabelian. Since the minimal natural b such that $2^b \equiv 1 \pmod{7}$, equals 3 and this number is odd, it follows from the structure of minimal nonnilpotent groups that G is abelian, which is a contradiction. We do not know if $p = 5$ is possible.

Exercise 4. Describe $\text{Aut}(A)$, where A is a group of Lemma 82.6.

According to Theorem 1.17(a), if a 2-group G is neither cyclic nor of maximal class, then the number of involutions in G is $\equiv 3 \pmod{4}$. Therefore, the next interesting case presents 2-groups with exactly seven involutions. To finish the classification of 2-groups G with exactly 7 involutions, it remains to consider the case $|\Omega_1(G)| = 8$ (in this case involutions generate elementary abelian subgroup of order 8; see Theorem 64.17). There exist 2-groups G with exactly seven involutions and such that $d(G) = 6$ (for example, the direct product of three generalized quaternion groups), however, we do not know if it is possible $d(G) > 6$ for such groups.

p -groups G with $\Omega_2(G)$ or $\Omega_2^*(G)$ extraspecial

In this section we classify the p -groups with the properties given in the title. This solves problems 157 and 1429 (see Research problems and themes, I and II, respectively). All results of this section are due to the second author.

Theorem 83.1. *If G is a p -group with extraspecial $\Omega_2(G)$, then $\Omega_2(G) = G$.*

Proof. Suppose that the theorem is false.

Case 1. Let $p = 2$. Set $E = \Omega_2(G)$ and $\langle z \rangle = Z(E)$ so that $|E| = 2^{2n+1}$, $n \geq 1$, where n is the width of E , and $o(z) = 2$. Let F be a subgroup of G containing E such that $|F : E| = 2$. We use induction on n . Suppose that $n = 1$. Then $E \cong D_8$ or Q_8 . If $C_F(E) \not\leq E$, then $C_F(E) - \langle z \rangle$ contains an element of order 2 and 4 since $|E \cap C_F(E)| = |Z(E)| = 2$, a contradiction. Hence $C_F(E) \leq E$ and then F is of maximal class (Proposition 10.17). But then $\Omega_2(F) = F$, a contradiction.

Now we assume that $n > 1$. Since $|E| \geq 2^5$ and $\exp(E) = 4$, F has no cyclic subgroup of index 2 and so F is not of maximal class. It follows that F possesses a normal four-subgroup R (Lemma 1.4). We have $R \leq \Omega_2(F) = E$. In particular, $z \in R$ and we may set $R = \langle z, u \rangle$ for some involution $u \in (E - \langle z \rangle)$ so that $C_F(R) = C_F(u)$. Since $|E : C_E(R)| = 2$, it follows that $C_F(R)$ covers F/E . By the structure of E , $C_E(u) = \langle u \rangle \times E_0$, where E_0 is extraspecial of order $2^{2(n-1)+1}$. Set $F_0 = C_F(u)$ so that $|F_0 : (\langle u \rangle \times E_0)| = 2$ and consider the factor-group $F_0/\langle u \rangle = \bar{F}_0$ (bar convention), where $|\bar{F}_0 : \bar{E}_0| = 2$ and \bar{E}_0 is extraspecial of width $n - 1$.

By induction, there is an element $x \in F_0 - (\langle u \rangle \times E_0)$ such that $o(\bar{x}) \leq 4$. If $o(\bar{x}) = 2$, then $x^2 \in \langle u \rangle$ and so $o(x) \leq 4$, a contradiction. Hence $o(\bar{x}) = 4$ and so $x^4 \in \langle u \rangle$ but $x^2 \notin \langle u \rangle$. We have $x^2 \in C_E(u)$. If x^2 is an involution, then $o(x) = 4$, a contradiction since $\Omega_2(F_0) = F_0 \cap E = \langle u \rangle \times E_0$. Hence x^2 is an element of order 4 in $C_E(u)$ and so, in view of $\Omega_1(C_E(u)) = \langle z \rangle$, we get $x^4 = z$, contrary to $x^4 \in \langle u \rangle$. Thus, F does not exist so $G = E$. The theorem is proved for $p = 2$.

Case 2. Now let $p > 2$ and let $E = \Omega_2(G)$ be extraspecial. Since $G > E$, we have $\exp(E) = p^2$. By the structure of E , we may set $E = E_1 * E_2 * \cdots * E_m$, $m \geq 1$, where $E_m \cong M_{p^3}$ and, in case $m > 1$, the subgroups E_1, \dots, E_{m-1} are nonabelian of order p^3 and exponent p . We have $S = \Omega_1(E) = \Omega_1(G) = E_1 \dots E_{m-1} \Omega_1(E_m)$ so that $|E : S| = p$, $R = \Omega_1(E_m) = Z(S) \cong E_{p^2}$, R is normal in G and $C_E(R) = S$. Set $C = C_G(R)$ so that $|G : C| = p$ and therefore $G = CE$ with $C \cap E = S$ and

$C > S$. But then $C - S$ contains an element of order p or p^2 , a contradiction. This completes Case 2. The theorem is proved. \square

Recall that if G is a p -group, then $\Omega_n^*(G) = \langle x \in G \mid o(x) = p^n \rangle$ if $\exp(G) \geq p^n$ and $\Omega_n^*(G) = \{1\}$ if $\exp(G) < p^n$.

Theorem 83.2. *Let G be a 2-group such that $\Omega_2^*(G)$ is extraspecial. Then either $\Omega_2^*(G) = G$ or $G \cong \text{SD}_{16}$.*

Proof. Set $E = \Omega_2^*(G)$, $|E| = 2^{2n+1}$, $n \geq 1$, $Z(E) = \langle z \rangle$, and assume $G > E$. Suppose that $C_G(E) > \langle z \rangle$. There are no elements of order 4 in $C_G(E) - \langle z \rangle$ and so $C_G(E)$ is elementary abelian. Let $i \in C_G(E) - \langle z \rangle$ so that i is an involution. If v is an element of order 4 in E , then vi is an element of order 4 in $G - E$, a contradiction. We have proved that $C_G(E) = \langle z \rangle$ and so $Z(G) = \langle z \rangle$.

By Theorem 83.1, there is an involution $t \in G - E$. Set $F = E\langle t \rangle$ so that $|F| = 2^{2n+2}$. If t centralizes an element v of order 4 in E , then tv is an element of order 4 and $tv \in F - E$, a contradiction. Hence $C_E(t)$ is elementary abelian and each element in $F - E$ is either an involution or an element of order 8 so that $\exp(F) = 8$.

If all elements in $F - E$ are involutions, then t inverts each element in E and so E would be abelian, which is not the case. Let r be an element of order 8 in $F - E$. Then $v = r^2$ generates a cyclic subgroup of order 4 in E so that $v^2 = z$ and $\langle v \rangle$ is normal in E . Thus, $N_G(\langle v \rangle) \geq \langle E, r \rangle = F$ so $\langle v \rangle$ is normal in F . Since $r \in C_F(v) - E$, it follows that $C_F(v)$ covers F/E . As above, all elements in $C_F(v) - E$ are not involutions so have order 8. Since $t \notin C_F(v)$ and $\langle v \rangle$ is normal in F , we get

$$(1) \quad v^t = v^{-1} = vz.$$

Act with the involution t on the elementary abelian group $E/\langle z \rangle$ of order 2^{2n} . It is easy to see that $E/\langle z \rangle$ is a direct product of t -invariant four-subgroups. Setting $E_1/\langle z \rangle = C_{E/\langle z \rangle}(t)$, we conclude that $|E_1/\langle z \rangle| \geq 2^n$, $E_2 = C_E(t) < E_1$ is elementary abelian, and $v \in E_1 - E_2$, by (1). Consider any element $x \in E_1 - E_2$. If x is an involution, then $x^t = xz$ implies that $\langle x, t \rangle \cong D_8$. But then $o(xt) = 4$ and $xt \in F - E$, a contradiction. Hence $o(x) = 4$ and therefore $x^2 = z$ and $x^t = xz = x^{-1}$. It follows that t inverts each element in E_1 and so E_1 is abelian, $\Omega_1(E_1) = E_2$ and all elements in the coset E_1t are involutions. If $x, y \in E_1 - E_2$, then $(xy)^2 = x^2y^2 = zz = 1$ and so $xy \in E_2$ which implies $|E_1 : E_2| = 2$. It is known (see §4) that maximal abelian subgroups of the extraspecial group E are of order 2^{n+1} . Since $|E_1| \geq 2^{n+1}$, we get $|E_1| = 2^{n+1}$ and $|E_2| = |E_1/\Omega_1(E_1)| = 2^n$. Note that te ($e \in E$) is an involution if and only if $(te)^2 = tete = 1$ or equivalently $e^t = e^{-1}$ and so $e \in E_1$. Hence E_1t is the set of all involutions in $F - E$ which implies that E_1t is a normal subset in F . But $F_1 = \langle E_1, t \rangle = \langle E_1t \rangle$ and so F_1 (of order 2^{n+2}) is normal in F . On the other hand, $F_2 = C_F(t) = \langle E_2, t \rangle$ is of order 2^{n+1} and $|F : F_2| = 2^{n+1}$. Since $|E_1t| = 2^{n+1}$, it follows that the set E_1t of all involutions in $F - E$ forms a single conjugacy class in F .

The nonabelian subgroup F_1 has exactly three abelian maximal subgroups: E_1 (of type $(4, 2, \dots, 2)$) and elementary abelian subgroups $F_2 = \langle E_2, t \rangle$ and $F_2^* = \langle E_2, tv \rangle$. Since $E_1t = E_2t \cup E_2tv$ and all involutions in E_1t form a single conjugacy class in F , we get that F_2 is not normal in F . Therefore, acting with F/F_1 on the set $\{F_2, F_2^*\}$, we get $F_3 = N_F(F_2) = N_F(F_2^*)$ and $|F : F_3| = 2$ with $F_3 \geq F_1$.

We have $|F| = 2^{2n+2}$ so that $|F_3| = 2^{2n+1}$. On the other hand, $|F_1| = 2^{n+2}$ and so, if $n > 1$, we get $F_3 > F_1$. In that case take an element $y \in F - E$ so that $y \in F_3 - F_1$. Since F_3/F_2 and F_2 are elementary abelian, we get $1 \neq y^2 \in F_2$ and so $o(y) = 4$ (noting that y is not an involution because all involutions in $F - E$ lie in $F_1 - E$). This is a contradiction.

We have proved that $n = 1$. In that case $E \cong Q_8$. But the Sylow 2-subgroup of $\text{Aut}(Q_8)$ is isomorphic to D_8 and $C_G(E) = \langle z \rangle$ imply that $G = F$, $|G : E| = 2$, and so G is a group of maximal class and order 2^4 (Proposition 10.17). Since there are involutions in $G - E$, we get $G \cong SD_{16}$ (Theorem 1.2), and we are done. \square

Recall that, given a p -group G , $H_p(G) = \langle x \in G \mid o(x) > p \rangle$ if $\exp(G) > p$ and $H_p(G) = \{1\}$ if $\exp(G) \leq p$.

Theorem 83.3. *Let G be a p -group, $p > 2$, such that $\Omega_2^*(G)$ is extraspecial. Then $\Omega_2^*(G) = H_p(G)$ and so, in the case $G > \Omega_2^*(G)$, all elements in $G - \Omega_2^*(G)$ are of order p .*

Proof. Set $E = \Omega_2^*(G)$, $Z = Z(E) \cong C_p$ and note that $\exp(E) = p^2$. Assuming $G > E$, we have to prove that all elements of the set $G - E$ are of order p .

Let F/E be a subgroup of order p in $G/E \neq \{1\}$. Let x be any element in $F - E$. Since $x^p \in E$, we have either $o(x) = p$ or $o(x) = p^3$. Suppose that $o(x) = p^3$. Then $\langle x^p \rangle = P$ is a cyclic subgroup of order p^2 in E . Since $P > Z$, P is normal in E and so $N_E(P) \geq \langle x, E \rangle = F$, and we conclude that P is normal in F . Because $|E : C_E(P)| = p$, we get that $C_F(P)$ covers F/E and each element in $C_F(P) - E$ must be of order p^3 (otherwise, if $u \in C_F(P) - E$ is of order p , then $ux^p \notin E$ has order p^2 , contrary to the hypothesis). By Theorem 83.1, $\Omega_2(F) = E$ is not possible and so $\Omega_2(F) = F$ and so there is an element y of order p in $F - E$. Since $y \notin C_F(P)$, we get $\langle P, y \rangle \cong M_{p^3}$. But then $o(yx^p) = p^2$ and $yx^p \notin E$, a contradiction. We have proved that all elements in $F - E$ are of order p .

Suppose that G/E is not of exponent p . Let S/E be a cyclic subgroup of order p^2 in G/E . Then $S = E\langle l \rangle$ for some $l \in G$. It follows that $E\langle l^p \rangle/E$ is a subgroup of order p in G/E and so by the above $o(l^p) = p$ and $o(l) = p^2$, $l \notin E$, a contradiction.

We have proved that $\exp(G/E) = p$ and so all elements in $G - E$ are of order p . We get $E = H_p(G)$, completing the proof. \square

2-groups whose nonmetacyclic subgroups are generated by involutions

Involutions play an important role in 2-groups. Here we classify nonmetacyclic 2-groups all of whose nonmetacyclic subgroups are generated by involutions. More precisely, we prove the following

Theorem 84.1 ([BozJ4]). *Let G be a nonmetacyclic 2-group all of whose nonmetacyclic subgroups are generated by involutions. Suppose that G is not elementary abelian. Then G is nonabelian and each abelian subgroup of G is either metacyclic or a self-centralizing elementary abelian group of order 8. Moreover, we have the following possibilities.*

- (a) *If G has no elementary abelian subgroups of order 8, then $G = D * C$, where $D \cong D_{2^n}$, $n \geq 3$, $C \cong C_4$ and $D \cap C = Z(D)$.*
- (b) *If G has a normal elementary abelian subgroup of order 8, then G is isomorphic to one of the following groups:*
 - (b1) $G \cong D_8 \times C_2$;
 - (b2) $G \cong Q_8 * Q_8$ (the central product of two quaternion groups), which is extraspecial of order 2^5 and type “+”;
 - (b3) $G = M \langle t \rangle$, where $M \cong C_4 \times C_4$ and t is an involution which inverts each element in M .
- (c) *If G has no normal elementary abelian subgroups of order 8 but G has an elementary abelian subgroup E of order 8, then $E \not\leq \Phi(G)$ and G is one of the groups appearing in Theorems 51.11 to 51.15.*

Proof. Let G be a nonmetacyclic 2-group all of whose nonmetacyclic subgroups are generated by involutions. Also, we suppose that G is not elementary abelian. Then G is nonabelian since G is nonmetacyclic and so G is generated by its involutions.

By Lemmas 65.1 and 65.2, each minimal nonabelian subgroup of G is metacyclic. Let A be a maximal abelian subgroup of G so that $C_G(A) = A$. Then A is either metacyclic (i.e., A is of rank ≤ 2) or A is of rank ≥ 3 in which case A must be elementary abelian of order ≥ 8 and we consider the second case. Let T be a subgroup of G such that $A < T \leq G$ and $|A : T| = 2$. Let v be an element of order 4 in $T - A$ so that $v^2 \in A$ and therefore v induces on A an involutory automorphism. In that case

it is well known that $T' \leq C_A(v)$, $C_A(v) = Z(T)$, $|T'| = |A/C_A(v)|$ which gives that $|C_A(v)| \geq |A/C_A(v)|$. Since $S = \langle v \rangle C_A(v)$ is abelian but not elementary abelian, S is not generated by its involutions and so S must be metacyclic. It follows that $U = C_A(v) \cong E_4$ and $v^2 \in U$ and so $A \cong E_8$ or $A \cong E_{16}$. Suppose that $|A| = 16$ in which case $T' = U = Z(T) \cong E_4$. Hence, there is an involution $a \in A - U$ such that $b = [a, v] \in U - \langle v^2 \rangle$. Set $M = \langle a, v \rangle$ so that $M' = \langle b \rangle$ and therefore M is nonmetacyclic minimal nonabelian (of order 2^4) because $\Omega_1(M) = \langle a, b, v^2 \rangle \cong E_8$, a contradiction. We have proved that each abelian subgroup of G is either metacyclic or a self-centralizing elementary abelian group of order 8.

Assume that G does not possess any elementary abelian subgroup of order 8. Since G is neither cyclic nor of maximal class, G has a normal four-subgroup U . If $\Omega_1(G) = U$, then G is not generated by involutions, a contradiction. Set $T = C_G(U)$ so that there is an involution $t \in G - T$, $|G : T| = 2$ and $\Omega_1(T) = U$. We have $C_G(t) = \langle t \rangle \times C_T(t)$ and since $C_T(t)$ contains only one involution z , where $\langle z \rangle = C_U(t)$, it follows that $C_T(t)$ is either cyclic or generalized quaternion. If $C_T(t)$ is generalized quaternion, then $C_G(t)$ is nonmetacyclic but $C_G(t)$ is not generated by involutions, a contradiction. Hence, $C_T(t)$ is cyclic. If $|C_T(t)| = 2$, then G is of maximal class and so G is metacyclic, a contradiction. We have proved that $C_T(t)$ is cyclic of order ≥ 4 , where $t \notin \Phi(G)$. By Theorem 48.1, $\Omega_1(G) = D * Z$, where $D \cong D_{2^n}$, $n \geq 3$, $Z \cong C_4$ and $D \cap Z = Z(D)$. Since in our case $\Omega_1(G) = G$, we have obtained a group stated in part (a) of the theorem.

Assume that G possesses a normal elementary abelian subgroup E of order 8. Let F/E be a cyclic subgroup of order 4 in G/E . Let T/E be a subgroup of order 2 in F/E . Then $\Omega_1(F) \leq T$ but F is nonmetacyclic. This is a contradiction and so $\{1\} \neq G/E$ is elementary abelian of order ≤ 4 since $C_G(E) = E$ and $\text{Aut}(E) \cong D_8$. Let H/E be any subgroup of order 2 in G/E . Since H is nonmetacyclic, there is an involution $t \in H - E$. Then $C_E(t) = V \cong E_4$ so that the coset Et consists of the set Vt of four involutions and the set Vtu of four elements of order 4, where u is an element in $E - V$. Since $[u, t] \neq 1$, $D = \langle u, t \rangle$ is dihedral of order 8. Because $|D \cap V| = 2$, there is an involution $z \in V - D$, where $V = Z(H)$. Hence $H = \langle z \rangle \times D \cong C_2 \times D_8$. If $H = G$, then we have obtained the group stated in part (b1) of the theorem.

Assume that $G/E \cong E_4$ so that $|G| = 2^5$. By the previous paragraph (since G/E has exactly three subgroups of order 2), $G - E$ consists of 12 involutions and 12 elements of order 4. Hence, G has exactly six cyclic subgroups of order 4. Suppose that $\Omega_2^*(G) = \{x \in G \mid o(x) = 4\}$ is of order $> 2^4$. Then $\Omega_2^*(G) = G$ is of order 2^5 and, by Lemma 89.6, $G \cong Q_8 * Q_8$ and so we have obtained the group in part (b2) of Theorem 85.1. Suppose that $\Omega_2^*(G)$ is of order $\leq 2^4$ so that $|\Omega_2^*(G)| = 2^4$ since G has exactly 12 elements of order 4. Set $M = \Omega_2^*(G)$, where all elements in $G - M$ must be involutions. If $t \in G - M$ is one of them, then t inverts each element in M which implies that M is abelian. Since M has exactly 12 elements of order 4, the only possibility is $M \cong C_4 \times C_4$ and $G = M\langle t \rangle$ is the group of part (b3) of the theorem.

Finally, suppose that G has no normal elementary abelian subgroups of order 8 but G has an elementary abelian subgroup E of order 8. We know that E is self-centralizing in G and suppose that $E \leq \Phi(G)$. By Theorem 51.6, G possesses a normal metacyclic subgroup N such that $G/N \cong C_4$ or $G/N \cong D_8$. Let T/N be a cyclic subgroup of order 4 in G/N so that $|G : T| \leq 2$. Then $\Phi(G) \leq T$ and so $E \leq T$ and therefore T is nonmetacyclic. Let T_0/N be the subgroup of order 2 in T/N . Then $\Omega_1(T) \leq T_0$ and therefore T is not generated by its involutions, a contradiction. We have proved that $E \not\leq \Phi(G)$. Therefore G satisfies the assumptions of the last part of §51 and so G must be a group appearing in Theorems 51.11 to 51.15. \square

2-groups with a nonabelian Frattini subgroup of order 16

According to a classical result of Burnside, if G is a finite 2-group, then the Frattini subgroup $\Phi(G)$ of G cannot be a nonabelian group of order 8. Here we study “the next possible case”, where G is a 2-group and $\Phi(G)$ is nonabelian of order 16 (see Research problems and themes II, #994). We show that in that case $\Phi(G) \cong M \times C_2$, where $M \cong D_8$ or $M \cong Q_8$ and we shall classify all such groups G (Theorem 85.1). (As it follows from Lemma 1.4, if G is p -group and N is a G -invariant subgroup of $\Phi(G)$, then N is cyclic if and only if $Z(N)$ is cyclic.)

To facilitate the proof, we make the following

Remark. Let G be a p -group and let N be a nonabelian G -invariant subgroup of $\Phi(G)$ of order p^4 . We claim that either $N = M \times C$, where M is nonabelian of order p^3 or $p > 2$ and N is metacyclic of exponent p^2 . Indeed, if $d(N) = 2$, then N is metacyclic (see Theorem 44.13). Since $Z(N)$ is noncyclic, we get $\exp(N) = p^2$. Assume, in addition, that $p = 2$. Then $N = \langle a, b \mid a^4 = b^4 = 1, a^b = a^3 \rangle$. In that case, $L = \langle a^2b^2 \rangle$ is characteristic in N so normal in G , and $N/L \cong Q_8$, contrary to Burnside’s result. Thus, if $d(N) = 2$, then $p > 2$ and N is metacyclic of exponent p^2 . Now let $d(N) = 3$. Then N contains a nonabelian subgroup M of order p^3 and $N = MZ(N)$. By Lemma 1.4, $Z(N) \cong E_{p^2}$ so $N = M \times C$, and we are done.

Theorem 85.1 (Z. Bozikov). *Let G be a finite 2-group such that $\Phi(G)$ is a nonabelian group of order 16. Then $\Phi(G) = M \times C_2$, where $M \cong D_8$ or Q_8 . The group G possesses normal subgroups H and C such that $G = HC$, $A = H \cap C \cong C_4 \times C_2$ or E_8 , $C_G(A) = C$, $d(H) = 2$, $A < \Phi(H) = \Phi(G)$, and $\Phi(C) \leq Z(\Phi(G)) \cong E_4$ so that C is a group of class ≤ 2 and exponent ≤ 4 . For the structure of H we have the following possibilities:*

- (a) *If $M \cong D_8$, then $A \cong E_8$ and H is isomorphic to one of the four groups of order 2^6 given in Theorem 51.4.*
- (b) *If $M \cong Q_8$, then $A \cong C_4 \times C_2$ and H is isomorphic to one of the following two groups of order 2^6 :*

$$\begin{aligned} &\langle x, y \mid x^8 = y^8 = 1, x^4 = y^4 = z, x^2 = a, y^2 = b, [a, b] = z, \\ &a^y = at, t^2 = [t, a] = [t, b] = 1, t^x = t^y = tz, b^x = btz, \\ &(xy)^2 = tz^\epsilon, \epsilon = 0, 1 \rangle. \end{aligned}$$

Here $\langle a, b \rangle \cong Q_8$, $\Phi(H) = \langle a, b \rangle \times \langle t \rangle \cong Q_8 \times C_2$, $Z(H) = \langle z \rangle \cong C_2$, $H' = \langle ab, t \rangle \cong C_4 \times C_2$, $Z(\Phi(H)) = \langle z, t \rangle \cong E_4$, $T_1 = C_H(\langle z, t \rangle) = \Phi(H)\langle xy \rangle$ is a characteristic subgroup of index 2 in H with $\Phi(T_1) = T'_1 = Z(T_1)$ and $Y = \langle ab, t, xy \rangle$ is the unique abelian maximal subgroup of T_1 , where Y is of type (4, 4). Finally, $A = \langle a, t \rangle$ and $B = \langle b, t \rangle$ are self-centralizing abelian normal subgroups of H and both are of type (4, 2).

Both groups (for $\epsilon = 0$ and $\epsilon = 1$) exist as transitive subgroups of the alternating group A_{16} and they are not isomorphic.

Proof. Let G be a finite 2-group such that $\Phi(G)$ is nonabelian of order 16. Then, by the Remark, $\Phi(G) = M \times \langle t \rangle$, where $M \in \{D_8, Q_8\}$ and t is an involution.

We can now use a theorem of Nekrasov (see Proposition 4.9) stating that if X is a 2-group with $\Phi(X) \cong E_4$, then $\Phi(X) \leq Z(X)$. Set $U = Z(\Phi(G))$. Then $U = Z(M) \times \langle t \rangle$. We get $\Phi(G/U) = \Phi(G)/U \cong E_4$ and so $\Phi(G)/U \leq Z(G/U)$. This implies that each subgroup S with $U \leq S \leq \Phi(G)$ is normal in G . This fact will be used often in our proof.

We have $C_G(U) = C_G(t)$ and $|G : C_G(U)| \leq 2$. Suppose that $C_G(U) = G$. Then $\Phi(G/\langle t \rangle) = \Phi(G)/\langle t \rangle \cong D_8$ or Q_8 , contrary to the above result of Burnside. It follows that $|G : C_G(U)| = 2$. Set $T = C_G(U) = C_G(t)$ so that $|G : T| = 2$.

We want to investigate the structure of $\bar{T} = T/\langle t \rangle$ and we use the bar convention. We have $\bar{M} \cong D_8$ or Q_8 , $\bar{M}' = \bar{U}$ and we know that each subgroup \bar{X} with $\bar{U} < \bar{X} < \bar{M}$ is normal in \bar{T} which implies that no element in \bar{T} induces an outer automorphism on \bar{M} . Hence $\bar{N} = C_{\bar{T}}(\bar{M})$ covers \bar{T}/\bar{M} and therefore $\bar{T} = \bar{M} * \bar{N}$ with $\bar{M} \cap \bar{N} = \bar{U}$. If N is the inverse image of \bar{N} , then we get $T = \Phi(G)N$, N is normal in T and $\Phi(G) \cap N = U = \langle t, z \rangle$. Note that $T/N \cong \Phi(G)/U \cong E_4$ and $[\Phi(G), N] \leq \langle t \rangle$ and so $\Phi(T) \leq U$ and $\exp(T) = 4$.

Suppose $[\Phi(G), N] = \{1\}$. Since $\Phi(G) > U$, there is $y \in G - T$ such that $y^2 = l \in \Phi(G) - U$. We have $l^2 \in \langle z \rangle = (\Phi(G))'$ and so $\langle l, z \rangle$ is a subgroup of order 4 which is normal in $\Phi(G)$. But N centralizes l (and z) and so $\langle l, z \rangle$ is normal in T . Also, $y \in G - T$ centralizes l (and z) and so $\langle l, z \rangle$ is normal in G . In that case, $|G : C_G(\langle l, z \rangle)| \leq 2$ and so $C_G(\langle l, z \rangle)$ contains $\Phi(G)$, a contradiction. We have proved that $[\Phi(G), N] = \langle t \rangle$ and so $T' = \Phi(T) = U \leq Z(T)$.

Since $\Phi(T) = U$, there is an element $x \in G - T$ such that $x^2 = a \in \Phi(G) - U$. If $\Phi(G) \cong D_8 \times C_2$, then $\Phi(G)$ has a maximal subgroup $X \cong C_4 \times C_2$ so that all elements in $\Phi(G) - X$ are involutions. In that case we may assume that $x^2 \in \Phi(G) - X$ so that $x^2 = a$ is an involution and so $A = \langle a, U \rangle \cong E_8$. However, if $\Phi(G) \cong Q_8 \times C_2$, then $A = \langle a, U \rangle \cong C_4 \times C_2$.

We have $\Phi(G) > A$ and so there is $y \in G - T$ such that $y^2 = b \in \Phi(G) - A$. Set $B = \langle b, U \rangle$ and note that both A and B are normal in G .

The subgroup $\langle a, b \rangle$ covers $\Phi(G)/U$ and $\langle a, b \rangle \cap U \neq \{1\}$ (because $\langle a, b \rangle \cap U = \{1\}$ would imply that $\Phi(G)$ is elementary abelian). Hence $|\langle a, b \rangle| \geq 8$. Since $d(\Phi(G)) = 3$, we have $|\langle a, b \rangle| = 8$ and $\langle a, b \rangle > \langle z \rangle$ because $\Phi(\Phi(G)) = \langle z \rangle$. It follows that $\langle a, b \rangle \cap U = \langle z \rangle$ and so $\Phi(G) = \langle a, b \rangle \times \langle t \rangle$ which implies that

$F = \langle a, b \rangle \cong D_8$ or Q_8 . Set $H = \langle x, y \rangle$ so that H is a 2-generator subgroup of G with $F \leq \Phi(H) \leq \Phi(G)$. By the above result of Burnside, $F = \Phi(H)$ is not possible. We have proved that $F < \Phi(H) = \Phi(G) \cong C_2 \times D_8$ or $C_2 \times Q_8$ and therefore $|H| = 2^6$ and H is normal in G .

It is easy to see that $A = \langle a, U \rangle$ is self-centralizing in H . Set $T_1 = T \cap H = C_H(U)$ and so $x, y \in H - T_1$, where $|H : T_1| = 2$ and $|T_1 : \Phi(H)| = 2$. Note that A is self-centralizing in $\Phi(H) = \Phi(G)$ and so $C_H(A) > A$ and $C_H(A) \leq T_1$ would imply that $C_H(A)$ covers $T_1/\Phi(H)$. In that case $\langle a, z \rangle$ is normal in H and so $|H : C_H(\langle a, z \rangle)| \leq 2$ and $C_H(\langle a, z \rangle) \geq \Phi(H)$, a contradiction. Hence A is self-centralizing in H and so $H/A \cong D_8$. This implies that $H' \not\leq A$. On the other hand, $\langle a, z \rangle$ is not normal in H and so there is $s \in H$ so that $a^s = atz^\epsilon$, $\epsilon = 0, 1$ which shows that $H' \geq \langle z, t \rangle = U$.

In the same way we see that $B = \langle b, U \rangle$ is self-centralizing in H . Therefore $H/B \cong D_8$ and so $H' \not\leq B$. On the other hand, $H' < \Phi(H)$. Indeed, if $H' = \Phi(H)$, then $|H/H'| = 4$ and so (by a well-known result of O. Taussky) the group H would be of maximal class, a contradiction. Since $H' \geq U$ and $H' \not\leq A$ and $H' \not\leq B$, we must have $H' = \langle ab, U \rangle$.

Since A is normal in G and A is self-centralizing in H with $H/A \cong \text{Aut}(A) \cong D_8$, we get that $C = C_G(A)$ covers G/H and so $G = HC$, where H and C are both normal in G and $H \cap C = A \cong E_8$ or $C_4 \times C_2$. On the other hand, $C \leq T = C_G(U)$ and we know that $\Phi(T) = T' = U \leq Z(T)$ and so $\Phi(C) \leq U$ and consequently C is of class ≤ 2 and exponent ≤ 4 .

If $M \cong F \cong D_8$, then $A \cong E_8$ and so A is a self-centralizing elementary abelian normal subgroup of order 8 in H with $A < \Phi(H)$. In this case H is isomorphic to one of four groups of order 2^6 given in Theorem 51.4.

We shall determine the structure of $H = \langle x, y \rangle$ in the case where $F \cong Q_8$ so that

$$x^2 = a, \quad y^2 = b, \quad a^2 = b^2 = z, \quad z^2 = 1, \quad \text{and} \quad [a, b] = z, \quad \text{where } \langle a, b \rangle = F.$$

Since $x, y \in H - T_1$, where $T_1 = C_H(\langle t, z \rangle)$, we get $t^x = t^y = tz$. We act with $\langle y \rangle$ on the abelian group $A = \langle a, t \rangle$ of type $(4, 2)$. Since $y^2 = b \notin A$ and A is self-centralizing in H , y induces an automorphism of order 4 on A and so we have $a^y = at$ or $a^y = atz$. However, if $a^y = atz$, we replace t with $t' = tz$ so that $a^y = at'$. Writing again t instead of t' , we may assume from the start that $a^y = at$. Similarly, acting with $\langle x \rangle$ on the self-centralizing normal abelian subgroup $B = \langle b, t \rangle$ (of type $(4, 2)$) in H and noting that $x^2 = a \notin B$, we see that $b^x = btz$ or $b^x = bt$. However, if $b^x = bt$, we replace x with $x' = x^{-1}$ and a with $a' = a^{-1}$ so that

$$(x')^2 = a', \quad (a')^y = (a^{-1})^y = (a^y)^{-1} = (at)^{-1} = a^{-1}t = a't$$

and $b = (bt)^{x^{-1}} = b^{x^{-1}}tz$ which gives $b^{x^{-1}} = btz$ and so $b^{x'} = btz$. Hence, writing again x and a instead of x' and a' , respectively, we may assume from the start that $b^x = btz$. We know that $H' = \langle ab, t \rangle \cong C_4 \times C_2$ and we compute:

$$(ab)^{xy} = (abtz)^y = atbtzz = ab.$$

Hence $Y = \langle ab, t, xy \rangle$ is abelian since $t^{xy} = t$ and so $xy \in T_1$. Since T_1 is a special group with $T'_1 = \Phi(T_1) = Z(T_1) = \langle t, z \rangle \cong E_4$, we get $(xy)^2 \in \langle t, z \rangle$ and Y is the unique abelian maximal subgroup of T_1 since $Z(T_1) = \langle t, z \rangle$ is of order 4.

It remains to show that $(xy)^2 = tz^\epsilon$, $\epsilon = 0, 1$. Suppose that this is false. Since $(xy)^2 \in \langle t, z \rangle$, we have in that case $(xy)^2 = z^\epsilon$, $\epsilon = 0, 1$. Recall that $H' = \langle ab, t \rangle$ and so $G/\langle z, t \rangle$ is nonabelian. Therefore $[x, y] \in H' - \langle z, t \rangle$ and so we may set $[x, y] = abz^\alpha t^\beta$, $\alpha, \beta = 0, 1$. Note that $xy \in T_1$ and so xy centralizes $\langle z, t \rangle$. We compute:

$$\begin{aligned} 1 &= [x, (xy)^2] = [x, xy][x, xy]^{xy} = [x, y][x, y]^{xy} = abz^\alpha t^\beta (abz^\alpha t^\beta)^{xy} \\ &= abz^\alpha t^\beta (at)(btz)^y z^\alpha t^\beta = abz^\alpha t^\beta (at)(btzz)z^\alpha t^\beta = (ab)^2, \end{aligned}$$

and this is a contradiction since $(ab)^2 = z$. We have proved that $(xy)^2 = tz^\epsilon$, $\epsilon = 0, 1$.

Finally, we see that both groups $H = \langle x, y \rangle$ for $\epsilon = 0$ and $\epsilon = 1$ exist as transitive subgroups of A_{16} . Indeed, for $\epsilon = 0$ we set:

$$x = (1, 2, 3, 4, 5, 6, 7, 8)(9, 13, 15, 12, 11, 14, 16, 10),$$

$$y = (1, 9, 10, 6, 5, 11, 12, 2)(3, 16, 14, 8, 7, 15, 13, 4),$$

and for $\epsilon = 1$ we set:

$$x = (1, 2, 3, 4, 5, 6, 7, 8)(9, 14, 15, 10, 11, 13, 16, 12),$$

$$y = (1, 9, 10, 6, 5, 11, 12, 2)(3, 15, 14, 4, 7, 16, 13, 8),$$

and we verify that all the defining relations for H are satisfied. The first group (for $\epsilon = 0$) has exactly 3 involutions and the second group (for $\epsilon = 1$) has exactly 11 involutions and so they are not isomorphic. Our theorem is proved. \square

p -groups G with metacyclic $\Omega_2^*(G)$

The main result of this section, Theorem 86.2, is due to the second author. The three proofs of Theorem 86.1 are given by the first author.

We classify here the p -groups G with $\Omega_2^*(G)$ metacyclic. We begin with the case $p > 2$.

Theorem 86.1 (Berkovich). *Let G be a nonmetacyclic p -group of exponent $> p$, $p > 2$, such that $H = \Omega_2^*(G)$ is metacyclic. Then G is a 3-group of maximal class. If $|H| = 3^3$, then all elements of the set $G - H$ have order 3. If $|G| > 3^4$, then all elements of the set $G - C_G(\Omega_1(H))$ have order 3.*

Proof. Since G is noncyclic, it has $\geq p$ cyclic subgroups of order p^2 (Theorem 1.10(b)). In that case, in view of regularity of H , we have $p^3 \leq |H| \leq p^4$ and $\Omega_1(H) \cong E_{p^2}$. If $|H| = p^3$, then $c_2(G) = c_2(H) = p$. If $|H| = p^4$, then $c_2(G) = c_2(H) = \frac{|H-\Omega_1(H)|}{\varphi(p^2)} = \frac{p^4-p^2}{p(p-1)} = p^2 + p$. In both cases, $c_2(G) \equiv p \pmod{p^{p-1}}$. It follows from Theorem 13.2(b) that G is absolutely regular or irregular of maximal class.

Let G is absolutely regular; then H is regular, by Hall's regularity criterion (Theorem 9.8(a)). In that case, $\Omega_2^*(G) = \Omega_2(G)$ so $\Omega_2(G) = H$ is metacyclic. Then G is metacyclic since it has no minimal nonmetacyclic subgroups (Theorem 41.1).

Now let G be of maximal class. Then G possesses an absolutely regular subgroup M of index p with $|\Omega_1(M)| = p^{p-1}$, and $\exp(M) > p$ in view of $|M| = \frac{1}{p}|G| \geq \frac{1}{p} \cdot p^{p+1} = p^p$ (Theorems 9.5 and 9.6). As in the previous paragraph, $\Omega_2(M) = \Omega_2^*(M) (\leq H)$ so $\Omega_1(M) \cong E_{p^2}$. It follows that $p-1=2$ so $p=3$. If $|H|=3^3$, then $M=H$ (indeed, if $|M| \geq 3^4$, then $|\Omega_2(M)| = 3^4$, by Theorem 9.6) so $|G|=3^4$; in this case, all elements of the set $G - H$ have order 3 since $\exp(G)=3^2$. Now we let $|G| > 3^4$; then $M = C_G(\Omega_1(H))$ (Theorem 9.6). Since all elements of G of order $> 3^2$ lie in M (Theorem 13.19), it follows that all elements of the set $G - M$ have order 3. \square

We turn now to more difficult case $p=2$ and prove the following classification result.

Theorem 86.2. *Let G be a nonmetacyclic 2-group of exponent > 2 such that $H = \Omega_2^*(G)$ is metacyclic. Then one of the following holds:*

- (a) $H \cong C_4 \times C_2$ is the unique abelian subgroup of G of type $(4, 2)$ and G is isomorphic to one of the groups given in (b) and (c) of Theorem 52.7.
- (b) $H \cong C_4 \times C_4$ and G is isomorphic to one of the groups given in (c) of Theorem 55.1.
- (c) $G = \langle t, c \mid t^2 = c^{2^{n+1}} = 1, n \geq 2, tc = b, b^4 = [b^2, c] = 1 \rangle$, where $|G| = 2^{n+3}, n \geq 2, H = \Omega_2^*(G) = \langle c^2, b \rangle$ with $(c^2)^b = c^{-2}$ and H is a splitting metacyclic maximal subgroup, $\langle b^2 \rangle \times \langle c \rangle$ is the unique abelian maximal subgroup (of type $(2, 2^{n+1})$), $Z(G) = \langle b^2, c^{2^n} \rangle \cong E_4$, $G' = \langle c^2 b^2 \rangle \cong C_{2^n}$, and $\langle t, b^2, c^{2^n} \rangle \cong E_8$ (so that G is nonmetacyclic).

The two families of groups in (a) are U_2 -groups (except the smallest members in each of these two families) and also all groups in (c) are U_2 -groups. However, no group given in (b) is a U_2 -group.

Proof. Let G be a nonmetacyclic 2-group of exponent > 2 such that the subgroup $H = \Omega_2^*(G)$ is metacyclic. If $H = \Omega_2(G)$, then a result of N. Blackburn (Theorem 41.1, Remark 2) implies that G is metacyclic, a contradiction. Hence $\Omega_2(G) > H$ and so there exist involutions in $G - H$.

Suppose that H is cyclic. Then $H \cong C_4$ and so $c_2(G) = 1$. But then Theorem 1.17(b) implies that G is dihedral so metacyclic, a contradiction. Hence H is noncyclic.

Assume that H is abelian (of rank 2). Since $H = \Omega_2^*(H)$, we have either $H \cong C_4 \times C_2$ or $H \cong C_4 \times C_4$.

Suppose $H \cong C_4 \times C_2$. In that case H is the unique abelian subgroup of type $(4, 2)$ in G since each such subgroup is generated by elements of order 4 so coincides with H .

Suppose $H \cong C_4 \times C_4$. In that case $c_2(G) = 6$ and $\Omega_2(G) > H$ and so G is isomorphic to a group given in the part (c) of Theorem 55.1.

From now on we assume that H is nonabelian. Suppose in addition that H has a cyclic subgroup of index 2. Since $\Omega_2^*(H) = H$, we get $H \cong Q_{2^n}, n \geq 3$. Let $H_0 \cong Q_8$ be a quaternion subgroup of H so that $C_H(H_0) = Z(H_0) = Z(H) \cong C_2$. If $C_G(H_0) \leq H_0$, then G is of maximal class (Proposition 10.17) and so G is metacyclic, a contradiction. Hence $D = C_G(H_0) \not\leq H_0$ so that $D \cap H = Z(H_0)$, $D > Z(H_0)$, and D must be elementary abelian. Let $d \in D - Z(H_0)$ and $s \in H_0$ with $o(s) = 4$. Then $o(ds) = 4$ and $ds \notin H$, a contradiction.

Our subgroup $H = \Omega_2^*(G)$ is metacyclic nonabelian and H has no cyclic subgroups of index 2 and so, by Theorem 82.1, H has exactly three involutions and $\Omega_1(H) \cong E_4$. Let $Z = \langle a \rangle$ be a cyclic normal subgroup of H such that H/Z is cyclic and we have $|H/Z| \geq 4$. Let K/Z be the subgroup of index 2 in H/Z . Since $\Omega_2^*(H) = H$, there is an element b of order 4 in $H - K$. This implies $|H/Z| = 4$, $H = \langle a \rangle \langle b \rangle$ with $\langle a \rangle \cap \langle b \rangle = \{1\}$ and so H is splitting over Z . We set $o(a) = 2^n$ with $n \geq 2$ since H is nonabelian. Since $K = \langle a \rangle \langle b^2 \rangle$ contains exactly three involutions, K is either abelian

of type $(2, 2^n)$, $n \geq 2$ or $K \cong M_{2^{n+1}}$, $n \geq 3$. In the last case, $\langle b \rangle \cong C_4$ acts faithfully on $\langle a \rangle$ and so in that case $n \geq 4$.

First assume $K \cong M_{2^{n+1}}$, $n \geq 4$, where $\langle b \rangle$ acts faithfully on $Z = \langle a \rangle$. We have $a^b = av$ or $a^b = a^{-1}v$, where v is an element of order 4 in $\langle a \rangle$. Set $v^2 = z$, where $z \in Z(H)$.

Suppose $a^b = av$ so that $H' = \langle v \rangle$ and $(a^4)^b = (av)^4 = a^4$. Since $\langle v \rangle \leq \langle a^4 \rangle$, we have $H' \leq Z(H)$. If $x, y \in H$ with $o(x) \leq 8$ and $o(y) \leq 8$, then $(xy)^8 = x^8y^8[y, x]^{28} = 1$ and so $\Omega_3(H) < H$ because $o(a) \geq 2^4$. This is a contradiction since we must have $\Omega_2^*(H) = H$ but $\Omega_2^*(H) \leq \Omega_3(H)$.

Assume $a^b = a^{-1}v$ so that $(a^2)^b = (a^{-1}v)^2 = a^{-2}z$ and $(a^4)^b = (a^{-1}v)^4 = a^{-4}$. Therefore b inverts $\langle a^4 \rangle$ and so $v^b = v^{-1}$. Also,

$$a^{b^2} = (a^{-1}v)^b = (a^{-1}v)^{-1}v^{-1} = av^{-2} = az, \quad \text{and} \quad a = (a^{b^{-1}})^{-1}v^{b^{-1}},$$

which gives $a^{b^{-1}} = a^{-1}v^{-1}$ and $a^{b^\eta} = a^{-1}v^\eta$, where $\eta = \pm 1$. We compute:

$$(ba^2)^2 = ba^2ba^2 = b^2(a^2)^b a^2 = b^2a^{-2}za^2 = b^2z,$$

and so $o(ba^2) = 4$. This implies $\Omega_2^*(H) \geq \langle b, a^2 \rangle$, where $L = \langle b, a^2 \rangle$ is a maximal subgroup of H . We claim that the set $H - L$ contains no elements of order 4 and this gives us a contradiction. Indeed, each element in $H - L$ has the form $(b^j a^{2i})a = b^j a^{2i+1}$ (i, j are integers). If $j = 2$, then

$$\begin{aligned} (b^2 a^{2i+1})^2 &= b^2 a^{2i+1} b^2 a^{2i+1} = b^4 (a^{b^2})^{2i+1} a^{2i+1} \\ &= (az)^{2i+1} a^{2i+1} = (a^{4i} z)a^2, \end{aligned}$$

which is an element of order ≥ 8 . If $j = \eta = \pm 1$, then

$$\begin{aligned} (b^\eta a^{2i+1})^2 &= b^\eta a^{2i+1} b^\eta a^{2i+1} = b^{2\eta} (a^{b^\eta})^{2i+1} a^{2i+1} \\ &= b^2 (a^{-1} v^\eta)^{2i+1} a^{2i+1} = b^2 (v^\eta)^{2i} v^\eta = b^2 z^i v^\eta, \end{aligned}$$

which is an element of order 4 since $[b^2, v] = 1$.

We have proved that $K = \langle b^2, a \rangle$ must be abelian of type $(2, 2^n)$, $n \geq 2$, $E_4 \cong \Omega_1(H) = \langle b^2, z \rangle \leq Z(H)$, where we have set $z = a^{2^{n-1}}$. The element b induces on $\langle a \rangle$ an involutory automorphism and so we have either $a^b = az$, $n \geq 3$ or $a^b = a^{-1}z^\epsilon$, $\epsilon = 0, 1$, $n \geq 2$ (and if $\epsilon = 1$, then $n \geq 3$).

First assume $a^b = az$, $n \geq 3$, where $H' = \langle z \rangle$ and so H is of class 2. In that case, if $x, y \in H$ with $o(x) \leq 4$ and $o(y) \leq 4$, then $(xy)^4 = x^4y^4[y, x]^6 = 1$ and so $\exp(\Omega_2(H)) = 4$. But $o(a) = 2^n \geq 8$ and so $\Omega_2^*(H) \leq \Omega_2(H) < H$, a contradiction.

We have proved that $a^b = a^{-1}z^\epsilon$, $\epsilon = 0, 1$, $n \geq 2$, and if $\epsilon = 1$, then $n \geq 3$. Assume $n = 2$ so that $H = \langle a, b \mid a^4 = b^4 = 1, a^b = a^{-1} \rangle$. By Theorem 55.1(b), G is isomorphic to the following (uniquely determined) group of order 2^5 :

$$(1) \quad G = \langle b, t \mid b^4 = t^2 = 1, b^t = ab, a^4 = 1, a^b = a^{-1}, a^t = a^{-1} \rangle,$$

where $\Omega_2^*(G) = \langle a, b \rangle$, $\Phi(G) = \langle a, b^2 \rangle \cong C_4 \times C_2$, and $\Omega_2(G) = G$.

It remains to study the case $n \geq 3$, where

$$H = \langle a, b \mid a^{2^n} = b^4 = 1, n \geq 3, a^b = a^{-1}z^\epsilon, \epsilon = 0, 1, z = a^{2^{n-1}} \rangle,$$

$H' = \langle a^2 \rangle \cong C_{2^{n-1}}$, $\Omega_1(H) = Z(H) = \langle b^2, z \rangle \cong E_4$, and $K = \langle b^2, a \rangle$ is the unique abelian maximal subgroup (of type $(2, 2^n)$) of H .

Let t be an involution in $G - H$ and set $L = H\langle t \rangle$. Since $\langle z \rangle = \Omega_1(H')$, $z \in Z(G)$ and let $\langle v \rangle$ be the cyclic subgroup of order 4 in H' so that $\langle v \rangle$ is normal in G . Note that $v^b = v^{-1}$ and $C_H(v) = K$ so that $C = C_G(v)$ covers G/H . Set $C_0 = C_L(v)$ and we see that $|G : C| = |L : C_0| = 2$, $L = C_0\langle b \rangle$, $G = C\langle b \rangle$, $C \cap H = K$. If t does not centralize $Z(H) = \langle b^2, z \rangle$, then $\langle t, Z(H) \rangle \cong D_8$ and tb^2 is an element of order 4 in $L - H$, a contradiction. Thus t centralizes $Z(H)$ and so $Z(H) \leq Z(L)$. Also, t does not centralize any element of order 4 in H and so $C_H(t) = \langle b^2, z \rangle = \Omega_1(H)$.

Since $\langle v \rangle$ is central in C , there are no involutions in $C - K$. But there are no elements of order 4 in $C - K$ and so $\Omega_2(C) = \Omega_2(K) = \langle b^2 \rangle \times \langle v \rangle \cong C_2 \times C_4$. The fact that $C_K(t) = Z(H)$ also implies $C_C(t) = Z(H) = \Omega_1(C)$. Note that $Z(H) \leq Z(L)$ implies that $Z(C_0) \geq \langle b^2, z \rangle$ and so $Z(C_0)$ is noncyclic. By Lemma 42.1, C_0 is abelian of type $(2, 2^{n+1})$.

We act with the involution t on the abelian group C_0 and apply Proposition 51.2. It follows that t inverts on $C_0/\langle b^2, z \rangle$. We get $a^t = a^{-1}s$, where $s \in \langle b^2, z \rangle$. Then $(ta)^2 = tata = a^t a = a^{-1}sa = s$ and so $s = 1$ since $ta \notin H$ and ta cannot be an element of order 4. We get $a^t = a^{-1}$ and so t inverts K . On the other hand, $b = tc_0$ with $c_0 \in K$ and so $a^b = a^{tc_0} = (a^{-1})^{c_0} = a^{-1}$ because C_0 is abelian. We have proved that $\epsilon = 0$ and so b also inverts K .

We show that the involution b^2z is not a square in H . Indeed, for any $x \in K$, we get $(bx)^2 = bxbx = b^2x^bx = b^2x^{-1}x = b^2$. On the other hand, b^2 and z are squares in H and so $\langle b^2z \rangle$ is a characteristic subgroup of H and therefore $b^2z \in Z(G)$. It follows that $Z(H) = \langle b^2, z \rangle \leq Z(G)$.

We use again Lemma 42.1 and get that C is also abelian (of type $(2, 2^k)$, $k \geq n+1$). If $C \neq C_0$, then there is an element $d \in C_0 - K$ such that $d \in \mathfrak{U}_1(C)$. By Proposition 51.2, t inverts $\mathfrak{U}_1(C)$ and so $d^t = t^{-1}$. But then t inverts each element in C_0 which implies that all elements in $tC_0 = L - C_0$ are involutions. This is a contradiction since $b \in L - C_0$ and $o(b) = 4$.

We have proved that $C = C_0$ and so $G = L$. Since t inverts K , all elements in tK are involutions. But b is not an involution and so $b = tc$ with a suitable element $c \in C_0 - K$ so that $o(c) = 2^{n+1}$. Since C_0 is abelian, we have $[b^2, c] = 1$. We have obtained the following group of order 2^{n+3} :

$$(2) \quad G = \langle c, t \mid c^{2^{n+1}} = t^2 = 1, n \geq 3, tc = b, b^4 = [b^2, c] = 1 \rangle,$$

where $\Omega_2^*(G) = \langle c^2, b \rangle$ with $(c^2)^b = c^{-2}$.

If we set $n = 2$ in (2), we get a group G of order 2⁵ with $\Omega_2^*(G) = \langle c^2, b \mid (c^2)^4 = b^4 = 1, (c^2)^b = c^{-2} \rangle$ and $\Omega_2(G) = G$ and so this group G (because Theorem

55.1(b) implies the uniqueness of such a group) must be isomorphic to the group given in (1). We have obtained the groups given in part (c) of our theorem for all $n \geq 2$. \square

The second proof of Theorem 86.1. Assume that G is neither metacyclic nor a 3-group of maximal class. Then G , by Theorem 13.7, possesses a normal subgroup S of order p^3 and exponent p . Let R be a minimal G -invariant subgroup of S not contained in H . Then $E = \Omega_1(H)R$ is of order p^3 and exponent p . Set $T = HE$. The subgroup T is irregular (otherwise, $\Omega_2^*(T) = \Omega_2(T) = T > H$, which is not the case). In that case, by Theorem 12.1(b), $\Omega_1(T) = E$. Since $\exp(T) = p^2$, we get $\Omega_2^*(T) = \langle T - E \rangle = T > H$, a contradiction. Thus, S does not exist so G is a 3-group of maximal class (Theorem 13.7), and the proof is complete. \square

The third proof of Theorem 86.1. We retain the notation of Theorem 86.1.

If G is regular, then $H = \Omega_2(G)$ so G is metacyclic since it has no minimal nonmetacyclic subgroups (Theorem 41.1).

Next let G be irregular. Set $R = \Omega_1(H)$; then $R \cong E_{p^2}$. Set $T = C_G(R)$. Assume that $H \not\leq T$; then H is nonabelian of order p^3 . If $C_G(H) \not\leq H$ and K/H is a subgroup of order p in $HC_G(H)/H$, then $d(K) = 3$ so K is regular and $\Omega_2^*(K) = \Omega_2(K) = K > H$, a contradiction. Thus, $H \leq T$.

Assume that there is no a G -invariant subgroup $L \cong E_{p^3}$ such that $R < L \leq T$. Then T is metacyclic, by Theorems 13.7 and 10.4. By Theorem 12.1, $G = T\Omega_1(G)$, where $\Omega_1(G)$ is of order p^3 and exponent p , and so $p = 3$. Assume that $|G| > 3^4$. Let $Z = Z(\Omega_1(G))$. Set $C = C_G(\Omega_1(G)/Z)$ and let $U/\Omega_1(G)$ be a subgroup of order 3 in $C/\Omega_1(G)$. Then U is of class ≤ 2 so regular, and $\exp(U) = 9$, and we conclude that $\Omega_2^*(U) = U$, a contradiction since U is nonmetacyclic. Thus, G is of order 3^4 so it is of maximal class.

Now let T contains a G -invariant subgroup $L \cong E_{p^3}$. Considering LR , one may assume that $R < L$. Then $K = HL$ is of class at most 2 so regular (indeed, K/R is elementary abelian). In that case, $\Omega_2^*(K) = \Omega_2(K) = K > H$, a final contradiction. \square

Exercise 1. Let $p > 2$, $n > 1$ and $\Omega_n^*(G)$ is absolutely regular.

- (a) If $n = 2$, then G is either absolutely regular or irregular of maximal class.
- (b) Is it true that, if $n > 2$ and $\Omega_n^*(G)$ is absolutely regular, then G is either absolutely regular or of maximal class?

Exercise 2. Let G be a metacyclic 2-group of order $> 2^4$ such that $\Omega_2^*(G) = G$ and $G \not\cong Q_{2^n}$ for all $n \in \mathbb{N}$. Then the following holds: (a) $R = \Omega_1(G) \cong E_4$. (b) G/R is dihedral. (c) $R \leq Z(G)$. (d) If $T/R < G/R$ is cyclic of index 2, then $\Omega_1(T) = R$, i.e., G is a U_2 -group (see §67).

Solution. By hypothesis, G is not of maximal class so (a) is true, by Proposition 1.19. Let $x \in G$ be of order 4. Then $o(xR) = 2$ so G/R is generated by involutions. It

follows that G/R is dihedral, proving (b). Let $K/R < G/R$ be of order 2. Since G is not of maximal class, K is abelian so that $C_G(R) \geq K$. It follows that $R \leq Z(G)$ since G is generated by such subgroups K . Now let T/R be a cyclic subgroup of index 2 in G . The subgroup T is metacyclic so T has a cyclic subgroup of index 2, and we conclude that $\Omega_1(T) = R$. (Obviously, T is abelian.)

Problem. Let $n > 2$. Classify the p -groups G such that $\Omega_n^*(G)$ is metacyclic.

2-groups with exactly one nonmetacyclic maximal subgroup

Let G be a nonmetacyclic 2-group. If all maximal subgroups of G are metacyclic, then G is minimal nonmetacyclic and then $d(G) = 3$, $|G| \leq 2^5$, and there are exactly four such groups (see Theorem 64.1(l) or §§66, 69).

It is natural to ask what happens if all maximal subgroups except one are metacyclic. In that case the situation is essentially more complicated since there exist many infinite families of such 2-groups.

We determine here the structure of all 2-groups G which have exactly one nonmetacyclic maximal subgroup. All such groups G will be given in terms of generators and relations but we shall also describe many important subgroups of these groups. It is easy to see that we must have $d(G) \leq 3$.

If $d(G) = 3$, then the problem is simpler because in this case the group G has six metacyclic maximal subgroups. Such groups are given in Theorem 87.8 and we see that there are exactly five infinite families of these groups. It is interesting to note that in all such groups the commutator subgroup G' is elementary abelian of order ≤ 4 .

Now assume that $d(G) = 2$. This is essentially more difficult. In this case we show that G/G' is abelian of type $(2, 2^m)$, $m \geq 2$, and $G' \neq \{1\}$ is abelian of rank ≤ 2 . If G has a normal elementary abelian subgroup of order 8, then these groups are determined in Theorems 87.9 and 87.10. If G has no normal elementary abelian subgroups of order 8, then many properties of such groups are described in details in Theorem 87.11. In fact, this theorem is a key result for further case-to-case investigations depending on the structure of G' and $G/\Phi(G')$. It is interesting to note that if G' is noncyclic but $G/\Phi(G')$ has no normal elementary abelian subgroups of order 8, then G' has a cyclic subgroup of index 2 and $m = 2$ (i.e., G/G' is abelian of type $(2, 4)$) and such groups are determined in Theorems 87.14 and 87.15, where we get an exceptional group of order 2^5 and two infinite classes. However, if G' has no cyclic subgroups of index 2, then $m = 2$, $Z(G)$ is elementary abelian of order ≤ 4 (Theorem 87.18) and all such groups are completely determined in Theorems 87.17, 87.19, 87.20, and 87.21 (where we get infinite classes of groups in each case). If G' is cyclic or if G' is noncyclic but G' has a cyclic subgroup of index 2 and $G/\Phi(G')$ has a normal elementary abelian subgroup of order 8, then such groups are determined in Theorems 87.12 and 87.16. This exhausts all possibilities.

The most impressive result is Corollary 87.13, where it is shown that in each case with $d(G) = 2$ such a group $G = AB$ is a product of two suitable cyclic subgroups A and B . The converse of the last result is Theorem 87.22 which was also proved independently by the first author. Here was proved that if $G = AB$ is a nonmetacyclic 2-group, where A and B are cyclic, then G has exactly one nonmetacyclic maximal subgroup and so all such groups have been completely determined in our previous theorems for $d(G) = 2$.

In each infinite class of 2-groups (given in terms of generators and relations) we have checked several smallest groups with a computer (coset enumeration program) and so we have proved that they exist. Actually, we have obtained faithful permutation representations for these groups.

From a description of the structure of the obtained groups (and their distinct orders in each series), we also see that such groups are pairwise nonisomorphic.

Finally, it is easily checked that all 2-groups given in our theorems have exactly one nonmetacyclic maximal subgroup.

1°. We assume in this section that G is a 2-group with exactly one nonmetacyclic maximal subgroup M and $d(G) = 3$.

Lemma 87.1. *We have $d(M) = 3$ and all other six maximal subgroups of G are metacyclic.*

Proof. Suppose at the moment that $d(M) = 2$ so that all maximal subgroups of G are two-generator. Obviously, M is nonabelian and so G is nonabelian. If G is of class 2, we may apply Theorem 70.1. It follows that either each maximal subgroup of G is metacyclic or G has more than one nonmetacyclic maximal subgroup. This is a contradiction and so G is of class > 2 . In that case we may apply Theorem 70.2 which implies that all maximal subgroups of G are nonmetacyclic, a contradiction. Hence $d(M) > 2$ and, considering $M \cap F$, where F is a metacyclic maximal subgroup of G , we get $d(M) = 3$. \square

Lemma 87.2. *The abelian group G/G' is of type $(2, 2, 2^m)$, $m > 1$.*

Proof. Since $G' \leq \Phi(G)$, we have $d(G/G') = 3$ and we want to show that $G' < \Phi(G)$. Assume that this is false. Then $\bar{G} = G/\Phi(M)$ is nonabelian of order 16. Let \bar{D} be a minimal nonabelian subgroup of \bar{G} ; then $\bar{D} \cong D_8$ since $\bar{D} \cap \bar{M} \cong E_4$. By Proposition 10.17, $\bar{G} = \bar{D}Z(\bar{D}) = \bar{D} \times \bar{C}$, where $|\bar{C}| = 2$. In that case, \bar{G} has two distinct elementary abelian subgroups of order 8, contrary to the hypothesis. \square

On the other hand, abelian groups of type $(2, 2, 2^m)$, $m > 1$, satisfy the assumptions of this section. Therefore, we assume in the sequel that $G' > \{1\}$.

Remark 1. By Lemma 87.2, G/G' is abelian of type $(2^m, 2, 2)$, $m > 1$. Therefore, $G/G' = (E/G') \times (F/G')$, where $E/G' \cong E_4$ and $F/F' \cong C_{2^m}$ (Lemma 4(b), Introduction, Volume 1). Let $R \leq G'$ be G -invariant. We claim that G/R satisfies

the hypothesis and, if M is the maximal subgroup of G , containing E , then M is not metacyclic. Indeed, write $H/G' = \Omega_1(G/G')$ ($\cong E_8$); then H/G' is not metacyclic. Then $E < H$ so, if $E < H < M \in \Gamma_1$, then M/G' is not metacyclic. Clearly, M/G' is the unique nonmetacyclic maximal subgroup of G/G' since M is the unique nonmetacyclic maximal subgroup of G . It follows that each of three maximal subgroups, say X , of G containing F , is metacyclic but not of maximal class (otherwise, $|G/G'| = 8$). It follows that $\Omega_1(X) \cong E_4$. Assume that F is noncyclic. We claim that then $\Omega_1(G) = \Omega_1(F)$ ($\cong E_4$). Indeed, if $i \in G - F$ is an involution, then, taking $X = F\langle i \rangle$, we get $\Omega_1(X) \cong E_4 \cong \Omega_1(F)$, which is absurd.

Lemma 87.3. *If the nonabelian group G has a normal subgroup $E \cong E_8$, then $G \cong C_2 \times M_{2m+2}$, $m \geq 1$.*

Proof. By Lemma 87.2 and our assumption that G is nonabelian, we have $|G| \geq 2^5$. Since G has exactly one nonmetacyclic maximal subgroup, G/E must be cyclic of order ≥ 4 . Let $a \in G - E$ be such that $\langle a \rangle$ covers G/E . Then $\{1\} < G' = [E, \langle a \rangle] < E$ and $\Phi(G) = G'\langle a^2 \rangle$. But $d(G) = 3$ implies $|G'| = 2$ so $|G| = 2^{m+3}$. Let U be minimal nonabelian subgroup of G not containing E (U exists since G has at most three abelian maximal subgroups). Since U is metacyclic and is not of maximal class, it has exactly three involutions so we get $\Omega_1(U) = U \cap E \cong E_4$. It follows from $U/\Omega_1(U) \cong G/E$ that $U \cong M_{2m+2}$. Since $G' = U'$, one may assume that $G' < A = \langle a \rangle < U$ so $A \triangleleft G$ and $\Phi(G) = \Omega_1(A) \leq Z(G)$. Let $U = U_1, U_2, U_3$ be all maximal subgroups of G containing A , and assume that all of them are nonabelian; then they are isomorphic with M_{2m+2} (Theorem 1.2). Let $U_i = \langle a, b_i \mid a^{2^{m+1}} = b_i^2 = 1, a^{b_i} = a^{1+2^m} \rangle$, $i = 1, 2, 3$. We have $b_i \in E$, all i , and $b_3b_2^{-1}$ is an involution centralizing a , so $\langle a, b_3b_2^{-1} \rangle$ is an abelian maximal subgroup of G containing A , a contradiction. Let, say U_2 , be abelian. Then $C_G(b_2) \geq \langle A, E \rangle = G$. In that case, $G = U_1 \times \langle b_2 \rangle$. \square

In the sequel we assume that G has no normal elementary abelian subgroups of order 8.

Lemma 87.4. *Suppose that G is nonabelian and G does not have a normal elementary abelian subgroup of order 8. Then the following two assumptions are equivalent:*

- (a) $\Phi(G)$ is cyclic.
- (b) G has two distinct normal four-subgroups.

If G satisfies (a) or (b), then $G = D * Z$ with $D \cong D_8$, $Z \cong C_{2^n}$, $n \geq 3$, and $D \cap Z = Z(D)$.

Proof. Suppose that $\Phi(G)$ is cyclic. Since $\Phi(G) = \Omega_1(G)$, it follows that G has a cyclic subgroup $A = \langle a \rangle$ of index 4, and $\Phi(G) = \langle a^2 \rangle$. Let $A = U \cap V$, where U and V are distinct maximal subgroups of G . It follows from Lemma 87.2 that G has no subgroups of maximal class and index 2. Therefore, U, V have G -invariant four-subgroups R_1, R_2 , respectively (Lemma 1.4). Clearly, $R_1 \neq R_2$ so (b) is proved and

$D = R_1 R_2 \cong D_8$. If $H/D < G/D$ is maximal, then H is not metacyclic (otherwise, H is of maximal class) so G/D must be cyclic. Next, $\Phi(G) \leq C_G(R_1) \cap C_G(R_2) = C_G(D)$. Since $C_G(D) \cap D = Z(D)$, we get, by the product formula, $G = D * C$, where $C = C_G(D)$. Note that $C \triangleleft G$. Assuming that C has a G -invariant four-subgroup R , we obtain a G -invariant subgroup $R_1 R \cong E_8$, a contradiction. Thus, C is either cyclic or of maximal class (Lemma 1.4). The second alternative is impossible since $d(G) = 3$.

Suppose that G has two distinct normal four-subgroups. By Theorem 50.2, $G = D * Z$ with $D \cong D_8$, $D \cap Z = Z(D)$, and Z is cyclic (see the previous paragraph). \square

In the sequel we assume that $\Phi(G)$ is noncyclic which is equivalent with the assumption that G has a unique normal four-subgroup W (Lemma 87.4).

Lemma 87.5. *Let G be nonabelian without a normal E_8 and having a unique normal four-subgroup W . If X is any metacyclic maximal subgroup of G , then $\Omega_1(X) = W$ and X is not of maximal class.*

Proof. Since $\Phi(G)$ is metacyclic but noncyclic, it follows that the subgroup $W = \Omega_1(Z(\Phi(G))) \cong E_4$ (Lemma 64.1(v)). Let X be a metacyclic maximal subgroup of G . Let $i \in X - W$ be an involution. Since i cannot centralize W (because X is metacyclic), it follows $\langle W, i \rangle \cong D_8$. By Proposition 10.19, X is of maximal class, contrary to Lemma 87.2. \square

Lemma 87.6. *Let the group G be nonabelian without normal elementary abelian subgroups of order 8 and having a unique normal four-subgroup. If G' is cyclic, then $G' \cong C_2$ and $G = Q \times Z$, where $Q \cong Q_8$ and $Z \cong C_{2^m}$, $m \geq 2$.*

Proof. Let $G' \cong C_{2^r}$, $r \geq 1$. By Lemma 87.2, $G = EF$ with normal subgroups E and F , where $E \cap F = G'$, $E/G' \cong E_4$, and $F/G' \cong C_{2^m}$, $m \geq 2$. Let $a \in F$ be such that $\langle a \rangle$ covers F/G' . Then $G = E\langle a \rangle$, $\Phi(G) = G'\langle a^2 \rangle$ and $W = \Omega_1(Z(\Phi(G)))$ is a unique normal four-subgroup of G . Since $W \not\leq E$, E does not have a G -invariant four-subgroup. Because E is noncyclic, E is of maximal class with $|E| = 2^{r+2}$ and $E' = G' = \Phi(E)$ (Lemma 1.4). We note that $M = E\Phi(G) = E\langle a^2 \rangle$ is the unique nonmetacyclic maximal subgroup of G since $E\langle a^{2^{m-1}} \rangle/G' \cong E_8$ (see also Remark 1). Hence each maximal subgroup of G containing F is metacyclic. Suppose that there is an involution $i \in E - G'$. Then $X = F\langle i \rangle$ is a metacyclic maximal subgroup of G with $\Omega_1(X) > W$, contrary to Lemma 87.5. Since there are no involutions in $E - G'$, we conclude that $E \cong Q_{2^{r+2}}$, $r \geq 1$.

Suppose $r > 1$. Let y be an element of order 4 in $E - G'$ so that $y^2 \in \Omega_1(G')$ and $Y = F\langle y \rangle$ is a metacyclic maximal subgroup of G . Since $|G'| \geq 4$, there is an element v of order 4 in G' so that $\langle y, v \rangle \cong Q_8$ is a nonabelian subgroup of order 8 contained in Y . By Proposition 10.19, Y is of maximal class, contrary to Lemma 87.5.

We have proved that $r = 1$ and so $G' \cong C_2$ and $E \cong Q_8$. Since $\Phi(G)$ is noncyclic, $\langle a \rangle$ splits over G' , and so we get $F = G' \times \langle a \rangle$ with $o(a) = 2^m$, $m \geq 2$. We

have $C_G(E) \cap E = G'$ so $G/C_G(E)$ is an abelian subgroup of D_8 . It follows that $G/C_G(E) \cong E_4 \cong \text{Inn}(E)$ so, by the product formula, $G = E * C_G(E)$. But then $(G' \geq) [E, \langle a \rangle] \cong C_4$, a contradiction. Hence a induces an inner automorphism on E which implies with $E \cap C = G'$ and $C/G' \cong C_{2^m}$. Since $\Phi(G) = \Phi(C)$ and $\Phi(G)$ is noncyclic, C splits over G' . \square

From now on we assume that G' is noncyclic. Then, by Lemma 87.3, G has no normal elementary abelian subgroups of order 8 and G has a unique normal four-subgroup W .

Lemma 87.7. *Suppose that G' is a four-group. Then $G = Q\langle a \rangle$, where $Q = \langle x, y \rangle \cong Q_8$, $o(a) = 2^n$, $n \geq 3$, $Q \cap \langle a \rangle = \{1\}$, a^2 centralizes Q , $[a, x] = 1$, and $[a, y] = a^{2^{n-1}} = z$. Here $G' = \langle u, z \rangle \cong E_4$, where $\langle u \rangle = Z(Q)$, $\Phi(G) = Z(G) = \langle a^2 \rangle \times \langle u \rangle \cong C_{2^{n-1}} \times C_2$, and $M = Q \times \langle a^2 \rangle$ is a unique nonmetacyclic maximal subgroup of G .*

Proof. Using Lemma 87.2, we have $G = EF$ with normal subgroups E and F , where $E \cap F = G'$, $E/G' \cong E_4$, and $F/G' \cong C_{2^m}$, $m \geq 2$. Let M be the maximal subgroup of G containing E so that $d(M) = 3$ (Remark 1). Since $F \not\leq M$, each maximal subgroup of G containing F is metacyclic but not of maximal class (Lemma 87.5). In particular, $\Omega_1(F) = G'$. Since F/G' is cyclic, F has a cyclic subgroup $\langle a \rangle$ of order 2^{m+1} (and index 2). Set $z = a^{2^m}$.

Since $F' \leq \langle a \rangle \cap G' = \langle z \rangle$, F is either abelian of type $(2^{m+1}, 2)$ or $F \cong M_{2^{m+2}}$. In any case, $\Phi(G) = G'\langle a^2 \rangle$ is abelian of type $(2^m, 2)$, $m \geq 2$.

Since F is noncyclic, we get $\Omega_1(G) = W$ (Remark 1) so G has only three involutions.

Let $x \in E - G'$ such that x does not centralize G' . Then $x^2 \in G'$ and so $\langle G', x \rangle \cong D_8$. But in that case there are involutions in $\langle G', x \rangle - G'$, a contradiction. We have proved that $G' \leq Z(E)$.

Set $v = a^{2^{m-1}}$ so that $o(v) = 4$ and $v^2 = z$. Since $v \in \Phi(G)$, v centralizes G' . If X is any maximal subgroup of G containing F , then X is metacyclic and therefore X' is cyclic of order at most 2 (since $X' \leq G' \cong E_4$). In particular, X is of class ≤ 2 . For any $x \in E - G'$, $F\langle x \rangle < G$ so $[x, a^2] = [x, a]^2 = 1$ which gives $[E, a^2] = \{1\}$. If for some $y \in E - G'$, $y^2 = z$, then $(yv)^2 = y^2v^2[v, y] = zz = 1$ and so yv is an involution in $G - E$, a contradiction. We have proved that z is not a square in E . In particular, E is nonabelian (since E has exactly three involutions and $\exp(E) = 4$).

Since $z \in \Phi(\Phi(G)) = \langle a^4 \rangle$, we have $z \in Z(G)$. Take an $x \in E - G'$ so that $x^2 \in G' - \langle z \rangle$; then $\text{cl}(F\langle x \rangle) \leq 2$. This gives $[x^2, a] = [x, a]^2 = 1$ and $C_G(x^2) \geq \langle E, a \rangle = G$. We have proved that $G' \leq Z(G)$ so $\text{cl}(G) = 2$ and F is abelian of type $(2^{m+1}, 2)$.

We have $\Phi(G) = G'\langle a^2 \rangle \leq Z(G)$. If $Z(G) > \Phi(G)$, then $G/Z(G) \cong E_4$, and so $|G'| \leq 2$ (Lemma 64.1(u)), a contradiction. Thus, $Z(G) = \Phi(G)$. If E is minimal nonabelian, then it follows from $\Omega_1(E) = G' \cong E_4$ that E is metacyclic of exponent 4

(Lemma 65.1) and so there are elements x and y of order 4 in $E - G'$ so that $E = \langle x, y \mid x^4 = y^4 = 1, x^y = x^{-1} \rangle$, where $E' = \langle x^2 \rangle$, $x^2 \neq y^2$, $x^2 \in G' - \langle z \rangle$, $y^2 \in G' - \langle z \rangle$, and $x^2 y^2 = z$ because z is not a square in E .

If E is not minimal nonabelian, then the fact that E has only three involutions and z is not a square in E implies $E = Q \times \langle z \rangle$ with $Q \cong Q_8$.

Suppose that E is minimal nonabelian given above. We note that $v = a^{2^{m-1}}$ centralizes E and $v^2 = z$. Replace y with $y' = vy$ so that $(y')^2 = (vy)^2 = v^2 y^2 = z y^2 = x^2$ and $x^{y'} = x^{vy} = x^y = x^{-1}$, and therefore $\langle x, y' \rangle = Q \cong Q_8$ and $E^* = Q \times \langle z \rangle$ is another complement of F modulo G' . Indeed, note that $E^* > G' = \Omega_1(G)$, $E^*/G' \cong E_4$, $E^* \triangleleft G$ and $E^* \cap F = G'$. Hence, replacing E with E^* (if necessary), we may assume from the start that E is not minimal nonabelian and so $E = Q \times \langle z \rangle$, $Q \cong Q_8$, and setting $\langle u \rangle = Q' = Z(Q)$, we have $G' = \langle u \rangle \times \langle z \rangle \cong E_4$, $M = Q \times \langle a^2 \rangle \cong Q_8 \times C_{2^m}$, and $\Phi(M) = \langle u \rangle \times \langle a^4 \rangle$, where $\langle a^4 \rangle \geq \langle z \rangle$.

Write $Q = \langle x, y \mid x^2 = y^2 = [x, y] = u \rangle$. We have $G = Q\langle a \rangle$ with $Q \cong Q_8$, $Q \cap \langle a \rangle = \{1\}$, $o(a) = 2^{m+1}$, $m \geq 2$, and a^2 centralizes Q .

Let $l \in G - M$ so that $l = a^i q$, where i is an odd integer and $q \in Q$. Then (noting that G is of class 2), we get $l^2 = a^{2i} q^2[q, a^i]$, where $q^2[q, a^i] \in G'$. Hence $o(l^2) = 2^m$ and $l^4 = (a^4)^i$ and so $\langle l^4 \rangle \geq \langle z \rangle$. Hence each element $l \in G - M$ is of order 2^{m+1} and $\langle l \rangle \geq \langle z \rangle$.

Since G' is noncyclic, Q is not normal in G . Since $|E : Q| = 2$ and $E \triangleleft G$, we have $Q \cap Q^a = \langle x \rangle \cong C_4$ and $(Q \cap Q^a)^a = Q^a \cap Q^{a^2} = Q^a \cap Q$ (since a^2 centralizes Q) so that $\langle x \rangle^a = \langle x \rangle$. If $x^a = x^{-1}$, then we replace a with $a' = ay$, where $y \in Q - \langle x \rangle$. We get $x^{a'} = x^{ay} = (x^{-1})^y = x$ and so a' centralizes x , $o(a') = 2^{m+1}$, and $\langle a' \rangle \geq \langle z \rangle$. Hence we may assume from the start that $x^a = x$ and the maximal subgroup $A = \langle x \rangle \times \langle a \rangle$ is abelian of type $(4, 2^{m+1})$. By Lemma 64.1(u), A is a unique abelian maximal subgroup of G . If $y \in Q - \langle x \rangle$, then $[y, a] \in G' - \langle u \rangle$ (otherwise Q would be normal in G). Suppose that $[y, a] = uz$. Then replace a with $a^* = ax$ (noting that a^* centralizes x , $o(a^*) = 2^{m+1}$, and $\langle a^* \rangle \geq \langle z \rangle$), we get $[y, a^*] = [y, ax] = [y, a][y, x] = uz \cdot u = z$. Thus, we may assume from the start that $[y, a] = z$. \square

In the rest of this section we assume that G' is noncyclic and $G' \not\cong E_4$. Since $G' < \Phi(G)$, G' is metacyclic and so $G'/\Phi(G') \cong E_4$ and $\Phi(G') > \{1\}$. Let R be a G -invariant subgroup of index 2 in $\Phi(G')$. We want to study the structure of G/R . To this end, in view of Remark 1, we may assume that $R = \{1\}$. In that case $\Phi(G') \cong C_2$ and G' is abelian of type $(4, 2)$. Here $W = \Omega_1(G)$ (see Remark 1) is a unique normal four-subgroup of G and $\langle z \rangle = \Omega_1(G') \leq Z(G)$. By Lemma 87.2, $G = EF$ with normal subgroups E and F , where $E \cap F = G'$, $E/G' \cong E_4$, and $F/G' \cong C_{2^m}$, $m \geq 2$. Let $a \in F$ be such that $\langle a \rangle$ covers F/G' and $\Phi(G) = G'\langle a^2 \rangle$. Also, $M = E\langle a^2 \rangle$ is the unique nonmetacyclic maximal subgroup of G (Remark 1), and so any proper subgroup of G which is not contained in M is metacyclic.

Suppose that $W \leq Z(G)$. In that case, take an involution $s \in W - \langle z \rangle$ and consider the group $G/\langle s \rangle$. We have $(G/\langle s \rangle)' \cong C_4$, which contradicts our previous results (which show that a cyclic commutator group is of order at most 2). Hence $W \not\leq Z(G)$ so that $C_G(W)$ is a maximal subgroup of G and $\Omega_1(Z(G)) = \langle z \rangle$ which implies that $Z(G)$ is cyclic.

Let v be an element of order 4 in G' and let $u \in W - \langle z \rangle$. Then $v^2 = z$ and the set $\{\langle v \rangle, \langle vu \rangle\}$ is the set of cyclic subgroups of order 4 in G' . Suppose that $\langle v \rangle$ is not normal in G (and then also $\langle vu \rangle$ is not normal in G). Let $\{X_1, X_2, X_3\}$ be the set of maximal subgroups of G containing F . Since X_i is metacyclic, X'_i is cyclic for each $i = 1, 2, 3$. By our assumption (and noting that $W \not\leq Z(G)$), we get $X'_i \leq \langle z \rangle$. However, by Lemma 64.1(u), this gives a contradiction.

We have proved that $\langle v \rangle$ and $\langle vu \rangle$ are normal subgroups in G . This implies that $\Phi(G) \leq C_G(v) \cap C_G(vu)$ and so $G' \leq Z(\Phi(G))$ because $G' = \langle v, vu \rangle$. But $\Phi(G)/G'$ is cyclic and so $\Phi(G)$ is abelian. In particular, a^2 centralizes G' .

We want to determine the subgroup $\langle a^{2^m} \rangle \leq G'$. If $a^{2^m} = 1$, then $a^{2^{m-1}}$ is an involution in $F - G'$, contrary to our result that $\Omega_1(G) = W \leq G'$. Hence $a^{2^m} \neq 1$. If $a^{2^m} = z$, then $a^{2^{m-1}} \in \Phi(G) - G'$, $o(a^{2^{m-1}}) = 4$, and $a^{2^{m-1}}v$ is an involution in $\Phi(G) - G'$, a contradiction. Suppose that $a^{2^m} = u \in W - \langle z \rangle$ and so $F = \langle a \rangle \langle v \rangle$, $\langle a \rangle \cap \langle v \rangle = \{1\}$ and a normalizes $\langle v \rangle$ (since $\langle v \rangle$ is normal in G). We get $v^a = vz^\epsilon$, $\epsilon = 0, 1$ and so $F' \leq \langle z \rangle$ which implies that $\mathfrak{U}_2(F) = \langle a^4 \rangle \geq \langle u \rangle$. It follows that $\langle u \rangle$ is a characteristic subgroup in F and so $u \in Z(G)$, a contradiction. Hence, replacing $\langle v \rangle$ with $\langle vu \rangle$ and v with v^{-1} (if necessary), we may assume that $a^{2^m} = v$. Thus, $o(a) = 2^{m+2}$ and so $\langle a \rangle$ is a cyclic subgroup of index 2 in F . Since F is not of maximal class ($W \cong E_4$ is normal in F and $|F| \geq 2^5$), F is either abelian or $F \cong M_{2^{m+3}}$. In any case, $F' \leq \langle z \rangle$ and $a^2 \in Z(F)$.

It is easy to see that $v \in Z(G)$. If q is an element in E , then $[q, a] \in G'$ and so

$$[q, a^2] = [q, a][q, a]^a = [q, a][q, a]z^\epsilon = [q, a]^2z^\epsilon = z^\eta, \quad \epsilon, \eta = 0, 1,$$

since $[q, a]^2 \in \mathfrak{U}_1(G') = \langle z \rangle$. This gives $[q, a^4] = [q, a^2][q, a^2]^{a^2} = z^\eta(z^\eta)^{a^2} = (z^\eta)^2 = 1$. But $a^{2^m} = v$, $m \geq 2$, and so $\langle a^4 \rangle \geq \langle v \rangle$ which implies that v centralizes E . It follows $C_G(v) \geq \langle E, a \rangle = G$ and we are done.

Now we use Lemma 87.7 for the group $G/\langle z \rangle$ since $(G/\langle z \rangle)' = G'/\langle z \rangle \cong E_4$. It follows that $G/\langle z \rangle$ possesses a quaternion subgroup $\tilde{Q}/\langle z \rangle \cong Q_8$. Suppose that $v \in \tilde{Q}$. Then $\Phi(\tilde{Q}) = \langle v \rangle$ and \tilde{Q} possesses a cyclic subgroup of index 2. But such groups cannot have a proper homomorphic image $\tilde{Q}/\langle z \rangle$ isomorphic to Q_8 . Hence $v \notin \tilde{Q}$ and so $\tilde{Q} \cap \langle v \rangle = \langle z \rangle$. If $|\tilde{Q}'| = 4$, then a result of O. Taussky (Lemma 64.1(s)) implies that \tilde{Q} is of maximal class. This is again a contradiction since $\tilde{Q}/\langle z \rangle \cong Q_8$. Hence $\tilde{Q}' = \langle u \rangle$ is of order 2 and $u \neq z$ since $\tilde{Q}/\langle z \rangle$ is nonabelian. We get $\langle u, v \rangle = G'$ and therefore $E^* = \tilde{Q} * \langle v \rangle$ is normal in G . But $(E^*)' = \tilde{Q}' = \langle u \rangle$ is a characteristic subgroup of E^* and so $u \in Z(G)$. This gives $W = \langle u, z \rangle \leq Z(G)$ and this is our final contradiction. We have proved that such a group G does not exist. We conclude with the following result which sums up all results of this section.

Theorem 87.8. Let G be a 2-group which possesses exactly one nonmetacyclic maximal subgroup M . Then $d(G) \leq 3$ and we assume here $d(G) = 3$. In that case $d(M) = 3$, G/G' is abelian of type $(2, 2, 2^m)$, $m \geq 2$, G' is elementary abelian of order ≤ 4 , and we have exactly the following five possibilities:

- (a) G is abelian of type $(2, 2, 2^m)$, $m \geq 2$.
- (b) $G \cong C_2 \times M_{2n+1}$, $n \geq 3$, where $M_{2n+1} = \langle a, v \mid a^{2^n} = v^2 = 1, [v, a] = a^{2^{n-1}} \rangle$.
- (c) $G = Q * Z$, where $Q \cong Q_8$, $Z \cong C_{2^n}$, $n \geq 3$, and $Q \cap Z = Z(Q)$.
- (d) $G = Q \times Z$, where $Q \cong Q_8$, $Z \cong C_{2^n}$, $n \geq 2$.
- (e) $G = QZ$, where $Q = \langle x, y \rangle \cong Q_8$, $Z = \langle a \rangle \cong C_{2^n}$, $n \geq 3$, $Q \cap Z = \{1\}$, a^2 centralizes Q , $[a, x] = 1$, and $[a, y] = a^{2^{n-1}} = z$. Setting $Z(Q) = \langle u \rangle$, we have here $G' = \langle u, z \rangle \cong E_4$, $\Phi(G) = Z(G) = \langle a^2 \rangle \times \langle u \rangle \cong C_{2^{n-1}} \times C_2$, and $M = Q \times \langle a^2 \rangle$.

Conversely, it is easily checked that all groups G given in (a) to (e) have exactly one nonmetacyclic maximal subgroup and $d(G) = 3$.

2°. We assume in this section that G is a 2-group with exactly one nonmetacyclic maximal subgroup M and $d(G) = 2$. By Lemma 64.1(n) follows at once that $d(M) = 3$, G is nonmetacyclic and so $G' \neq \{1\}$.

First we treat the easy case $|G'| = 2$. By Lemma 65.2, G is minimal nonabelian. By Lemma 65.1, we have

$$\begin{aligned} G &= \langle a, b \mid a^{2^m} = b^{2^n} = c^2 = 1, [a, b] = c, [a, c] = [b, c] = 1, \\ &\quad m \geq n \geq 1, m \geq 2 \rangle, \end{aligned}$$

where $|G| = 2^{m+n+1}$, $\Omega_1(G) = \langle a^{2^{m-1}}, b^{2^{n-1}}, c \rangle \cong E_8$, and $G/\Omega_1(G) \cong C_{2^{m-1}} \times C_{2^{n-1}}$. Since there is only one maximal subgroup of G containing $\Omega_1(G)$, $G/\Omega_1(G)$ must be cyclic and this implies $n = 1$ so that G/G' is abelian of type $(2^m, 2)$, $m \geq 2$. We have $|G : \langle a \rangle| = 4$, $(ab)^2 = a^2c$, $(ab)^4 = a^4$, and so $|\langle ab \rangle : ((ab) \cap \langle a \rangle)| = 4$ which gives (by the product formula) $G = \langle a \rangle \langle ab \rangle$. Also, $\langle c \rangle = G'$ is a maximal cyclic subgroup of G . We have proved:

Theorem 87.9. Let G be a 2-group with exactly one nonmetacyclic maximal subgroup and $d(G) = 2$. If $|G'| = 2$, then $G = \langle a, b \mid a^{2^m} = b^2 = c^2 = 1, m \geq 2, [a, b] = c, [a, c] = [b, c] = 1 \rangle$, which is a nonmetacyclic minimal nonabelian group with G/G' being abelian of type $(2^m, 2)$, $m \geq 2$, $G' = \langle c \rangle$ is a maximal cyclic subgroup of G , $G = \langle a \rangle \langle ab \rangle$, and $\Omega_1(G) \cong E_8$ so that G has a normal elementary abelian subgroup of order 8.

Now assume that G has a normal elementary abelian subgroup E of order 8 but $|G'| > 2$. Then $G/E \neq \{1\}$ must be cyclic and since $G' < E$, we have $G' \cong E_4$.

Let $a \in G - E$ be such that $\langle a \rangle$ covers G/E . Since $G' = [E, \langle a \rangle]$, a induces on E an automorphism of order 4 which implies $|G/E| \geq 4$. We have $\Phi(G) = G'\langle a^2 \rangle$ and so $E \cap \langle a \rangle \leq G'$ (noting that $|G : \Phi(G)| = 4$). The maximal subgroup $M = E\langle a^2 \rangle$ is nonmetacyclic and so the maximal subgroup $X = G'\langle a \rangle$ is metacyclic (of order $\geq 2^4$) with a normal four-subgroup G' . This implies that X is not of maximal class. If i is an involution in $X - G'$, then i cannot centralize G' (since X is metacyclic). But in that case $G'\langle i \rangle \cong D_8$ and so, by Proposition 10.19, X is of maximal class, a contradiction. Hence $\Omega_1(X) = G'$ and so $G' \cap \langle a \rangle = \langle z \rangle \cong C_2$. Let $v \in E - G'$ so that $[v, a] = u \in G' - \langle z \rangle$ and $[u, a] = z$. This gives $v^a = vu$, $u^a = uz$, $\langle z \rangle \leq Z(G)$, $o(a) = 2^n$, $n \geq 3$, and $a^{2^{n-1}} = z$. The structure of G is uniquely determined. We compute: $(av)^2 = avav = a^2v^a v = a^2(vu)v = a^2u$ and $(av)^4 = (a^2u)^2 = a^4$. Thus, $\langle av \rangle \cap \langle a \rangle = \langle a^4 \rangle$ and since $|G : \langle a \rangle| = 4$ and $|\langle av \rangle : (\langle av \rangle \cap \langle a \rangle)| = 4$, we get $\langle av \rangle \langle a \rangle = G$. If $n \geq 4$, then $C_G(E) > E$ and therefore $\Omega_1(G) = E$. If $n = 3$, then $C_G(E) = E$ and $\Omega_1(G) = E\langle a^2 \rangle = \langle u \rangle \times \langle v, a^2 \rangle \cong C_2 \times D_8$. We have proved:

Theorem 87.10. *Let G be a 2-group with exactly one nonmetacyclic maximal subgroup and $d(G) = 2$. Suppose that G has a normal elementary abelian subgroup E of order 8 and $|G'| > 2$. Then $G' \cong E_4$ and we have $G = EZ$, $Z = \langle a \rangle$ is of order 2^n , $n \geq 3$, $E \cap Z = \langle z \rangle \cong C_2$, $z = a^{2^{n-1}}$, and setting $E = \langle u, v, z \rangle$, we have $u^a = uz$, $v^a = vu$. We have $G' = \langle u, z \rangle \cong E_4$, $Z(G) = \langle a^4 \rangle \cong C_{2^{n-2}}$, $\Phi(G) = \langle u \rangle \times \langle a^2 \rangle \cong C_2 \times C_{2^{n-1}}$, and $G = \langle av \rangle \langle a \rangle$. If $n > 3$, then $\Omega_1(G) = E$ and if $n = 3$, then $\Omega_1(G) = E\langle a^2 \rangle \cong C_2 \times D_8$.*

In the rest of this section we assume that G has no normal elementary abelian subgroups of order 8. We prove the following key result which will be used (with the introduced notation and with all details) in the rest of this section.

Theorem 87.11. *Let G be a 2-group with exactly one nonmetacyclic maximal subgroup and $d(G) = 2$. Assume in addition that G has no normal elementary abelian subgroups of order 8. Then the following holds:*

- (a) $|G'| > 2$ and $|G| \geq 2^5$.
- (b) G has exactly one normal four-subgroup $W = \Omega_1(Z(\Phi(G)))$.
- (c) For each metacyclic maximal subgroup X of G , $\Omega_1(X) = W$.
- (d) Let R be a G -invariant subgroup of index 2 in G' . Then R is unique and G/R is isomorphic to a group of Theorem 87.9. In particular, G/G' is abelian of type $(2^m, 2)$, $m > 1$, $\Omega_1(G/R) \cong E_8$, and if y is any element in G such that $y^2 \in G'$, then $y^2 \in R$. Also, each proper characteristic subgroup of G' is contained in R .
- (e) G' is abelian of rank ≤ 2 .
- (f) There are normal subgroups E and F of G such that $G = EF$, $E \cap F = G'$, $F/G' \cong C_{2^m}$, $m \geq 2$, $E/G' \cong C_2$, and there is an element $x \in E - G'$ of order ≤ 4 and we fix such an element x . Let $a \in F - G'$ be such that $\langle a \rangle$ covers F/G' .

Then $\Phi(G) = G'\langle a^2 \rangle$, $\Omega_1(G/R) = (E\langle a^{2^{m-1}} \rangle)/R \cong E_8$, $M = E\langle a^2 \rangle$ is the unique nonmetacyclic maximal subgroup of G , $F = G'\langle a \rangle$ and $F_1 = G'\langle ax \rangle$ are two distinct metacyclic maximal subgroups of G , and $F'F'_1 = R$. We have $G = \langle a, x \rangle$ and $v = [a, x] \in G' - R$.

(g) Assuming in addition that G' is noncyclic, we have the following properties:

- (g1) All elements in $G' - R$ are of order $2^e = \exp(G')$. In particular, $o(v) = 2^e$.
- (g2) If R is cyclic, then $|R| = 2$ and $G' \cong E_4$.
- (g3) We have $G'/\langle v \rangle \cong R/\langle v^2 \rangle$ is cyclic of order $\leq 2^e$ and if y is any element in $R - \phi(G')$, then $\langle y \rangle$ covers $R/\langle v^2 \rangle$ and $\langle v^2 \rangle$ has a cyclic complement of order $\leq 2^e$ in R .
- (g4) If $\exp(R) = \exp(G') = 2^e$, then $G' \cong C_{2^e} \times C_{2^e}$ is homocyclic of rank 2 and if $\exp(R) < \exp(G') = 2^e$, then $\exp(R) = 2^{e-1}$.
- (g5) We have $a^{2^m} \in R - \Phi(G')$ and $(ax)^{2^m} \in R - \Phi(G')$.
- (g6) If $G/\Phi(G')$ has a normal elementary abelian subgroup of order 8, then $\Phi(G') \neq \{1\}$ and we may assume that $E/\Phi(G') \cong E_8$ so that our fixed element $x \in E - G'$ with $o(x) \leq 4$ has in this case the additional property $x^2 \in \Phi(G')$.
- (g7) We have $x^2 \in W \leq G'$ and if $G' \not\cong E_4$, then $W \leq R$.
- (g8) We have $v^x = v^{-1}z^\epsilon$, where $\epsilon = 0, 1$ and $\epsilon = 1$ if and only if $x^2 \in W - Z(G)$ in which case $W \not\leq Z(G)$ and $\langle z \rangle = E \cap Z(G)$.
- (g9) We have $F = \langle a \rangle \langle v \rangle$, $F_1 = \langle ax \rangle \langle v \rangle$, and $\Phi(G) = \langle a^2 \rangle \langle v \rangle$.
- (g10) Setting $b = [v, a]$ (which is equivalent with $v^a = vb$) and $b_1 = [v, ax]$, we have $F' = \langle b \rangle$, $F'_1 = \langle b_1 \rangle$ with $b, b_1 \in R - \Phi(G')$, $\langle b \rangle \langle b_1 \rangle = R$, $o(b) = \exp(R)$, and $b_1 = v^{-2}z^\epsilon b^{-1}$.
- (g11) We have $b^x = b^{-1}$, $b_1^x = b_1^{-1}$ so that x inverts each element in R . Also, $b_1^{-1}b_1^a = (bb^a)^{-1} \in \langle b \rangle \cap \langle b_1 \rangle$.
- (g12) We have $(\Phi(G))' = \langle bb^a \rangle$ and $\Phi(G)$ is powerful.
- (g13) We have $G = \langle ax \rangle \langle a \rangle$ and so G is a product of two cyclic subgroups.

Proof. Since G has no normal subgroups isomorphic to E_8 , we get $|G'| > 2$ (Theorem 87.10) and $|G| \geq 2^5$ because $|G/G'| \geq 2^3$ (O. Taussky). If G has two distinct normal four-subgroups, then Theorem 50.2 implies that $d(G) > 2$, a contradiction. Hence, by Lemma 1.4, G has exactly one normal four-subgroup W .

Let X be a metacyclic maximal subgroup of G so that $|X : \Phi(G)| = 2$. If $\Phi(G)$ is cyclic, then G has a cyclic subgroup of index 2, a contradiction. Hence $\Phi(G)$ is noncyclic and a result of Burnside (Lemma 64.1(v)) implies that $Z(\Phi(G))$ is noncyclic. This gives $W = \Omega_1(Z(\Phi(G)))$ noting that $\Phi(G)$ is metacyclic. Since $|X| \geq 2^4$ and X has a normal four-subgroup, X is not of maximal class. Let i be an involution in $X - W$. Since X is metacyclic, i cannot centralize W . It follows $\langle W, i \rangle \cong D_8$ and then Proposition 10.19 implies that X is of maximal class, a contradiction. Hence we have $\Omega_1(X) = W$ for each metacyclic maximal subgroup X of G .

Let R be a G -invariant subgroup of index 2 in G' . By Lemma 44.1, we have $R = \Phi(G')K_3(G)$ and so such a subgroup R is unique. Since G is nonmetacyclic, $\bar{G} = G/R$ is also nonmetacyclic (Proposition 44.2). If X is a metacyclic maximal subgroup of G , then \bar{X} (bar convention) is metacyclic. If M is the unique nonmetacyclic maximal subgroup of G , then \bar{M} is also nonmetacyclic (otherwise, Lemma 64.1(n) would imply that \bar{G} is metacyclic). Since $|\bar{G}| = 2$, \bar{G} must be isomorphic to a group of Theorem 87.9. In particular, G/G' is abelian of type $(2^m, 2)$, $m > 1$, $\Omega_1(G/R) \cong E_8$, and if y is any element in G such that $y^2 \in G'$, then $y^2 \in R$. The uniqueness of R also implies that each proper characteristic subgroup of G' is contained in R .

Let $X_1 \neq X_2$ be two metacyclic maximal subgroups of G so that X'_1 and X'_2 are cyclic normal subgroups of G . Since G/R is minimal nonabelian, we have $X'_1 X'_2 \leq R$. By a result of A. Mann (Lemma 64.1(u)), we get $R = X'_1 X'_2$. On the other hand, $G/C_G(X'_1)$ and $G/C_G(X'_2)$ are abelian groups and so G' centralizes $X'_1 X'_2 = R$. But $|G' : R| = 2$ and therefore G' is abelian (of rank ≤ 2).

Now we use the structure of G/R . There are normal subgroups E and F of G such that $G = EF$, $E \cap F = G'$, $F/G' \cong C_{2^m}$, $m \geq 2$, and $E/G' \cong C_2$. Let $a \in F - G'$ be such that $\langle a \rangle$ covers F/G' . Then $\Phi(G) = G'\langle a^2 \rangle$ and $\Omega_1(G/R) = S/R \cong E_8$, where $S = E\langle a^{2^{m-1}} \rangle$ (because $E/R \cong E_4$ and $a^{2^m} \in R$). It follows that $M = E\langle a^2 \rangle$ is the unique nonmetacyclic maximal subgroup of G (noting that already S is nonmetacyclic). Let x be any element in $E - G'$ so that $G = \langle a, x \rangle$, $F = G'\langle a \rangle$ and $F_1 = G'\langle ax \rangle$ are two metacyclic maximal subgroups of G , where we use the facts that $\langle ax \rangle$ also covers $G/E \cong C_{2^m}$ and $(ax)^2 \in \Phi(G)$. Set $S_0 = G'\langle a^{2^{m-1}} \rangle$ and $E_1 = G'\langle a^{2^{m-1}}x \rangle$ so that S_0 is a metacyclic maximal subgroup of S , E_1/G' is another complement of F/G' in G/G' , and $S - S_0 = (E - G') \cup (E_1 - G')$. By Lemma 64.1(l), $\Omega_2(S) \not\leq S_0$ and so there are elements of order ≤ 4 in $S - S_0$. Interchanging E and E_1 (if necessary), we may assume from the start that there is an element $x \in E - G'$ with $o(x) \leq 4$ and we choose and fix such an element x . We set $v = [a, x]$ so that $v \in G' - R$. Indeed, we have $G = \langle a, x \rangle$ and so if $v \in R$, then G/R would be abelian.

In what follows we assume that G' is noncyclic so that $\Phi(G') < R$ and $G'/\Phi(G') \cong E_4$. Let $2^e = \exp(G')$, $e \geq 1$, be the exponent of G' . If there is an element in $G' - R$ of order $< 2^e$ (in which case $e > 1$), then $\Omega_{e-1}(G')$ is a proper characteristic subgroup of G' which is not contained in R , a contradiction. Hence all elements in $G' - R$ are of order 2^e . In particular, the element $v \in G' - R$ of the previous paragraph is of order 2^e . By Lemma 4 (Introduction, Volume 1), $\langle v \rangle$ has a cyclic complement $\langle s \rangle$ of order $\leq 2^e$ (noting that G' is of rank 2). Hence $G'/\langle v \rangle \cong R/\langle v^2 \rangle$ is cyclic of order $\leq 2^e$. Since $v^2 \in \Phi(G')$, we have $\Phi(G') = \langle s^2 \rangle \times \langle v^2 \rangle$ and if y is any element in $R - \Phi(G')$, then $\langle y \rangle$ covers $R/\langle v^2 \rangle$.

Suppose that R is cyclic of order > 2 . Since G' is noncyclic, there is an involution in $G' - R$, contrary to the fact that all elements in $G' - R$ are of order $2^e = \exp(G')$. Hence, if R is cyclic, then $|R| = 2$ and $G' \cong E_4$.

Suppose that $\exp(R) = \exp(G') = 2^e$, $e > 1$. Let y be an element of order 2^e in R . Suppose also that $\langle y \rangle \cap \langle v^2 \rangle \neq \{1\}$. Then we have $|\langle y \rangle : (\langle y \rangle \cap \langle v \rangle)| = |\langle v \rangle : (\langle y \rangle \cap \langle v \rangle)| = 2^{e'}, e' < e$, and so there is an element y' of order 2^e in $\langle y \rangle$ such that $(y')^{2^{e'}} = v^{-2^{e'}}$. But then $(y')^{2^{e'}} = 1$ and $y'v \in G' - R$, a contradiction. Thus, $\langle y \rangle$ splits over $\langle v^2 \rangle$, $R = \langle y \rangle \times \langle v^2 \rangle$, and so $G' \cong C_{2^e} \times C_{2^e}$ is homocyclic of rank 2. But if G' is not homocyclic, then $\exp(R) = 2^{e-1}$ and so (by Lemma 4 (Introduction, Volume 1)) $\langle v^2 \rangle$ has a cyclic complement in R . It follows that in any case $\langle v^2 \rangle$ has a cyclic complement in R .

Since $a^{2^m} \in G'$, we know that $a^{2^m} \in R$. Suppose that $a^{2^m} \in \Phi(G')$. We look at $F/\Phi(G') = \bar{F}$ so that $\bar{G}' = G'/\Phi(G') \cong E_4$ is a normal four-subgroup of the metacyclic group \bar{F} (of order $\geq 2^4$) and so \bar{F} is not of maximal class. But $\overline{a^{2^{m-1}}}$ is an involution in $\bar{F} - \bar{G}'$ and $\overline{a^{2^{m-1}}}$ cannot centralize \bar{G}' . It follows that $(\bar{G}', \overline{a^{2^{m-1}}}) \cong D_8$ and this is a contradiction (by Proposition 10.19). We have proved that $a^{2^m} \in R - \Phi(G')$. With the same argument (working in $\bar{F}_1 = F_1/\Phi(G')$), we get $(ax)^{2^m} \in R - \Phi(G')$.

Assume for a moment that $G/\Phi(G')$ has a normal elementary abelian subgroup $S^*/\Phi(G')$ of order 8 so that $S^* < S$ and $|S : S^*| = 2$ (where $S/R = \Omega_1(G/R) \cong E_8$). Since S^* is nonmetacyclic, there is only one maximal subgroup of G containing S^* and so G/S^* must be cyclic. In particular, $G' \leq S^*$. Hence S^* is equal to one of the three maximal subgroups of S containing G' . They are E , E_1 , and $S_0 = G'\langle a^{2^{m-1}} \rangle$. But S_0 is metacyclic (as a subgroup of F) and so $S_0/\Phi(G')$ cannot be elementary abelian of order 8. It follows that S^* is equal to E or E_1 . Interchanging E and E_1 (if necessary), we may assume that $S^* = E$ and so $E/\Phi(G') \cong E_8$. Since E is not metacyclic and G' is a metacyclic maximal subgroup of E , there is (by Lemma 64.1(l)) an element x of order ≤ 4 in $E - G'$ (as before) and we have here (in our case where $G/\Phi(G')$ has a normal E_8) in addition that $x^2 \in \Phi(G')$.

We have $W \leq G'$ and if G' is not a four-group, then also $W \leq R$. If $W \not\leq Z(G)$, then we always set $\langle z \rangle = W \cap Z(G)$. Since $x^2 \in G'$ and $o(x) \leq 4$, we have $x^2 \in W$ and therefore $[a, x^2] = z^\epsilon$, where $\epsilon = 0, 1$ and $\epsilon = 1$ if and only if a does not centralize x^2 (in which case $W \not\leq Z(G)$). We have $z^\epsilon = [a, x^2] = [a, x][a, x]^x = vv^x$, and so $v^x = v^{-1}z^\epsilon$.

We know that $a^{2^m} \in R - \Phi(G')$, $(ax)^{2^m} \in R - \Phi(G')$ and so $\langle a^{2^m} \rangle$ and $\langle ax \rangle^{2^m}$ cover $G'/\langle v \rangle$ and therefore $G' = \langle a^{2^m} \rangle \langle v \rangle = \langle (ax)^{2^m} \rangle \langle v \rangle$. But $\langle a \rangle$ covers F/G' and $\langle ax \rangle$ covers F_1/G' and so $F = \langle a \rangle \langle v \rangle$ and $F_1 = \langle ax \rangle \langle v \rangle$. Set $b = [v, a]$ and $b_1 = [v, ax]$ so that $F' = \langle b \rangle$ and $F'_1 = \langle b_1 \rangle$, where we have used the facts that F and F_1 are metacyclic and $F = \langle a, v \rangle$, $F_1 = \langle ax, v \rangle$. Since $\langle b \rangle \langle b_1 \rangle = R$, we may assume (interchanging $F = G'\langle a \rangle$ with $F_1 = G'\langle ax \rangle = G'\langle xa \rangle$, if necessary) that $b \in R - \Phi(G')$. Indeed, we have $[xa, x] = [a, x] = v$. Then we compute

$$\begin{aligned} b_1 &= [v, ax] = [v, x][v, a]^x = v^{-1}(x^{-1}vx)b^x \\ &= v^{-1}(v^{-1}z^\epsilon)b^x = v^{-2}z^\epsilon b^x \in R - \Phi(G'), \end{aligned}$$

since $v^{-2} \in \Phi(G')$, $b^x \in R - \Phi(G')$, and $z^\epsilon \in \Phi(G')$. Indeed, if $\Phi(G') \neq \{1\}$ and $W \not\leq Z(G)$, then $\langle z \rangle = W \cap Z(G) \leq \Phi(G')$. If $\Phi(G') = \{1\}$, then $|R| = 2$ and $R \leq Z(G)$ and so the fact that $x^2 \in R$ gives $\epsilon = 0$. Hence, in any case we get $b \in R - \Phi(G')$ and $b_1 \in R - \Phi(G')$ and (interchanging F and F_1 , if necessary) we may assume that $o(b) = \exp(R)$.

Conjugating the relation $[v, a] = b$ (which gives $v^a = vb$ and $(v^{-2})^a = v^{-2}b^{-2}$) with x we get:

$$\begin{aligned} b^x &= [v^{-1}z^\epsilon, a^x] = [v^{-1}, a(a^{-1}x^{-1}ax)] = [v^{-1}, av] = [v^{-1}, v][v^{-1}, a]^v \\ &= [v^{-1}, a] = v(a^{-1}v^{-1}a) = v(v^a)^{-1} = v(vb)^{-1} = b^{-1}, \end{aligned}$$

and so we get $b^x = b^{-1}$. From the above we also get: $b_1 = v^{-2}z^\epsilon b^{-1}$, and so $b_1^x = v^2z^\epsilon b = b_1^{-1}$. Thus, x inverts R . We compute

$$\begin{aligned} b_1^a &= (v^{-2})^a z^\epsilon (b^a)^{-1} = v^{-2}b^{-2}z^\epsilon (b^a)^{-1} = b^{-1}(v^{-2}z^\epsilon b^{-1})(b^a)^{-1} \\ &= b^{-1}b_1(b^a)^{-1} \end{aligned}$$

and so $b_1^{-1}b_1^a = (bb^a)^{-1} \in \langle b_1 \rangle \cap \langle b \rangle$, since $\langle b \rangle$ and $\langle b_1 \rangle$ are normal subgroups of G .

We show that $\Phi(G)$ is a powerful 2-group and $(\Phi(G))' = \langle bb^a \rangle$. Indeed, we have $F = \langle a \rangle \langle v \rangle$, $a^2, v \in \Phi(G)$, $|F : \Phi(G)| = 2$ and so $\Phi(G) = \langle a^2 \rangle \langle v \rangle$. This gives $(\Phi(G))' = \langle [v, a^2] \rangle$ and since $[v, a^2] = [v, a][v, a]^a = bb^a$, we get $(\Phi(G))' = \langle bb^a \rangle$. But $\langle b \rangle = F'$ is normal in G and so $\langle b \rangle = \langle b^a \rangle$ and therefore $\langle bb^a \rangle \leq \mathfrak{O}_1(\langle b \rangle)$. On the other hand, F is metacyclic and therefore b is a square in F and so $b = y^2$ for some $y \in F$. But F/G' is cyclic of order ≥ 4 and $b \in G'$ and so $y \in \Phi(G)$. It follows that $bb^a \in \mathfrak{O}_2(\langle y \rangle)$ and so $\Phi(G)' \leq \mathfrak{O}_2(\Phi(G))$ and this means that $\Phi(G)$ is powerful.

We have $[a, x^2] = [a, x][a, x]^x = vv^x = v(v^{-1}z^\epsilon) = z^\epsilon$, and so

$$(ax)^2 = axax = ax(xa)[a, x] = ax^2av = a^2x^2z^\epsilon v = a^2v(x^2z^\epsilon).$$

It is easy to see that $x^2z^\epsilon \in \Phi(\Phi(G))$. Indeed, $x^2z^\epsilon \in W$ and the facts that $a^{2^m} \in R - \Phi(G')$ and $|R : \Phi(G')| = 2$ give $R = \langle a^{2^m}, \Phi(G') \rangle \leq \Phi(\Phi(G))$ because $a^{2^{m-1}} \in \Phi(G)$ ($m \geq 2$). Hence, if $W \leq R$, we are done. If $W \not\leq R$, then R is cyclic and we know that in that case $G' \cong E_4$ and so $|R| = 2$. But then $x^2 \in R \leq Z(G)$ and so $\epsilon = 0$ and again $a^{2^m} \in R - \Phi(G') = R - \{1\}$ and therefore $\langle a^{2^m} \rangle = R \leq \Phi(\Phi(G))$. We get again $x^2z^\epsilon = x^2 \in R \leq \Phi(\Phi(G))$. We have proved that in any case $x^2z^\epsilon \in \Phi(\Phi(G))$.

Since $(ax)^2 = a^2v(x^2z^\epsilon)$ and $x^2z^\epsilon \in \Phi(\Phi(G))$, we get

$$\Phi(G) = \langle v, a^2 \rangle = \langle a^2v, a^2 \rangle = \langle a^2v(x^2z^\epsilon), a^2 \rangle = \langle (ax)^2, a^2 \rangle.$$

But $\Phi(G)$ is powerful and so Theorem 26.25 implies $\Phi(G) = \langle (ax)^2 \rangle \langle a^2 \rangle$. We conclude:

$$\begin{aligned} G &= \langle ax \rangle F = \langle ax \rangle (\Phi(G) \langle a \rangle) = \langle ax \rangle (\langle (ax)^2 \rangle \langle a^2 \rangle) \langle a \rangle \\ &= (\langle ax \rangle \langle (ax)^2 \rangle) (\langle a^2 \rangle \langle a \rangle) = \langle ax \rangle \langle a \rangle. \end{aligned}$$

□

In the rest of this section we make case-to-case investigations depending on the structure of G' and $G/\Phi(G')$. We shall use freely the notation and the results stated in Theorem 87.11.

Theorem 87.12. *Let G be a 2-group with exactly one nonmetacyclic maximal subgroup M and $d(G) = 2$. Suppose that G' is cyclic of order 2^n , $n > 1$. Then $G = EZ$, where E is normal in G and $E = \langle v, x \mid v^{2^n} = 1, n > 1, x^2 \in \langle z \rangle, z = v^{2^{n-1}}, v^x = v^{-1} \rangle$ is dihedral or generalized quaternion, $Z = \langle a \rangle$, $Z \cap E \leq \langle z \rangle = Z(E)$, $|Z/(Z \cap E)| = 2^m$, $m > 1$, $[a, x] = v$, $v^a = v^{-1+4i}$ (i integer), and $[v, a^{2^{m-1}}] = 1$. Here $G' = \langle v \rangle \cong C_{2^n}$, $n > 1$, $\Phi(G) = G'\langle a^2 \rangle$, $M = E\langle a^2 \rangle$, $G = \langle ax \rangle \langle a \rangle$ is a product of two cyclic subgroups and $C_G(E) \not\leq E$.*

Proof. By Theorem 87.10, G has no normal subgroups isomorphic to E_8 and so we may use Theorem 87.11 (a) to (f). Since $v = [a, x] \in G' - R$, we have $G' = \langle v \rangle$. Also, $R = F'F'_1$ implies that interchanging $F = G'\langle a \rangle$ and $F_1 = G'\langle ax \rangle = G'\langle xa \rangle$ (and noting that $[xa, x] = [a, x] = v$), if necessary, we may assume that $F' = R = \langle b \rangle$, where $b = [v, a]$ which gives $v^a = vb$. Set $W \cap G' = \langle z \rangle = \Omega_1(R) = \Omega_1(G') \leq Z(G)$. Since $o(x) \leq 4$, $x^2 \in \langle z \rangle$ and so $x^2 = z^\eta$, $\eta = 0, 1$. Therefore $1 = [a, x^2] = [a, x][a, x]^x = vv^x$ and so $v^x = v^{-1}$. It follows that E is dihedral or generalized quaternion. Since

$$(v^{2^{n-2}})^a = (vb)^{2^{n-2}} = v^{2^{n-2}}b^{2^{n-2}} = v^{2^{n-2}}z = v^{-2^{n-2}},$$

where $o(v^{2^{n-2}}) = 4$, it follows that $\langle a \rangle \cap E \leq \langle z \rangle = Z(E)$.

Since $\langle v^{-2} \rangle = \langle b \rangle$, we may set $b = v^{-2+4i}$ for some integer i . We have $v^a = v^{-1+4i}$ and $v^{ax} = v^{1-4i} = vv^{-4i}$ so that $F_1 = \langle v \rangle \langle ax \rangle$ is ordinary metacyclic (since F_1 centralizes $\langle v \rangle / \mathcal{O}_2(\langle v \rangle) = \langle v \rangle / \langle v^4 \rangle$). By Proposition 26.27, F_1 is powerful. Since $(ax)^2 = axax = axxa[a, x] = ax^2av = a^2vz^\eta$, where $z^\eta \in \Phi(F_1)$, we get $F_1 = \langle ax, v \rangle = \langle ax, a^2 \rangle = \langle ax \rangle \langle a^2 \rangle$, where we have used Proposition 26.25. But then $G = F_1\langle a \rangle = (\langle ax \rangle \langle a^2 \rangle)\langle a \rangle = \langle ax \rangle \langle a \rangle$, and so G is a product of two cyclic subgroups.

Consider $E_1 = G'\langle xa^{2^{m-1}} \rangle$, where $E_1 \cap F = G'$ and so $W \not\leq E_1$. Hence E_1 is a normal subgroup of G which does not possess a G -invariant four-subgroup. By Lemma 1.4, E_1 is of maximal class (since E_1 cannot be cyclic). But then $(xa^{2^{m-1}})^2 \in \langle z \rangle$ and therefore $xa^{2^{m-1}}$ also inverts $G' = \langle v \rangle$. Indeed, setting $xa^{2^{m-1}} = x'$, we get $G = \langle a, x' \rangle$ and so $[a, x'] = v' \in G' - R$ and $G' = \langle v' \rangle$. This gives $1 = [a, (x')^2] = [a, x'][a, x']^{x'} = v'(v')^{x'}$ and $(v')^{x'} = (v')^{-1}$. It follows that $a^{2^{m-1}}$ centralizes $\langle v \rangle$. Since $a^{2^{m-1}}$ does not fuse x and vx (noting that a fuses x and vx), there is $g \in \langle v \rangle$ with $ga^{2^{m-1}}$ centralizing x and $ga^{2^{m-1}}$ centralizes E and so $C_G(E) \not\leq E$. \square

From Theorems 87.9, 87.10, 87.11(g13), and 87.12, we get the following important result.

Corollary 87.13. Let G be a 2-group with exactly one nonmetacyclic maximal subgroup and $d(G) = 2$. Then $G = AB$ with cyclic A and B .

The next two results are devoted to the case, where $G/\Phi(G')$ has no normal elementary abelian subgroups of order 8.

Theorem 87.14. Let G be a 2-group with exactly one nonmetacyclic maximal subgroup M and $d(G) = 2$. Assume that $G' \cong E_4$ and G has no normal elementary abelian subgroups of order 8. Then G is a unique group of order 2^5 :

$$G = \langle a, x \mid a^8 = x^4 = 1, a^4 = x^2 = z, [a, x] = v, v^2 = 1, [v, a] = z \rangle,$$

where $Z(G) = \langle z \rangle \cong C_2$, $G' = \langle z, v \rangle \cong E_4$, $M = \langle v \rangle \times \langle a^2, x \rangle \cong C_2 \times Q_8$ (and in fact this group is isomorphic to the group of Theorem 74.2(f)).

Proof. We may use Theorem 87.11 (a) to (g) (except (g6)). Here $|R| = 2$ so that $R = \langle z \rangle \leq Z(G)$ and $G' = \langle z \rangle \times \langle v \rangle$ with $v = [a, x]$. Since $x^2 \in R$, we have $v^x = v^{-1} = v$ and so $E = G'\langle x \rangle$ is abelian. But (by our assumption) E is not elementary abelian and so $x^2 = z$. We know that $b = [v, a] \in R - \{1\}$ and so $[v, a] = z$, $W = G' \not\leq Z(G)$ and $C_G(G') = M = E\langle a^2 \rangle$. Also, $a^{2^m} \in R - \{1\}$ and so $a^{2^m} = z$. Since $(E\langle a^{2^{m-1}} \rangle)/R \cong E_8$, we have $[a^{2^{m-1}}, x] \leq R$. If $[a^{2^{m-1}}, x] = 1$, then $i = xa^{2^{m-1}}$ is an involution in $M - F$ and so $\langle i \rangle \times G'$ is a normal elementary abelian subgroup of order 8, a contradiction. Hence $[a^{2^{m-1}}, x] = z$ and so $E\langle a^{2^{m-1}} \rangle = \langle v \rangle \times \langle x, a^{2^{m-1}} \rangle \cong C_2 \times Q_8$. We compute:

$$[a^2, x] = [a, x]^a[a, x] = v^a v = (vz)v = z, \quad [a^4, x] = [a^2, x]^{a^2}[a^2, x] = zz = 1,$$

and so if $m > 2$, then $\langle a^4 \rangle \geq \langle a^{2^{m-1}} \rangle$ and in that case $[a^{2^{m-1}}, x] = 1$, a contradiction. Hence $m = 2$ and the structure of G is uniquely determined. \square

Theorem 87.15. Let G be a 2-group with exactly one nonmetacyclic maximal subgroup and $d(G) = 2$. Assume that G' is noncyclic, $\Phi(G') \neq \{1\}$, and $G/\Phi(G')$ has no normal elementary abelian subgroups of order 8. Then G' has a cyclic subgroup of index 2, $G/G' \cong C_4 \times C_2$, $\Phi(G)$ is abelian, and we have one of the following possibilities (depending on whether $Z(G)$ is noncyclic or cyclic):

- (a) $G = \langle a, x \mid a^8 = x^4 = 1, x^2 = u, a^4 = uz^\eta, \eta = 0, 1, [a, x] = v, v^{2^n} = 1, n \geq 2, [u, a] = 1, v^{2^{n-1}} = z, v^x = v^{-1}, [v, a] = uv^{-2}z^\xi, \xi = 0, 1 \rangle,$

where $|G| = 2^{n+4}$, $Z(G) = \langle u, z \rangle \cong E_4$, and $G' = \langle u, v \rangle \cong C_2 \times C_{2^n}$.

- (b) $G = \langle a, x \mid a^{16} = x^4 = 1, x^2 = u, a^4 = uv^{2^{n-2}}z^\eta, \eta = 0, 1, [a, x] = v, v^{2^n} = 1, n \geq 4, u^a = uz, v^{2^{n-1}} = z, v^x = v^{-1}z, [u, v] = 1, [v, a] = uv^{-2+2^{n-2}}z^\xi, \xi = 0, 1 \rangle,$

where $|G| = 2^{n+4}$, $Z(G) = \langle z \rangle \cong C_2$, and $G' = \langle u, v \rangle \cong C_2 \times C_{2^n}$.

Proof. We may use Theorem 87.11(a) to (g) (except (g6)). Indeed, since $|G'| > 4$, Theorem 87.10 implies that G has no normal subgroups isomorphic to E_8 . Applying Theorem 87.14 on the factor-group $G/\Phi(G')$, we get at once $m = 2$, i.e., $F/G' \cong C_4$ and $x^2 \in R - \Phi(G')$. But $x^2 = u$ is an involution and if C is a maximal subgroup of G' not containing u , then $C \cap R = \Phi(G')$, $G' = \langle u \rangle \times C$ and therefore C is cyclic of order 2^n , $n \geq 2$ (since G' is of rank 2). Hence, G' has a cyclic subgroup of index 2 and since $[a, x] = v \in G' - R$, we have $G' = \langle u \rangle \times \langle v \rangle$, $o(v) = 2^n$, $n \geq 2$, and $\Phi(G') = \langle v^2 \rangle$ with $R = \langle u \rangle \times \langle v^2 \rangle$. Let $\langle z \rangle = \mathcal{U}_{n-1}(G')$ so that $z = v^{2^{n-1}}$, $W = \langle u, z \rangle \cong E_4$ and $z \in Z(G)$. It follows that E centralizes W and so $C_G(W) \geq M = E\langle a^2 \rangle$.

We know that $a^4 \in R - \Phi(G')$ and the element $b = [v, a]$ is of order $\exp(R) = 2^{n-1}$ so that $b = uv^{2i}$ for an odd integer i . Suppose that $C_{\langle v^2 \rangle}(a) > \langle z \rangle$ which forces $n \geq 3$. From $v^a = vb$, we get in this case $(v^{2^{n-2}})^a = (vb)^{2^{n-2}} = v^{2^{n-2}}b^{2^{n-2}} = v^{2^{n-2}}z = v^{-2^{n-2}}$ since $v^{2^{n-2}}$ is an element of order 4 in $\langle v^2 \rangle$ and $v^{2^{n-1}} = z$. This is a contradiction and so $C_{\langle v^2 \rangle}(a) = \langle z \rangle$. In particular, $a^8 \in \langle z \rangle$ and so we have either $a^4 = uz^\eta$ (first case) or $n \geq 3$ and $a^4 = uv^{2^{n-2}}z^\eta$ (second case), where $\eta = 0, 1$.

Since $F' = \langle b \rangle$ and F is metacyclic, there is $y \in F$ such that $y^2 = b$. But $b \in G' - \Phi(G')$ and so $y \in F - G'$. The fact that $F/G' \cong C_4$ implies that $y \in G'a^2 \leq M$. Since G' is abelian, $C_{G'}(y) = C_{G'}(a^2)$ and so a^2 centralizes b . But $b = uv^{2i}$ (i odd) and $y \in M$ and so a^2 centralizes u which gives that a^2 centralizes $\langle v^{2i} \rangle = \langle v^2 \rangle$. On the other hand, $\langle v^2 \rangle = \Phi(G')$ is normal in G and so in case $n > 2$, a induces an involutory automorphism on $\langle v^2 \rangle$. From $v^a = vb$, we get $(v^2)^a = (vb)^2 = v^2b^2$ and so $[v^2, a] = b^2 = v^{4i}$ (i odd). Hence, in case $n > 2$, a induces on $\langle v^2 \rangle$ an involutory automorphism such that $(\langle v^2, a \rangle)' = \langle v^4 \rangle$ and so $(v^2)^a = v^{-2}z^\xi$, $\xi = 0, 1$, where $\xi = 1$ is possible only if $n > 3$. Thus $b^2 = v^{-4}z^\xi$ which gives $v^{4i} = v^{-4}v^\xi 2^{n-1}$ and so $4i \equiv -4 + \xi 2^{n-1} \pmod{2^n}$ and therefore $2i \equiv -2 + \xi 2^{n-2} \pmod{2^{n-1}}$. We get $b = uv^{2i} = uv^{-2+\xi 2^{n-2}+\xi 2^{n-1}}$ (ξ an integer) and so $b = uv^{-2}v^\xi 2^{n-2}z^\xi$, $\xi = 0, 1$, $\xi = 0, 1$, and $\xi = 1$ is possible only if $n > 3$.

In the first case, where $a^4 = uz^\eta$, we have $C_G(W) \geq \langle M, a \rangle = G$ and so $W \leq Z(G)$ which implies $\epsilon = 0$ and $v^x = v^{-1}$. It is easy to see that in this case $Z(G) = W \cong E_4$ (since x inverts G' , $Z(G) \leq \Phi(G) = G'\langle a^2 \rangle$ and $[a^2, x] = v^a v = (vb)v = v^2b \neq 1$). Suppose that in this case $\xi = 1$, i.e., $b = uv^{-2}v^{2^{n-2}}z^\xi$, $n \geq 4$. Then $[a^2, x] = [a, x]^a[a, x] = v^a v = v^2b = uv^{2^{n-2}}z^\xi$, and noting that a^2 centralizes v^2 , we get

$$1 = [uz^\eta, x] = [a^4, x] = [a^2, x]^{a^2}[a^2, x] = (uv^{2^{n-2}}z^\xi)^{a^2}uv^{2^{n-2}}z^\xi = v^{2^{n-1}} = z,$$

a contradiction. Hence in this case $\xi = 0$.

Suppose that we are in the second case, where $n \geq 3$ and $a^4 = uv^{2^{n-2}}z^\eta$. In this case we show first that $u^a = uz$ and so $W \not\leq Z(G)$, $x^2 = u \in W - Z(G)$ and $\epsilon = 1$, $v^x = v^{-1}z$. Indeed, $u = a^4v^{-2^{n-2}}z^\eta$ and so

$$u^a = a^4(v^{-2^{n-2}})^a z^\eta = a^4v^{2^{n-2}}z^\eta = (a^4v^{-2^{n-2}}z^\eta)z = uz.$$

Also, it is easy to show that in this case $n \geq 4$. If $n = 3$, then

$$b_1 = v^{-2}zb^{-1} = v^{-2}z(uv^{-2i}) = u(zv^{-2(1+i)}) \in W - \langle z \rangle$$

since $1 + i$ is even and so $v^{-2(1+i)} \in \langle z \rangle$. But then $\langle b_1 \rangle = F'_1 \leq Z(G)$ and $W \leq Z(G)$, a contradiction. Assume that $\zeta = 0$ so that $b = uv^{-2}z^{\xi}$. But then $b_1 = v^{-2}zb^{-1} = uz^{\xi+1}$ is an involution in $W - \langle z \rangle$ and $\langle b_1 \rangle = F'_1 \leq Z(G)$ which gives $W \leq Z(G)$, a contradiction. Hence, in this case we must have $\zeta = 1$. It is easy to see that in this case $Z(G) = \langle z \rangle$.

In both cases, using the obtained relations, we compute $bb^a = 1$ and so $(\Phi(G))' = \langle bb^a \rangle = \{1\}$ and $\Phi(G)$ is abelian. \square

In what follows we may assume that G' is noncyclic of order > 4 and $G/\Phi(G')$ has a normal elementary abelian subgroup of order 8.

Theorem 87.16. *Let G be a 2-group with exactly one nonmetacyclic maximal subgroup and $d(G) = 2$. Assume that $G' \cong C_2 \times C_{2^n}$, $n \geq 2$, and $G/\Phi(G')$ has a normal elementary abelian subgroup of order 8. Then we have:*

$$\begin{aligned} G = & \langle a, x \mid [a, x] = v, v^{2^n} = 1, n \geq 2, v^{2^{n-1}} = z, x^2 \in \langle z \rangle, \\ & [v, a] = uv^{2+4s} \text{ (s integer)}, u^2 = [v, u] = 1, u^x = u, v^x = v^{-1}, \\ & a^{2^m} = uz^\eta \text{ or } a^{2^m} = uv^{2^{n-2}}z^\eta, (\eta = 0, 1) \rangle, \end{aligned}$$

where $m \geq 2$ and, in the second case, $n \geq 4$, $1 + s \not\equiv 0 \pmod{2^{n-3}}$, and $n \geq m + 2$. Here $|G| = 2^{n+m+2}$, $n \geq 2$, $m \geq 2$, $G' = \langle u \rangle \times \langle v \rangle \cong C_2 \times C_{2^n}$, where in case $o(a) = 2^{m+1}$ we have $\langle u, z \rangle \leq Z(G)$ and so $Z(G)$ is noncyclic and in case $o(a) = 2^{m+2}$ we have $\langle u, z \rangle \not\leq Z(G)$ and so $Z(G)$ is cyclic in which case $n \geq 4$.

Proof. Since $|G'| \geq 8$, Theorem 87.10 implies that G has no normal normal subgroups isomorphic to E_8 and so we may use Theorem 87.11 (a) to (g). Since $[a, x] = v$ is of order 2^n , we get $G' = \langle u \rangle \times \langle v \rangle$ for some involution u , $\Phi(G') = \langle v^2 \rangle$, and $R = \langle u \rangle \times \langle v^2 \rangle$. By Theorem 87.11(g6), $E/\Phi(G') \cong E_8$ and $x^2 \in \langle z \rangle$, where we set $v^{2^{n-1}} = z$ and so $\langle z \rangle = \Omega_1(\Phi(G')) \leq Z(G)$. This gives $\epsilon = 0$ and $v^x = v^{-1}$ and therefore x inverts G' . We have $W = \langle u \rangle \times \langle z \rangle$ and since $|G : C_G(W)| \leq 2$ and $W = Z(E)$, we have $C_G(W) \geq M = E\langle a^2 \rangle$. Also, $F/G' \cong C_{2^m}$, $m \geq 2$.

Since $b = [v, a] \in R - \Phi(G')$ is of order $\exp(R) = 2^{n-1}$, we may set $b = uv^{2i}$ with an odd integer i and we may also write $b = uv^{2+4s}$ (s integer). Suppose that $C_{\langle v^2 \rangle}(a) > \langle z \rangle$ which implies $n \geq 3$. From $b = [v, a]$ we get $v^a = vb$ and so

$$(v^{2^{n-2}})^a = (vb)^{2^{n-2}} = v^{2^{n-2}}(uv^{2i})^{2^{n-2}} = v^{2^{n-2}}z = v^{-2^{n-2}},$$

where $o(v^{2^{n-2}}) = 4$. This is a contradiction and so $C_{\langle v^2 \rangle}(a) = \langle z \rangle$. But we know that $a^{2^m} \in R - \Phi(G')$ and so $a^{2^{m+1}} \in \langle z \rangle$ which gives either $a^{2^m} = uz^\eta$ or $n \geq 3$

and $a^{2^m} = uv^{2^{n-2}}z^\eta$, where $\eta = 0, 1$. If $a^{2^m} = uz^\eta$, then $o(a) = 2^{m+1}$, $C_G(W) \geq \langle M, a \rangle = G$ and so $W \leq Z(G)$ and $Z(G)$ is noncyclic.

Suppose that we are in the second case, where $n \geq 3$, $a^{2^m} = uv^{2^{n-2}}z^\eta$, $\eta = 0, 1$, and $o(a) = 2^{m+2}$. In this case $u = a^{2^m}v^{-2^{n-2}}z^\eta$ and so

$$u^a = a^{2^m}v^{2^{n-2}}z^\eta = (a^{2^m}v^{-2^{n-2}}z^\eta)z = uz,$$

which implies that $W \not\leq Z(G)$ and so $Z(G)$ is cyclic. In this case we must have $n \geq 4$. Indeed, if $n = 3$, then $b_1 = v^{-2}b^{-1} = v^{-2}(uv^{-2}) = uv^{-2(1+i)}$, and so the fact that $1+i$ is even and $o(v) = 8$ implies $v^{-2(1+i)} \in \langle z \rangle$. Hence b_1 is an involution in $W - \langle z \rangle$ and since $\langle b_1 \rangle = F'_1 \leq Z(G)$, we get $W \leq Z(G)$, a contradiction. Since

$$b_1 = v^{-2}b^{-1} = v^{-2}uv^{-2-4s} = uv^{-4(1+s)}$$

and $b_1 \in R - \Phi(G')$ cannot be an involution ($Z(G)$ is cyclic), it follows $1+s \not\equiv 0 \pmod{2^{n-3}}$. We have $G = \langle a \rangle \langle ax \rangle$, where $a^{2^m} = uv^{2^{n-2}}z^\eta$ and $a^{2^{m+1}} = z$. Since $o(a^{2^m}) = 4$ and a^{2^m} is inverted by x , it follows that $\langle a^{2^m} \rangle \not\leq Z(G)$ and so $\langle a^{2^m} \rangle \not\leq \langle a \rangle \cap \langle ax \rangle \leq Z(G)$. Since $\langle ax \rangle^{2^m} \in R - \Phi(G')$ cannot be an involution (because $W \not\leq Z(G)$), it follows that $\langle \langle ax \rangle^{2^m} \rangle$ being distinct from $\langle a^{2^m} \rangle$, $o(\langle ax \rangle^{2^m}) \geq 8$ and so $\langle \langle ax \rangle^{2^{m+1}} \rangle \leq \langle v^2 \rangle$ and $\langle \langle ax \rangle^{2^{m+1}} \rangle > \langle z \rangle$. This implies that $\langle a \rangle \cap \langle ax \rangle = \langle z \rangle$ and so $o(a) = 2^{m+2}$ and $|G| = 2^{n+m+2}$ gives $o(ax) = 2^{m+1+r}$, where $o(\langle ax \rangle^{2^{m+1}}) = 2^r$, $r \geq 2$. This implies (by the product formula) $m+r = n$ and so $n \geq m+2$. \square

In the rest of this section we consider the remaining case, where G' has no cyclic subgroups of index 2. By Theorems 87.10 and 87.15, G has no normal elementary abelian subgroups of order 8 but $G/\Phi(G')$ has a normal elementary abelian subgroup of order 8. We shall use freely the notation and all results from Theorem 87.11.

Theorem 87.17. *Let G be a 2-group with exactly one nonmetacyclic maximal subgroup and $d(G) = 2$. Assume that $G' \cong C_{2^r} \times C_{2^r}$, $r \geq 2$, is homocyclic. Then $G/G' \cong C_2 \times C_4$ and*

$$\begin{aligned} G = \langle a, x \mid a^{2^{r+2}} = 1, r \geq 2, [a, x] = v, [v, a] = b, v^{2^r} = b^{2^r} = [v, b] = 1, \\ v^{2^{r-1}} = u, b^{2^{r-1}} = z, x^2 \in \langle u, z \rangle, b^x = b^{-1}, v^x = v^{-1}z^\epsilon, \\ \epsilon = 0, 1, \text{ and } \epsilon = 1 \text{ if and only if } x^2 \notin \langle z \rangle, b^a = b^{-1}z^\eta, \eta = 0, 1, \\ a^4 = v^{-2}b^{-1}u^\eta z^\zeta, \zeta = 0, 1 \rangle. \end{aligned}$$

Here $|G| = 2^{2r+3}$, $r \geq 2$, $G' = \langle v \rangle \times \langle b \rangle \cong C_{2^r} \times C_{2^r}$, $Z(G) = \langle z \rangle \cong C_2$, and $(\Phi(G))' = \langle z^\eta \rangle$, where $\Phi(G) = \langle a^2 \rangle \langle v \rangle$.

Proof. The element $v = [a, x] \in G' - R$ is of order 2^r and if $\langle b' \rangle \cong C_{2^r}$ is a complement of $\langle v^2 \rangle$ in R , then $R = \langle b' \rangle \times \langle v^2 \rangle$, $\Phi(G') = \langle (b')^2 \rangle \times \langle v^2 \rangle$ and all

elements in $R - \Phi(G')$ are of order 2^r . Hence $b = [v, a] \in R - \Phi(G')$ is of order 2^r and so $G' = \langle b \rangle \times \langle v \rangle$, $R = \langle b \rangle \times \langle v^2 \rangle$, $\Phi(G') = \langle b^2 \rangle \times \langle v^2 \rangle$. We set $v^{2^{r-1}} = u$, $b^{2^{r-1}} = z$ so that $W = \langle u, z \rangle$, $\langle z \rangle = \mathfrak{V}_{r-1}(R) \leq Z(G)$ and we know that x inverts R . From $b = [v, a]$ follows $v^a = vb$, $(v^{2^{r-1}})^a = v^{2^{r-1}}b^{2^{r-1}}$ and $u^a = uz$ so that $W \not\leq Z(G)$ and $W \cap Z(G) = \langle z \rangle$. Since $W \leq Z(E)$, we get $C_G(W) = M = E\langle a^2 \rangle$. We have $x^2 \in W$ and $v^x = v^{-1}z^\epsilon$, $\epsilon = 0, 1$, where $\epsilon = 1$ if and only if $x^2 \notin \langle z \rangle$. It follows $Z(E) = W$.

We have $b_1 = v^{-2}z^\epsilon b^{-1} \in R - \Phi(G')$, where $o(b_1) = 2^r$, $\langle b_1 \rangle = F'_1$, $F_1 = G'\langle ax \rangle$, and $b_1^{2^{r-1}} = (b^{-1})^{2^{r-1}} = z$. But $R = \langle b \rangle \langle b_1 \rangle$, $|R| = 2^{2r-1}$, and so (by the product formula) $\langle b \rangle \cap \langle b_1 \rangle = \langle z \rangle$. Since $bb^a \in \langle b \rangle \cap \langle b_1 \rangle$ (Theorem 87.11(g11)), we get $b^a = b^{-1}z^\eta$, $\eta = 0, 1$, and $(\Phi(G))' = \langle bb^a \rangle = \langle z^\eta \rangle$. Hence, $\Phi(G) = G'\langle a^2 \rangle = \langle a^2 \rangle \langle v \rangle$ is either abelian or minimal nonabelian (Lemma 65.2). Also, $b_1^{-1}(b_1)^a = (bb^a)^{-1} = z^\eta$ and $(b_1)^a = b_1z^\eta$ which gives $(b_1u^\eta)^a = b_1z^\eta(uz)^\eta = b_1u^\eta = v^{-2}b^{-1}u^\eta z^\epsilon$, so that $C_{G'}(a) = \langle v^{-2}b^{-1}u^\eta z^\epsilon \rangle$ is of order 2^r (noting that $G' = \langle b_1u^\eta \rangle \times \langle v \rangle$ and $u^a = uz$ forces $C_{\langle v \rangle}(a) = \{1\}$). But $a^{2^m} \in R - \Phi(G')$ is of order 2^r and so $\langle a^{2^m} \rangle = \langle v^{-2}b^{-1}u^\eta z^\epsilon \rangle$ which gives $\langle a^{2^{m+1}} \rangle = \langle v^{-4}b^{-2} \rangle = \langle v^4b^2 \rangle$.

We claim that for all $s \geq 1$, $[a^{2^s}, x] = v^{2^s}b^{2^{s-1}}$. Indeed, $[a^2, x] = [a, x]^a[a, x] = v^a v = (vb)v = v^2b$ and, using the facts that $v^2 \in \Phi(\Phi(G)) \leq Z(\Phi(G))$ and $b^{a^2} = (b^{-1}z^\eta)^a = b$, we get $[a^4, x] = [a^2, x]^{a^2}[a^2, x] = (v^2b)^{a^2}v^2b = v^4b^2$. Assuming $s > 2$ and using the induction on s (since $a^{2^{s-1}} \in Z(\Phi(G))$), we get

$$\begin{aligned} [a^{2^s}, x] &= [a^{2^{s-1}}a^{2^{s-1}}, x] = [a^{2^{s-1}}, x]^{a^{2^{s-1}}} [a^{2^{s-1}}, x] \\ &= (v^{2^{s-1}}b^{2^{s-2}})^{a^{2^{s-1}}}(v^{2^{s-1}}b^{2^{s-2}}) = (v^{2^{s-1}}b^{2^{s-2}})^2 = v^{2^s}b^{2^{s-1}}. \end{aligned}$$

Since $a^{2^m} \in R - \Phi(G')$, $m \geq 2$, and x inverts R , we get $(a^{2^m})^x = a^{-2^m}$, and so $[a^{2^m}, x] = a^{-2^{m+1}}$. By the above relation, $[a^{2^m}, x] = v^{2^m}b^{2^{m-1}} = a^{-2^{m+1}}$ and so using a result from the previous paragraph we get $\langle v^{2^m}b^{2^{m-1}} \rangle = \langle v^4b^2 \rangle$ which forces $m = 2$. We have proved that G/G' is abelian of type $(4, 2)$ and so $a^4 \in R - \Phi(G')$.

Because $\langle a^4 \rangle = \langle v^{-2}b^{-1}u^\eta z^\epsilon \rangle$, we get $a^4 = v^{-2}b^{-1}u^\eta z^\epsilon(v^{-2}b^{-1}u^\eta z^\epsilon)^{2i}$ for some integer i , and so $a^4 = v^{-2-4i}b^{-1-2i}u^\eta z^\epsilon$. Then (noting that $a^8 = v^{-4}b^{-2}$) $a^8 = v^{-4-8i}b^{-2-4i} = v^{-4}b^{-2}$ implies $i \equiv 0 \pmod{2^{r-2}}$ and so we have $a^4 = v^{-2}b^{-1}z^{-i}u^\eta z^\epsilon$ and $a^4 = v^{-2}b^{-1}u^\eta z^\zeta$, $\zeta = 0, 1$. We see also $Z(G) = \langle z \rangle$. \square

Theorem 87.18. *Let G be a 2-group with exactly one nonmetacyclic maximal subgroup and $d(G) = 2$. Assume that G' has no cyclic subgroups of index 2. Then $Z(G)$ is elementary abelian of order at most 4, $Z(G) \leq \Omega_1(G')$, and $G/G' \cong C_4 \times C_2$.*

Proof. We consider $G/\mathfrak{V}_2(G')$, where $G'/\mathfrak{V}_2(G') = (G/\mathfrak{V}_2(G'))' \cong C_4 \times C_4$ and so by Theorem 87.17, $G/G' \cong C_4 \times C_2$. We may use Theorem 87.11 with $m = 2$. We have $Z(G) \leq \Phi(G) = G'\langle a^2 \rangle$, where $|G'\langle a^2 \rangle : G'| = 2$ and $W \leq \Phi(G')$. Note that x inverts R . If x commutes with an element $y \in G' - R$, then $y^2 \in R$ must

be an involution and so $\exp(G') = 4$ and $G' \cong C_4 \times C_4$. But in that case (Theorem 87.17), $Z(G) \cong C_2$ and $Z(G) \leq W$ and we are done. Hence, we may assume that $C_{G'}(x) = C_R(x) = W$ and so $Z(G) \cap G' \leq W$. Suppose that there is an element $l \in \Phi(G) - G'$ such that $l \in Z(G)$. We have $l^2 \in G'$ and so $l^2 \in R$ and therefore l^2 must be an involution in W (since $\Omega_1(\Phi(G)) = W$). But $W \leq \Phi(G')$ and so there is an element $k \in G'$ such that $k^2 = l^2$. In that case, kl is an involution in $\Phi(G) - G'$, a contradiction. Hence, $Z(G) \leq W$ and we are done. \square

Theorem 87.19. *Let G be a 2-group with exactly one nonmetacyclic maximal subgroup and $d(G) = 2$. Assume that $G' \cong C_{2^r} \times C_{2^{r+1}}$, $r \geq 2$. Then we have:*

$$\begin{aligned} G = \langle a, x \mid a^{2^{r+2}} = 1, r \geq 2, [a, x] = v, [v, a] = b, v^{2^{r+1}} = b^{2^r} = [v, b] = 1, \\ v^{2^r} = z, b^{2^{r-1}} = u, x^2 \in \langle u, z \rangle \cong E_4, b^x = b^{-1}, v^x = v^{-1}, \\ b^a = b^{-1}, a^4 = v^{-2}b^{-1}w, w \in \langle u, z \rangle \rangle. \end{aligned}$$

Here $|G| = 2^{2r+4}$, $r \geq 2$, $G' = \langle b \rangle \times \langle v \rangle \cong C_{2^r} \times C_{2^{r+1}}$, $Z(G) = \langle u, z \rangle \cong E_4$, and $\Phi(G) = G'\langle a^2 \rangle$ is abelian.

Proof. By Theorem 87.18, we have $m = 2$ in Theorem 87.11. The element $v = [a, x] \in G' - R$ is of order 2^{r+1} so that R is homocyclic of rank 2 and exponent 2^r . It follows $R = \langle b \rangle \times \langle v^2 \rangle = \langle b_1 \rangle \times \langle v^2 \rangle = \langle b \rangle \times \langle b_1 \rangle$, and so $\epsilon = 0$, $W = \langle v^{2^r} \rangle \times \langle b^{2^{r-1}} \rangle = Z(G)$, x inverts G' , $x^2 \in W$, $b^a = b^{-1}$ and $b_1^a = b_1$, where $v^a = vb$ and $b_1 = v^{-2}b^{-1}$. We set $v^{2^r} = z$ and $b^{2^{r-1}} = u$. Since $C_{\langle v \rangle}(a) = \langle z \rangle$, we have $C_{G'}(a) = \langle b_1 \rangle \times \langle z \rangle$. On the other hand, $a^4 \in R - \Phi(G')$ is of order 2^r and so $\langle a^4 \rangle$ is a cyclic subgroup of index 2 in $C_{G'}(a)$. This gives $\langle a^4 \rangle = \langle b_1 z^\zeta \rangle = \langle v^{-2}b^{-1}z^\zeta \rangle$, $\zeta = 0, 1$. Also, $(\Phi(G))' = \langle bb^a \rangle = \{1\}$ and therefore $\Phi(G) = G'\langle a^2 \rangle$ is abelian.

We get $a^4 = v^{-2}b^{-1}z^\zeta(v^{-2}b^{-1}z^\zeta)^{2i} = v^{-2-4i}b^{-1-2i}z^\zeta$, where i is an integer. On the other hand, $[a^2, x] = [a, x]^a[a, x] = v^a v = v^2 b$ and $[a^4, x] = [a^2, x]a^2[a^2, x] = (v^2 b)^a(v^2 b) = (v^2 b)^2 = v^4 b^2$. Since x inverts G' , $[a^4, x] = a^{-8}$ and so $a^8 = v^{-4}b^{-2}$. This gives $a^8 = v^{-4}b^{-2} = v^{-4-8i}b^{-2-4i}$ and $-2i \equiv 0 \pmod{2^{r-1}}$, which implies $a^4 = v^{-2}b^{-1}w$ with $w \in \langle u, z \rangle$ since $v^{-4i} \in \langle z \rangle$ and $b^{-2i} \in \langle u \rangle$. \square

Somewhat more difficult is the next special case, where $G' \cong C_{2^r} \times C_{2^{r+2}}$, $r \geq 2$. After that we shall be able to investigate the general case.

Theorem 87.20. *Let G be a 2-group with exactly one nonmetacyclic maximal subgroup and $d(G) = 2$. Assume that $G' \cong C_{2^r} \times C_{2^{r+2}}$, $r \geq 2$. Then we have:*

$$\begin{aligned} G = \langle a, x \mid a^{2^{r+2}} = 1, r \geq 2, [a, x] = v, [v, a] = b, v^{2^{r+2}} = b^{2^{r+1}} = [v, b] = 1, \\ v^{2^{r+1}} = b^{2^r} = z, v^{2^r}b^{2^{r-1}} = u, x^2 \in \langle u, z \rangle \cong E_4, \\ b^x = b^{-1}, v^x = v^{-1}, b^a = b^{-1}, a^4 = v^{-2}b^{-1}w, w \in \langle u, z \rangle \rangle. \end{aligned}$$

Here $|G| = 2^{2r+5}$, $r \geq 2$, $G' = \langle b, v \rangle \cong C_{2r} \times C_{2^{r+2}}$, $Z(G) = \langle u, z \rangle \cong E_4$, and $\Phi(G) = G'\langle a^2 \rangle$ is abelian.

Proof. We use freely Theorem 87.18 and 87.11 with $m = 2$. The element $v = [a, x] \in G' - R$ is of order 2^{r+2} and we set $z = v^{2^{r+1}}$ so that $z \in Z(G)$ since $\langle z \rangle = \mathcal{V}_{r+1}(G')$. The element $b = [v, a] \in R - \Phi(G')$ is of order $\exp(R) = 2^{r+1}$ and since $\langle b \rangle$ covers $R/\langle v^2 \rangle \cong C_{2r}$, we get $\langle b \rangle \cap \langle v^2 \rangle = \langle b \rangle \cap \langle v \rangle = \langle z \rangle$. We have $b_1 = [v, ax] \in R - \Phi(G')$ and $\langle b_1 \rangle$ also covers $R/\langle v^2 \rangle$. We know that $b_1 = v^{-2}z\epsilon b^{-1}$ and so $b_1^{2^r} = v^{-2^{r+1}}b^{-2^r} = zz = 1$ and therefore b_1 is of order 2^r . Thus $\langle b_1 \rangle \cap \langle v^2 \rangle = \{1\}$ and so $R = \langle b_1 \rangle \times \langle v^2 \rangle = \langle b_1 \rangle \times \langle b \rangle$. Set $u = b_1^{2^{r-1}} = v^{-2^r}b^{-2^{r-1}} = v^{2^r}b^{2^{r-1}}$ so that $W = \langle u, z \rangle \cong Z(G)$ (noting that $\langle b_1 \rangle = F'_1$ is normal in G and so $u \in Z(G)$), which gives $\epsilon = 0$ and $v^x = v^{-1}$. We have $x^2 \in W$ and we know that x inverts on R and so $b^x = b^{-1}$. We have also $b_1^{-1}b_1^a = (bb^a)^{-1} \in \langle b \rangle \cap \langle b_1 \rangle = \{1\}$ and so $b^a = b^{-1}$, $b_1^a = b_1$, and $(\Phi(G))' = \langle bb^a \rangle = \{1\}$. Since $v^a = vb$, we get $(v^{2^r})^a = v^{2^r}b^{2^r} = v^{2^r}z = v^{-2^r}$ (since $(v^{2^r})^2 = z$) and so $C_{G'}(a) = \langle b_1 \rangle \times \langle z \rangle$. On the other hand, $a^4 \in R - \Phi(G')$, $\langle a^4 \rangle$ covers $R/\langle v^2 \rangle$ and $a^4 \in C_{G'}(a)$ which gives $\langle a^4 \rangle = \langle b_1 z^\eta \rangle = \langle v^{-2}b^{-1}z^\eta \rangle$, $\eta = 0, 1$.

We compute (noting that x inverts a^4):

$$\begin{aligned} [a^2, x] &= [a, x]^a[a, x] = v^a v = v^2 b, \quad [a^4, x] = a^{-8} \\ &= [a^2, x]^{a^2}[a^2, x] = (v^2 b)^{a^2}(v^2 b) = v^4 b^2 \end{aligned}$$

and so $a^8 = v^{-4}b^{-2}$. Using the last result from the previous paragraph, we get

$$a^4 = v^{-2}b^{-1}z^\eta(v^{-2}b^{-1}z^\eta)^{2i} = v^{-2-4i}b^{-1-2i}z^\eta \quad (i \text{ integer}),$$

$a^8 = v^{-4}b^{-2} = v^{-4-8i}b^{-2-4i}$ and so $v^{-8i}b^{-4i} = 1$. This gives $i \equiv 0 \pmod{2^{r-2}}$ since $\langle v \rangle \cap \langle b \rangle = \langle z \rangle$ and $v^{2^{r+1}}b^{2^r} = z^2 = 1$. We may set $i = \zeta 2^{r-2}$ (ζ integer) and then

$$a^4 = v^{-2}b^{-1}z^\eta(v^{-2^r}b^{-2^{r-1}})^\zeta = v^{-2}b^{-1}z^\eta u^\zeta, \quad \zeta = 0, 1. \quad \square$$

Finally, we consider the general case, where $G' \cong C_{2r} \times C_{2^{r+s+1}}$ with $r \geq 2$ and $s \geq 2$.

Theorem 87.21. Let G be a 2-group with exactly one nonmetacyclic maximal subgroup and $d(G) = 2$. Assume that $G' \cong C_{2r} \times C_{2^{r+s+1}}$, $r \geq 2$, $s \geq 2$. Then we have one of the following two possibilities (depending on $Z(G)$ being noncyclic or cyclic):

- (a) $G = \langle a, x \mid a^{2^{r+2}} = 1, r \geq 2, [a, x] = v, [v, a] = b,$
- $$v^{2^{r+s+1}} = b^{2^{r+s}} = [v, b] = 1, s \geq 2, b^{2^r} = v^{-2^{r+1}},$$
- $$v^{2^{r+s}} = z, a^{2^{r+1}} = u, x^2 \in W = \langle u, z \rangle \cong E_4,$$
- $$b^a = b^{-1}, b^x = b^{-1}, v^x = v^{-1}, a^4 = v^{-2}b^{-1}w, w \in W \rangle.$$

Here $|G| = 2^{2r+s+4}$, $r \geq 2$, $s \geq 2$, $G' = \langle b, v \rangle \cong C_{2r} \times C_{2r+s+1}$, $\langle b \rangle \cap \langle v \rangle \cong C_{2s}$, $Z(G) = W = \langle u, z \rangle \cong E_4$, and $\Phi(G) = G'\langle a^2 \rangle$ is abelian.

$$\begin{aligned}
 (b) \quad G &= \langle a, x \mid a^{2^{r+3}} = 1, r \geq 2, [a, x] = v, [v, a] = b, \\
 &\quad v^{2^{r+s+1}} = b^{2^{r+s}} = [v, b] = 1, s \geq 2, \\
 &\quad v^{2^{r+s}} = a^{2^{r+2}} = z, b^{2^r} = v^{-2^{r+1}}z, \\
 &\quad u = v^{-2^r(1+2^{s-1})}b^{-2^{r-1}}, u^a = uz, x^2 \in W = \langle u, z \rangle \cong E_4, \\
 &\quad b^a = b^{-1}z^\delta, \delta = 0, 1, b^x = b^{-1}, v^x = v^{-1}z^\epsilon, \epsilon = 0, 1, \\
 &\quad \epsilon = 0 \text{ if and only if } x^2 \in \langle z \rangle, a^4 = v^{-2}b^{-1}u^\delta z^\tau, \tau = 0, 1 \rangle.
 \end{aligned}$$

Here $|G| = 2^{2r+s+4}$, $r \geq 2$, $s \geq 2$, $G' = \langle b, v \rangle \cong C_{2r} \times C_{2r+s+1}$, $\langle b \rangle \cap \langle v \rangle \cong C_{2s}$, $Z(G) = \langle z \rangle \cong C_2$, $\Phi(G) = G'\langle a^2 \rangle$, $(\Phi(G))' = \langle z^\delta \rangle$ and so $\Phi(G)$ is either abelian ($\delta = 0$) or minimal nonabelian ($\delta = 1$).

Proof. We use freely Theorem 87.11 with $m = 2$ and $Z(G) \leq W$ (see Theorem 87.18). The element $v = [a, x] \in G' - R$ is of order 2^{r+s+1} and the element $b = [v, a] \in R - \phi(G')$ is of order $\exp(R) = 2^{r+s}$. Since $\langle b \rangle$ covers $R/\langle v^2 \rangle \cong C_{2r}$, we have $c = b^{2^r} \in \langle v^2 \rangle$, $o(c) = 2^s$ and $\langle v^2 \rangle / \langle c \rangle \cong C_{2r}$. Set $z = v^{2^{r+s}}$ so that $\langle z \rangle = \mathfrak{V}_{r+s}(G') \leq Z(G)$ and $\langle z \rangle < \langle c \rangle$. We know that the element $x \in E - G'$ (with $x^2 \in W = \Omega_1(G')$) inverts each element in R and $v^x = v^{-1}z^\epsilon$, where $\epsilon = 0, 1$ and $\epsilon = 1$ if and only if $x^2 \in W - Z(G)$. We note that $W \leq Z(E)$ and so $C_G(W) \geq M = E\langle a^2 \rangle$. Also, $b_1 = [v, ax] = v^{-2}b^{-1}z^\epsilon$, $b^x = b^{-1}$ and $b_1^x = b_1^{-1}$.

Set $S = \langle c \rangle$ and $S^* = \mathfrak{V}_r(G') = \langle v^{2^r} \rangle$ so that S^* is normal in G and $|S^* : S| = 2$. We have $(v^{2^{r+s-1}})^a = v^{2^{r+s-1}}b^{2^{r+s-1}} = v^{2^{r+s-1}}z = v^{-2^{r+s-1}}$ since $v^{2^{r+s-1}}$ is an element of order 4. This gives $C_{\langle v \rangle}(a) = \langle z \rangle$. Also, $(v^{2^r})^a = (bv)^{2^r} = cv^{2^r}$. Since $a^4 \in R - \Phi(G')$ and $\langle a^4 \rangle$ covers $R/\langle v^2 \rangle$, we have either $o(a) = 2^{r+2}$ with $\langle a \rangle \cap \langle v \rangle = \{1\}$ or $o(a) = 2^{r+3}$ with $\langle a \rangle \cap \langle v \rangle = \langle z \rangle$. On the other hand, $(ax)^4 \in R - \Phi(G')$ and $\langle (ax)^4 \rangle$ covers $R/\langle v^2 \rangle$ so that $o(ax) = 2^{r+2+t}$, where $2^t = |\langle ax \rangle \cap \langle v^2 \rangle|$. Since $|G| = 2^{2r+s+4}$, $G = \langle a \rangle \langle ax \rangle$ and $o(a) \leq 2^{r+3}$, it follows that $o(ax) = 2^{r+2+t} \geq 2^{r+s+1}$ and so $t \geq s - 1$. By our assumption, $s \geq 2$ and so $t \geq 1$, which implies that $\langle ax \rangle \geq \langle z \rangle$. If $\langle a \rangle \cap \langle v \rangle = \{1\}$, then $\langle a \rangle \cap \langle ax \rangle = \{1\}$, $o(ax) = 2^{r+s+2}$ and therefore $t = s$. If $\langle a \rangle \cap \langle v \rangle = \langle z \rangle$, then $\langle a \rangle \cap \langle ax \rangle = \langle z \rangle$, $o(a) = 2^{r+3}$ and so again $t = s$. In any case, $\langle ax \rangle \cap \langle v^2 \rangle = S = \langle c \rangle$ and so ax centralizes c . But x inverts c and so $c^a = c^{-1}$. From $(v^{2^r})^a = cv^{2^r}$ follows $(v^{2^r})^{a^2} = c^a(v^{2^r})^a = c^{-1}(cv^{2^r}) = v^{2^r}$. Hence a induces an involutory automorphism on $S^* = \langle v^{2^r} \rangle$ with $c^a = c^{-1}$, where $o(c) \geq 4$ and $|S^* : \langle c \rangle| = 2$. This gives $(v^{2^r})^a = cv^{2^r} = v^{-2^r}z^\xi$, $\xi = 0, 1$, and so $c = b^{2^r} = v^{-2^{r+1}}z^\xi$, where $o(v^{2^r}) = 2^{s+1} \geq 8$.

We compute $b_1^{2^r} = (v^{-2}b^{-1}z^\epsilon)^{2^r} = v^{-2^{r+1}}v^{2^{r+1}}z^\xi = z^\xi$ and so $\langle b \rangle \cap \langle b_1 \rangle = \langle z^\xi \rangle$. From Theorem 87.11(g11) follows $b_1^{-1}b_1^a = (bb^a)^{-1} \in \langle z^\xi \rangle$, and so $b^a =$

$b^{-1}z^\delta, b_1^a = b_1 z^\delta, \delta = 0, 1$, where $\zeta = 0$ implies $\delta = 0$. Also, $(\Phi(G))' = \langle bb^a \rangle = \langle z^\delta \rangle$ and therefore $\Phi(G)$ is either abelian or minimal nonabelian.

We get $b^{a^2} = (b^{-1}z^\delta)^a = b$ and $(v^2)^{a^2} = v^2$ since $v^2 \in \Phi(\Phi(G)) \leq Z(\Phi(G))$, where $\Phi(G) = G'\langle a^2 \rangle$. Also we know that x inverts R and $a^4 \in R - \Phi(G')$ and all this gives:

$$[a^2, x] = [a, x]^a [a, x] = v^a v = (vb)v = v^2 b,$$

$$[a^4, x] = a^{-8} = [a^2, x]^{a^2} [a^2, x] = (v^2 b)^{a^2} (v^2 b) = (v^2 b)^2 = v^4 b^2,$$

and so $a^8 = v^{-4}b^{-2}$. From this result also follows

$$(a^8)^{2^{r-1}} = a^{2^{r+2}} = v^{-2^{r+1}} b^{-2^r} = v^{-2^{r+1}} v^{2^{r+1}} z^\xi = z^\xi$$

and, since $\langle ax \rangle \cap \langle v \rangle = \langle c \rangle \cong C_{2^s}$, we get $\langle ax \rangle \cap \langle a \rangle = \langle z^\xi \rangle$.

Suppose $\zeta = 0$. In that case $b^{2^r} = v^{-2^{r+1}}$, $\langle b \rangle \cap \langle b_1 \rangle = F' \cap F'_1 = \{1\}$, $\delta = 0$, $o(b_1) = 2^r$, $a^{2^{r+1}} = u \in Z(G)$ and so $W = \langle u, z \rangle = Z(G)$, $\epsilon = 0$, $v^x = v^{-1}$, $b^a = b^{-1}$, $b_1^a = b_1$, and $(\Phi(G))' = \{1\}$. Since $C_{G'}(a) = \langle b_1 \rangle \times \langle z \rangle$ and $b_1 = v^{-2}b^{-1}$, we get $\langle a^4 \rangle = \langle v^2 b z^\xi \rangle$, $\xi = 0, 1$. Hence $a^4 = v^2 b z^\xi (v^2 b z^\xi)^{2i} = v^{2+4i} b^{1+2i} z^\xi$ (i integer), and so, using a result from the previous paragraph, we get

$$a^8 = v^{-4}b^{-2} = v^{4+8i} b^{2+4i}, \quad v^{8+8i} b^{4+4i} = 1, \quad i + 1 \equiv 0 \pmod{2^{r-2}},$$

and we set $i = -1 + t2^{r-2}$ (t an integer). This gives

$$a^4 = v^{-2+t2^r} b^{-1+t2^{r-1}} z^\xi = v^{-2} b^{-1} (v^{2^r} b^{2^{r-1}})^t z^\xi$$

and since $(v^{2^r} b^{2^{r-1}})^2 = v^{2^{r+1}} b^{2^r} = 1$, we get $(v^{2^r} b^{2^{r-1}})^t z^\xi = w \in W = Z(G)$.

Suppose $\zeta = 1$. In that case we have $\langle b \rangle \cap \langle b_1 \rangle = F' \cap F'_1 = \langle z \rangle$, $b^{2^r} = v^{-2^{r+1}} z$, $b_1^{2^r} = z$, $(\Phi(G))' = \langle z^\delta \rangle$, $\delta = 0, 1$, $b^a = b^{-1}z^\delta$, $b_1^a = b_1 z^\delta$. We set $u_0 = b_1^{2^{r-1}} c^{2^{s-2}}$ so that $u_0^2 = b_1^{2^r} c^{2^{s-1}} = zz = 1$ and

$$u_0^a = (b_1^{2^{r-1}} c^{2^{s-2}})^a = b_1^{2^{r-1}} c^{-2^{s-2}} = b_1^{2^{r-1}} c^{2^{s-2}} z = u_0 z,$$

where we have used the facts that a inverts c and a centralizes an element of order 4 in $\langle b_1 \rangle$. Hence $Z(G) = \langle z \rangle$. This implies that $a^{2^{r+2}} = z$ and so $o(a) = 2^{r+3}$. Since $c = v^{-2^{r+1}} z$ and $b_1 = v^{-2}b^{-1}z^\epsilon$, where $v^x = v^{-1}z^\epsilon$, $\epsilon = 0, 1$ (and $\epsilon = 0$ if and only if $x^2 \in \langle z \rangle$), we get:

$$u_0 = (v^{-2}b^{-1}z^\epsilon)^{2^{r-1}} (v^{-2^{r+1}} z)^{2^{s-2}} = (v^{-2^{r+1}} b^{-2^{r-1}})^{2^{s-2}} = uz^{2^{s-2}},$$

where we have set $u = v^{-2^{r+1}} b^{-2^{r-1}}$. We see that $u^2 = 1$, $u^a = uz$ (since $u_0^a = u_0 z$), and so $W = \langle u, z \rangle \cong E_4$.

Since $(b_1 u^\delta)^a = b_1 z^\delta (uz)^\delta = b_1 u^\delta$, $(b_1 u^\delta)^{2^r} = b_1^{2^r} = z$, and $C_{\langle v \rangle}(a) = \langle z \rangle$, we have $C_{G'}(a) = \langle b_1 u^\delta \rangle$, and so $\langle a^4 \rangle = \langle b_1 u^\delta \rangle = \langle v^{-2}b^{-1}z^\epsilon u^\delta \rangle = \langle v^2 b u^\delta \rangle$ since

$z^\epsilon \in \Phi(\langle b_1 u^\delta \rangle)$. This gives $a^4 = v^2 b u^\delta (v^2 b u^\delta)^{2i} = v^{2+4i} b^{1+2i} u^\delta$ (i integer), and therefore

$$a^8 = v^{-4} b^{-2} = v^{4+8i} b^{2+4i}, \quad v^{8+8i} b^{4+4i} = 1, \quad \text{and so } i+1 \equiv 0 \pmod{2^{r-2}}.$$

We set $i = -1 + t2^{r-2}$ (t an integer) and compute:

$$1 = v^{t2^{r+1}} b^{t2^r} = (v^{2^{r+1}} b^{2^r})^t = (v^{2^{r+1}} v^{-2^{r+1}} z)^t = z^t$$

and this forces $t \equiv 0 \pmod{2}$. Hence we may set $t = 2\tau$ (τ an integer) and then $i = -1 + \tau 2^{r-1}$ so that

$$\begin{aligned} a^4 &= v^{2-4+\tau 2^{r+1}} b^{1-2+\tau 2^r} u^\delta = v^{-2} b^{-1} u^\delta (v^{2^{r+1}} b^{2^r})^\tau \\ &= v^{-2} b^{-1} u^\delta (v^{2^{r+1}} v^{-2^{r+1}} z)^\tau = v^{-2} b^{-1} u^\delta z^\tau, \quad \tau = 0, 1, \end{aligned}$$

and we are done. \square

3^o. The result of this section was also proved independently by the first author (see Supplement to Corollary 36.11).

Theorem 87.22. *Let $G = AB$ be a nonmetacyclic 2-group, where the subgroups A and B are cyclic. If $\{U, V, M\}$ is the set of maximal subgroups of G , where $A < U$ and $B < V$, then U and V are metacyclic and $d(M) = 3$. Hence, M is a unique nonmetacyclic maximal subgroup of G and these groups have been completely determined in section 2^o.*

Proof. Assume, for example, that U is nonmetacyclic. Then $U/\mathfrak{U}_2(U)$ is nonmetacyclic (Lemma 64.1(o)) and so, in particular, $|U/\mathfrak{U}_2(U)| \geq 2^4$. We set $A = \langle a \rangle$ and $B = \langle b \rangle$ so that $U = \langle a \rangle \langle b^2 \rangle$, $|A : (A \cap B)| \geq 4$, and $|\langle b^2 \rangle : (A \cap B)| \geq 4$ (otherwise, U would be metacyclic). Since $a^4 \in \mathfrak{U}_2(U)$, $b^8 \in \mathfrak{U}_2(U)$, and $|U : \langle a^4, b^8 \rangle| = 2^4$ (noting that [Hup2, Satz 2] implies that $\langle a^4, b^8 \rangle = \langle a^4 \rangle \langle b^8 \rangle$), we get $\mathfrak{U}_2(U) = \langle a^4 \rangle \langle b^8 \rangle$ and so $|U : \mathfrak{U}_2(U)| = 2^4$. We want to investigate the structure of $G/\mathfrak{U}_2(U)$ and so we may assume that $\mathfrak{U}_2(U) = \{1\}$. In that case $G = \langle a \rangle \langle b \rangle$ is a group of order 2^5 with $o(a) = 4$, $o(b) = 8$, $\langle a \rangle \cap \langle b \rangle = \{1\}$, and G has a nonmetacyclic subgroup $U = \langle a \rangle \langle b^2 \rangle$ of order 2^4 and exponent 4 which is a product of two cyclic subgroups $\langle a \rangle$ and $\langle b^2 \rangle$ of order 4.

The subgroup U is nonabelian and U is not of maximal class (otherwise, U would be metacyclic). By a result of O. Taussky (Lemma 64.1(s)), $|U'| = 2$ and so U is minimal nonabelian (Lemma 65.2). By Lemma 65.1, $Z(U) = \Phi(U) = \langle a^2 \rangle \times \langle b^4 \rangle \cong E_4$ and $U' = \langle a^2 b^4 \rangle \leq Z(G)$ since $a^2 b^4$ is not a square in U . But $b^4 \in Z(U)$ and so $[b^4, a] = 1$ which gives $b^4 \in Z(G)$. Hence $a^2 \in Z(G)$ and we get $E_4 \cong \langle a^2, b^4 \rangle \leq Z(G)$. We have $G' \leq \Phi(G) = \langle a^2 \rangle \times \langle b^2 \rangle \cong C_2 \times C_4$ and $G' \geq U' = \langle a^2 b^4 \rangle$. We have $G' > U'$ because in case $G' = U'$, G would be minimal nonabelian and then U would be abelian, which is not the case. By the result of O. Taussky (and noting that G

is not of maximal class), we get $|G/G'| \geq 8$ and so $|G'| = 4$. Hence G' is a maximal subgroup of $\Phi(G)$ and so $G' \geq \mathfrak{U}_1(\Phi(G)) = \langle b^4 \rangle$. Hence $E_4 \cong G' = \langle a^2, b^4 \rangle \leq Z(G)$ and so G is of class 2. By Lemma 44.1, G' must be cyclic and this is our final contradiction.

We have proved that U and V are metacyclic. If $d(M) \leq 2$, then Lemma 64.1(n) implies that G is metacyclic, a contradiction. Hence $d(M) = 3$ and M is a unique nonmetacyclic maximal subgroup of G . \square

Hall chains in normal subgroups of p -groups

This section supplements Theorem 24.1. We assume throughout this section that

$$(*) \quad H > \{1\} \text{ is a normal subgroup of a } p\text{-group } G.$$

We begin with the following definitions.

Definition 1. Given $k \in \mathbb{N}$, let

$$\mathcal{C} : \{1\} = L_0 < L_1 < \cdots < L_n = H$$

be a chain (of length $|\mathcal{C}| = n$) of G -invariant subgroups in (a normal subgroup) H such that $\exp(L_i/L_{i-1}) = p$ and $|L_i/L_{i-1}| \leq p^k$, $i = 1, \dots, n$. Then \mathcal{C} is called a k -admissible chain in H . Given a k -admissible chain \mathcal{C} , set $i_0(\mathcal{C}) = \max\{i \geq 0 \mid |L_i| = p^{ki}\}$.

Thus, if $i_0(\mathcal{C}) = 0$, then H has no G -invariant subgroups of order p^k and exponent p . We have $|L_{i_0(\mathcal{C})}| = p^{ki_0(\mathcal{C})}$ and, if $n > i_0(\mathcal{C})$, then $|L_{i_0(\mathcal{C})+1}| < p^{k(i_0(\mathcal{C})+1)}$. In what follows, \mathcal{C} is such as in Definition 1. We have $\exp(L_i) \leq p^i$ for all i .

Definition 2. A k -admissible chain \mathcal{C} in H dominates over a k -admissible chain $\mathcal{C}_1 : \{1\} = M_0 < M_1 < \cdots < M_s = H$ if, with respect to lexicographic ordering, the sequence $\{|L_1|, |L_2 : L_1|, \dots, |L_n : L_{n-1}|\}$ is greater or equal than the sequence $\{|M_1|, |M_1 : M_0|, \dots, |M_s : M_{s-1}|\}$. In that case, we write $\mathcal{C} \geq \mathcal{C}_1$.

In the sequel, \mathcal{C}_1 is such as in Definition 2.

Definition 3. A k -admissible chain \mathcal{C} in H is said to be dominating if, for each k -admissible chain \mathcal{C}_1 in H , we have $\mathcal{C} \geq \mathcal{C}_1$.

Thus, two k -admissible dominating chains in H have the same sequence of indices, and such chains exist. We also consider k -admissible chains in other G -invariant subgroups A of H and in H/A .

Definition 4. A k -admissible chain \mathcal{C} in H is said to be a Hall chain (or \mathcal{H}_k -chain, for brevity), if $L_{i_0+j} = \Omega_{i_0+j}(H)$, where $i_0 = i_0(\mathcal{C})$ and $j > 0$.

In contrast to k -admissible dominating chains which exist always, this is not the case for \mathcal{H}_k -chains (the group D_{16} has no \mathcal{H}_2 -chains). It follows that if, in Definition 4, $L_{i_0+1} < H$, then $\exp(L_{i_0+1}) = p^{i_0+1}$, and so $\exp(L_i) = p^i$ for all $i \leq n$. A 1-admissible chain in H is an \mathcal{H}_1 -chain.

Clearly, if $i_0(\mathcal{C}) \geq n - 1$, then a k -admissible dominating chain \mathcal{C} must be an \mathcal{H}_k -chain. As Lemma 88.3(a) shows, \mathcal{H}_k -chains are k -admissible dominating chains, however, the converse is true under additional assumptions only.

It is asserted in Theorem 24.1 and Supplement 1 to Theorem 24.1 that there exists in H an \mathcal{H}_k -chain for $k \leq p - 1$ (the proof of the Supplement is the same as the proof of Theorem 24.1), however, this is not true for $k = p$ as any p -group H of maximal class and order $\geq p^{2p}$ shows (Theorem 9.6). Moreover, if H is a p -group of maximal class and order $> p^{p+1}$ with $|\Omega_1(H)| > p^{p-1}$, then H has no \mathcal{H}_p -chains. So, there is an \mathcal{H}_p -chain in H provided it satisfies additional conditions, and some such conditions are stated in Theorem 88.10. Theorem 88.11 shows, in particular, that there is in regular H an \mathcal{H}_k -chain for any k . Corollary 88.12 asserts that an abelian p -group G has only one \mathcal{H}_k -chain if and only if $|\Omega_1(G)| \leq p^k$. Note that Theorem 24.1 is not a consequence of Theorem 88.10. In Proposition 88.13 we study the p -groups without \mathcal{H}_p -chains.

Example. Each 2-group of order $\leq 2^3$ has an \mathcal{H}_2 -chain. If G is a 2-group of maximal class and order $\geq 2^4$ then, as we have noticed, G has no \mathcal{H}_2 -chains. (i) We claim that if a group G of order 2^4 is not of maximal class, it has an \mathcal{H}_2 -chain. Indeed, take $E_4 \cong R \triangleleft G$. If G/R is noncyclic, then $\{1\} < R < G$ is an \mathcal{H}_2 -chain. Now suppose that G/R is cyclic. If G has a cyclic subgroup of index 2, then $R = \Omega_1(G)$ and $\{1\} < R < \Omega_2(G) < G$ is the desired chain. If G has no cyclic subgroups of index 2, then $G = C \cdot R$, where C is cyclic of order 4. Let $U \leq R \cap Z(G)$ be of order 2 and $R_1 = U \times \Omega_1(C)$; then $G/R_1 \cong E_4$, and so $\{1\} < R_1 < G$ is an \mathcal{H}_2 -chain. (ii) A 2-group of order $> 2^4$ with cyclic subgroup of index 2, which is not of maximal class, has the unique \mathcal{H}_2 -chain $\{1\} < \Omega_1(G) < \Omega_2(G) < \dots < G$ (Theorem 1.2). (iii) We claim that a 2-group G of order 2^5 , which is not of maximal class, has an \mathcal{H}_2 -chain. One may assume that G has no cyclic subgroups of index 2. Let $E_4 \cong R \triangleleft G$. If $H/R < G/R$ is abelian of type $(2, 2)$, then $\{1\} < R < H < G$ is an \mathcal{H}_2 -chain. Now assume that G/R has no four-subgroups. Then $G/R \in \{C_8, Q_8\}$. (iii1) Let G/R be cyclic. Then $G = Z \cdot R$ is a semidirect product, where Z is cyclic of order 8. In that case, $R_1 = (R \cap Z(G)) \times \Omega_1(Z) \triangleleft G$ is a four-subgroup and G/R_1 has a four-subgroup; then G has an \mathcal{H}_2 -chain, as above. (iii2) Now let $G/R \cong Q_8$. If $\Omega_1(G) = R$, then $\{1\} < \Omega_1(G) < \Omega_2(G) < G$ is the unique \mathcal{H}_2 -chain in G . It remains to consider the case where $\Omega_1(G) = U \cong E_8$; then $\exp(G) = 4$. Let $F/R \leq T/R$ be of order 4, where $T = C_G(R)$; then $F = L \cdot R$, where L is cyclic of order 4 and $R \cap L = \{1\}$. Let $K \leq R \cap Z(G)$ be of order 2. Set $R_1 = K \times \Phi(F)$; then $\{1\} < R_1 < F < G$ is the desired \mathcal{H}_2 -chain in G . We suggest to the reader to check whether the following assertion is true. If H is a normal subgroup of order 2^5 in a 2-group G , then there is no \mathcal{H}_2 -chain in H if and only if H is of maximal class.

We are interested in the following statements concerning a p -group G and all n :

1. Each element of $\mathfrak{O}_n(G)$ is a p^n -th power.
2. $\exp(\Omega_n(G)) \leq p^n$.

$$3. |\Omega_n(G)| = |G : \mathfrak{U}_n(G)|.$$

Definition 5 (see §11). For $i \in \{1, 2, 3\}$, a p -group G is called a \mathcal{P}_i -group, if all sections of G satisfy condition (i) for all n , and G is called a \mathcal{P} -group, if it is a \mathcal{P}_i -group for $i = 1, 2, 3$ simultaneously. (According to Mann, the following unexpected result holds: $\mathcal{P}_3 \subset \mathcal{P}_2 \subset \mathcal{P}_1$.)

Remark 1. For a \mathcal{P} -group G , the following assertions hold:

- (i) $|\Omega_1(G)| \geq |\Omega_2(G)/\Omega_1(G)| \geq |\Omega_3(G)/\Omega_2(G)| \geq \dots,$
- (ii) $|G/\mathfrak{U}_1(G)| \geq |\mathfrak{U}_1(G)/\mathfrak{U}_2(G)| \geq |\mathfrak{U}_2(G)/\mathfrak{U}_3(G)| \geq \dots,$

so that G is pyramidal (see §8). We have $\exp(\Omega_1(G)) = \exp(\Omega_2(G)/\Omega_1(G)) = p$ so $\mathfrak{U}_1(\Omega_2(G)) \leq \Omega_1(G)$ and

$$|\Omega_1(G)| = |\Omega_1(\Omega_2(G))| = |\Omega_2(G)/\mathfrak{U}_1(\Omega_2(G))| \geq |\Omega_2(G)/\Omega_1(G)|.$$

We have, for $k > 1$, $\Omega_k(G)/\Omega_{k-1}(G) = \Omega_1(G/\Omega_{k-1}(G))$. Therefore, the inequality $|\Omega_k(G)/\Omega_{k-1}(G)| \geq |\Omega_{k+1}(G)/\Omega_k(G)|$ follows by induction on k , completing the proof of (i). As to (ii), we have

$$|G/\mathfrak{U}_1(G)| = |\Omega_1(G)| \geq |\Omega_2(G)/\Omega_1(G)| = \frac{|G : \mathfrak{U}_2(G)|}{|G : \Omega_1(G)|} = |\mathfrak{U}_1(G)/\mathfrak{U}_2(G)|.$$

We suggest to the reader to finish the proof of (ii). The groups satisfying (i) and (ii), are called upper and lower pyramidal, respectively. Next we prove that (iii) if $A < G$, then $|A/\mathfrak{U}_1(A)| \leq |G/\mathfrak{U}_1(G)|$. Indeed, $|A/\mathfrak{U}_1(A)| = |\Omega_1(A)| \leq |\Omega_1(G)| = |G/\mathfrak{U}_1(G)|$ since G is a \mathcal{P}_3 -group.

In what follows we use freely the following fact: if $\exp(G) = p^e$ and $k < e$, then $\exp(G/\Omega_k(G)) \leq p^{e-k}$.

Lemma 88.1. Let $F \trianglelefteq G$, where G is a p -group, and let K be a G -invariant subgroup of order p in F . Write $\bar{G} = G/K$.

- (a) Suppose that $\{\bar{1}\} = \bar{F}_0 < \bar{F}_1 < \dots < \bar{F}_n = \bar{F}$ is an \mathcal{H}_p -chain in \bar{F} such that $|\bar{F}_i| = p^{pi}$ for $i = 1, \dots, n$. If all sections of F of order p^{p+1} are \mathcal{P} -groups, then there exists in F an \mathcal{H}_p -chain $\{1\} = L_0 < L_1 < \dots < L_n < L_{n+1} = F$ such that $|F_i : L_i| = p$ for $i = 0, 1, \dots, n$ so that L_n is of order p^{pn} and exponent $\leq p^n$.
- (b) Let k be fixed and suppose that all sections of F of order p^{k+1} are \mathcal{P}_3 -groups. Suppose that $\{\bar{1}\} = \bar{F}_0 < \bar{F}_1 < \dots < \bar{F}_n = \bar{F}$ is an \mathcal{H}_k -chain in \bar{F} such that $|\bar{F}_i| = p^{ki}$ for $i = 1, \dots, n$. Then there exists in F an \mathcal{H}_k -chain $\{1\} = L_0 < L_1 < \dots < L_n < L_{n+1} = F$ such that $|F_i : L_i| = p$ for $i = 0, 1, \dots, n$ so that L_n is of order p^{kn} and exponent $\leq p^n$.

Proof. We proceed by induction on $|F|$.

(a) By hypothesis, F_1 is of order p^{p+1} and F_1/K is of order p^p and exponent p . Suppose that F_1 is irregular. Then $\exp(F) = p^2$ so $K = \Omega_1(F_1)$ and, since F_1 is a \mathcal{P}_3 -group, we get $|\Omega_1(F_1)| = |F_1/\Omega_1(F_1)| = p^p$, and hence $\Omega_1(F_1)$ is of order p^p and exponent p . In that case, we set $L_1 = \Omega_1(F_1)$. Now suppose that F_1 is regular. Then $\Omega_1(F_1) \leq K$ so $|\Omega_1(F_1)| = |F_1/\Omega_1(F_1)| \geq |F_1/K| = p^p$, and we conclude that $\Omega_1(F_1)$ is of order $\geq p^p$ and exponent p . As L_1 we take, in this case, an arbitrary G -invariant subgroup of order p^p in $\Omega_1(F_1)$. If $F_1 = F$, we are done, so we assume that $F_1 < F$. The group F/L_1 is an extension of F_1/L_1 of order p by F/F_1 of order $p^{p(n-1)}$. By induction, there is an \mathcal{H}_p -chain $L_1/L_1 < L_2/L_1 < \dots < L_n/L_1 < F/L_1$ such that $|(F_i/L_1) : (L_i/L_1)| = p$ for all $i = 2, \dots, n$. Then $\{1\} = L_0 < L_1 < \dots < L_n < F$ is the desired chain. (Let $K = F' < F < G$, where G is dihedral of order 16 and F is dihedral of order 8. Then there is an \mathcal{H}_2 -chain in F/K but there is no \mathcal{H}_2 -chain in F . Notice that F is not a \mathcal{P} -group.)

(b) is proved in the same way as (a). \square

Lemma 88.2. Let $F = \Omega_n(H)$ and let $\mathcal{C}_1 : \{1\} = L_0 < L_1 < \dots < L_n = F$ be an \mathcal{H}_k -chain of length n in F .

(a) Suppose that

$$\mathcal{C}_2 : \{1\} < L_{n+1}/L_n < L_{n+2}/L_n < \dots < L_{n+m}/L_n = H/L_n,$$

where $\{L_{n+i}/L_n = \Omega_i(H/L_n)\}$ is an \mathcal{H}_k -chain in the quotient group $H/L_n = H/F$. Then

$$\mathcal{C} : \{1\} = L_0 < L_1 < L_n = F < L_{n+1} < \dots < L_{n+m} = H$$

is an \mathcal{H}_k -chain in H .

(b) If, in addition, $k = p$ and H/F is absolutely regular, then the chain \mathcal{C} from (a) is an \mathcal{H}_p -chain.

Proof. (b) follows from (a) immediately since H/F has an \mathcal{H}_p -chain with $L_{n+i}/L_n = \Omega_i(H/L_n)$. It remains to prove (a).

One may assume that $F < H$; then $\exp(H) > p^n$ so $\exp(F) = p^n$. For $j \leq n$, we have $\Omega_j(F) = \Omega_j(\Omega_n(H)) = \Omega_j(H)$. To prove that \mathcal{C} is an \mathcal{H}_k -chain, it suffices to prove that $L_{n+i} = \Omega_{n+i}(H)$ for $1 \leq i \leq m$. Take $x \in H$ with $o(x) \leq p^{n+i}$. We have to prove that $x \in L_{n+i}$. It follows from $F = L_n = \Omega_n(H)$ and $\exp(L_n) = p^n$ that $\langle x \rangle \cap L_n = \Omega_n(\langle x \rangle)$ so (in H/L_n) we have $o(xL_n) \leq p^i$, and hence $xL_n \in \Omega_i(H/L_n) = L_{n+i}/L_n$. \square

Lemma 88.3. Let \mathcal{C} be an \mathcal{H}_k -chain in H . Then:

- (a) \mathcal{C} is a k -admissible dominating chain,
- (b) all k -admissible dominating chains in H are \mathcal{H}_k -chains.

Proof. Suppose that all considered chains are k -admissible.

(a) Let \mathcal{C}_1 be a dominating chain in H . We have to prove that $|L_i| = |M_i|$ for all i . Let t be such that $|M_t| < p^{kt}$. We have $|L_t| \leq |M_t| < p^{kt}$ and $L_t = \Omega_t(H)$ since \mathcal{C} is an \mathcal{H}_k -chain. Since $\exp(M_t) \leq p^t$, we get $M_t \leq \Omega_t(H) = L_t$ so $L_t = M_t$.

(b) Let \mathcal{C}_1 be an arbitrary dominating chain in H ; we have to show that \mathcal{C}_1 is also an \mathcal{H}_k -chain. By (a), the chain \mathcal{C} is dominating so $|L_i| = |M_i|$ for all i , and we get $i_0 = i_0(\mathcal{C}) = i_0(\mathcal{C}_1)$. Since \mathcal{C} is an \mathcal{H}_k -chain and $\exp(M_{i_0+u}) \leq p^{i_0+u}$, we get $L_{i_0+u} = \Omega_{i_0+u}(H) \geq M_{i_0+u}$ for all $u > 0$ so $M_{i_0+u} = \Omega_{i_0+u}(H)$, and we are done. \square

The point of Lemma 88.3(b) is that if we want to prove that all k -admissible dominating chains in H are \mathcal{H}_k -chains, it suffices to show that at least one of these chains is an \mathcal{H}_k -chain. It follows from this lemma and Theorem 24.1 that all $(p-1)$ -admissible dominating chains in H are \mathcal{H}_{p-1} -chains. If \mathcal{C} and \mathcal{C}_1 are \mathcal{H}_k -chains in H , then $L_{i_0+u} = \Omega_{i_0+u}(H) = M_{i_0+u}$, where $i_0 = i_0(\mathcal{C})$ and $u \geq 1$.

Lemma 88.4. *Let \mathcal{C} be a k -admissible dominating chain in H . Set $\bar{G} = G/L_1$. Then $\bar{\mathcal{C}} : \{\bar{1}\} < \bar{L}_2 < \dots < \bar{L}_n = \bar{H}$ is a k -admissible dominating chain in \bar{H} .*

Proof. Indeed, suppose that $\bar{\mathcal{C}}$ is a k -admissible dominating chain in \bar{H} and assume that $\bar{\mathcal{C}}_1 > \bar{\mathcal{C}}$; then the chain \mathcal{C}_1 , which is the ‘inverse image’ of the chain $\bar{\mathcal{C}}_1$, is k -admissible and satisfies $\mathcal{C}_1 > \mathcal{C}$, a contradiction. \square

If $\bar{\mathcal{C}}$ is a k -admissible dominating chain in $\bar{G} = G/N$ (here N is of order p^k and exponent p), then its inverse image \mathcal{C} is k -admissible but can be not dominating in G . Indeed, let $G = U \times V \times W$, where U, V and W are cyclic of orders p, p, p^2 , respectively. Let $k = 2$ and $L_1 = U \times V$, $\bar{G} = G/L_1$. Then the chain \mathcal{C} with $L_i = L_1 \times \Omega_{i-1}(W)$, $i = 1, 2, 3$, is not an \mathcal{H}_2 -chain in G although $\{\bar{1}\} < \bar{L}_2 < \bar{L}_3 = \bar{G}$ is an \mathcal{H}_2 -chain in the cyclic p -group \bar{G} . Indeed, if $M_1 = U \times \Omega_1(W)$ and $M_2 = G$, then the chain $\mathcal{C}_1 : \{1\} < M_1 < M_2 = G$ dominates strongly over \mathcal{C} .

Lemma 88.5 follows easily from Theorems 9.5 and 9.6.

Lemma 88.5. *Let G be an irregular p -group of maximal class. Then:*

- (a) *All sections of G of order p^{p+1} are \mathcal{P}_3 -groups if and only if $|G| = p^{p+1}$ and $|\Omega_1(G)| = p^p$.*
- (b) *All sections of G of order p^{p+1} are \mathcal{P}_2 -groups if and only if $|G| = p^{p+1}$ and $\Omega_1(G) < G$.*

Assuming, for example, that in (b), $|G| > p^{p+1}$, we get $\exp(G/Z(G)) > p$ and $\Omega_1(G/Z(G)) = G/Z(G)$, which is a contradiction

Lemma 88.6. *If H has a G -invariant subgroup B of order p^p and exponent p , then each maximal G -invariant subgroup of H of exponent p is of order $\geq p^p$.*

Proof. Let A be a maximal G -invariant subgroup of exponent p in H . We have to prove that $|A| \geq p^p$. Assume that this is false; then $A \not\leq B$. Let $R < B$ be a least G -invariant subgroup such that $R \not\leq A$. Then $|A| < |AR| = p|A| \leq p^p$ so AR is regular. It follows from $\Omega_1(AR) = AR$ that $\exp(AR) = p$, contrary to the choice of A . \square

Lemma 88.7 (= Theorem 13.5). *Let a p -group G be neither absolutely regular nor of maximal class. Then the number of subgroups of order p^p and exponent p in G is $\equiv 1 \pmod{p}$.*

Let G be a p -group. Set $\mathfrak{V}^1(G) = \mathfrak{V}_1(G)$. If $\mathfrak{V}^i(G)$ has been defined, we set $\mathfrak{V}^{i+1}(G) = \mathfrak{V}_1(\mathfrak{V}^i(G))$. Since $\exp(G/\mathfrak{V}^k(G)) \leq p^k$, we get $\mathfrak{V}_k(G) \leq \mathfrak{V}^k(G)$ for all $k > 0$. If G is a \mathcal{P} -group of exponent p^e , then $\mathfrak{V}^i(G) = \mathfrak{V}_i(G)$ for all i .

Lemma 88.8. *Let $|G| = p^m$, $\exp(G) \leq p^e$ and $m \leq pe$. Then $\mathfrak{V}^{e-1}(G)$ is either absolutely regular or of order p^p and exponent $\leq p$. In either case, $\mathfrak{V}_{e-1}(G) (\leq \mathfrak{V}^{e-1}(G))$ is of exponent p . If, in addition, $m < pe$, then we have $|\Omega_1(\mathfrak{V}^{e-1}(G))| < p^p$ so $\mathfrak{V}_{e-1}(G)$ is of order $\leq p^{p-1}$ and exponent p .*

For a proof, see §24.

The following two assertions hold:

- (a) Let G be an absolutely regular p -group. If $|G| > p^{(p-1)k}$, then $\exp(G) > p^k$.
- (b) Let G be a p -group of maximal class and order p^m , $m > p + 1$. If $m - 1 = (p - 1)k$, then $\exp(G) = p^k$. If $m - 1 > (p - 1)k$, then $\exp(G) > p^k$. Assertion (i) follows since absolutely regular p -groups are pyramidal. As to (ii), a p -group G of maximal class has an absolutely regular subgroup G_1 of order p^{m-1} (the fundamental subgroup of G), and $\exp(S) = \exp(G)$ so the result follows from (i).

Lemma 88.9. (a) *Let H be of order p^{pe} and exponent $\leq p^e$. Then all indices of any p -admissible dominating chain in H equal p^p so it is an \mathcal{H}_p -chain of length e .*

(b) *Let $H \leq G$ be a pyramidal \mathcal{P}_2 -subgroup of order p^{ke} and exponent $\leq p^e$. Then all indices of any k -admissible dominating chain in H equal p^k so it is an \mathcal{H}_k -chain of length e .*

Proof. By agreement, $H \trianglelefteq G$. One may assume that $e > 1$. We use induction on $|H|$.

(a) By the paragraph preceding the lemma, H is neither absolutely regular nor of maximal class. Therefore, by Lemma 88.7, H has a G -invariant subgroup, say R_1 , of order p^p and exponent p . Suppose that $\exp(H) < p^e$. Then $\exp(H/R_1) \leq p^{e-1}$ and $|H/R_1| = p^{p(e-1)}$. Therefore, by induction, there is in H/R_1 an \mathcal{H}_p -chain $\{1\} = R_1/R_1 = T_1/R_1 < T_2/R_1 < \dots < T_e/R_1 = H/R_1$, and all indices of this chain are equal p^p . In that case, $\{1\} < T_1 < \dots < T_e = H$ is the desired \mathcal{H}_p -chain. Therefore,

one may assume, in what follows, that $\exp(H) = p^e$. In that case, $\Omega_{e-1}(H)$ is of order $\leq p^p$ and exponent $\leq p$ (Lemma 88.8 so $\Omega_{e-1}(H) \leq R$, where $R < H$ is a G -invariant subgroup of order p^p and exponent p (Lemma 88.6). Then H/R is a normal subgroup of order $p^{p(e-1)}$ and exponent $\leq p^{e-1}$ in G/R . By induction, there exists an \mathcal{H}_p -chain $\{1\} = R/R = L_1/R < L_2/R < \dots < L_e/R = H/R$ in H/R such that all indices of this chain equal p^p , and so $\{1\} < R = L_1 < L_2 < \dots < L_e = H$ is the desired \mathcal{H}_p -chain.

(b) Since H is lower pyramidal, $|\Omega_{e-1}(H)| \leq p^k$. Since $\Omega_{e-1}(H)$ is generated by elements of order $\leq p$, we get $\exp(\Omega_{e-1}(H)) \leq \exp(\Omega_1(H)) = p$. Since H is upper pyramidal, we get $|\Omega_1(H)| \geq p^k$. Let $\Omega_{e-1}(H) \leq R \leq \Omega_1(H)$, where R is G -invariant of order p^k . Then H/R is of order $p^{k(e-1)}$ and exponent $\leq p^{e-1}$. Now the result follows by induction in H/R , as in (a). \square

Remark 2. Let H be a normal subgroup of order $\leq p^{pe}$ and exponent p^e in a p -group G . Suppose that there exists an \mathcal{H}_p -chain $\mathcal{C} : \{1\} = L_0 < L_1 < \dots < L_n = H$ in H . We claim that then $n = e$. Indeed, this is trivial for $e = 1$ so we assume that $e > 1$. Clearly, $n \geq e$. Assume that $n > e$. Then $|L_{n-1}| < |H| \leq p^{pe} \leq p^{p(n-1)}$ so $\Omega_{n-1}(H) = L_{n-1} < H$ since \mathcal{C} is an \mathcal{H}_p -chain. It follows that $\exp(L_{n-1}) = p^{n-1} \geq p^e$, a contradiction since $\Omega_{n-1}(H) = H$.

Suppose that G is a group of order p^n possessing an \mathcal{H}_k -chain, say $\mathcal{C} : \{1\} = L_0 < L_1 < \dots < L_{i_0} < \dots < G$. Let $n = [n/k]k + s$, where $s < k$. Assume that $|\Omega_t(G)| \geq p^{kt}$ for all $t \leq [n/k]$. We claim that then $i_0 = i_0(\mathcal{C}) = [n/k]$, where $[x]$ is the integer part of the real number x . Clearly, $i_0 \leq [n/k]$. Assume that $i_0 < [n/k]$. Then $|\Omega_{i_0+1}(G)| < p^{k(i_0+1)}$ so, since $i_0+1 \leq [n/k]$, we get $|\Omega_{[n/k]}(G)| < p^{[n/k]k}$, contrary to the assumption.

Let \mathcal{C} be an \mathcal{H}_k -chain of length n in H with $i_0 = i_0(\mathcal{C})$. Suppose that $\exp(L_{i_0}) < p^{i_0}$. We claim that then $n \leq i_0 + 1$. Assume that $n > i_0 + 1$. We have $\exp(L_{i_0+1}) < p^{i_0+1}$. Since $\Omega_{i_0+1}(H) = L_{i_0+1} < H$, it follows that $\exp(L_{i_0+1}) = p^{i_0+1}$, contrary to what has just been said.

Let \mathcal{C} be a k -admissible chain in H . We use freely the following assertions. (i) If $|\mathcal{C}| = i_0(\mathcal{C}) + 1$, then \mathcal{C} is an \mathcal{H}_k -chain. (ii) If $i < j$ and $|L_i| < p^{ki}$, then $|L_j| < p^{kj}$.

Remark 3. Suppose that G is irregular p -group of maximal class (i) If G has an \mathcal{H}_p -chain, then either $|G| = p^{p+1}$ or $p^{p+1} < |G| < p^{2p}$ and $|\Omega_1(G)| = p^{p-1}$. (ii) Conversely, if $|\Omega_1(G)| = p^{p-1}$ and $|G| < p^{2p}$, then G has the unique \mathcal{H}_p -chain $\{1\} < \Omega_1(G) < G$ of length 2. Let us prove these assertions using results §9. Let \mathcal{C} be an \mathcal{H}_p -chain in G and assume that $|G| > p^{p+1}$. Since G has no normal subgroups of order p^p and exponent p , we get $|\Omega_1(G)| = p^{p-1}$. Since $|L_2| < p^{2p}$, we get $L_2 = \Omega_2(G)$. Since $\Omega_2(G) = G$, we have $|G| < p^{2p}$. In that case, $\mathcal{C} : \{1\} < \Omega_1(G) < G$. Next, any group G of order p^{p+1} has an \mathcal{H}_p -chain. This is obvious provided G is regular. If G is irregular, $\Phi(G)$ is of order p^{p-1} and exponent

p . If $\Omega_1(G) = \Phi(G)$, then $\{1\} < \Phi(G) < G$ is an \mathcal{H}_p -chain. If $\Omega_1(G) > \Phi(G)$, then G has a maximal subgroup M of exponent p ; then $\{1\} < M < G$ is an \mathcal{H}_p -chain. Now assertion (ii) is obvious.

If a subgroup H has a G -invariant subgroup R of order p^k and exponent p such that $\exp(H/R) = p$, then H has an \mathcal{H}_k -chain. Indeed, H/R has an \mathcal{H}_k -chain $R/R = L_1/R < L_2/R < \dots < L_n/R = H/R$. Then $\{1\} < L_1 < L_2 < \dots < L_n = H$ is an \mathcal{H}_k -chain in H .

Theorem 88.10. *Let $H > \{1\}$ be a normal \mathcal{P}_2 -subgroup of a p -group G . Suppose, in addition, that every irregular section of H of order p^{p+1} has a (characteristic) subgroup of order p^p and exponent p . Then there exists in H a chain*

$$\mathcal{C} : \{1\} = L_0 < L_1 < \dots < L_n = H$$

of G -invariant subgroups with the following properties ($i = 1, \dots, n$):

- (a) L_i/L_{i-1} is of order $\leq p^p$ and exponent p , and
- (b) either $|L_i| = p^{pi}$ or else $L_i = \Omega_i(H)$.

In other words, there is in H an \mathcal{H}_p -chain. Then it follows from Lemma 88.3(b) that each p -admissible dominating chain in H is an \mathcal{H}_p -chain. Next, if, in our theorem, $p = 2$, then the subgroup H is powerful, i.e., $H/\mathfrak{U}_2(H)$ is abelian (see subsection 2^o of §26). To prove this, we suppose that H is a minimal counterexample. By hypothesis, all sections of H of order 8 are abelian so H is also modular (Iwasawa). One may assume that $\exp(H) = 4$. Then H is minimal nonabelian so $|H| \leq 2^5$. It follows from Redei's classification of minimal nonabelian 2-groups that H has a nonabelian section of order 8, contrary to the hypothesis. In what follows, we do not use this result. Also note that if U is an irregular section of G of order p^{p+1} , then $|\Omega_1(U)| = |U/\mathfrak{U}_1(U)| = p^p$. Indeed, $|U/\mathfrak{U}_1(U)| = p^p$ (Theorem 9.5). Next, $|\Omega_1(U)| \geq p^p$, by hypothesis. Since U is a \mathcal{P}_2 -group and $\exp(U) > p$, we get $|\Omega_1(U)| < U$ so $|\Omega_1(U)| = p^p$, completing the proof.

Proof of Theorem 88.10. If $\{1\} < N \leq H$ is G -invariant, then the pairs $H/N \leq G/N$ and $N \leq G$ satisfy the hypothesis. We use induction on $|H|$. Let $\exp(H) = p^e$.

(i) Assume that H has no G -invariant subgroups of order p^p and exponent p . Then H is either absolutely regular so $\{1\} = \Omega_0(H) < \Omega_1(H) < \dots < \Omega_e(H) = H$ is an \mathcal{H}_p -chain in H , or of maximal class and order p^{p+1} (Theorem 12.1(a) and Lemma 88.5), contrary to the assumption (by hypothesis, every irregular section of H of order p^{p+1} has a characteristic subgroup of order p^p and exponent p).

In the sequel we assume that H has a G -invariant subgroup of order p^p and exponent p . Since the theorem is trivial for $e = 1$, we also assume that $e > 1$.

Let $F_0 < H$ be a G -invariant subgroup of order p and set $\bar{G} = G/F_0$. By induction, there exists an \mathcal{H}_p -chain $\bar{\mathcal{C}}' : \{1\} = \bar{F}_0 < \bar{F}_1 < \dots < \bar{F}_n = \bar{H}$ in \bar{H} . Write

$i_0 = i_0(\bar{\mathcal{C}}')$. By Lemma 88.1, there exists an \mathcal{H}_p -chain $\mathcal{C}'' : \{1\} = L_0 < L_1 < \dots < L_{i_0} < F_{i_0}$ in F_{i_0} with $|F_{i_0} : L_{i_0}| = p$, so that

(α) F_{i_0} contains a G -invariant subgroup L_{i_0} of order p^{pi_0} and exponent $\leq p^{i_0}$.

Therefore, one may assume that $i_0 < n$ (otherwise, \mathcal{C}'' is the desired chain; see the paragraph preceding Remark 3) so $F_{i_0} < F_{i_0+1}$. Next, $H/F_{i_0} (\cong \bar{H}/\bar{F}_{i_0})$ has no G -invariant subgroups of order p^P and exponent p (otherwise, if $U/F_{i_0} \leq H/F_{i_0}$ is such a subgroup, then the p -admissible chain $\{\bar{1}\} = \bar{F}_0 < \bar{F}_1 < \dots < \bar{F}_{i_0} < \bar{U} < \dots < \bar{H}$ dominates strongly over $\bar{\mathcal{C}}'$, contrary to Lemmas 88.4 and 88.3(a)). Therefore, by Lemma 88.7, H/F_{i_0} is either absolutely regular or irregular of maximal class. Assume that H/F_{i_0} is irregular of maximal class. Then $|H/F_{i_0}| = p^{p+1}$ (Lemma 88.5(b)). In that case, H/F_{i_0} has a characteristic subgroup U/F_{i_0} of order p^P and exponent p , contrary to what has just been said. Thus, H/F_{i_0} is absolutely regular so H/L_{i_0} is regular, by Remark 7.2. We have

(β) H/F_{i_0} is absolutely regular, H/L_{i_0} is regular (Remark 7.2) and

$$|\Omega_1(H/L_{i_0})| \leq p \cdot |\Omega_1(H/F_{i_0})| \leq p \cdot p^{p-1} = p^P,$$

and so:

(γ) If $j \geq i_0 + 1$, then $|\bar{F}_j| < p^{pj}$ so that $|F_j| \leq p^{pj}$.

Since $\bar{\mathcal{C}}'$ is an \mathcal{H}_p -chain, one has $\Omega_{i_0+1}(\bar{H}) = \bar{F}_{i_0+1}$, so, by Remark 24.3,

(δ) $\Omega_{i_0+1}(H) \leq F_{i_0+1}$ hence $\Omega_{i_0+1}(H) = \Omega_{i_0+1}(F_{i_0+1})$ so, if $F_{i_0+1} < H$, then $\exp(\bar{F}_{i_0+1}) \geq p^{i_0+1}$.

Since $\exp(\bar{F}_i) \leq p^i$, we get $\exp(F_i) \leq p \cdot \exp(\bar{F}_i) \leq p^{i+1}$ for all i so

(ϵ) $\exp(F_{i_0+1}) \leq p^{i_0+2}$. Therefore, the following three possibilities must be considered: $\exp(F_{i_0+1}) \leq p^{i_0}$, $\exp(F_{i_0+1}) = p^{i_0+1}$, $\exp(F_{i_0+1}) = p^{i_0+2}$.

Suppose that $i_0 = 0$. Then $\bar{F}_1 = \Omega_1(\bar{H})$ is of order $< p^P$, by (δ), so $F_1 = \Omega_1(H)$ is of order p^P and exponent p since, by assumption, H has a G -invariant subgroup of order p^P and exponent p , and $H/\Omega_1(H) = H/F_1$ is absolutely regular, by (β). In this case, by Lemma 88.2(b), there exists an \mathcal{H}_p -chain in H .

Next we assume that $i_0 > 0$; then $|F_1| = p^{p+1}$ and $\exp(F_1) \leq p^2$.

(ii) Suppose that $\exp(F_{i_0+1}) < p^{i_0+1}$. Then, by (δ), $F_{i_0+1} = H$ so $i_0 + 1 = n$. We also have $|H| = |F_{i_0+1}| \leq p^{p(i_0+1)}$. Let $\{1\} = L_0 < L_1 < \dots < L_{i_0} < F_{i_0}$ be an \mathcal{H}_p -chain in F_{i_0} with $|F_{i_0} : L_{i_0}| = p$ (Lemma 88.1).

If $\exp(H/L_{i_0}) = p$, then $\{1\} = L_0 < L_1 < \dots < L_{i_0} < H$ is an \mathcal{H}_p -chain in H since all indices of this chain but last one are equal to p^P and $|H : L_{i_0}| \leq p^P$. Since $\exp(H/L_{i_0}) \leq p^2$, one may assume that $\exp(H/L_{i_0}) = p^2$. Therefore, since $H/F_{i_0} (= F_{i_0+1}/F_{i_0})$ is of order $\leq p^{p-1}$ and exponent p , the G -invariant subgroup $U/L_{i_0} = \Omega_1(H/L_{i_0})$ is of exponent p and index p in H/L_{i_0} . In that case, $\{1\} = L_0 < L_1 < \dots < L_{i_0} < U$ is an \mathcal{H}_p -chain in U since only the last index of this chain is $< p^P$. Since $\exp(H/F_{i_0}) = p$ and $|H/F_{i_0}| \leq p^{p-1}$, we get $\Omega_1(H) < F_{i_0}$ since

H is not absolutely regular, by Hall's regularity criterion (Theorem 9.8(a)). It follows that $|\mathfrak{U}_1(H)| \leq p^{-p} \cdot |H| \leq p^{pi_0}$. Therefore, there exists a G -invariant subgroup T_{i_0} satisfying $\mathfrak{U}_1(H) \leq T_{i_0} < F_{i_0}$ and $|T_{i_0}| = p^{pi_0}$. Since, in addition, we also have $\exp(T_{i_0}) \leq \exp(H) \leq p^{i_0}$, there exists an \mathcal{H}_p -chain $\{1\} = T_0 < T_1 < \dots < T_{i_0}$ in T_{i_0} of length i_0 and all indices of that chain equal p^P (Lemma 88.9(a)). Then $\{1\} = T_0 < T_1 < \dots < T_{i_0} < H$ is an \mathcal{H}_p -chain in H since $|H/T_{i_0}| \leq p^P$ and $\exp(H/T_{i_0}) = p$.

(iii) Let $\exp(F_{i_0+1}) = p^{i_0+1}$. By (δ) , $\Omega_{i_0+1}(H) = F_{i_0+1}$, and H/F_{i_0+1} is absolutely regular, by (β) .

Suppose that $F_{i_0+1} < H$. To prove that there is an \mathcal{H}_p -chain in H , it suffices to show, in view of Lemma 88.2(b), that F_{i_0+1} has an \mathcal{H}_p -chain of length $i_0 + 1$. Let $U = \Omega_{i_0}(F_{i_0+1}) (= \Omega_{i_0}(H))$; then $\exp(U) = p^{i_0}$ since H is a \mathcal{P}_2 -group and $\exp(F_{i_0+1}) = p^{i_0+1}$. Since $L_{i_0} \leq U$, we get $|U| \geq |L_{i_0}| = p^{pi_0}$. We have $\exp(F_{i_0+1}/U) = p$ since the \mathcal{P}_2 -group F_{i_0+1}/U is generated by elements of order p . It follows that $\mathfrak{U}_1(F_{i_0+1}) \leq U$. Since $i_0 > 0$, we get $|F_{i_0+1}/\mathfrak{U}_1(F_{i_0+1})| \geq p^P$ so $|\mathfrak{U}_1(F_{i_0+1})| \leq p^{-P}|F_{i_0+1}| \leq p^{pi_0}$. It follows that there is a G -invariant subgroup T_{i_0} of order p^{pi_0} such that $\mathfrak{U}_1(F_{i_0+1}) \leq T_{i_0} \leq U$; then $\exp(T_{i_0}) \leq \exp(U) = p^{i_0}$. By Lemma 9(a), there is an \mathcal{H}_p -chain $\{1\} = T_0 < T_1 < \dots < T_{i_0}$ in T_{i_0} of length i_0 , and all indices of that chain equal p^P . Then $\{1\} = T_0 < T_1 < \dots < T_{i_0} < F_{i_0+1}$ is an \mathcal{H}_p -chain in F_{i_0+1} of length $i_0 + 1$ since $\exp(F_{i_0+1}/T_{i_0}) = p$ and $|F_{i_0+1}/T_{i_0}| \leq p^P$.

Now we assume that $F_{i_0+1} = H$; then $\exp(H) = p^{i_0+1}$ and $p^{pi_0} = |L_{i_0}| < |H| \leq p^{p(i_0+1)}$. Write $U = \Omega_{i_0}(H)$; then $\exp(U) = p^{i_0}$ since H is a \mathcal{P}_2 -group, $\exp(H/U) = p$ (see the paragraph following Remark 1) and $|U| \geq |L_{i_0}| = p^{pi_0}$ so $|H : U| \leq p^P$. In that case, there exists a G -invariant subgroup T_{i_0} of order p^{pi_0} such that $\mathfrak{U}_1(H) \leq T_{i_0} \leq U$ since $|H : \mathfrak{U}_1(H)| \geq p^P$: H is not absolutely regular. We have $\exp(T_{i_0}) \leq \exp(U) = p^{i_0}$ and $\exp(H/T_{i_0}) = p$. Therefore, if $\mathcal{C}' : \{1\} = T_0 < T_1 < \dots < T_{i_0}$ is an \mathcal{H}_p -chain in T_{i_0} all of whose indices equal p^P (Lemma 88.9(a)), then $\{1\} = T_0 < T_1 < \dots < T_{i_0} < H$ is an \mathcal{H}_p -chain in H since $|H/T_{i_0}| \leq p^P$.

(iv) It remains to consider the possibility $\exp(F_{i_0+1}) = p^{i_0+2}$; then $\exp(F_{i_0}) = p^{i_0+1}$ since $\exp(F_{i_0}) \leq p^{i_0+1}$ and $p^{i_0+2} = \exp(F_{i_0+1}) \leq p \cdot \exp(F_{i_0})$. By (δ) , $\Omega_{i_0+1}(H) = \Omega_{i_0+1}(F_{i_0+1})$. By (γ) , $|F_{i_0+1}| \leq p^{p(i_0+1)}$.

(iv1) First suppose that $F_{i_0+1} < H$ and let $\mathcal{C}' : \{1\} = L_0 < L_1 < \dots < L_{i_0} < \dots < F_{i_0+1}$ be an \mathcal{H}_p -chain in F_{i_0+1} existing by induction. By (β) , H/L_{i_0} is regular and $|\Omega_1(H/L_{i_0})| \leq p^P$. We have $L_{i_0+1} = \Omega_{i_0+1}(F_{i_0+1}) (= \Omega_{i_0+1}(H))$ since \mathcal{C}' is an \mathcal{H}_p -chain. Also, $L_{i_0+1} < F_{i_0+1}$ in view of $\exp(L_{i_0+1}) \leq p^{i_0+1}$ and (δ) . Next, $L_{i_0+1}/L_{i_0} = \Omega_1(H/L_{i_0})$ (indeed, if $D/L_{i_0} = \Omega_1(H/L_{i_0})$, then $\exp(D) \leq p^{i_0+1}$ so $D \leq \Omega_{i_0+1}(H) = \Omega_{i_0+1}(F_{i_0+1}) = L_{i_0+1}$), so $F_{i_0} \leq L_{i_0+1}$. It follows that H/L_{i_0+1} is absolutely regular as an epimorphic image of H/F_{i_0} (see (β)). In that case, there is an \mathcal{H}_p -chain in H since $\{1\} = L_0 < L_1 < \dots < L_{i_0} < L_{i_0+1}$ is an \mathcal{H}_p -chain in $L_{i_0+1} = \Omega_{i_0+1}(H)$ of length $i_0 + 1$ (Lemma 88.2(b)).

(iv2) Now let $F_{i_0+1} = H$; then $|H| \leq p^{p(i_0+1)}$ and $\exp(H) = p^{i_0+2}$. Set $U = \Omega_{i_0+1}(H)$; then $\exp(U) = p^{i_0+1}$ since H is a \mathcal{P}_2 -group, $\exp(H/U) = p$ since $\Omega_1(H/U) = H/U$ and U contains a G -invariant subgroup L_{i_0} of order p^{pi_0} and exponent p^{i_0} . By induction, there is in U an \mathcal{H}_p -chain, say $\mathcal{C}' : \{1\} = L_0 < L_1 < \dots < L_{i_0} < \dots < U$. We have $L_{i_0+1} = \Omega_{i_0+1}(U) = U$ so $|\mathcal{C}'| = i_0 + 1$. It follows that $\{1\} = L_0 < L_1 < \dots < L_{i_0} < L_{i_0+1} = U < H$ is an \mathcal{H}_p -chain in H since H/U is of order $< |H/L_{i_0}| \leq p^p$ and exponent p . \square

Theorem 88.11. *Let $H > \{1\}$ be a normal \mathcal{P} -subgroup of a p -group G and let k be fixed. Then there exists in H a chain*

$$\mathcal{C} : \{1\} = L_0 < L_1 < \dots < L_n = H$$

of G -invariant subgroups with the following properties ($i = 1, \dots, n$):

- (a) L_i/L_{i-1} is of order $\leq p^k$ and exponent p , and
- (b) either $|L_i| = p^{ik}$ or $L_i = \Omega_i(H)$.

It is possible to prove Theorem 88.11 in the same way as Theorem 88.10, however, the offered proof is shorter and more elementary.

Proof of Theorem 88.11. We proceed by induction on $|H|$. Set $\exp(H) = p^e$ and assume that $e > 1$ and $k > 1$ (otherwise, there is nothing to prove).

(i) Suppose that H has no G -invariant subgroups of order p^k and exponent p . Then $|\Omega_1(H)| < p^k$. Since H is a pyramidal (Remark 1) \mathcal{P} -group, $\{1\} < \Omega_1(H) < \dots < \Omega_e(H) = H$ is the unique \mathcal{H}_k -chain in H .

In what follows we assume that H has a G -invariant subgroup of order p^k and exponent p so $|H : \Omega_1(H)| = |\Omega_1(H)| \geq p^k$ since H is a \mathcal{P}_3 -group.

(ii) Suppose that H is of order p^{tk} with $e \leq t$. In that case, the theorem is true, by Lemma 88.9(b).

(iii) Suppose that H is of order p^{tk+s} with $t \geq e$ and $1 \leq s < k$; then $|\Omega_1(H)| \leq p^{-k} \cdot |H| < p^{tk}$ since H is a \mathcal{P}_3 -group. Therefore, there exists a G -invariant subgroup $U < H$ of order p^{tk} such that $\Omega_1(H) < U$. We have $\exp(U) \leq p^e \leq p^t$ so, by Lemma 88.9(b), there is an \mathcal{H}_k -chain $\{1\} = U_0 < U_1 < \dots < U_t = U$ of length t ; since all indices of that chain are equal to p^k and H/U is of order $p^s < p^k$ and exponent p , it follows that $\{1\} = U_0 < U_1 < \dots < U_t < H$ is an \mathcal{H}_k -chain in H .

(iv) Suppose that $|\Omega_t(H)| = p^{tk}$ for some $t \leq e$. If $t = e$, then there is an \mathcal{H}_k -chain in H (Lemma 88.9(b) and Remark 1). Now let $t < e$; then $\exp(\Omega_t(H)) = p^t$ since H is a \mathcal{P}_2 -group. By Lemma 88.9(b), there is an \mathcal{H}_k -chain $\{1\} = L_0 < L_1 < \dots < L_t = \Omega_t(H)$ of length t in $\Omega_t(H)$, and all indices of this chain are equal to p^k . Set $\tilde{G} = G/L_t$. By induction, there is an \mathcal{H}_k -chain $\{\bar{1}\} < \bar{L}_{t+1} < \dots < \bar{L}_{t+m} = \bar{H}$ in \bar{H} . Then, by Lemma 88.2(a), $\{1\} = L_0 < L_1 < \dots < L_t < L_{t+1} < \dots < L_{t+m} = H$ is an \mathcal{H}_k -chain in H .

(v) Suppose that $|\Omega_t(H)| > p^{tk}$ for all $t \leq e$. In particular, $|H| > p^{ek}$. Then $|H| = p^{t_0k+s}$ for some positive integers t_0 and $s < k$. It follows that $p^{ek} < p^{t_0k+s}$ so $t_0 \geq e$. As we have noticed, $|H : \Omega_1(H)| \geq p^k$. Let $U_{t_0}/\Omega_1(H)$ be a G -invariant subgroup of index p^s in $H/\Omega_1(H)$; then $|U_{t_0}| = p^{t_0k}$ and $\exp(U_{t_0}) \leq p^e \leq p^{t_0}$. By Lemma 88.9(b), there is an \mathcal{H}_k -chain $\{1\} = U_0 < U_1 < \dots < U_{t_0}$ in U_{t_0} with all indices equal p^k ; then $\{1\} = U_0 < U_1 < \dots < U_{t_0} < H$ is an \mathcal{H}_k -chain in H .

(vi) Suppose that $|\Omega_t(H)| < p^{tk}$ for some positive $t \leq e$. Let t be minimal subjecting to that inequality. Then $t > 1$ since H has a G -invariant subgroup of order p^k and exponent p . By the choice of t , we get $|\Omega_{t-1}(H)| \geq p^{(t-1)k}$. In view of (iv), one may assume that $|\Omega_{t-1}(H)| > p^{(t-1)k}$. It follows that $|\Omega_t(H)/\Omega_{t-1}(H)| < p^{k-1}$ so that $|\Omega_1(H/\Omega_{t-1}(H))| < p^{k-1}$ (indeed, if $A/\Omega_{t-1}(H) \leq H/\Omega_{t-1}(H)$ is of order p^{k-1} and exponent p , then $A \leq \Omega_t(H)$ and A is of order $\geq p^{tk} > |\Omega_t(H)|$, which is not the case). Thus, the quotient group $H/\Omega_{t-1}(H)$ is pyramidal (Remark 1) and has no normal subgroups of order p^k and exponent p . So, setting $\bar{G} = G/\Omega_{t-1}(H)$, we conclude that $\{\bar{1}\} < \Omega_1(\bar{H}) < \dots < \bar{H}$ is an \mathcal{H}_k -chain in \bar{H} . Therefore, in view of Lemma 88.2, it suffices to prove that there is in $\Omega_t(H)$ an \mathcal{H}_k -chain of length $t - 1$. Assume that this is false; then the length of our chain is $> t - 1$ so let $\{1\} = T_0 < T_1 < \dots < T_{t-1} < \dots < \Omega_{t-1}(H)$ be an \mathcal{H}_k -chain in $\Omega_{t-1}(H)$. Since $T_{t-1} < \Omega_{t-1}(H)$, we get $|T_{t-1}| = p^{(t-1)k}$. By assumption, H/T_{t-1} has no normal subgroup of order p^k and exponent p . It follows from Lemma 88.2(b) that there is an \mathcal{H}_k -chain in H . \square

Let G be an arbitrary p -group of order p^n . Then $W = G \times E$, where E is the elementary abelian p -group of order $p^{n(k-1)}$, has a chain of normal subgroups of length n all of whose factors are of order p^k and exponent p .

Let G be an abelian p -group of exponent $p^e > p$. We claim that G is homocyclic if and only if $\Omega_{e-1}(G) = \Omega_1(G)$. Suppose that the last equality holds. Set $|\Omega_1(G)| = p^d$. Then $d = d(G)$ so $G = Z_1 \times \dots \times Z_d$, where Z_i are all cyclic. In that case, $\Omega_{e-1}(G) = \Omega_{e-1}(Z_1) \times \dots \times \Omega_{e-1}(Z_d)$ is of order p^d so $|\Omega_{e-1}(Z_i)| = p$ for all i , and so G is homocyclic. The converse assertion is obvious.

Remark 4. Given a normal subgroup H of a p -group G , let $Ch_k(H)$ be the number of \mathcal{H}_k -chains in H . We claim that if $\mathcal{C} : \{1\} = L_0 < L_1 < \dots < L_n = G$ is an \mathcal{H}_k -chain in G , then $Ch_k(G) \geq Ch_k(L_j)$ for all $j \leq n$. This is true for $j \leq i_0 = i_0(\mathcal{C})$. Now let $j > i_0$; then $L_j = \Omega_j(G)$. Assume that $\{1\} = M_0 < M_1 < \dots < M_j = L_j$ is an \mathcal{H}_k -chain in L_j . Then

$$\mathcal{C}' : \{1\} = M_0 < M_1 < \dots < M_j = L_j < L_{j+1} < \dots < L_n = G$$

is an \mathcal{H}_k -chain in G . Let $j > i_0$ and $i_0 < i_1 \leq j$. Then $M_{i_1} = \Omega_{i_1}(M_j) = \Omega_{i_1}(L_j) = \Omega_{i_1}(\Omega_j(G)) = \Omega_{i_1}(G)$. If $i_2 > j$, then $L_{i_2} = \Omega_{i_2}(G)$ so \mathcal{C}' is an \mathcal{H}_k -chain in G , and we are done.

Corollary 88.12. *An abelian p -group G has exactly one \mathcal{H}_k -chain if and only if $|\Omega_1(G)| \leq p^k$.*

Proof. Let $\exp(G) = p^e$. If $|\Omega_1(G)| \leq p^k$, then $\{1\} < \Omega_1(G) < \dots < \Omega_e(G) = G$ is the unique \mathcal{H}_k -chain in G . It remains to prove that if G has exactly one \mathcal{H}_k -chain, then $|\Omega_1(G)| \leq p^k$. Assume that G is a counterexample of minimal order; then $k > 1$, $e > 1$ and $|\Omega_1(G)| > p^k$. It follows that $|G/\mathfrak{U}_1(G)| = |\Omega_1(G)| > p^k$. By Theorem 88.11, there is in G an \mathcal{H}_k -chain $\mathcal{C} : \{1\} < L_1 < \dots < L_n = G$, and this chain is unique; by assumption, $|L_1| = p^k$. Since, by Remark 4, $Ch_k(L_j) = 1$, we get, by induction, $|\Omega_1(L_j)| = p^k$ for $1 \leq j < n$. Set $i_0 = i_0(\mathcal{C})$.

(i) Suppose that $n > i_0 + 1$. Then $L_{i_0+1} < G$ and $\Omega_{i_0+1}(G) = L_{i_0+1}$. By the previous paragraph, $|\Omega_1(L_{i_0+1})| = p^k$, contrary to the assumption since $\Omega_1(G) = \Omega_1(L_{i_0+1})$. Thus, $n \leq i_0 + 1$.

(ii) Suppose that $n = 2$. Then $|G| \leq p^{2k}$ so $|\mathfrak{U}_1(G)| = |G/\Omega_1(G)| < p^k$ whence $\mathfrak{U}_1(G) < \Omega_1(G)$ and $|\Omega_1(G) : \mathfrak{U}_1(G)| \geq p^2$. Let $\mathfrak{U}_1(G) < L_1 < \Omega_1(G)$, where $|L_1| = p^k$; then $\{1\} < L_1 < G$ is an \mathcal{H}_k -chain. However, L_1 can be chosen in more than one way, a contradiction. Thus, $n > 2$ so $i_0 > 1$, by (i).

(iii) Write $\bar{G} = G/L_1$. Then $\bar{\mathcal{C}} : \{1\} = \bar{L}_1 < \bar{L}_2 < \dots < \bar{L}_n = \bar{G}$ is the unique \mathcal{H}_k -chain in \bar{G} (Lemma 88.4). By induction, $L_2/L_1 = \Omega_1(G/L_1)$. Then $\Omega_1(G) = \Omega_1(L_2)$ and so $|\Omega_1(G)| = p^k$ since $|\Omega_1(L_2)| = p^k$, by Remark 4 and induction. Thus, G is not a counterexample. \square

Let $p > 3$ and let P be a Sylow p -subgroup of the symmetric group of degree p^2 . Set $G = P/\mathfrak{U}_1(P)$; then $|G| = p^P$. Let H be the unique abelian subgroup of index p in G and $k > 1$ a proper divisor of $p - 1$. Then there is only one \mathcal{H}_k -chain in H and $\Omega_1(H) = H$ is of order $p^{p-1} > p^k$. Let $p = 2$ and let H be dihedral of order 8. The group H has exactly two \mathcal{H}_2 -chains. Now let $H < G$, where G is dihedral of order 16. Then there are no \mathcal{H}_2 -chains in H as a normal subgroup of G .

Let G be a p -group of maximal class and order $> p^3$ and $R \triangleleft G$ with $|G : R| = p^4$. Then G/R has the unique abelian subgroup G_1/R of index p . This G_1 is called the *fundamental* subgroup of G . Clearly, G_1 is characteristic in G .

In conclusion we consider an arbitrary p -group G without \mathcal{H}_p -chains. By Theorem 88.11, G must be irregular. Let \mathcal{M} be the set of all normal subgroups H of G such that there is an \mathcal{H}_p -chain in H . To every $H \in \mathcal{M}$ we associate an \mathcal{H}_p -chain \mathcal{C}_H in H as a normal subgroup of G . Given $H, H_1 \triangleleft G$ and $\mathcal{C}_H : \{1\} = L_0 < L_1 < \dots < L_m = H$ and $\mathcal{C}_{H_1} : \{1\} = M_0 < M_1 < \dots < M_n$, we write $\mathcal{C}_H \geq \mathcal{C}_{H_1}$ provided the sequence $\{|L_1|, |L_2 : L_1|, \dots, |L_n : L_{m-1}|\}$ dominates over the sequence $\{|M_1|, |M_2 : M_1|, \dots, |M_n : M_{n-1}|\}$ in lexicographic ordering. Let \mathcal{M}_0 be the set of all $H \in \mathcal{M}$ such that, whenever $H_1 \in \mathcal{M}$, then $\mathcal{C}_H \geq \mathcal{C}_{H_1}$ (so that we compare only \mathcal{H}_p -chains, possibly, in distinct G -invariant subgroups). If $H, H_1 \in \mathcal{M}_0$, then $i_0(\mathcal{C}_H) = i_0(\mathcal{C}_{H_1})$, $|\mathcal{C}_H| = |\mathcal{C}_{H_1}|$, $|H| = |H_1|$ and corresponding indices of these chains are equal. In what follows we use the notation introduced in this paragraph.

Proposition 88.13. *Let a p -group G , $p > 2$, have no \mathcal{H}_p -chains and $H \in \mathcal{M}_0$. Suppose that H has no normal subgroups of order p^p and exponent p , or, what is the same, $i_0(\mathcal{C}_H) = 0$. Then G is of maximal class and order $\geq p^{2p}$ and H is either absolutely regular or irregular of maximal class.*

- (a) *If H is absolutely regular, then $H = G_1$, the fundamental subgroup of G , and $\mathcal{M}_0 = \{H\}$.*
- (b) *Suppose that H is irregular of maximal class. Then $|G : H| = p$, $|H| = p^{2p-1}$ and $|\Omega_1(H)| = p^{p-1}$. In that case, $G_1 \notin \mathcal{M}_0$.*

Proof. Since regular p -groups are \mathcal{P} -groups, G is irregular (Theorem 88.11). We also have $|G| > p^{p+1}$ (otherwise, G has an \mathcal{H}_p -chain as Remark 3 shows). By Lemma 88.7, H is either absolutely regular or irregular of maximal class. Assume that there is $R \triangleleft G$ of order p^p and exponent p . Then the \mathcal{H}_p -chain $\mathcal{C}_R : \{1\} < R$ satisfies $i_0(\mathcal{C}_R) = 1 > 0 = i_0(\mathcal{C}_H)$ so $\mathcal{C}_R > \mathcal{C}_H$, contrary to the choice of H . Thus, G has no normal subgroups of order p^p and exponent p so, by Lemma 88.7, G is of maximal class. Since G has a normal subgroup of order p^{p-1} and exponent p , we get $|\Omega_1(H)| = p^{p-1}$. It is worth while to note that any normal subgroup K of index $> p$ in G is contained in $\Phi(G)$ so absolutely regular (Theorem 9.6); then $K \leq \Phi(G) < G_1$. Since G has no \mathcal{H}_p -chains, we get $|G| > p^{2p-1}$ (Remark 3).

Let H be absolutely regular. Then $|G : H| = p$ (otherwise, $H < G_1$ and there is an \mathcal{H}_p -chain in G_1). Since G_1 is the unique regular maximal subgroup of G (Theorem 9.6), we get $H = G_1$. Suppose, in addition, that $H_0 \in \mathcal{M}_0 - \{H\}$. In that case, H_0 is irregular of maximal class and index p in G . Since H_0 has an \mathcal{H}_p -chain, we get $|H| \leq p^{2p-1}$ so we have $|H_0| = p^{2p-1}$ since $|G : H_0| = p$ and $|G| > p^{2p-1}$. In that case, the last index of the \mathcal{H}_p -chain of H_0 equals p^p so it is not equal to every index of the \mathcal{H}_p -chain of the absolutely regular group H , and this is a contradiction. Thus, we have $\mathcal{M}_0 = \{H\}$, completing the proof of (a).

Now suppose that H is irregular of maximal class. Then, as we have noticed already, $|G : H| = p$. By Remark 3, since $|G| \geq p^{2p}$, we get $|H| = p^{2p-1}$. Since G has no normal subgroups of order p^p and exponent p^p , we get $|\Omega_1(H)| = p^{p-1}$. Since the \mathcal{H}_p -chain of G_1 has no indices $= p^p$, we get $G_1 \notin \mathcal{M}_0$, completing the proof of (b) and thereby the proposition. \square

Proposition 88.14. *Suppose that a p -group G has no \mathcal{H}_p -chains. Let $H \in \mathcal{M}_0$ and let*

$$\mathcal{C} = \mathcal{C}_H : \{1\} = L_0 < L_1 < \cdots < L_n = H$$

be an \mathcal{H}_p -chain in H with $i_0 = i_0(\mathcal{C}) > 0$ (the case $i_0 = 0$ is considered in the previous proposition). Write $U = L_{i_0}$ and $\bar{G} = G/U$. Then $|\mathcal{C}| > i_0$ and one of the following holds:

- (a) *\bar{G} is absolutely regular and $\exp(\bar{G}) > p$. In that case, if $|\mathcal{C}_H| > i_0 + 1$, then $\exp(L_{i_0+1}) = p^{i_0+1}$, $L_{i_0+1} < \Omega_{i_0+1}(G)$ and $L_{i_0+2}/L_{i_0+1} < \Omega_1(G/L_{i_0+1})$.*

(b) \bar{G} is irregular of maximal class. Then \bar{H} is either absolutely regular or irregular of maximal class.

(b1) If $|\bar{G}| = p^{p+1}$, then all maximal subgroups of \bar{G} are absolutely regular so $|\Omega_1(\bar{G})| = p^{p-1}$. In that case, $L_{i_0} < \Omega_{i_0}(G)$.

(b2) Let \bar{H} be irregular of maximal class. Then $|G : H| = p$, $|\Omega_1(\bar{H})| = p^{p-1}$, $|\bar{G}| \leq p^{2p}$ and $|\mathcal{C}_H| = i_0 + 2$.

Proof. By hypothesis, $H < G$. Write $i_0 = i_0(\mathcal{C})$ and $U = L_{i_0}$. As in the proof of Theorem 88.10, $\bar{G} = G/U$ has no normal subgroups of order p^p and exponent p so it is either absolutely regular or irregular of maximal class (Lemma 88.7). Assume that $|\mathcal{C}| = i_0$; then $U = H$. Take in \bar{G} a normal subgroup \bar{F} of order p . Then there is in F an \mathcal{H}_k -chain $\{1\} = L_0 < L_1 < \dots < L_n = H < F$ so $H \notin \mathcal{M}_0$, a contradiction. Thus, $|\mathcal{C}| > i_0$.

(a) Suppose that $\bar{G} = G/U$ is absolutely regular; then $\exp(\bar{G}) > p$ (otherwise, G has an \mathcal{H}_p -chain $\{1\} = L_1 < L_2 < \dots < L_{i_0} = U < G$). Since L_{i_0+1} has an \mathcal{H}_p -chain of length $i_0 + 1$ and G/L_{i_0+1} is absolutely regular, it follows that $L_{i_0+1} < \Omega_{i_0+1}(G)$ (otherwise, by Lemma 88.2(b), G has an \mathcal{H}_p -chain). Next, suppose that $|\mathcal{C}_H| > i_0 + 1$. Consider the subgroup $W = L_{i_0+2}$. We have $\Omega_{i_0+1}(H) = L_{i_0+1}$ since $\mathcal{C} = \mathcal{C}_H$ is an \mathcal{H}_p -chain, and so $\exp(L_{i_0+1}) = p^{i_0+1}$. Assume that $W/L_{i_0+1} = \Omega_1(G/L_{i_0+1})$. Let $x \in G - L_{i_0+1}$ be of minimal order; then, by what has been said already, $o(x) \leq p^{i_0+1}$ and $x^p \in L_{i_0+1}$. Then, by assumption, $x \in W = L_{i_0+2}$. However, $x \in \Omega_{i_0+1}(W) = L_{i_0+1}$, contrary to the choice of x . Thus, $W/L_{i_0+1} < \Omega_1(G/L_{i_0+1})$, completing this case.

(b) Suppose that $\bar{G} = G/U$ is irregular of maximal class.

(b1) Let $|\bar{G}| = p^{p+1}$. If $\bar{H}_1 < \bar{G}$ is of order p^p and exponent p , then $\{1\} = L_0 < L_1 < \dots < L_{i_0} < H_1 < G$ is an \mathcal{H}_p -chain in G (all indices of that chain, apart of the last one, equal p^p , the last index equals p), so, comparing indices of that chain with indices of the chain \mathcal{C} , we get $H \notin \mathcal{M}_0$, a contradiction. Thus, all maximal subgroups of \bar{G} are absolutely regular (Lemma 88.7) so $\Omega_1(\bar{G}) = \Phi(\bar{G})$ is of order p^{p-1} and exponent p . Since G has no \mathcal{H}_p -chains, it follows that $L_{i_0} < \Omega_{i_0}(G)$ (otherwise, G has an \mathcal{H}_p -chain, whose $(i_0 + 1)$ -th member coincides with the inverse image of $\Omega_1(\bar{G})$ in G , and the following member is G), completing the proof of (b1).

(b2) Now let \bar{H} be irregular of maximal class; then $|G : H| = |\bar{G} : \bar{H}| = p$ (Theorem 9.6). Since \bar{H} has no G -invariant subgroups of order p^p and exponent p , we get $|\Omega_1(\bar{H})| = p^{p-1}$ since \bar{H} has an \mathcal{H}_p -chain. All remaining assertions follow from Proposition 88.13. \square

Metacyclic p -groups, $p > 2$, are regular so they have exactly one \mathcal{H}_2 -chain.

Proposition 88.15. *The following conditions for a metacyclic 2-group G of order $\geq 2^4$ are equivalent:*

(a) G has no \mathcal{H}_2 -chains.

- (b) Either G is of maximal class or there is $k > 0$ such that $|\Omega_i(G)| = 2^{2i}$ for all $i \leq k$ and $G/\Omega_k(G)$ is of maximal class and order $\geq 2^4$.

Proof. Let the set \mathcal{M}_0 be such as in Propositions 13 and 14. Take $H \in \mathcal{M}_0$ and set $\mathcal{C} = \mathcal{C}_H$. Set $i_0 = i_0(\mathcal{C})$. Then $U = L_{i_0} = \Omega_{i_0}(G)$ so G/U is of maximal class, by the above and Lemma 88.2(b). If $G/U \cong Q_8$, then $\{1\} < \Omega_1(G) < \dots < U < \Omega_{i_0+1}(G) < G$ is an \mathcal{H}_2 -chain in G , a contradiction. Now assume that $G/U \cong D_8$. Let $F/U < G/U$ be abelian of type $(2, 2)$. Then $\{1\} < \Omega_1(G) < \dots < U < F < H$ is an \mathcal{H}_2 -chain in G , a contradiction. Thus, $|G/U| \geq 2^4$. Clearly, $|\Omega_i(G)| = 2^{2i}$ for all $i \leq i_0$.

It remains to show that G has no \mathcal{H}_2 -chains. Assume that \mathcal{C} is an \mathcal{H}_2 -chain in G as in Definition 1. Since G/U is of maximal class, we get $L_{i_0+2} = G$. We have $|L_{i_0+1}/L_{i_0}| = 2$ so $\Omega_{i_0+1}(G) = L_{i_0+1}$. It follows that G/L_{i_0} is a generalized quaternion group. Then $|L_{i_0+2}| \leq 2^{2k+3} < 2^{2k+4} \leq |G|$, a contradiction since $G = \Omega_{i_0+2}(G) = L_{i_0+2}$. \square

Supplement to Proposition 88.15. Let G be a metacyclic 2-group with $Ch_2(G) > 1$. Then there is k such that $|\Omega_i(G)| = 2^{2i}$ for all $i \leq k$ and $G/\Omega_k(G)$ is dihedral of order 8 (in the last case, $Ch_2(G) = 2$).

This follows easily from the proof of Proposition 88.15.

Problems

Below $H > \{1\}$ is a normal subgroup of a p -group G .

Problem 1. Let $p > 2$. Study the structure of H if there exists only one \mathcal{H}_{p-1} -chain in H .

Problem 2. Is it true that the number of \mathcal{H}_k -chains in any abelian p -group is congruent with $1 \pmod{p}$?

Problem 3. Find an algorithm producing all \mathcal{H}_k -chains in abelian p -groups.

Problem 4. Classify the 2-groups which have no \mathcal{H}_2 -chains.

Problem 5. Given a natural number k , a chain $\mathcal{C}_0 : H = H_0 > H_1 > \dots > H_n = \{1\}$ of G -invariant subgroups is said to be a lower k -admissible chain in H provided H_{i-1}/H_i is of order $\leq p^k$ and exponent p for $i = 1, \dots, n$. The above chain is said to be a lower \mathcal{H}_k -chain in G if, whenever $|H/H_i| < p^{ki}$, then $H_i = \mathfrak{V}_i(H)$. (i) Is it true that, whenever H is a lower pyramidal (see Remark 1), it possesses a lower \mathcal{H}_p -chain? (ii) Study the p -groups without lower \mathcal{H}_p -chains.

Problem 6. Suppose that $H \trianglelefteq G$ is a \mathcal{P}_2 -subgroup such that all sections of H are pyramidal. Is it true that there exists in H an \mathcal{H}_k -chain for any k ?

Problem 7. Does there exist in H an \mathcal{H}_p -chain if all sections of H of order p^{p+1} are \mathcal{P}_2 -groups?

Problem 8. Suppose that p -groups G and G_0 are lattice isomorphic and G has an \mathcal{H}_p -chain. Is it true that also G_0 has an \mathcal{H}_p -chain?

Problem 9. Suppose that a p -group H has an \mathcal{H}_k -chain. Now let $H \triangleleft G$, where G is a p -group. Find sufficient conditions for existing an \mathcal{H}_k -chain in H (as a normal subgroup in G).

2-groups with exactly six cyclic subgroups of order 4

If $c_2(G) = 6$, then such 2-groups G have been determined only in the special case where $|\Omega_2^*(G)| = 2^4$, where $\Omega_2^*(G) = \langle x \in G \mid o(x) = 4 \rangle$. Such 2-groups G with $|G| > 2^4$ are determined in Theorem 52.1 when $|\Omega_2(G)| = 2^4$ (since in that case $\Omega_2(G) \cong Q_8 \times C_2$ or $\Omega_2(G) \cong C_4 \times C_4$) and in Theorem 55.1 when $|\Omega_2(G)| > 2^4$. Here we shall classify 2-groups G with $c_2(G) = 6$ and $|\Omega_2^*(G)| > 2^4$. First we show that we must have $|\Omega_2^*(G)| = 2^5$ and we get three possibilities for the structure of $\Omega_2^*(G)$ (Lemma 89.6). The corresponding 2-groups G are determined up to isomorphism in Theorem 89.7. This solves #425 for $p = 2$. The general case, where $c_2(G) \equiv 2 \pmod{4}$ and $c_2(G) \geq 10$ is very difficult and is still open. Note that, for $n > 2$, the 2-groups G with $c_n(G) \cong 2 \pmod{4}$ are classified in Corollary 18.7.

At the end we consider 2-groups G which possess only one conjugate class of cyclic subgroups of order 4 and we show that in that case G has only one cyclic subgroup of order 4 and therefore G is either cyclic or dihedral (Theorem 89.8). This solves a part of #1379.

In what follows G will denote a 2-group with $c_2(G) = 6$ and $H = \Omega_2^*(G)$ is of order $> 2^4$. Since H has exactly six cyclic subgroups of order 4, H is neither cyclic nor a group of maximal class. It follows that H has a G -invariant four-subgroup W (Lemma 1.4).

Lemma 89.1. *If a cyclic subgroup V of order 4 in G normalizes another cyclic subgroup U of order 4, then U normalizes V and either $UV \cong C_4 \times C_2$ or $UV \cong Q_8$.*

Proof. First suppose $U \cap V = \{1\}$. Then $|UV| = 2^4$ and $(UV)' < U$ and we have either $UV = U \times V \cong C_4 \times C_4$ or $(UV)' \cong C_2$ in which case UV is a metacyclic minimal nonabelian group of order 2^4 and exponent 4. In any case, $c_2(UV) = 6$ and so $UV = H = \Omega_2^*(G)$, contrary to our assumption that $|H| > 2^4$. Thus, $U \cap V \cong C_2$ and so $|UV| = 2^3$. In this case, U also normalizes V and the only possibilities are $UV \cong C_4 \times C_2$ or $UV \cong Q_8$. \square

Lemma 89.2. *Suppose that $H = \Omega_2^*(G)$ contains a quaternion subgroup $Q \cong Q_8$. Then $|H| = 2^5$ and we have the following two possibilities: (a) $H \cong Q_8 * Q_8$, (b) $H \cong Q_{16} * C_4$.*

Proof. First we determine the structure of $S = WQ$, where W is a normal four-subgroup in H and $|W \cap Q| \leq 2$. Let z be an involution in $W \cap Z(S)$. If $z \notin Q$, then $c_2(Q \times \langle z \rangle) = 6$ and therefore $Q \times \langle z \rangle = \Omega_2^*(G) = H$, a contradiction. Hence $Q \cap W = \langle z \rangle \cong C_2$, $|S| = 2^4$, and $[W, Q] = \langle z \rangle$. This gives $S = Q * \langle v \rangle$, where $\langle v \rangle \cong C_4$ and $\langle v \rangle \cap Q = \langle z \rangle$. We have $c_2(S) = 4$, $\langle v \rangle = Z(S)$ and Q is a unique quaternion subgroup of S so Q is characteristic in S (see Appendix 16).

Assume that $S \not\trianglelefteq H$ and set $K = N_H(S)$ so that $|K : S| \geq 2$ and $|H : K| \geq 2$. Let $K < M < H$ be such that $|M : K| = 2$ and take $m \in M - K$. Since $Q^m \neq Q$, we get $Q^m \not\leq S$, and $Q^m \leq K$. We have $|Q^m \cap S| \leq 4$ and so $Q^m - S$ contains at least two cyclic subgroup of order 4. It follows that $c_2(K) = 6$. But $\Omega_2^*(G) = H > K$, a contradiction. We have proved that $S \triangleleft H$ and so Q and $Z(S) = \langle v \rangle$ are also normal in H . Since $c_2(S) = 4$, we have exactly two cyclic subgroups of order 4, not contained in S . Set $C = C_H(Q)$ so that $C \triangleleft H$ and $|H : (QC)| \leq 2$ (since $\text{Aut}(Q) \cong S_4$).

If there is an involution u in $C - \langle v \rangle$, then $c_2(Q \times \langle u \rangle) = 6$ and $Q \times \langle u \rangle = H$, a contradiction. Hence C is either generalized quaternion or cyclic. In the first case (since $C - \langle v \rangle$ can contain at most four elements of order 4), $C \cong Q_8$, $QC \cong Q_8 * Q_8$, $c_2(QC) = 6$ and therefore $QC = H$ is an extraspecial group of order 2^5 (case (a)).

We may assume that C is cyclic so that $|H : (QC)| = 2$ because $H - S$ must contain exactly four elements of order 4. Since $H/C \cong D_8$, there is $x \in H - (QC)$ such that $x^2 \in C$ and x induces an involutory outer automorphism on Q . There are elements $a, b \in Q$ such that $\langle a, b \rangle = Q$, $a^x = a^{-1}$ and $b^x = ab$.

Suppose that $\langle x, C \rangle$ is cyclic so that $\langle x, C \rangle = \langle x \rangle$ and $o(x) \geq 2|C| \geq 8$. If $o(x) \geq 16$, then there are no elements of order 4 in $H - (QC)$, a contradiction. Hence $o(x) = 8$ so that we may assume that $x^2 = v$. In that case, $T = \langle x, Q \rangle$ is of maximal class (Theorem 1.2) so x does not normalize $\langle a \rangle$ since $\langle a \rangle$ is not normal in $T = \langle a, x \rangle$. Hence $\langle x, C \rangle$ is noncyclic.

Assume that $\langle x, C \rangle$ is abelian or $\langle x, C \rangle \cong M_{2^m}$, $m \geq 4$, so that in both cases we may assume that x is an involution centralizing $\langle v \rangle$. We have $o(xv) = o(xva) = 4$ and we see that $c_2(S\langle x \rangle) = 6$ and so $H = S\langle x \rangle = \langle Q, xv \rangle * \langle v \rangle$, where $\langle Q, xv \rangle \cong Q_{16}$ (see Proposition 10.17 and Theorem 1.2) and $H \cong Q_{16} * C_4$ (case (b)).

Assume that $\langle x, C \rangle \cong Q_{2^n}$ or $\langle x, C \rangle \cong SD_{2^n}$. In both cases we may assume that $x^2 = z$ and $\langle v, x \rangle \cong Q_8$ since Q_8 is a subgroup of Q_{2^n} and SD_{2^n} and Q_8 contains the subgroup $\langle v \rangle$ of C . But then x inverts $\langle v \rangle$ and $\langle a \rangle$ (see above) and so all eight elements in $\langle a, v \rangle x$ from $H - (QC)$ are of order 4, a contradiction. Indeed, we compute for any integers i, j :

$$(a^i v^j x)^2 = a^i v^j x a^i v^j x = a^i v^j x^2 (a^i v^j)^x = a^i v^j z a^{-i} v^{-j} = z.$$

Finally, suppose that $\langle x, C \rangle \cong D_{2^n}$, $n \geq 3$, where x is an involution. But then all elements in $\langle a, C \rangle x$ from $H - (QC)$ are involutions since x inverts $\langle a \rangle$ and C and all other elements in $(QC - \langle a, C \rangle)x$ from $H - (QC)$ are elements of order 8, a contradiction (since $H - S$ does not contain any elements of order 4). Indeed, we set $C = \langle c \rangle$ and we know that $b^x = ab$ so that for any integers i, j we compute (noting

that in Q we have $ba^i = a^i bz^i$ and $bab = a$):

$$\begin{aligned} (ba^i c^j x)^2 &= ba^i c^j (ba^i c^j)^x = ba^i c^j \cdot aba^{-i} c^{-j} = a^i bz^i c^j aba^{-i} c^{-j} \\ &= a^i z^i (bab) c^j a^{-i} c^{-j} = a^i z^i \cdot a \cdot c^j a^{-i} c^{-j} = z^i a, \end{aligned}$$

which is an element of order 4. Hence, all elements $ba^i c^j x$ are of order 8, as claimed. Our lemma is proved. \square

In the next three lemmas we assume, in addition, that Q_8 is not a subgroup of H . We turn out to prove that $|H| = 2^5$.

Lemma 89.3. *Assuming that Q_8 is not a subgroup of H , we have $|H : N_H(X)| \leq 2$ for each cyclic subgroup X of order 4 in H .*

Proof. Suppose that the lemma is false. Then there is a cyclic subgroup U_1 of order 4 in H such that $K = N_H(U_1)$ is of index 4 in H (take into account that $c_2(H) = 6$). Let M be a maximal subgroup of H containing K so that $|H : M| = |M : K| = 2$, and let $m \in M - K$. Then $U_2 = U_1^m \neq U_1$, $N_H(U_2) = K$ and so $A = U_1 U_2 \cong C_4 \times C_2$ (Lemma 89.1) and $A \not\trianglelefteq H$ since $c_2(A) = 2$. Let $x \in H - M$ so that $A^x \neq A$ and $A^x < M$. We have $c_2(M) \in \{3, 4, 5\}$ because $M < H$. If $c_2(M)$ is odd, then M is of maximal class (Theorem 1.17), a contradiction since M has an abelian subgroup of type $(4, 2)$. Hence $c_2(M) = 4$ since $c_2(M) > C_2(A) = 2$.

Suppose that $|M| > 2^4$. If $|\Omega_2(M)| > 2^4$, then (see [§53, Introduction]) $U_1 \triangleleft M > K = N_H(U_1)$, a contradiction. Hence we must have $|\Omega_2(M)| = 2^4$. In that case we may use Theorems 52.2, 52.4, and 52.5 since Q_8 is not a subgroup of M and $c_2(\Omega_2(M)) = 4$. This implies that $\Omega_2(M)$ is abelian of type $(4, 2, 2)$ and there is a cyclic subgroup of order 4 which is normal in M . This is a contradiction since $\Omega_2(M) = AA^x$ and so all four cyclic subgroups of order 4 in M are conjugate in H and so no one of them could be normal in M .

We have proved that $|M| = 2^4$ so that $K = A = N_H(U_1)$, $AA^x = M$ is of order 2^4 and $|H| = 2^5$. In this case A and A^x are two distinct abelian maximal subgroups of M which implies $|Z(M)| = 4$, $|M'| = 2$, $\text{cl}(M) = 2$ and M is of exponent 4. Suppose that M is not minimal nonabelian. Then M possesses a subgroup $D \cong D_8$ (H has no subgroups isomorphic to Q_8) and, since M is not of maximal class, we have $C_M(D) \not\leq D$ (see Proposition 10.17). Since $c_2(M) = 4$, we get $M = D * C$ with $C \cong C_4$ and $D \cap C = Z(D)$. But $D_8 * C_4 \cong Q_8 * C_4$, contrary to our assumption. Hence M is minimal nonabelian. If M is metacyclic, then M has a cyclic normal subgroup of order 4, contrary to the fact that all four cyclic subgroups of order 4 in M are conjugate in H . Hence M is a uniquely determined nonmetacyclic minimal nonabelian group of order 2^4 and exponent 4 (see Lemma 65.1).

Since $N_H(X) < M$ for each cyclic subgroup X of order 4 in M , there are no elements of order 8 in $H - M$. It follows that $H - M$ consists of four elements of order 4 and 12 involutions. Set $E = \Omega_1(M)$ so that E is elementary abelian of order

8, $Z(M) = \Phi(M) \cong E_4$ and $Z(H) \leq Z(M)$. Let $v \in H - M$ be of order 4 such that $v^2 \in E$ and $C_E(v) \cong E_4$ since $H - M$ contains exactly four elements of order 4 and they are all contained in $(E\langle v \rangle) - E$ (here we used Proposition 1.8). All eight elements in $H - (M \cup E\langle v \rangle)$ are involutions and so if $u \in H - (M \cup E\langle v \rangle)$, then u centralizes E and so $F = E \times \langle u \rangle \cong E_{16}$ (take into account that two noncommuting involution generate a dihedral group). In particular, $Z(M) < E < F$ and so $Z(M) = Z(H)$. Let $y \in M - E$ and we know that all cyclic subgroups of order 4 in M are conjugate in H to $\langle y \rangle$. But $y^2 \in \Phi(M) = Z(H)$ and so $\mathfrak{U}_1(M) = \langle y^2 \rangle$, contrary to $\Phi(M) \cong E_4$. \square

Lemma 89.4. *Assuming that Q_8 is not a subgroup of H , we have $|H : N_H(X)| = 2$ for each cyclic subgroup X of order 4 in H .*

Proof. Suppose that the lemma is false. Then there are at least two distinct cyclic subgroups U_1 and U_2 which are normal in H (Lemma 89.3). Let $\{U_1, U_2, \dots, U_6\}$ be the set of six cyclic subgroups of H . Since each U_i , $i = 1, 2, \dots, 6$, normalizes U_1 and U_2 , it follows (Lemma 89.1) that $A = \langle U_1, U_2 \rangle \cong C_4 \times C_2$, $U_i U_j$ is abelian of type $(4, 2)$, $i = 1, 2$, $j > 2$, and so $A \leq Z(H)$. Therefore, for each U_j , $j = 3, \dots, 6$, we have $U_1 \cap U_j = U_2 \cap U_j = U_1 \cap U_2 = \langle z \rangle = \mathfrak{U}_1(A)$. It follows that $B = AU_3 = \langle U_1, U_2, U_3 \rangle$ is abelian of order 2^4 and exponent 4 with $\mathfrak{U}_1(B) = \langle z \rangle$ and so B is abelian of type $(4, 2, 2)$. Since $c_2(B) = 4$, we may assume that $\{U_1, U_2, U_3, U_4\}$ is the set of cyclic subgroups of order 4 in B . Similarly, $C = AU_5$ is abelian of type $(4, 2, 2)$ with $\mathfrak{U}_1(C) = \langle z \rangle$ so that $\{U_1, U_2, U_5, U_6\}$ is the set of cyclic subgroups of order 4 in C . We have $B \cap C = A$ and $H = \langle B, C \rangle$. Thus, H/A is generated with two distinct cyclic subgroups B/A and C/A of order 2, and so $H/A \cong E_4$ or $H/A \cong D_{2^n}$, $n \geq 3$. In particular, B and C are not conjugate in H . Let t be an involution in $H - (B \cup C)$ and let v be an element of order 4 in $A \leq Z(H)$. Then tv is an element of order 4 in $H - (B \cup C)$, a contradiction. Hence, all elements in $H - (B \cup C)$ are of order ≥ 8 . This implies that B and C are normal in H and so $H = \langle B, C \rangle = BC$ is of order 2^5 with two distinct abelian maximal subgroups B and C . It follows that $|H'| \leq 2$ and so H is of class ≤ 2 . But H is generated by its elements of order 4 and so H is of exponent 4, a contradiction. \square

Lemma 89.5. *Assuming that Q_8 is not a subgroup of H , we have $c_2(N_H(X)) = 2$ for each cyclic subgroup X of order 4 in H .*

Proof. Let U_1 be a cyclic subgroup of order 4 in H so that $|H : N_H(U_1)| = 2$ (Lemma 89.4). Set $M = N_H(U_1)$ and, taking an element $h \in H - M$, we get $U_2 = U_1^h \neq U_1$, $N_H(U_2) = M$, $A = \langle U_1, U_2 \rangle \cong C_4 \times C_2$ (Lemma 89.1), and $A \triangleleft H$. Assume that M has a further cyclic subgroup $U_3 \not\leq A$ of order 4 so that $\langle U_1, U_3 \rangle \cong \langle U_2, U_3 \rangle \cong C_4 \times C_2$, and therefore $B = \langle U_1, U_2, U_3 \rangle$ is abelian of type $(4, 2, 2)$. Since $c_2(B) = 4$, we may assume that $\{U_1, U_2, U_3, U_4\}$ is the set of all cyclic subgroups of order 4 in B . There is an element g of order 4 in $H - M$ and since $|H : N_H(\langle g \rangle)| = 2$, $U_5 = \langle g \rangle$ and $U_6 = \langle g^x \rangle$ (with an $x \in H - N_H(\langle g \rangle)$) give two

last cyclic subgroups of order 4 in H which give exactly four elements of order 4 in $H - M$. This implies that $B = \Omega_2^*(M) \triangleleft H$ and U_3 and U_4 are conjugate in H .

Set $H_0 = BU_5$. Since H_0 is not of maximal class, we get $c_2(H_0) = 6$ (Theorem 1.17(b)), and so $H_0 = BU_5 = H$. Set $B_0 = \Omega_1(B) \cong E_8$. Suppose that $B \cap U_5 = \{1\}$ so that $|H : B| = 4$. Since $|H : N_H(U_5)| = 2$, U_5 centralizes a four-subgroup S in B_0 . But then all eight elements of order 4 in $S \times U_5$ lie in $H - B$, a contradiction. Hence $B \cap U_5 \cong C_2$ and so $|H : B| = 2$, $|H| = 2^5$, $B = M$, and $N_H(U_3) = N_H(U_4) = B$. This implies that there are no elements of order 8 in $H - B$ and so $H - B$ consists of four elements of order 4 and twelve involutions.

We have $|B : N_B(\langle g \rangle)| = 2$, where $\langle g \rangle = U_5$ and $N_B(\langle g \rangle)$ cannot contain an element x of order 4 (otherwise, that element x would centralize U_5 , contrary to the fact that $C_H(x) = B$). Hence $N_B(\langle g \rangle) = B_0$. If g centralizes B_0 , then there are eight elements of order 4 in $H - B$, a contradiction. Hence $C_B(g) = C_{B_0}(g) = Z \cong E_4$ and so $Z(H) = Z$. The set B_0g consists of four elements of order 4 and four involutions. Hence all eight elements in $H - (B \cup B_0\langle g \rangle)$ are involutions and if t is one of them, then $H - B = B_0g \cup B_0t$ and $B_0g \cap B_0t = \emptyset$ so that t must centralize B_0 and therefore $B_0 \leq Z(H)$, contrary to the fact that $Z(H) = Z \cong E_4$. \square

Lemma 89.6. *Let G be a 2-group with exactly six cyclic subgroups of order 4 and let $H = \Omega_2^*(G) = \langle x \in G \mid o(x) = 4 \rangle$ be of order $> 2^4$. Then H is of order 2^5 and we have the following three possibilities:*

- (a) $H \cong Q_8 * Q_8$ is extraspecial;
- (b) $H \cong Q_{16} * C_4$ with $Q_{16} \cap C_4 = Z(Q_{16})$ (by Exercise A in Appendix 16, indeed $c_2(H) = 6$);
- (c) H is a special group possessing a unique elementary abelian subgroup E of order 2^4 and there is an involution $t \in H - E$ such that $H = \langle E, t \rangle$ and $C_E(t) = Z(H) \cong E_4$.

Proof. In view of Lemma 89.2, we may assume that Q_8 is not a subgroup of H and so we may use Lemmas 89.1, 89.4, and 89.5. Let U_1 be a cyclic subgroup of order 4 in H . Set $K = N_H(U_1)$ so that $|H : K| = 2$ and if $h \in H - K$, then $U_2 = U_1^h \neq U_1$, $A = \langle U_1, U_2 \rangle = \Omega_2^*(K) \cong C_4 \times C_2$ is normal in H , $N_H(U_2) = K$ and so no one of U_1, U_2 is characteristic in K . Note that $|H| > 2^4$ and so $|K| > 2^3$.

We are in a position to use Proposition 53.2 which gives that K is a uniquely determined group of order 2^5 or 2^4 . We may assume that we have the following conjugacy classes of our six cyclic subgroups of order 4 in H : $U_1 \sim U_2$, $U_3 \sim U_4$, and $U_5 \sim U_6$. Assume that $|K| = 2^5$ in which case $|H| = 2^6$. It follows that $\Phi(N_H(U_1)) = \langle U_1, U_2 \rangle$ and similarly (since $|H : N_H(U_3)| = |H : N_H(U_5)| = 2$), $N_H(U_3) \cong N_H(U_5) \cong K$. But then $\Phi(N_H(U_3)) = \langle U_3, U_4 \rangle$, $\Phi(N_H(U_5)) = \langle U_5, U_6 \rangle$ and therefore $\Phi(H) \geq \langle U_1, U_2, U_3, U_4 \rangle = H$, a contradiction.

We have proved that $K = N_H(U_1) = N_H(U_2)$ is of order 2^4 and then $K \cong D_8 \times C_2$ (Proposition 53.2(b)) and $|H| = 2^5$. The subgroup K has exactly three

abelian maximal subgroups: $F_1 \cong E_8$, $F_2 \cong E_8$, and $A = \langle U_1, U_2 \rangle \cong C_4 \times C_2$, where $F_1 \cap F_2 = F_0 = Z(K) \cong E_4$. There are no elements of order 8 in $H - K$ since $N_H(U_1) = N_H(U_2) = K$ and so $H - K$ consists of eight elements of order 4 and eight involutions. Let r be an involution in $H - K$. Then the coset $rK = H - K$ has exactly eight involutions, and let rk be one of them. Then $(rk)^2 = 1$ or, what is the same, $k^r = k^{-1}$ so $o(k) \leq 2$ since r does not normalize any cyclic subgroup of order 4 in K , and we get $k \in C_K(r)$. It follows that $|C_K(r)| = 8$ so $C_H(r) \cong E_{16}$. Since $Z(K) = F_1 \cap F_2$, it follows that $Z(K) = Z(H)$. By Lemma 1.4, $|H'| = 4$. Next, $H/A \cong E_4$ (if not and $x \in H - A$ is of order 4, then $C_H(x)$ is abelian of type $(4, 2, 2)$, which is impossible since $C_H(r)$ is the unique abelian maximal subgroup of H in view $|H'| = 4$). Thus, $Z(H) = \Omega_1(A)$ and, since H is not minimal nonabelian, we get $H/Z(H) \cong E_8$. Thus, H is special so it is the group given in (c). \square

Theorem 89.7 (Janko). *Let G be a 2-group with exactly six cyclic subgroups of order 4 and let $H = \Omega_2^*(G)$ be of order $> 2^4$. Then H is of order 2^5 and we have three possibilities for the structure of H (Lemma 89.6). However, if $G > H$, then $H \cong Q_{16} * C_4$, $|G : H| = 2$, $|G| = 2^6$, and we have the following two possibilities:*

- (i) *G has a dihedral subgroup $D = \langle f, \xi \mid f^{16} = \xi^2 = 1, f^\xi = f^{-1} \rangle \cong D_{32}$ of index 2 and an involution $u \in G - D$ so that $[u, \xi] = 1$ and $f^u = fz, z = f^8$.*
- (ii) *$G = \langle a, t \mid a^{16} = t^2 = 1, a^8 = z, a^4 = v, a^t = a^{-1}vu, u^2 = 1, [u, a] = 1, u^t = uz \rangle$, where G is a U_2 -group with respect to $U = \langle u, z \rangle \cong E_4$, $G/U \cong SD_{16}$ and $Z(G) = \langle uv \rangle \cong C_4$.*

Proof. For the structure of $H = \Omega_2^*(G)$ we use Lemma 89.6. We assume in addition that $G > H$. If $H \cong Q_8 * Q_8$ is extraspecial (Lemma 89.6(a)), then we have a contradiction, by Theorem 83.2.

Suppose that H is a special group given in Lemma 89.6(c). Let $H < L \leq G$ be such that $|L : H| = 2$. Let E be a unique elementary abelian subgroup of order 16 in H so that $E \triangleleft L$. Let $j \in H - E$ be an involution so that $C_E(j) = E_0 = Z(H) \cong E_4$ (see the proof of Lemma 89.6); then $E_0 \triangleleft L$ and $F = E_0 \times \langle j \rangle = C_H(j) \cong E_8$ is normal in L since all 12 elements in $H - (E \cup F)$ are of order 4 and $E \triangleleft L$. Four involutions in $F - E_0$ form a single conjugate class in H and an L -invariant set so $I = C_L(j)$ covers L/H and $I \cap H = F$ hence $I \cong E_{16}$ since I is abelian, and $E_0 \leq Z(L)$. Let $i \in I - F$ and consider the subgroup $J = E\langle i \rangle$ of order 2^5 ; then $J \cap H = E$. All 16 elements in $J - E = J - H$ must be involutions since $\exp(J) \leq 4$, and so $J \cong E_{32}$. We get $C_H(i) \geq \langle E, F \rangle = H$. If v is an element of order 4 in H , then $o(vi) = 4$ and $vi \notin H$, a contradiction.

Thus, by Lemma 89.6, we must have $H \cong Q_{16} * C_4$. Let $H = Q * C$, where $Q = \langle b, t \mid b^8 = 1, t^2 = b^4 = z, b^t = b^{-1} \rangle \cong Q_{16}$, $C = \langle v \rangle \cong C_4$, $v^2 = z$, and $Q \cap C = \langle z \rangle$. Since Q is generated by all (five) noncentral cyclic subgroups of order 4 in H , we get $Q \triangleleft G$. Set $D = C_G(Q)$ so that $D \triangleleft G$, $D \geq C$ and $D \cap H = C$. If there is an involution $i \in D - C$, then $o(b^2i) = 4$ and $b^2i \notin H$, a contradiction.

Hence z is a unique involution in D . Since $c_2(D) = 1$, D is cyclic (Theorem 1.17(b)). Let $d \in D - C$ be an element of order 8. Then $b^4 = d^4 = z$ and so $o(bd) = 4$ with $bd \notin H$, a contradiction. We have proved that $D = C = C_G(Q)$.

The group $\text{Aut}(Q)$ is generated by $\text{Inn}(Q) \cong D_8$ and two involutory outer automorphisms α and β induced by $t^\alpha = tb$, $b^\alpha = b^{-1}$, $t^\beta = t$, $b^\beta = bz$, where $[\alpha, \beta] = i_{b^2}$ (the inner automorphism of Q induced by conjugation with the element b^2) and so $\text{Aut}(Q)/\text{Inn}(Q) \cong E_4$ (and in fact $\langle \alpha, \beta \rangle \cong D_8$); see Theorem 34.8. The subgroup Q contains exactly two quaternion subgroups Q_1 and Q_2 and we have $Q_1^\beta = Q_1$, $Q_2^\beta = Q_2$, and $Q_1^\alpha = Q_2$. It follows that $G/H \neq \{1\}$ is elementary abelian of order ≤ 4 (here we use the N/C-Theorem).

Assume that $L = N_G(Q_1) > H$ so that $|L : H| = 2$. Since $Q/\langle z \rangle \cong D_8$ is isomorphic to a Sylow 2-subgroup of $\text{Aut}(Q_1) \cong S_4$, it follows that $C_0 = C_L(Q_1) > C$ and $|C_0 : C| = 2$. If $y \in C_0 - C$ is an involution, then $o(b^2y) = 4$ (because $b^2 \in Q_1$) and $b^2y \notin H$, a contradiction. Since $c_2(C_0) = 1$, we get that $C_0 = \langle c \rangle \cong C_8$ is cyclic with $c^4 = z$. Now, c normalizes $\langle b \rangle$ (since $Q \triangleleft G$ and $\langle b \rangle$ is a unique cyclic subgroup of index 2 in Q) and centralizes $\langle b^2 \rangle = \langle b \rangle \cap Q_1$, but c does not centralize $\langle b \rangle$ (otherwise, c would centralize $\langle b, Q_1 \rangle = Q$, a contradiction) and so we get $b^c = bz$, $\langle b, c \rangle' = \langle z \rangle$, $\text{cl}(\langle b, c \rangle) = 2$, $(bc)^4 = b^4c^4[c, b]^6 = zzz^6 = 1$, $o(bc) = 4$ (Theorem 1.2), and $bc \notin H$, a contradiction.

We have proved that $|G/H| = 2$, $|G| = 2^6$, and if $g \in G - H$, then $Q_1^g = Q_2$. In particular, $C_G(t) = \langle t, v \rangle \cong C_4 \times C_2$ and so eight elements of order 4 in $Q - \langle b \rangle$ form a single conjugate class in G . Set $T = \langle b \rangle \langle v \rangle \cong C_8 \times C_2$ which is normal in G and eight elements in $H - (Q \cup T)$ are involutions which form a single conjugate class in G and so if tv is one of them, then $C_G(tv) = \langle t, v \rangle$. In particular, if $x \in G - H$, then $x^2 \in T$. We have $U = \Omega_1(T) = \langle z, b^2v \rangle \cong E_4$ is normal in G , $\Omega_2(T) = \langle b^2, v \rangle \cong C_4 \times C_2$, and $\langle b^2 \rangle$ and $\langle v \rangle$ are normal in G .

Suppose that there is an involution $\xi \in G - H$. Then ξ inverts $\langle v \rangle$ and $\langle b^2 \rangle$ (otherwise, ξ centralizes v or b^2 and then ξv or ξb^2 would be an element of order 4 in $G - H$, a contradiction). If $b^\xi = b^{-1}z$, then $(\xi b)^2 = b^\xi b = z$ and $o(\xi b) = 4$ with $\xi b \notin H$, a contradiction. Hence ξ inverts each element in T and so, in particular, ξ centralizes U . Since $Q_1^\xi = Q_2$, we have $t^\xi = tb^i$, where i is odd. Set $b^2v = u$ and $\xi t = f$ so that ξ centralizes the involution u ,

$$\begin{aligned} f^2 &= \xi t \xi t = t^\xi t = (b^i)^t = b^{-i}, \quad o(f) = 16, \quad f^8 = (b^{-i})^4 = z, \\ f^\xi &= (\xi t)^\xi = \xi t^\xi = \xi t b^i = f b^i = f^{-1}(f^2 b^i) = f^{-1} b^{-i} b^i = f^{-1}, \end{aligned}$$

$$\langle f, \xi \rangle \cong D_{32}$$

and

$$\begin{aligned} f^u &= (\xi t)^{b^2v} = v^{-1} b^{-2} \xi t b^2 v = \xi (v^{-1} b^{-2})^\xi t b^2 v = \xi v b^2 t b^2 v \\ &= (\xi t)(v b^2)^t b^2 v = (\xi t)v b^{-2} b^2 v = \xi t v^2 = fz. \end{aligned}$$

We have obtained the group given in part (i) of our theorem.

It remains to investigate the case, where there are no involutions in $G - H$. Then 32 elements in $G - H$ are of order 8 or 16. If all 32 elements in $G - H$ are of order 8, then $c_3(G) = 10$ and therefore G is a U_2 -group (see Corollary 18.7). But then G must also have elements of order 16 which is not the case. If all 32 elements in $G - H$ are of order 16, then $c_4(G) = 4$ and $c_3(G) = 2$. Again, G is a U_2 -group. But a U_2 -group of order 2^6 has exactly two cyclic subgroups of order 16, a contradiction. Hence $G - H$ contains elements of order 8 and 16. Since the number of cyclic subgroups of order 16 must be even (otherwise, G would be of maximal class), it follows that $G - H$ has exactly 16 elements of order 16 (and so $c_4(G) = 2$) and exactly 16 elements of order 8. Hence $c_3(G) = 6$ and so G is a U_2 -group with respect to U since in a U_2 -group a normal four-subgroup is unique. If R/U is a cyclic subgroup of index 2 in G/U , then $G - R$ contains exactly eight involutions, eight elements of order 4, and 16 elements of order 8. Hence $G/U \cong SD_{16}$ and $\Phi(R) \cong C_8$. Since H is nonmetacyclic, G is also nonmetacyclic. We have $\Phi(G) \leq T$ and so there are exactly three maximal subgroups of G containing T . They are H , R and a certain subgroup V with the property that all 16 elements in $V - T$ are of order 8. Since $\Omega_2(V) = \Omega_2(T) = \langle b^2, v \rangle \cong C_4 \times C_2$, $|V| = 2^5$, and V has no elements of order 16, V must be isomorphic to a group (c) given in Lemma 42.1 and so $\Phi(V) = \Omega_2(V)$ and $Z(V) \cong C_4$. We get $\Phi(G) \geq \langle \Phi(R), \Phi(V) \rangle = T$ and so G is 2-generated, i.e., $d(G) = 2$. Also, $Z(V) \cong C_4$ implies that $U \not\leq Z(V)$ and so $C_G(U) = R$ (because $C_G(U)$ must be a maximal subgroup of G containing T and also $U \not\leq Z(H)$). Since $\Phi(T) = \langle b^2 \rangle$ and $\Phi(V) = \langle b^2, v \rangle$ (and no involution in $\Phi(V) - \langle z \rangle$ could be a square of an element in $V - T$ because $U \not\leq Z(V)$), there is an element $s \in V - T$ such that $s^2 = v$. Hence, $C_G(v) \geq \langle H, s \rangle = G$ and so $Z(G) \cong C_4$. We have obtained a nonmetacyclic U_2 -group G of order 2^6 with respect to $U \cong E_4$ such that $G/U \cong SD_{16}$, $d(G) = 2$, and $Z(G) \cong C_4$. It follows that G must be isomorphic to a U_2 -group given in Theorem 67.3(c). We have obtained the group given in part (ii) of our theorem. \square

Note that the group H of Lemma 89.6(c) has exactly 16 elementary abelian subgroups of order 8 so there is in H an odd number of metacyclic subgroups of order 8 (Sylow).

Theorem 89.8 (Janko). *Let G be a 2-group of exponent > 2 all of whose cyclic subgroups of order 4 are conjugate. Then G has exactly one cyclic subgroup of order 4 and G is either cyclic or dihedral.*

Proof. First suppose that G has more than one cyclic subgroup of order 4. Let U be one of them and set $K = N_G(U)$ so that $|G : K| \geq 2$ and let M be a maximal subgroup of G containing K . Then each cyclic subgroup of order 4 is contained in M and if X is one of them, then $N_G(X) \leq M$ (since X is conjugate in G to U). Let x be any element in $G - M$. We know that x is not of order 4 and suppose that $o(x) \geq 8$. But then $x^2 \in M$ and $o(x^2) \geq 4$ and so x centralizes a cyclic subgroup of order 4 in

M , a contradiction. Hence each element x in $G - M$ is an involution and so M must be abelian and x inverts M . But then U is normal in G , a contradiction.

We have proved that G has a unique cyclic subgroup $V = \langle v \rangle$. Then, by Theorem 1.17(b), G is either cyclic or dihedral. \square

Nonabelian 2-groups all of whose minimal nonabelian subgroups are of order 8

In this section we determine the structure of the title groups and show that this class of groups coincides with the class of nonabelian 2-groups in which any two noncommuting elements generate a group of maximal class (Corollary 90.2). This solves Problem 920 for $p = 2$.

Theorem 90.1 (Janko). *Let G be a nonabelian 2-group all of whose minimal nonabelian subgroups are isomorphic to D_8 or Q_8 . Then G is one of the following groups:*

- (a) G is generalized dihedral (i.e., $|G : H_2(G)| = 2$).
- (b) $G = HZ(G)$, where H is of maximal class and $\mathfrak{V}_1(Z(G)) \leq Z(H)$.
- (c) $G = HZ(G)$, where H is extraspecial and $\mathfrak{V}_1(Z(G)) \leq Z(H)$.

Proof. Let A be a maximal normal abelian subgroup of G . We see at once that G/A is elementary abelian. Indeed, let $x \in G - A$ with $o(x) = 4$ and $A \cap \langle x \rangle = \{1\}$. According to Lemma 57.1, let $a \in A$ be such that $[a, x] \neq 1$ and $F = \langle a, x \rangle$ be minimal nonabelian. Since $|F| = 8$, we have $F \cap A = \langle a \rangle$ is of order 2 and so $[a, x] = 1$, a contradiction. We shall also use induction on $|G|$.

(i) First we deal with the case $\exp(G) = 4$. In this case we show that each cyclic subgroup of order 4 is normal in G . Suppose that this is false. Let $X = \langle x \rangle$ be a cyclic subgroup of order 4 which is not normal in G . Set $M = N_G(X)$ so that $M \neq G$. Let $M_0 > M$ be such that $|M_0 : M| = 2$ and assume $M_0 \neq G$. By induction, the nonabelian group M_0 is a group of our theorem with exponent 4 and so X is normal in M_0 , a contradiction. Thus $|G : M| = 2$ and with the same argument we see that M is a unique maximal subgroup of G containing X . In particular, $d(G) = 2$, $X \not\leq \Phi(G)$ and $\langle x, y \rangle = G$ for each $y \in G - M$. Let y be a fixed element in $G - M$ so that $y^2 \in M$, $o(y^2) \leq 2$, y^2 normalizes X and set $x^2 = z$. We have $x^y \notin \langle x \rangle$, $N_G(\langle x^y \rangle) = M$ and $A = \langle x, x^y \rangle = \langle x \rangle \langle x^y \rangle$ is normal in G since $(x^y)^y = x^{y^2} \in \langle x \rangle$. Since $A \langle y \rangle$ contains X , we have, by the above. $G = A \langle y \rangle$ and $M = A \langle y^2 \rangle$. If $[x, x^y] = 1$, then A is abelian of type $(4, 2)$ or $(4, 4)$. If $[x, x^y] \neq 1$, then $[x, x^y] \in \langle x \rangle \cap \langle x^y \rangle$ and so $[x, x^y]$ is a central involution in A which implies that A is minimal nonabelian. But A contains two distinct cyclic subgroups of order 4 and so in this case $A \cong Q_8$ is quaternion.

First suppose that $y^2 \notin A$ so that $o(y) = 4$, $G/A \cong C_4$ and $M = A\langle y^2 \rangle \neq A$. Since $\langle x \rangle$ is normal in M , y^2 either centralizes or inverts $\langle x \rangle$. Because $yx \in G - M$ and $\exp(G) = 4$, $(yx)^2 = yxyx = y^2(x^y x)$ is an involution in $M - A$. Hence $y^2(x^y x)y^2(x^y x) = 1$ and so $(x^y x)^{y^2} = (x^y x)^{-1}$. First consider the possibility $\langle x, x^y \rangle = A \cong Q_8$ so that $\langle x \rangle \cap \langle x^y \rangle = \langle z \rangle = Z(A)$ and $\langle x \rangle, \langle x^y \rangle$ and $\langle x^y x \rangle$ are the three cyclic subgroups of order 4 in A . If y^2 inverts $\langle x \rangle$, then y^2 also inverts $\langle x^y \rangle$. By the above, y^2 inverts $\langle x^y x \rangle$ and so y^2 inverts A and therefore A must be abelian, a contradiction. Hence, y^2 centralizes $\langle x \rangle$ and $\langle x^y \rangle$ and so y^2 centralizes A , contrary to the above fact that y^2 inverts $\langle x^y x \rangle$. We have proved that A is abelian. Assume that y^2 inverts $\langle x \rangle$ and then y^2 also inverts $\langle x^y \rangle$ which implies that y^2 inverts A and so $M = A\langle y^2 \rangle$ is generalized dihedral. Hence A is a maximal normal abelian subgroup in G (since $C_G(A) = A$), a contradiction because G/A is not elementary abelian. We have proved that y^2 centralizes $\langle x \rangle$ and $\langle x^y \rangle$ and so $M = A \times \langle y^2 \rangle$ is abelian. By the above, y^2 also inverts $x^y x$ and so $u = x^y x$ must be an involution, A is abelian of type $(4, 2)$, $|G| = 2^5$, $\langle z, u \rangle = \Omega_1(A) \cong E_4$, and $\langle x \rangle \cap \langle x^y \rangle = \langle z \rangle = \Omega_1(A)$. Since

$$u^y = (x^y x)^y = x^{y^2} x^y = x x^y = x^y x = u,$$

we get $C_M(y) = Z(G) = \langle y^2, z, u \rangle \cong E_8$ is of index 4 in G and therefore, by Lemma 64.1(q), $|G'| = 2$. But $G = \langle y, x \rangle$ is two-generated and so, by Lemma 65.2(a), G is minimal nonabelian of order 2^5 , a contradiction.

We have proved that $y^2 \in A$ and so $A = M$ and $|G : A| = 2$. Suppose that $A \cong Q_8$. If $C_G(A) \leq A$, then Proposition 10.17 implies that G is of maximal class (and order 2^4). This is not possible since $\exp(G) = 4$. Hence, $C_G(A) \not\leq A$ and so $d(G) = 3$, a contradiction. Thus, A is abelian of type $(4, 2)$ or $(4, 4)$. We have $(yx)^2 = y^2(x^y x)$, where $o(y^2) \leq 2$. It follows that $o(x^y x) \leq 2$ since yx cannot be of order 8. This forces $\langle x \rangle \cap \langle x^y \rangle = \langle z \rangle$, A is of type $(4, 2)$ and $|G| = 2^4$. Set $u = x^y x$ so that u is an involution and $\langle z, u \rangle = \Omega_1(A) \cong E_4$. We have $u^y = (x^y x)^y = x^{y^2} x^y = x x^y = x^y x = u$ and so $C_A(y) = Z(G) = \langle z, u \rangle \cong E_4$ is of index 4 in G . By Lemma 64.1(q), $|G'| = 2$. But $G = \langle y, x \rangle$ and so, by Lemma 65.2(a), G is minimal nonabelian (of order 2^4), a contradiction. We have proved that each cyclic subgroup of order 4 is normal in G .

If $\Omega_2^*(G) \neq G$, then G is generalized dihedral. Therefore we may assume that $\Omega_2^*(G) = G$ in which case there is a cyclic subgroup $X = \langle x \rangle$ of order 4 which is not central in G (otherwise, G would be abelian). Set $H = C_G(x)$ and $x^2 = z$. Then $|G : H| = 2$ and for each $g \in G - H$, $g^2 \in \langle z \rangle$ (otherwise, $\langle g \rangle \cap \langle x \rangle = \{1\}$ implies $[g, x] = 1$, a contradiction). We have proved that $G/\langle z \rangle$ is generalized dihedral. Let $g \in G - H$ with $g^2 = z$ and assume that there is $h \in H$ with $h^2 \notin \langle z \rangle$. Then $h^g = h^{-1}$ since $G/\langle z \rangle$ is generalized dihedral and $\langle h \rangle$ is normal in G . But then $\langle h \rangle \cap \langle g \rangle = \{1\}$ implies $[h, g] = 1$, a contradiction. Hence, for each $h \in H$, $h^2 \in \langle z \rangle$ and so $\langle z \rangle = \Phi(G) = G'$. By Lemma 4.2, $G = H_1 * \cdots * H_s Z(G)$, $s \geq 1$, where each H_i is minimal nonabelian and so $H = H_1 * \cdots * H_s$ is extraspecial and $\Omega_1(Z(G)) \leq Z(H) = \Phi(G)$.

(ii) We assume that $\exp(G) > 4$. Then Lemma 57.2 implies that $|G : A| = 2$, where A is a maximal normal abelian subgroup of G with $\exp(G) = \exp(A) > 4$.

(ii1) Suppose $\Omega_1(A) \not\leq Z(G)$ so that $C_G(\Omega_1(A)) = A$. Let $x \in G - A$ and $v \in \Omega_1(A) - C_A(x)$ so that $1 = [v, x^2] = [v, x][v, x]^x, [v, x]^x = [v, x]$ and $\langle v, x \rangle \cong D_8$. For any $a \in A$ we have $C_A(ax) = C_A(x), [v, ax] = [v, x]$ and therefore $\langle v, ax \rangle \cong D_8$ which implies that $G/\langle [v, x] \rangle$ is generalized dihedral. The subgroup $B = \{b \mid b \in A, b^x = b^{-1}\}$ is of index at most 2 in A and in fact $|B : A| = 2$ since $v^x \neq v^{-1} = v$. We have $A = \langle v, B \rangle$, where B covers $A/\Omega_1(A)$. Either x or vx is of order 4 and so if $w \in B$ with $o(w) = 4$, then we consider the subgroups $\langle x, w \rangle$ and $\langle vx, w \rangle$ to get $w^2 = [v, x]$. Hence $B = \langle b \rangle \Omega_1(B)$, where $\Omega_1(\langle b \rangle) = \langle [v, x] \rangle$ and $H = \langle b, x \rangle$ is of maximal class. Let b_0 be an element of order 4 in $\langle b \rangle$ and set $z = [v, x]$ so that $b_0^2 = z$. We get $(vb_0)^x = (vz)(b_0z) = vb_0$ and so $G = HZ(G)$ with $Z(G) = \Omega_1(B)\langle vb_0 \rangle$ and $\mathfrak{V}_1(Z(G)) = Z(H) = \langle z \rangle$.

(ii2) Suppose $\Omega_1(A) \leq Z(G)$. Let $x \in G - A$ so that $x^2 \in \Omega_1(A)$ and x inverts each element in $A/\Omega_1(A)$ (Lemma 57.2). Thus, $[\Omega_2(A), G] \leq \Omega_1(A)$ and $[\Omega_2(A), x] \neq 1$. Indeed, by Lemma 57.1, there is $a \in A$ with $\langle a, x \rangle$ minimal nonabelian and so $a \in \Omega_2(A)$ and $[a, x] \neq 1$. Let $v \in \Omega_2(A) - C_A(x)$ so that $1 \neq [v, x] \in \Omega_1(A) \leq Z(G)$ and therefore $\langle v, x \rangle$ is minimal nonabelian (of order 8) and so $v^x = v^{-1}$. Assume that there is $w \in \Omega_2(A) - \Omega_1(A)$ with $[w, x] = 1$. Then $vw \in \Omega_2(A) - C_A(x)$ and therefore vw is inverted by x . We get $v^{-1}w^{-1} = (vw)^{-1} = (vw)^x = v^{-1}w$ which implies $w^2 = 1$, a contradiction. We have proved that x inverts each element in $\Omega_2(A)$ and so $C_A(x) = \Omega_1(A) = Z(G)$. If each element in $G - A$ is an involution, then G is generalized dihedral. Therefore, we may take a fixed element $x \in G - A$ with $o(x) = 4$. Then for each $v \in A$ with $o(v) = 4$ we have $v^x = v^{-1}$ which forces $v^2 = x^2$. Indeed, if $v^2 \neq x^2$, then $\langle v, x \rangle$ would be metacyclic minimal nonabelian of order 2^4 , a contradiction. We have proved that $A = \langle b \rangle \Omega_1(A)$ with $o(b) \geq 8$ and $\langle x^2 \rangle = \langle b \rangle \cap \Omega_1(A)$. By Lemma 57.2, $b^x = b^{-1}\zeta$ with $\zeta \in \Omega_1(A)$. We compute $(xb)^2 = x^2b^xb = x^2b^{-1}\zeta b = x^2\zeta$ and let b_0 be an element of order 4 in $\langle b \rangle$ so that $b_0^{xb} = b_0^{-1}$. If $\zeta \notin \langle b \rangle$, then $\langle b_0, xb \rangle$ is metacyclic minimal nonabelian of order 2^4 , a contradiction. Hence $\zeta \in \langle b \rangle$ and so $\zeta \in \langle x^2 \rangle$ and $H = \langle b, x \rangle$ is of maximal class and $G = HZ(G)$ with $\mathfrak{V}_1(Z(G)) = \{1\}$. \square

Corollary 90.2. *Let G be a nonabelian 2-group in which any two noncommuting elements generate a subgroup of maximal class. Then G is one of the groups (a), (b) or (c) from Theorem 90.1. Conversely, each group in (a), (b) and (c) of Theorem 90.1 satisfies the assumption of our corollary.*

Proof. Since each minimal nonabelian subgroup of G is isomorphic to D_8 or Q_8 , the result follows from Theorem 90.1. It is necessary to prove only for groups (b) and (c) of Theorem 90.1 that any two noncommuting elements generate a group of maximal class. Indeed, let h_1z_1 and h_2z_2 be any noncommuting elements in G , where $h_1, h_2 \in H$ and $z_1, z_2 \in Z(G)$. Then $[h_1z_1, h_2z_2] = [h_1, h_2] \neq 1$ and so $H_0 = \langle h_1, h_2 \rangle \leq H$ is a group of maximal class with $H'_0 \geq Z(H)$. On the other hand, a 2-group $\langle h_1, h_2 \rangle$

is of maximal class if and only if $[h_1, h_2] \neq 1$, $\langle [h_1, h_2] \rangle$ is normal in H_0 and $h_1^2, h_2^2 \in \langle [h_1, h_2] \rangle$. Hence $H_1 = \langle h_1 z_1, h_2 z_2 \rangle$ is of maximal class since $[h_1 z_1, h_2 z_2] = [h_1, h_2] \neq 1$, $h_1 z_1$ and $h_2 z_2$ normalize $\langle [h_1 z_1, h_2 z_2] \rangle = \langle [h_1, h_2] \rangle$ and $(h_1 z_1)^2, (h_2 z_2)^2$ are contained in $\langle [h_1, h_2] \rangle$ (noting that $z_1^2, z_2^2 \in Z(H) \leq H'_0 = H'_1$). \square

Maximal abelian subgroups of p -groups

Abelian subgroups in 2-groups G play an important role. Therefore, it is not very surprising that our assumption that every two distinct maximal abelian subgroups have cyclic intersection determines completely the structure of G . We obtain five classes of 2-groups with this property. More precisely, we prove here the following result.

Theorem 91.1 (Janko). *Let G be a nonabelian 2-group in which any two distinct maximal abelian subgroups have cyclic intersection. Then $Z(G)$ is cyclic, each abelian subgroup of G is of rank at most 2, the intersection of any two distinct maximal abelian subgroups is equal $Z(G)$, and G has (at least) one abelian subgroup of index 2. Moreover, G is isomorphic to one of the following groups:*

- (a) *Group of maximal class.*
- (b) M_{2^n} .
- (c) *$G = D * C$ (central product), where $D \cong D_{2^n}$, $C \cong C_{2^m}$, $m \geq 2$, is cyclic of order 2^m and $D \cap C = Z(D)$.*
- (d) *$G = \langle x, t \mid (xt)^2 = a, a^{2^m} = t^2 = 1, m \geq 2, x^2 = ab, b^{2^{n-1}} = 1, n \geq 3, b^t = b^{-1}, [a, x] = [a, t] = 1, t^x = tb, a^{2^{m-1}} = b^{2^{n-2}} \rangle$, where $|G| = 2^{m+n}$, $m \geq 2, n \geq 3$, $Z(G) = \langle a \rangle \cong C_{2^m}$, $G' = \langle b \rangle \cong C_{2^{n-1}}$, and $M = \langle x, a \rangle$ is a unique abelian maximal subgroup of G . We have $C_G(t) = \langle t \rangle \times \langle a \rangle \cong C_2 \times C_{2^m}$ and $\langle b, t \rangle \cong D_{2^n}$.*
- (e) *$G = \langle g, h \mid g^{2^n} = h^{2^m} = 1, m \geq 3, n \geq 3, g^{2^{n-1}} = h^{2^{m-1}}, hg = h^{-1} \rangle$, where G is metacyclic, $|G| = 2^{m+n-1}$ since $\langle g \rangle \cap \langle h \rangle = \langle g^{2^{n-1}} \rangle \cong C_2$. Also, $Z(G) = \langle g^2 \rangle \cong C_{2^{n-1}}$, $G' = \langle h^2 \rangle \cong C_{2^{m-1}}$ and $M = \langle h, g^2 \rangle$ is a unique abelian maximal subgroup of G .*

The more general problem to determine the structure of a nonabelian p -group G such that $A \cap B = Z(G)$ for any two distinct maximal abelian subgroups A and B is very difficult. First we show that a p -group G has this property if and only if $C_G(x)$ is abelian for each $x \in G - Z(G)$ (Theorem 91.2). Then we show that such a 2-group G has either an abelian subgroup of index 2 or G is of class 2 and G' is elementary abelian (Theorem 91.3). In Corollary 91.5 we get a new result for an arbitrary 2-group.

We also classify 2-groups G such that $A/Z(G)$ is cyclic for each maximal abelian subgroup A of G (a problem of Heineken–Mann). It is surprising that such groups

have the property that $C_G(x)$ is abelian for each element $x \in G - Z(G)$. Then we may use our Theorems 91.2 and 91.3 to classify such groups (Theorem 91.4). In this classification we distinguish the cases, where G has an abelian subgroup of index 2 and the case where $|G : A| > 2$ for each maximal abelian subgroup A of G .

Proof of Theorem 91.1. Let G be a nonabelian 2-group in which any two distinct maximal abelian subgroups have cyclic intersection. Since $Z(G)$ is contained in each maximal abelian subgroup of G , it follows that $Z(G)$ is cyclic.

Suppose that G possesses a subgroup $E \cong E_8$. Let A be a maximal abelian subgroup containing E and set $F = \Omega_1(A)$ so that $E \leq F$. Let $B \leq G$ be such that $A < B$ and $|B : A| = 2$ and let $x \in B - A$. Then $x^2 \in A$ and therefore x induces on F an automorphism of order ≤ 2 . It follows that $|C_F(x)| \geq 4$ (Proposition 1.8) and the abelian subgroup $C_F(x)\langle x \rangle$ is contained in a maximal abelian subgroup C which is distinct from A since $x \notin A$. But $A \cap C \geq C_F(x)$ and so $A \cap C$ is noncyclic, a contradiction. We have proved that each abelian subgroup of G is of rank ≤ 2 .

We may assume that G is not of maximal class (case (a) of Theorem 91.1) and so there is $E_4 \cong U \triangleleft G$. Set $M = C_G(U)$ so that $|G : M| = 2$ since $Z(G)$ is cyclic. Let A be a maximal abelian subgroup of G which contains U so that $A \leq M$. Suppose that $A \neq M$ and let $y \in M - A$ be such that $y^2 \in A$. Let B be a maximal abelian subgroup of G containing the abelian subgroup $U\langle y \rangle$. Then $B \neq A$ (since $y \notin A$) and $A \cap B \geq U$ is noncyclic, a contradiction. Thus, $M = A$. We have proved that whenever U is a normal four-subgroup of G , then $M = C_G(U)$ is an abelian maximal subgroup of G .

If x is any element in $G - M$, then $C_M(x) = Z(G)$ and $Z(G)\langle x \rangle$ is a maximal abelian subgroup of G . Thus, the intersection of any two distinct maximal abelian subgroups of G is equal to $Z(G)$ and this is also true for 2-groups of maximal class.

Suppose that G has two distinct normal four-subgroups. Then, by Theorem 50.2, $G = D * C$ with $D \cong D_8$, $D \cap C = Z(D)$ and C is either cyclic of order ≥ 4 or of maximal class $\not\cong D_8$. Let U be a four-subgroup in D ; then $U \triangleleft G$. By the above, $C_G(U)$ is abelian and so C must be cyclic. We have obtained a group stated in part (c). In the sequel we assume that G has a unique normal four-subgroup U and set $M = C_G(U)$ so that M is an abelian maximal subgroup of rank 2 with $\Omega_1(M) = U$.

(i) First assume $\Omega_2(G) \not\leq M$. Then there is an element $y \in G - M$ of order ≤ 4 so that $y^2 \in U$ (recall that $U = \Omega_1(M)$). We have $U\langle y \rangle \cong D_8$ since y does not centralize U , and so there is an involution $t \in G - M$. Since t does not centralize U and M is abelian of rank two, we get $C_G(t) = \langle t \rangle \times C_M(t)$, where $C_M(t)$ is cyclic of order 2^m , $m \geq 2$. Indeed, if $m = 1$, then G is of maximal class. Also, we have $t \notin \Phi(G)$, G has no elementary abelian subgroups of order 8 and $G \not\cong M_{2^s}$, $s \geq 4$ (since M_{2^s} has only three involutions). We are now in a position to use Theorem 48.1. It follows that G has a subgroup S of index ≤ 2 , where $S = AL$, L is normal in G , $L = \langle b, t \mid b^{2^{n-1}} = t^2 = 1, b^t = b^{-1} \rangle \cong D_{2^n}$, $n \geq 3$, $A = \langle a \rangle \cong C_{2^m}$, $m \geq 2$, $A \cap L = Z(L) = \langle z \rangle$, $[a, t] = 1$, $C_G(t) = \langle t \rangle \times \langle a \rangle$, $\Omega_1(G) = \Omega_1(S) = \Omega_2(A) * L$,

$\Omega_2(A) \cap L = Z(L)$ and if $|G : S| = 2$, then there is an element $x \in G - S$ such that $t^x = tb$.

Since $\langle b \rangle$ is a unique cyclic subgroup of index 2 in L , $\langle b \rangle$ is normal in G . Set $B = \Omega_2(A) * L = \Omega_1(G)$, $\Omega_2(A) = \langle l \rangle$, $l^2 = z$, and $\langle v \rangle = \Omega_2(\langle b \rangle)$ so that $\langle v \rangle$ and $\langle l \rangle = Z(B)$ are normal in G . Hence $\langle l, v \rangle \cong C_4 \times C_2$ is normal in G . Set $u = lv$ so that $U = \langle z, u \rangle = \Omega_1(\langle l, v \rangle) \cong E_4$ is a unique normal four-subgroup in G . We know that $M = C_G(U)$ is abelian and $|G : M| = 2$. Note that b centralizes U and $u^t = (lv)^t = lv^{-1} = lvz = uz$. If $v^a = v^{-1} = vz$, then $A = \langle a \rangle > \Omega_2(A) = \langle l \rangle$ and we replace a with $a' = at$. In that case $o(a') = o(a)$, $\Omega_2(\langle a' \rangle) = \langle l \rangle$ and

$$u^{a'} = (lv)^{at} = (avz)^t = av^{-1}z = lv = u,$$

so that $\langle a' \rangle$ centralizes U and $S = \langle a' \rangle L$. Writing again a instead of a' , we may assume from the start that $A = \langle a \rangle$ centralizes U . Hence $C_S(U) = \langle a, b \rangle$ is of index 2 in S and therefore $M = C_G(U)$ covers G/S and $G = M\langle t \rangle$. But M is abelian and t centralizes $\langle a \rangle$ and so $\langle a \rangle \leq Z(G)$. On the other hand, $C_G(t) = \langle t \rangle \times \langle a \rangle$ and $C_M(t) = \langle a \rangle$ so that $A = \langle a \rangle = Z(G)$.

If $G = S$, then $G = L * A$, where $L \cong D_{2^n}$, $n \geq 3$, $A \cong C_{2^m}$, $m \geq 2$, and $L \cap A = Z(L)$. We have obtained groups stated in part (c) of Theorem 91.1. In what follows we assume that $|G : S| = 2$ and we know that in that case there is an element $x \in G - S$ such that $t^x = tb$. We may assume that $x \in M - S$. Indeed, if $x = tx'$ with $x' \in M - S$, then $tb = t^x = t^{tx'} = t^{x'}$.

Since M is abelian and $C_M(t) = \langle a \rangle = Z(G)$, it follows that $C_M(xt) = \langle a \rangle$ and so $(xt)^2 \in \langle a \rangle$. Set $(xt)^2 = a'$ and assume that $\langle a' \rangle \neq \langle a \rangle$. This implies that there is an element $a'' \in \langle a \rangle - \langle a' \rangle$ such that $(a'')^2 = (a')^{-1}$. We get $(xt \cdot a'')^2 = (xt)^2(a'')^2 = 1$ and so $x(ta'')$ (with $ta'' \in S$) is an involution in $G - S$, contrary to $\Omega_1(G) = \Omega_1(S)$. It follows that $\langle a' \rangle = \langle a \rangle$ and so replacing a with a' (and writing again a instead of a'), we may assume from the start that $(xt)^2 = a$. From the last relation and $t^x = tb$ we get $a = (xt)^2 = xt \cdot xt = x^2(x^{-1}tx)t = x^2tbt = x^2b^{-1}$, and so $x^2 = ab$. The structure of G is uniquely determined and we have obtained the group stated in part (d) of Theorem 91.1.

(ii) Finally, assume that $\Omega_2(G) \leq M$. Note that M is abelian of rank 2 and so M is metacyclic. Hence G is also metacyclic. If G has a cyclic subgroup of index 2, then G is either of maximal class or $G \cong M_{2^n}$, $n \geq 4$, and these are the groups stated in parts (a) and (b) of Theorem 91.1. In what follows we assume that G has no cyclic subgroups of index 2. We have $U = \Omega_1(M) = \Omega_1(G) \cong E_4$, where $M = C_G(U)$ is an abelian maximal subgroup of G .

Let H be a normal cyclic subgroup with cyclic G/H so that $|H| \geq 4$ and $|G/H| \geq 4$. We have $U \cap H = \langle z \rangle \cong C_2$ and $z \in Z(G)$ so that if $u \in U - \langle z \rangle = U - H$, then $M = C_G(u)$, where $|G : M| = 2$ and M is abelian. Suppose that u does not centralize H . Then $|H : (H \cap M)| = 2$ and therefore M covers G/H . Let $m \in M$ be such that $\langle m \rangle$ covers $M/M \cap H$ and note that $C_G(H) = H$ since u does not centralize H . Let

$h \in H - M$ so that $H = \langle h \rangle$ and $h^m = hz$. Then $h^{m^2} = (hz)^m = hz \cdot z = h$. This is a contradiction since $|G/H| \geq 4$ and so $m^2 \notin H$.

We have proved that u centralizes H and so $M > H$. Let $g \in G - M$ so that $\langle g \rangle$ covers G/H , $g^2 \in M$ and g^2 centralizes H and therefore g induces on $H = \langle h \rangle$ an involutory automorphism. Also, $u^g = uz$ since $Z(G)$ is cyclic. If $h^g = hz$, then $G' = \langle z \rangle$ and G is minimal nonabelian. In that case G is splitting metacyclic, i.e., there is $g' \in G - M$ such that $\langle g' \rangle$ covers G/H and $\langle g' \rangle \cap H = \{1\}$. It follows that $\Omega_1(\langle g' \rangle) \leq Z(G)$ and so $Z(G) \geq \langle z, \Omega_1(\langle g' \rangle) \rangle \cong E_4$, a contradiction. We have proved that $h^g = h^{-1}z^\epsilon$, $\epsilon = 0, 1$ and $|H| \geq 8$. (Indeed, if $|H| = 4$, then $h^g = h^{-1} = hz$ and we have again $G' = \langle z \rangle$, as above.) In particular, $C_H(g) = \langle z \rangle$ and so $\langle g \rangle \cap H \leq \langle z \rangle$. However, if $\langle g \rangle \cap H = \{1\}$, then $C_G(\Omega_1(\langle g \rangle)) \geq \langle M, g \rangle = G$ and so $E_4 \cong \langle z, \Omega_1(\langle g \rangle) \rangle \leq Z(G)$, a contradiction.

We have proved that $\langle g \rangle \cap H = \langle z \rangle$ and so $o(g) \geq 8$ and $Z(G) = \langle g^2 \rangle$. If $h^g = h^{-1}z$, then we replace h with $h' = hu$, where $[h, u] = 1$ and so $o(h') = o(h)$ and

$$(h')^g = (hu)^g = h^{-1}z \cdot uz = h^{-1}u = (hu)^{-1} = (h')^{-1}$$

and $\langle h', g \rangle = \langle hu, g \rangle = \langle h, g \rangle = G$ since $u \in U \leq \Phi(G)$. (Indeed, $\Phi(G) \leq M$ is abelian and so if $\Phi(G) = \Omega_1(G)$ were cyclic, then $|G : \Phi(G)| = 4$ implies that G would have a cyclic subgroup of index 2.) Writing h instead of h' , we see that we may assume from the start that $h^g = h^{-1}$. We have obtained the group stated in part (e). \square

Theorem 91.2. *Let G be a nonabelian p -group. Then $A \cap B = Z(G)$ for any two distinct maximal abelian subgroups A, B if and only if $C_G(x)$ is abelian for each $x \in G - Z(G)$.*

Proof. Let $x \in G - Z(G)$ and suppose that $C_G(x)$ is nonabelian. Let A be a maximal abelian subgroup of $C_G(x)$ so that $A \neq C_G(x)$ and $A \geq Z(G)\langle x \rangle > Z(G)$. Let $b \in C_G(x) - A$ and let B be a maximal abelian subgroup of $C_G(x)$ containing $\langle b \rangle$ so that $A \neq B$ and B also contains the abelian subgroup $Z(G)\langle x \rangle$. Obviously, A and B are also maximal abelian subgroups of G but $A \cap B \geq Z(G)\langle x \rangle > Z(G)$.

Conversely, let $C \neq D$ be maximal abelian subgroups of G such that $C \cap D > Z(G)$. Let $y \in (C \cap D) - Z(G)$ so that $C_G(y) \geq \langle C, D \rangle$, where $\langle C, D \rangle$ is non-abelian. \square

Theorem 91.3. *Let G be a nonabelian 2-group such that $A \cap B = Z(G)$ for every two distinct maximal abelian subgroups A and B . Then one of the following holds: (a) G has an abelian subgroup of index 2. (b) G is of class 2, G' is elementary abelian and $\Phi(G) \leq Z(G)$.*

Proof. Let A be a maximal normal abelian subgroup of G . Then $G/A \neq \{1\}$ acts faithfully on A and $\{1\} \neq Z(G) < A$. Let K be a G -invariant subgroup such that $Z(G) < K \leq A$ and $|K : Z(G)| = 2$. Let x be any element in $G - A$. Then $C_A(x) = Z(G)$ and so $\langle x \rangle \cap A \leq Z(G)$. Indeed, let B be a maximal abelian subgroup

containing the abelian subgroup $C_A(x)\langle x \rangle$. Then $A \neq B$ and $A \cap B \geq C_A(x) = Z(G)$. Let $k \in K - Z(G)$ so that $k^2 \in Z(G)$ and $k^x = kl$ with some $l \neq 1 \in Z(G)$. We get $k^2 = (k^2)^x = (k^x)^2 = (kl)^2 = k^2l^2$, and so $l^2 = 1$ and therefore l is an involution in $Z(G)$. This gives

$$k^{x^2} = (k^x)^x = (kl)^x = k^x l = (kl)l = kl^2 = k,$$

and so (by the above) $x^2 \in A$ and (since $\langle x \rangle \cap A \leq Z(G)$) $x^2 \in Z(G)$. In particular, G/A is elementary abelian. Let $a \in A - Z(G)$ and set $a^x = a' \in A - Z(G)$ so that $(a')^x = (a^x)^x = a^{x^2} = a$ (since $x^2 \in Z(G)$). Therefore, $(aa')^x = a'a = aa'$ which implies that $aa' = z \in Z(G)$ and $a' = a^x = a^{-1}z$ and so x inverts $A/Z(G)$.

Suppose that $|G/A| \geq 4$. Then there are elements $x, y \in G - A$ such that $xy \in G - A$. In this case x and y both invert $A/Z(G)$ and so xy centralizes $A/Z(G)$. But xy also must invert $A/Z(G)$ which implies that $A/Z(G)$ is elementary abelian. Hence $\Phi(G) \leq Z(G)$ (noting that for each $x \in G - A$, $x^2 \in Z(G)$) and so G is of class 2. For each $g, h \in G$, $[g, h]^2 = [g^2, h] = 1$ and so G' is elementary abelian. \square

Theorem 91.4. *Let G be a nonabelian 2-group such that $A/Z(G)$ is cyclic for each maximal abelian subgroup A of G . Then one of the following holds:*

- (a) *G has an abelian subgroup M of index 2 and we have either $G = HZ(G)$ with H minimal nonabelian or $G/Z(G) \cong D_{2^n}$, $n \geq 3$, is dihedral of order 2^n with G' cyclic of order ≥ 4 , $G' \cap Z(G) \cong C_2$, and if $x \in G - M$, then $x^2 \in Z(G)$ and x inverts G' .*
- (b) *G is of class 2, G' is elementary abelian of order ≥ 8 , $\Phi(G) \leq Z(G)$ and whenever A is a maximal abelian subgroup of G , then $|A : Z(G)| = 2$.*

Proof. Suppose that there is an element $a \in G - Z(G)$ such that $H = C_G(a)$ is nonabelian. Let A be a maximal abelian subgroup of G containing $\langle a \rangle$. Then $Z(G)\langle a \rangle \leq A < H < G$. By our assumption, $A/Z(G) \neq \{1\}$ is cyclic. Assume that $H/Z(G)$ contains a subgroup of order 2 distinct from $\Omega_1(A/Z(G))$. In that case there is $x \in H - A$ such that $x^2 \in Z(G)$. Since $[a, x] = 1$, $\langle a, x \rangle$ is abelian but $\langle a, x \rangle Z(G)/Z(G)$ is noncyclic, a contradiction. We have proved that $H/Z(G)$ has only one subgroup of order 2 and so $H/Z(G) \cong Q_{2^n}$, $n \geq 3$, is generalized quaternion of order 2^n . Indeed, if $H/Z(G)$ were cyclic, then H is abelian, a contradiction. Since $H/Z(G) \cong Q_{2^n}$, it follows that $a^2 \in Z(G)$, $Z(H) = Z(G)\langle a \rangle$, $|Z(H) : Z(G)| = 2$ and for each $y \in Z(H) - Z(G)$, $C_G(y) = H = C_G(a)$. Set $|Z(G)| = 2^m$, $m \geq 1$, so that $|H| = 2^{m+n}$. Let $A_0/Z(G)$ be a cyclic subgroup of index 2 in $H/Z(G)$ so that A_0 is abelian and $Z(H) < A_0$. Let $A_1/Z(G) = (H/Z(G))'$ so that $Z(H) \leq A_1 < A_0$ and $|H : A_1| = 4$ and therefore $|A_1| = 2^{m+n-2}$. Since $A_1 = H'Z(G)$, H' covers $A_1/Z(G)$ and so $|H'| \geq 2^{n-2} = |A_1/Z(G)|$. By Lemma 1.1, we get $|H| = 2|Z(H)||H'|$ and so $2^{m+n} = 2 \cdot 2^{m+1}|H'|$ and therefore $|H'| = 2^{n-2}$. This gives $H' \cap Z(G) = \{1\}$ and so H' is cyclic with $H' \cap Z(H) = \langle y \rangle \cong C_2$. It follows that $\langle y \rangle$ is characteristic in H and so if T is

a subgroup of G such that $H < T \leq G$ and $|T : H| = 2$, then $\langle y \rangle$ is central in T , contrary to the above fact that $C_G(y) = H$, where $y \in Z(H) - Z(G)$. We have proved that for each $a \in G - Z(G)$, $C_G(a)$ is abelian.

By Theorem 91.2, $A \cap B = Z(G)$ for any two distinct maximal abelian subgroups A and B of G . We may use Theorem 91.3 and so either G has an abelian subgroup of index 2 or $G' \leq Z(G)$, $\Phi(G) \leq Z(G)$ and G' is elementary abelian.

(i) First we consider the case, where G has an abelian subgroup M of index 2. Then $Z(G) < M$ and for each $x \in G - M$, $C_M(x) = Z(G)$ and so $x^2 \in Z(G)$. By our assumption, $M/Z(G) \neq \{1\}$ is cyclic. If G has another abelian maximal subgroup N , then $M \cap N = Z(G)$ and this implies that $|M : Z(G)| = 2$. Conversely, suppose that $|M/Z(G)| = 2$. In that case $G/Z(G) \cong E_4$ (because $G/Z(G) \cong C_4$ would imply that G is abelian) and so G has more than one abelian maximal subgroup. We analyze this case further. Let H be a minimal nonabelian subgroup of G . Then $|H : (H \cap Z(G))| = 4$, H covers $G/Z(G)$ and so $G = HZ(G)$ and $G' \cong C_2$. We have obtained the first possibility stated in part (a) of our theorem.

It remains to consider the case, where $M/Z(G) \cong C_{2^n}$, $n \geq 2$, where M is a unique abelian maximal subgroup of G . We know that for each $x \in G - M$, $x^2 \in Z(G)$. It follows that x inverts the cyclic group $M/Z(G)$ of order ≥ 4 and so $G/Z(G) \cong D_{2^{n+1}}$ is dihedral of order 2^{n+1} . Set $|Z(G)| = 2^m$, $m \geq 1$, and $(G/Z(G))' = L/Z(G)$ so that $G/L \cong E_4$ and $L = G'Z(G)$. Since G has an abelian maximal subgroup, we may use Lemma 1.1 and we get $|G| = 2^{m+n+1} = 2 \cdot 2^m |G'|$ and so $|G'| = 2^n$. Hence $G' \cap Z(G) = \langle z \rangle \cong C_2$, $G'/\langle z \rangle$ is cyclic of order 2^{n-1} and G' is abelian.

Suppose that G' is not cyclic. Then G' splits over $\langle z \rangle = G' \cap Z(G)$. Since $\mathfrak{U}_1(G')$ is normal in G and $\mathfrak{U}_1(G') \cap Z(G) = \{1\}$, it follows that $\mathfrak{U}_1(G') = \{1\}$ and so $G' \cong E_4$ and $G/Z(G) \cong D_8$. Let $a \in M - (Z(G)G')$ so that $\langle a \rangle$ covers $M/Z(G) \cong C_4$ and so $a^2 \notin Z(G)$. For an $x \in G - M$, we have $[a, x] = t \in G' - \langle z \rangle$. Then we get

$$[a^2, x] = [a, x]^a [a, x] = t^a t = t^2 = 1.$$

But then $G(a^2) = \langle M, x \rangle = G$ and so $a^2 \in Z(G)$, a contradiction. We have proved that G' is cyclic of order ≥ 4 .

For any $x \in G - M$ and any $m \in M - L$ (where $L = G'Z(G)$), we have $x^2 \in Z(G)$ and $[m, x] = g$ with $\langle g \rangle = G' \cong C_{2^n}$. This gives $m^x = mg$ and so $m = m^{x^2} = (mg)^x = mgg^x$ and this implies $g^x = g^{-1}$ and therefore x inverts G' . We have obtained the second possibility in part (a) of our theorem.

(ii) Now we consider the case, where G has no abelian subgroups of index 2, $G' \leq Z(G)$, $\Phi(G) \leq Z(G)$ and G' is elementary abelian. It follows that $|A : Z(G)| = 2$ for each maximal abelian subgroup A of G . If $|G : Z(G)| = 4$, then G would have an abelian subgroup of index 2, a contradiction. Hence, $G/Z(G) \cong E_{2^m}$, $m \geq 3$, and so there exist elements $g, h, i \in G - Z(G)$ such that $\langle g, h, i \rangle Z(G)/Z(G) \cong E_8$. We have $[g, h] \neq 1$, $[g, i] \neq 1$, and $[h, i] \neq 1$.

Suppose that $|G'| = 2$. Then $[g, h] = [g, i]$ and so $[g, hi] = [g, h][g, i] = 1$ and therefore $\langle g, hi \rangle Z(G)/Z(G) \cong E_4$, a contradiction.

Suppose that $G' \cong E_4$. In that case $[g, h] = t_1$, $[g, i] = t_2$ and $[h, i] = t_3$, where t_1, t_2, t_3 are pairwise distinct involutions in G' . In this case,

$$[gh, gi] = [g, i][h, g][h, i] = t_2t_1t_3 = 1,$$

and so $\langle gh, gi \rangle Z(G)/Z(G) \cong E_4$, a contradiction. We have proved that $|G'| \geq 8$. \square

Corollary 91.5. *Let G be an arbitrary nonabelian 2-group. Let A and B be any two distinct maximal abelian subgroups in G with intersection $A \cap B$ of maximal possible order. Then the nonabelian subgroup $H = \langle A, B \rangle$ either possesses an abelian subgroup of index 2 or H is of class 2 and H' is elementary abelian.*

Proof. Obviously, $A \cap B = Z(H)$. If C and D are any two distinct maximal abelian subgroups in H , then $C \cap D \geq Z(H)$ and the maximality of $|A \cap B|$ forces $C \cap D = Z(H)$. Then our result follows from Theorem 91.3. \square

On minimal nonabelian subgroups of p -groups

1^o . In studying the structure of nonabelian p -groups G , the minimal nonabelian subgroups of G play an important role since they generate the group G (Theorem 10.28). More precisely, if A is a maximal normal abelian subgroup of G , then minimal nonabelian subgroups of G cover the set $G - A$ (Lemma 57.1).

It is an open problem to classify nonabelian p -groups which are covered by its minimal nonabelian subgroups. Here we consider two special cases of this problem.

First we determine in Theorem 92.1 nonabelian p -groups G with the property that $C_G(x) \leq H$ for any minimal nonabelian subgroup H of G and each $x \in H - Z(G)$. It is easily seen that the assumption of Theorem 92.1 implies that each abelian subgroup of G is contained in a minimal nonabelian subgroup and so in this case G is covered by its minimal nonabelian subgroups.

In Theorem 92.2 we shall classify nonabelian p -groups G such that whenever A is a maximal subgroup of any minimal nonabelian subgroup H in G , then A is also a maximal abelian subgroup of G . Again, it easily seen that the assumption of Theorem 92.2 implies that each abelian subgroup of G is contained in a minimal nonabelian subgroup in G and so the minimal nonabelian subgroups of G cover G .

Theorem 92.1 (Janko). *Let G be a nonabelian p -group such that for each minimal nonabelian subgroup H of G and each $x \in H - Z(G)$, we have $C_G(x) \leq H$. Then G is one of the following groups:*

- (a) G is minimal nonabelian.
- (b) $p = 2$, $d(G) = 3$ and

$$G = \langle a, b, c \mid a^4 = b^4 = c^4 = 1, [a, b] = c^2, [a, c] = b^2c^2, [b, c] = a^2b^2,$$

$$[a^2, b] = [a^2, c] = [b^2, a] = [b^2, c] = [c^2, a] = [c^2, b] = 1 \rangle,$$

where G is a special 2-group of order 2^6 with $\langle a^2, b^2, c^2 \rangle = G' = Z(G) = \Phi(G) = \Omega_1(G) \cong E_8$ and G is isomorphic to a Sylow 2-subgroup of the simple group $Sz(8)$.

- (c) $p > 2$, $d(G) = 2$, G is of order 2^5 and

$$G = \langle a, x \mid a^{p^2} = x^{p^2} = 1, [a, x] = b, [a, b] = y_1, [x, b] = y_2,$$

$$b^p = y_1^p = y_2^p = [a, y_1] = [x, y_1] = [a, y_2] = [x, y_2] = 1,$$

$$a^p = y_1^\alpha y_2^\beta, x^p = y_1^\gamma y_2^\delta \rangle,$$

where in case $p > 3$, $4\beta\gamma + (\delta - \alpha)^2$ is a quadratic non-residue mod p . Here $\Phi(G) = G' = \langle b, y_1, y_2 \rangle = \Omega_1(G) \cong E_{p^3}$, $Z(G) = K_3(G) = \mathfrak{U}_1(G) = \langle y_1, y_2 \rangle \cong E_{p^2}$.

Conversely, all the above groups satisfy the assumptions of the theorem.

Proof. Let G be a nonabelian p -group such that for each minimal nonabelian subgroups H of G and each $x \in H - Z(G)$, we have $C_G(x) \leq H$. Let A be a maximal normal abelian subgroup of G . Then for each $x \in G - A$, there is an element $x \in A$ such that $H = \langle a, x \rangle$ is minimal nonabelian (Lemma 57.1). Since $a \notin Z(H)$, it follows that $C_G(a) \leq H$ and so $A \leq H$. But A is a maximal abelian subgroup in H and so $|H : A| = p$ and $x^p \in A$. It follows that $\exp(G/A) = p$. If $H = G$, then G is minimal nonabelian so it is as in (a).

In what follows we assume that $|G/A| \geq p^2$. For each $x \in G - A$, $x^p \in A$, $A\langle x \rangle$ is minimal nonabelian and $x \notin Z(A\langle x \rangle)$ so that $C_G(x) \leq A\langle x \rangle$ and $C_G(x) = \langle x \rangle C_A(x)$ is abelian and $|A : C_A(x)| = p$. Therefore, A and $C_G(x)$ ($x \in G - A$) are all maximal abelian subgroups in G . Let K/A be a normal subgroup of order p in G/A and set $A_0 = Z(K)$ so that $A_0 < A$ and $|A : A_0| = p$. Suppose that there is $g \in G - K$ such that $A_1 = C_A(g) \neq A_0$. Let $y \in A_1 - A_0$ so that $y \in K - Z(G)$ and so we must have $C_G(y) \leq K$. This is a contradiction since $g \in G - K$ and g centralizes y .

We have proved that for each $g \in G - K$, $C_A(g) = A_0$ and so $A_0 = Z(G)$, and $A = \langle A_0, a \rangle$ with an element $a \in A - A_0$. For any $g_1, g_2 \in G$ we have $a^{g_1} = az_1$, $a^{g_2} = az_2$ with $z_1, z_2 \in A_0 = Z(G)$ so that $a^{g_1^{-1}} = az_1^{-1}$ and $a^{g_2^{-1}} = az_2^{-1}$ and therefore $a^{[g_1, g_2]} = a$ which gives $[g_1, g_2] \in C_G(A) = A$. Thus, G/A is elementary abelian and also $\mathfrak{U}_1(G) \leq A_0 = Z(G)$. In addition, $A_0 = Z(G) = Z(K) = \Phi(K) \leq \Phi(G)$ which implies that either $\Phi(G) = Z(G)$ or $\Phi(G) = A$.

Let $S/A \cong E_{p^2}$ be a subgroup of order p^2 in G/A . Since $\mathfrak{U}_1(S) \leq Z(G) = Z(S)$, $S/\mathfrak{U}_1(S)$ is of exponent p and order $\geq p^3$ so that S is non-metacyclic. If $|Z(G)| = p$, then $|A| = p^2$ and $C_G(A) = A$ implies that $|G : A| = p$, a contradiction. Hence $|Z(G)| > p$ so that $|S| > p^4$.

(i) First assume that $\Phi(S) = A$. In that case each maximal subgroup of S is minimal nonabelian and we are in a position to use Proposition 71.5. Since $d(S) = 2$, we get $p > 2$, $|S| = p^5$, $A = S' = \Omega_1(S) \cong E_{p^3}$ and $Z(S) = K_3(S) = \mathfrak{U}_1(S) \cong E_{p^2}$. Since $C_G(A) = A$ and G/A is elementary abelian, we get (by the structure of $\mathrm{GL}(3, p)$) $S = G$ and we have obtained the groups from (c).

(ii) Now assume that $\Phi(S) = Z(G)$ so that $d(S) = 3$. Each maximal subgroup of S containing A is minimal nonabelian. Let M be a maximal subgroup of S which does not contain A so that $M/M \cap A \cong E_{p^2}$ and $M \cap A = Z(G) = \Phi(S)$. If $m \in M - A$, then $C_G(m) = \langle m \rangle Z(G)$ with $m^p \in Z(G)$ so that M is nonabelian. Let M_0 be a minimal nonabelian subgroup of M . Then $M_0 > Z(G)$ and since $|M_0/Z(G)| \geq p^2$, we have $M_0 = M$. Hence, each maximal subgroup of S is minimal nonabelian, $|S| > p^4$, S is non-metacyclic and $d(S) = 3$. By Proposition 71.5, $p = 2$, $|S| = 2^6$, $Z(G) = Z(S) = \Omega_1(S) = \Phi(S) \cong E_8$ and so A is abelian of type $(4, 2, 2)$. Let $a \in A - Z(G)$ so that $o(a) = 4$ and for each $g \in G$, $a^g = az$ with $z \in Z(G)$. Since

$C_G(A) = A$, we get $|G/A| \leq 8$. Suppose that $|G/A| = 8$. Then there is $h \in G - A$ such that $h^2 \in Z(G)$ and $a^h = aa^2 = a^{-1}$. If $h^2 = a^2$, then $\langle h, a \rangle \cong Q_8$ which is minimal nonabelian. If $h^2 \neq a^2$, then $\langle h, a \rangle$ is metacyclic minimal nonabelian of order 2^4 . But in any case, $Z(G) \not\leq \langle h, a \rangle$, contrary to our assumption. Hence $|G/A| = 4$ and so $S = G$ and we have obtained the group stated in part (b) of our theorem. \square

Theorem 92.2. *Let G be a nonabelian p -group such that whenever A is a maximal subgroup of any minimal nonabelian subgroup H in G , then A is also a maximal abelian subgroup of G . Then each abelian subgroup of G is contained in a minimal nonabelian subgroup and one of the following holds:*

- (a) G is minimal nonabelian.
- (b) G is metacyclic.
- (c) G is isomorphic to the group of order 2^6 defined in Theorem 92.1(b).
- (d) G is isomorphic to a group of order p^5 defined in Theorem 92.1(c).

Proof. Let G be a nonabelian p -group such that whenever A is a maximal subgroup of any minimal nonabelian subgroup H in G , then A is also a maximal abelian subgroup of G . First we note that our assumption is hereditary for all nonabelian subgroups of G . Let A be any maximal abelian subgroup of G . Let $B > A$ be a subgroup of G such that $|B : A| = p$ and let $b \in B - A$. By Proposition 57.1, there is $a \in A$ such that $H = \langle a, b \rangle$ is minimal nonabelian. Then $|H : H \cap A| = p$ and so $H \cap A$ must be a maximal abelian subgroup in G . This gives $H \cap A = A$ and so $H = A\langle b \rangle = B$ is minimal nonabelian. We have proved that whenever A is a maximal abelian subgroup of G and a subgroup X contains A as a subgroup of index p , then X is minimal nonabelian. We may assume that G is not minimal nonabelian (case (a) of our theorem) and so G does not possess any abelian maximal subgroup. Moreover, if U is a nonabelian subgroup of G and if U possesses an abelian maximal subgroup, then U is minimal nonabelian.

(i) Assume $p > 2$. First we consider the case that G has no normal elementary abelian subgroups of order p^3 and use Theorem 13.7. In case (a) of that theorem G is metacyclic so it is as in (b). The case (b) of Theorem 13.7 cannot occur. Indeed, in that case G is a 3-group of maximal class which possesses a self-centralizing subgroup X of order 9. If $Y/X < G/X$ is of order 3 and $Y \not\leq G_1$, where G_1 is the fundamental subgroup of G , then $C_G(X) = G_1 \not\leq Y$, a contradiction since Y is minimal nonabelian. It remains to consider part (c) of Theorem 13.7, where $G = EH$, $E = \Omega_1(G)$ is nonabelian of order p^3 and exponent p , H is cyclic with $E \cap H = Z(E)$. Let E_0 be a normal abelian subgroup of type (p, p) contained in E so that $C_G(E_0)$ covers G/E . But $C_G(E_0)/E_0$ is cyclic so that $C_G(E_0)$ is an abelian maximal subgroup of G , a contradiction.

It remains to consider the case, where G has an abelian subgroup of type (p, p, p) . Let A be a maximal normal abelian subgroup of G with $|\Omega_1(A)| \geq p^3$. We have $|G/A| \geq p^2$ since G does not have an abelian maximal subgroup.

(i1) Suppose that G/A is cyclic. Let H/A be the subgroup of order p in G/A so that H is a non-metacyclic minimal nonabelian group of order $\geq p^4$ and so $\Omega_1(H) = \Omega_1(A) \cong E_{p^3}$ which implies that there are no elements of order p in $G - A$. Let $K > H$ be a subgroup with $|K : H| = p$ so that $K/A \cong C_{p^2}$. Let $k \in K - H$ so that $\langle k \rangle$ covers K/A and since $\langle k \rangle \cap A \neq \{1\}$, we have $\exp(K) \geq p^3$. Let M be any maximal subgroup of K which does not contain A . Then M covers K/A . Since K is not minimal nonabelian, it follows that M is nonabelian. On the other hand, $M \cap H < H$ is an abelian maximal subgroup of M which implies that M is minimal nonabelian. We have proved that each maximal subgroup of K is minimal nonabelian. By Proposition 71.5, $|K| = p^5$ and $\exp(K) = p^2$, a contradiction.

(i2) Assume that G/A is noncyclic. Let S/A be a normal elementary abelian subgroup of order p^2 in G/A . Then S is non-metacyclic and for each subgroup X_i/A of order p in S/A , X_i is minimal nonabelian ($i = 1, 2, \dots, p+1$). Set $Z_i = Z(X_i) = \Phi(X_i) \leq \Phi(S)$ and we may assume that for a fixed i' , $X_{i'}$ is normal in G . Let Y be a maximal subgroup of S which does not contain A so that Y covers S/A . If Y is abelian, then S is minimal nonabelian, a contradiction. Hence Y is nonabelian with an abelian maximal subgroup $Y \cap X_{i'} < X_{i'}$ so that Y is minimal nonabelian. We use Proposition 71.5 and see that $|S| = p^5$, $S' = \Omega_1(S) = A \cong E_{p^3}$ and $Z(S) = \mathcal{U}_1(S) = Z_{i'} \cong E_{p^2}$. Note that $C_G(A) = A$ and so either $S = G$ and we have obtained groups stated in (d) or G/A is non-abelian of order p^3 and exponent p . In the second case, we consider another subgroup $S^*/A \cong E_{p^2}$ in G/A (distinct from S/A). We have $S \cap S^* = X_{i'}$ since $X_{i'}/A$ is central in G/A and so $X_{i'}/A = \Phi(G/A)$. We show (as above) that each maximal subgroup of S^* is minimal nonabelian and so S^* is isomorphic to a group of Proposition 71.5(b) which gives $Z_{i'} = Z(X_{i'}) = Z(S^*)$ and so $Z_{i'} = Z(G)$. But then G/A stabilizes the chain $A > Z_{i'} > \{1\}$ which gives that G/A is elementary abelian, a contradiction.

(ii) We suppose $p = 2$ and we may assume that G is non-metacyclic. Let E be a minimal non-metacyclic subgroup of G . We use Theorem 66.1 and see that in cases (b), (c) and (d) of that theorem, E is nonabelian and possesses an abelian maximal subgroup. It follows that in these cases E must be minimal nonabelian which is not the case. Hence $E \cong E_8$ which is case (a) of Theorem 66.1. We claim that whenever A is a maximal abelian subgroup of rank ≥ 3 in G and $K > A$ is a subgroup of G such that $|K : A| = 4$, then $|K| = 2^6$ and K is isomorphic to the group of Proposition 71.5(a) so that $K' = Z(K) = \Phi(K) = \Omega_1(K) = \Omega_1(A) \cong E_8$ and A is abelian of type $(4, 2, 2)$. Indeed, if $X > A$ is a maximal subgroup of K containing A , then $|X : A| = 2$ and therefore X is minimal nonabelian with $E_8 \cong \Omega_1(A) = \Omega_1(X)$. Let Y be a maximal subgroup of K distinct from X . Since K is not minimal nonabelian, Y is nonabelian. But $Y \cap X (< X)$ is an abelian maximal subgroup of Y and so Y is minimal nonabelian. We have proved that K is a non-metacyclic group of order $> 2^4$ all of whose maximal subgroups are minimal nonabelian. It follows that K is isomorphic to the group of Proposition 71.5(a) and our claim is proved.

Suppose that $K \neq G$ and let $L > K$ be a subgroup of G with $|L : K| = 2$. Acting with L/K on seven subgroups $A_i/\Omega_1(A)$ ($i = 1, 2, \dots, 7$) of order 2 in $K/\Omega_1(A) \cong E_8$ (where all A_i are abelian of type $(4, 2, 2)$ and they are also maximal abelian subgroups in G), we see that one of them $A_{i'}$ is certainly normal in L . We note that $L/A_{i'}$ is a noncyclic group of order 8 since $K/A_{i'} \cong E_4$. Let $K^*/A_{i'}$ be a maximal subgroup of $L/A_{i'}$ distinct from $K/A_{i'}$. By the preceding paragraph, K^* is isomorphic to the group of Proposition 71.5(a). It follows $\Omega_1(A) = Z(K^*)$ so that $\Omega_1(A) = Z(L)$. Set $A_{i'} = \langle a, \Omega_1(A) \rangle$, where $o(a) = 4$ and $L/A_{i'}$ acts faithfully on $A_{i'}$ stabilizing the chain $A_{i'} > \Omega_1(A) > \{1\}$. In particular, there is $l \in L$ such that $a^l = aa^2 = a^{-1}$. Hence $\langle a, l \rangle$ is a metacyclic minimal nonabelian subgroup so that $\Omega_1(A) \not\leq \langle a, l \rangle$. This is a contradiction since $\Omega_1(A)$ centralizes $\langle a, l \rangle$. Hence $K = G$ and we have obtained the group of part (c) of our theorem. \square

2^o . In Theorem 92.6 we classify nonabelian 2-groups all of whose minimal nonabelian subgroups are isomorphic to Q_8 or $\mathcal{H}_2 = \langle a, b \mid a^4 = b^4 = 1, a^b = a^{-1} \rangle$. This theorem generalizes a result of N. Blackburn [Bla7] concerning p -groups G which possess nonnormal subgroups and such that the intersection of all nonnormal subgroups is nontrivial (Corollary 92.7). Namely, it is easy to see that in such p -groups G we must have $p = 2$ and each minimal nonabelian subgroup of G is isomorphic to Q_8 or \mathcal{H}_2 .

Let G be a nonabelian 2-group all of whose minimal nonabelian subgroups are isomorphic to Q_8 or \mathcal{H}_2 . Then we prove the following three key lemmas which play an important role in the proof of Theorem 92.6.

Lemma 92.3. *We have $\Omega_1(G) \leq Z(G)$.*

Proof. Since D_8 is not a subgroup of G , $\Omega_1(G)$ is elementary abelian. Let $x \in G$ be any element of order 4 so that $x^2 \in \Omega_1(G)$ and assume that $G_0 = \Omega_1(G)\langle x \rangle$ is nonabelian. By Lemma 57.1 applied to the group G_0 , there is $a \in \Omega_1(G)$ such that $\langle a, x \rangle$ is minimal nonabelian. But then a is a noncentral involution in $\langle a, x \rangle$, contrary to the structure of Q_8 or \mathcal{H}_2 . Hence x centralizes $\Omega_1(G)$. Since G is generated by its minimal nonabelian subgroups, we have $\Omega_2(G) = G$ which implies $\Omega_1(G) \leq Z(G)$. \square

Lemma 92.4. *Suppose that G possesses an element v of order 4 such that $C_G(v)$ is nonabelian. Then $C_G(v)$ has minimal nonabelian subgroups isomorphic to \mathcal{H}_2 and for each such subgroup $H = \langle a, b \mid a^4 = b^4 = 1, a^b = a^{-1} \rangle$, we have $v^2 = a^2b^2$ (which is a unique involution in H which is not a square in H) and $H\langle v \rangle = \langle a, vb \rangle \times \langle v \rangle \cong Q_8 \times C_4$. In particular, G does not possess a subgroup isomorphic to $\mathcal{H}_2 \times C_4$.*

Proof. Since $C_G(v)$ possesses central elements of order 4, Corollary A.17.3 implies that $C_G(v)$ has subgroups isomorphic to \mathcal{H}_2 and let $H = \langle a, b \mid a^4 = b^4 = 1, a^b = a^{-1} \rangle$ be one of them. First suppose that $\langle v \rangle \cap H = \{1\}$. Then $(av)^2 = a^2v^2 \notin H$

and $(av)^b = a^b v = a^{-1}v = (av)a^2$ so that $\langle av, b \rangle$ is a nonmetacyclic minimal nonabelian subgroup of order 2^5 and exponent 4, a contradiction. Hence $v \notin H$ and $v^2 \in \{a^2, b^2, a^2b^2\}$. If $v^2 = a^2$, then $i = va \notin H$ is an involution and $i^b = va^{-1} = ia^2$ so that $i \notin Z(G)$, contrary to Lemma 92.3. If $v^2 = b^2$, then $j = vb \notin H$ is an involution and $j^a = vb^a = ja^2$ so that $j \notin Z(G)$, contrary to Lemma 92.3. It follows that we must have $v^2 = a^2b^2$ which is a unique involution in H which is not a square in H . In that case $(vb)^2 = v^2b^2 = (a^2b^2)b^2 = a^2$ and $a^{vb} = a^b = a^{-1}$ so that $\langle a, vb \rangle \cong Q_8$ and $H\langle v \rangle = \langle a, vb \rangle \times \langle v \rangle \cong Q_8 \times C_4$. \square

Lemma 92.5. *The group G has no subgroups isomorphic to $Q_8 \times C_4 \times C_4$.*

Proof. Suppose that $K = Q \times \langle c \rangle \times \langle d \rangle$ is a subgroup of G , where $Q = \langle a, b \rangle \cong Q_8$ and $\langle c \rangle \cong \langle d \rangle \cong C_4$. We have $\Omega_1(K) = \langle a^2, c^2, d^2 \rangle \cong E_8$, where $[ac, bd] = [a, b] = a^2$ so that $\langle ac, bd \rangle' = \langle a^2 \rangle$ and therefore $\langle ac, bd \rangle$ is minimal nonabelian (Lemma 65.1). But $(ac)^2 = a^2c^2$ and $(bd)^2 = a^2d^2$ so that $\Omega_1(\langle ac, bd \rangle) = \langle a^2c^2, a^2d^2, a^2 \rangle = \langle a^2, c^2, d^2 \rangle \cong E_8$ and so $\langle ac, bd \rangle$ is nonmetacyclic, a contradiction. \square

Theorem 92.6. *Let G be a nonabelian 2-group all of whose minimal nonabelian subgroups are isomorphic to Q_8 or $\mathcal{H}_2 = \langle a, b \mid a^4 = b^4 = 1, a^b = a^{-1} \rangle$. Then the following holds:*

- (a) *If G is of exponent > 4 , then G has a unique abelian maximal subgroup A , $|G'| > 2$, and all elements in $G - A$ are of order 4. We have $\Omega_1(A) = \Omega_1(G) \leq Z(G)$ and if $x \in G - A$, then x inverts each element of $A/\Omega_1(A)$.*
- (b) *If G is of exponent 4, then $G = K \times V$, where $\exp(V) \leq 2$ and for the group K we have one of the following possibilities:*
 - (b1) $K \cong Q_8$ or $K \cong \mathcal{H}_2$;
 - (b2) $K = \langle a, b, c \mid a^4 = b^4 = c^4 = [a, b] = 1, c^2 = a^2, [a, c] = b^2, [b, c] = a^2 \rangle$ is the minimal nonmetacyclic group of order 2^5 ;
 - (b3) K is a unique special group of order 2^6 with $Z(K) \cong E_4$ given in Theorem 57.3(b3) in which every maximal subgroup is isomorphic to the minimal nonmetacyclic group of order 2^5 (from (b2));
 - (b4) $K \cong Q_8 \times C_4$;
 - (b5) $K \cong Q_8 \times Q_8$;
 - (b6) $G = K \times V$ has an abelian maximal subgroup B of exponent 4 and an element $v \in G - B$ of order 4 which inverts each element of B ;
 - (b7) $K = Q * C$ is a central product of $Q = \langle a, b \rangle \cong Q_8$ and $C = \langle c, d \mid c^4 = d^4 = 1, c^d = c^{-1} \rangle \cong H_2$ with $Q \cap C = \langle c^2d^2 \rangle = Z(Q)$, where K is special of order 2^6 and $Z(K) = \Omega_1(K) \cong E_4$.

Conversely, in each of the above groups in part (b) every minimal nonabelian subgroup is isomorphic to Q_8 or \mathcal{H}_2 .

Proof. Let G be a nonabelian 2-group all of whose minimal nonabelian subgroups are isomorphic to Q_8 or \mathcal{H}_2 . Let A be a maximal normal abelian subgroup of G so that $\Omega_1(G) = \Omega_1(A) \leq Z(G)$ (Lemma 92.3) and $\Omega_1(A) < A$. By Proposition 57.2, all elements in $G - A$ are of order 4 and so G/A is elementary abelian.

Suppose that $\exp(A) > 4$. Then by Proposition 57.2, $|G : A| = 2$ and if $x \in G - A$, then $o(x) = 4$ and x inverts each element in $A/\Omega_1(A)$. Let $a \in A$ with $o(a) = 8$. Then $a^x = a^{-1}z$ with $z \in \Omega_1(A)$ so that $[a, x] = a^{-2}z$ is of order 4 and so $|G'| > 2$. If G has more than one abelian maximal subgroup, then $|G : Z(G)| = 4$ and Lemma 1.1 gives $|G| = 2|Z(G)||G'|$ and $|G'| = 2$, a contradiction. Hence A is a unique abelian maximal subgroup of G .

In what follows we assume that $\exp(A) = \exp(G) = 4$. In view of Corollary A.17.3 and Theorem 57.3 we may also assume that both Q_8 and \mathcal{H}_2 are subgroups of G . We have $\Phi(G) \leq \Omega_1(A) \leq Z(G)$ and $|\Phi(G)| \geq 4$. If x, y are elements of order 4 in G with $[x, y] \neq 1$, then $[x, y]$ is an involution in $Z(G)$ and so (Lemma 65.1) $\langle x, y \rangle \cong \mathcal{H}_2$ or Q_8 which implies that in case $x^2 \neq y^2$, we have $\langle x, y \rangle \cong \mathcal{H}_2$ and $y^x \in \{y^{-1}, yx^2\}$.

Considering $G/\Phi(G)$ we get $G = K \times V$, where $\Omega_1(A) = \Phi(G) \times V$, $\exp(V) \leq 2$, $\Omega_1(K) = \Phi(K) = \Phi(G) \leq Z(K)$ and $A \cap K$ is a maximal normal abelian subgroup of K . We have to determine the structure of K and so in the sequel we may assume $K = G$ and so in that case $\Omega_1(A) = \Omega_1(G) = \Phi(G) \leq Z(G)$.

First assume $|\Phi(G)| = 4$ so that our group G has exactly three involutions. By the results stated in the introduction to §82, G has a metacyclic normal subgroup M such that G/M is elementary abelian of order ≤ 4 . But $\exp(M) \leq 4$ and so $|M| \leq 2^4$ and $|G| \leq 2^6$. Since both \mathcal{H}_2 and Q_8 are subgroups of G , we have $|G| \geq 2^5$.

Suppose that $|G| = 2^5$. In this case G is nonmetacyclic since $\exp(G) = 4$. If G were minimal nonmetacyclic, then each minimal nonabelian subgroup of G is isomorphic to \mathcal{H}_2 (see Theorem 66.1), contrary to our assumptions. But G has only three involutions and so Theorem 66.1 implies that G has a minimal nonmetacyclic subgroup $H = Q \times \langle u \rangle$ with $Q = \langle a, b \rangle \cong Q_8$, $Z(Q) = \langle z \rangle$ and u is an involution. Since $\Phi(G) = \langle z, u \rangle \cong E_4$, we may assume (interchanging u and uz if necessary) that there is an element $v \in G - H$ such that $v^2 = u$. If $G' = Q' = \langle z \rangle$, then Q is normal in G , $G/Q \cong C_4$ and v induces an inner automorphism on Q . In that case $G = QC_G(Q)$ with $Q \cap C_G(Q) = \langle z \rangle$ and $C_G(Q)/\langle z \rangle \cong C_4$. But $\exp(G) = 4$ and so $C_G(Q)$ splits over $\langle z \rangle$ and we get $G \cong Q_8 \times C_4$ which is a group of part (b4) of our theorem. We assume that $G' = \langle z, u \rangle = \Omega_1(G) = \Phi(G)$. If $[a, v] \in \langle z \rangle$ and $[b, v] \in \langle z \rangle$, then $G = \langle a, b, v \rangle$ implies that $G/\langle z \rangle$ would be abelian and so $G' = \langle z \rangle$, contrary to our assumption. It follows that we may assume (interchanging a and b if necessary) that $[a, v] \in \langle z, u \rangle - \langle z \rangle$. Since $a^2 = z \neq [a, v]$, we have $\langle a, v \rangle \cong H_2$ and so $[a, v] = u = v^2$ and $v^a = v^{-1}$. We have $[a, bv] = [a, b][a, v] = zu \neq a^2 = z$ and therefore $\langle a, bv \rangle \cong H_2$. It follows that $(bv)^2 = zu$ or z . If $zu = (bv)^2 = b^2v^2[v, b] = zu[v, b]$, then $[v, b] = 1$. If $z = (bv)^2 = b^2v^2[v, b] = zu[v, b]$, then $[v, b] = u$ which implies $[v, ab] = [v, a][v, b] = uu = 1$ and so in that case replacing

b with $b' = ab$ we get $[v, b'] = 1$. Hence writing again b instead of b' we may assume again $[v, b] = 1$. In both cases we may assume $[v, b] = 1$ so that $\langle v, b \rangle \cong C_4 \times C_4$. We get $G = \langle v, b \rangle \langle a \rangle$, where a inverts $\langle v, b \rangle$ and so we have obtained a group of part (b6).

Suppose that $|G| = 2^6$. First assume that G has a normal subgroup $Q = \langle a, b \rangle \cong Q_8$ and set $Z(Q) = \langle z \rangle$. Since $G' \leq \Phi(G) = \Omega_1(G) \leq Z(G)$, no element in $G - Q$ induces an outer automorphism on Q (if $x \in G - Q$ induces an outer automorphism on Q , then $(Q\langle x \rangle)' \cong C_4$). We get $G = Q * C$, where $C = C_G(Q)$ and $Q \cap C = \langle z \rangle$. Also, z is not a square in C . Indeed, if $x \in C$ with $x^2 = z$, then $\langle a, bx \rangle \cong D_8$, a contradiction. We have $\exp(C) = 4$, $|C| = 2^4$ and $\Omega_1(C) = \Omega_1(G) \cong E_4$. If C is abelian, then $C \cong C_4 \times C_4$ in which case z is a square in C , a contradiction. Hence C is nonabelian. If C is minimal nonabelian, then $C = \langle c, d \mid c^4 = d^4 = 1, c^d = c^{-1} \rangle \cong H_2$. Since z is not a square in C , we must have $z = c^2 d^2$ and this is the group of part (b7) of our theorem. If C is not minimal nonabelian, it possesses a subgroup $Q^* \cong Q_8$ with $Q^* \cap \langle z \rangle = \{1\}$. We get $G = Q \times Q^*$ and this is a group of part (b5).

Now we treat the case, where no quaternion subgroup is normal in G . Let $Q = \langle a, b \rangle \cong Q_8$ be a quaternion subgroup of G with $Z(Q) = \langle z \rangle$. Set $W = \Omega_1(G)$ so that $\Phi(G) = W \cong E_4$, $W \leq Z(G)$ and $W \cap Q = \langle z \rangle$. Since Q is not normal in G , we have $Q' = \langle z \rangle \neq G'$ which gives $G' = W$. Since $|G| = 2^6$, $\exp(G) = 4$, and G has only three involutions, G does not have an abelian maximal subgroup. Set $H = QW$ so that H is normal in G . Since Q is not normal in G , there is $c \in G - H$ such that $[Q, c] \not\leq \langle z \rangle$. Interchanging a and b if necessary, we may assume $[a, c] \not\leq \langle z \rangle$ and so $[a, c] = u \in W - \langle z \rangle$ and $H = Q \times \langle u \rangle$. Since $\langle a, c \rangle$ is minimal nonabelian and $a^2 = z \neq [a, c] = u$, we have $\langle a, c \rangle \cong H_2$ so that z and u are the only involutions which are squares in $\langle a, c \rangle$. If $c^2 = z$, then $(ac)^2 = a^2 c^2 [c, a] = zzu = u$ and $[a, ac] = u$ so that replacing c with $c' = ac$ (if necessary), we may assume (writing again c instead of c') from the start that $c^2 = u$. We consider the subgroup $\langle a, bc \rangle$ noting that $[a, bc] = zu$ and $a^2 = z$. It follows that $\langle a, bc \rangle \cong H_2$ so that $(bc)^2 \in \{zu, z\}$. If $zu = (bc)^2 = b^2 c^2 [c, b] = zu[c, b]$, then $[c, b] = 1$. If $z = (bc)^2 = b^2 c^2 [c, b] = zu[c, b]$, then $[c, b] = u$ so that $[c, ab] = uu = 1$. Therefore, replacing b with $b' = ab$ if necessary and writing again b instead of b' , we may assume from the start that $[c, b] = 1$. Hence a inverts the abelian subgroup $\langle b, c \rangle \cong C_4 \times C_4$. Set $M = \langle a, b, c \rangle$ and consider the abelian subgroup $X = \langle a, W \rangle$ of type $(4, 2)$. We have $C_M(X) = X$, X is normal in G , $\text{Aut}(X) \cong D_8$ and $G/X \cong E_8$. It follows that there is $d \in G - M$ centralizing X so that $\langle a, d \rangle W$ is abelian of order 2^4 and therefore $\langle a, d \rangle W \cong C_4 \times C_4$. Replacing d with a suitable element in $\langle a, d \rangle - X$, we may assume from the start that $d^2 = u$. If $[c, d] = 1$, then cd would be an involution in $G - W$, a contradiction. Hence $[c, d] \neq 1$, $[a, d] = 1$ and $G = \langle a, b, c, d \rangle$ and so it remains to determine the action of d on $\langle b, c \rangle \cong C_4 \times C_4$. We have $\langle c, d \rangle \cong Q_8$ or H_2 and so $[c, d] \in \{u, z, uz\}$. Also, $[b, d] = 1$ or $\langle b, d \rangle \cong H_2$ and so we have $[b, d] \in \{1, z, u\}$. If $[b, d] = z$ and $[c, d] = u$, then d inverts $\langle b, c \rangle$. But in that case ad centralizes $\langle b, c \rangle$ and so $\langle b, c \rangle \langle ad \rangle$ would be an abelian maximal

subgroup of G , a contradiction. It follows that we have to consider the following eight possibilities for $[b, d]$ and $[c, d]$:

- (1) If $[b, d] = 1$ and $[c, d] = u$, then $\langle c, d \rangle \cong Q_8$ and $\langle c, d \rangle$ is normal in G , a contradiction.
- (2) If $[b, d] = 1$ and $[c, d] = z$, then $[b, cd] = 1$ and $(cd)^2 = c^2d^2[d, c] = z = b^2$ so that bcd is an involution in $G - W$, a contradiction.
- (3) If $[b, d] = 1$ and $[c, d] = uz$, then $[ad, c] = z$ and $(c \cdot ad)^2 = 1$ so that cad is an involution in $G - W$, a contradiction.
- (4) If $[b, d] = z$ and $[c, d] = z$, then $\langle bc, ad \rangle \cong Q_8$ and $\langle bc, ad \rangle$ is normal in G since $[a, bc] = zu, [d, bc] = 1, [b, ad] = 1, [c, ad] = zu$. This contradicts our assumption.
- (5) If $[b, d] = z$ and $[c, d] = uz$, then $[ad, c] = z$ and $(c \cdot ad)^2 = 1$ so that cad is an involution in $G - W$, a contradiction.
- (6) If $[b, d] = u$ and $[c, d] = u$, then $\langle c, d \rangle \cong Q_8$ and $\langle c, d \rangle$ is normal in G since $[a, c] = u, [b, c] = 1, [a, d] = 1, [b, d] = u$. This contradicts our assumption.
- (7) If $[b, d] = u$ and $[c, d] = z$, then $[bc, ad] = 1, (bc)^2 = zu, (ad)^2 = zu$, so that $bcad$ is an involution in $G - W$, a contradiction.
- (8) If $[b, d] = u$ and $[c, d] = uz$, then $[ad, c] = z$ and $(c \cdot ad)^2 = 1$ so that cad is an involution in $G - W$, a contradiction.

In the rest of the proof we assume that $|\Phi(G)| > 4$. First we consider the case that G possesses an element v of order 4 such that $C_G(v)$ is nonabelian. By Lemma 92.4, there is a quaternion subgroup $Q = \langle a, b \rangle$ contained in $C_G(v)$ such that $Q \cap \langle v \rangle = \{1\}$ and we set $Z(Q) = \langle z \rangle$. Let A be a maximal abelian subgroup of G containing $\langle v \rangle \times \langle a \rangle \cong C_4 \times C_4$. It follows that A is a maximal normal abelian subgroup of G since $A > Z(G)$ and G is of class 2. Moreover, we have $\Omega_1(A) = \Omega_1(G) \leq Z(G)$ and $\Phi(G) \leq \Omega_1(A)$. Suppose there is $x \in A$ such that $x^2 \notin \langle v^2, z \rangle$ and so $\langle x^2, v^2, z \rangle \cong E_8$. By Lemma 92.5, b does not commute with x and so $\langle b, x \rangle \cong H_2$ since $x^2 \neq b^2 = z$. But then $\langle b, x, v \rangle = \langle b, x \rangle \times \langle v \rangle \cong \mathcal{H}_2 \times C_4$ which contradicts Lemma 92.4. We have proved $|\mathcal{O}_1(A)| = 4$ so that A is of type $(4, 4, 2, \dots, 2)$, $AQ = A\langle b \rangle, C_G(\langle v, a \rangle) = A, \Phi(AQ) = \langle v^2, z \rangle \cong E_4$ and $(AQ)' = \langle z \rangle$. Since $|\Phi(G)| > 4$, there is an element $u \in G - (AQ)$ such that $u^2 \notin \langle v^2, z \rangle$ and therefore $\langle u^2, v^2, z \rangle \cong E_8$. Suppose that u commutes with an element x of order 4 in $\langle v, a \rangle$. We may set $\langle v, a \rangle = \langle x, y \rangle$ for a suitable element y of order 4 in $\langle v, a \rangle$. The fact that $C_G(\langle x, y \rangle) = A$ implies that $[u, y] \neq 1$ so that $\langle u, y \rangle \cong H_2$ because $u^2 \neq y^2$. But $\Omega_1(\langle u, y \rangle) = \langle u^2, y^2 \rangle$ and so $x^2 \notin \langle u^2, y^2 \rangle$ (because $\langle u^2, x^2, y^2 \rangle \cong E_8$). We have $\langle u, y, x \rangle = \langle u, y \rangle \times \langle x \rangle \cong \mathcal{H}_2 \times C_4$, contrary to Lemma 92.4. We have proved that u does not commute with any element of order 4 in $\langle v, a \rangle$. Suppose that u does not invert an element x of order 4 in $\langle v, a \rangle$. Then $\langle u, x \rangle \cong H_2$ implies that $x^u = xu^2$. If y is any element of order 4 in $\langle v, a \rangle$ with $y^2 \neq x^2$ and $y^u \neq y^{-1}$, then $y^u = yu^2$.

But then $(xy)^u = (xu^2)(yu^2) = xy$, a contradiction. Hence $y^u = y^{-1}$ and noting that $(xy)^2 = x^2y^2 \neq x^2$, we also get $(xy)^u = (xy)^{-1}$. But we get then

$$x^u = ((xy)y^{-1})^u = (xy)^u(y^u)^{-1} = (xy)^{-1}y = x^{-1}y^{-1}y = x^{-1},$$

a contradiction. We have proved that u inverts $\langle v, a \rangle$. If u commutes with any element $s \in Q - \langle a \rangle = Q - A$, then $s^2 = z$ and $\langle u, v, s \rangle = \langle u, v \rangle \times \langle s \rangle \cong \mathcal{H}_2 \times C_4$, contrary to Lemma 92.4. Hence u does not commute with any element of $Q - \langle a \rangle$. Suppose that u inverts an element $w \in Q - \langle a \rangle$ so that $[u, w] = z$. But then $[u, aw] = [u, a][u, w] = zz = 1$, a contradiction. Hence u does not invert any element in $Q - \langle a \rangle$. Since $\langle u, b \rangle \cong \langle u, ab \rangle \cong H_2$, the above results imply $[u, b] = [u, ab] = u^2$. But then $u^2 = [u, ab] = [u, a][u, b] = zu^2$ which gives $z = 1$, a final contradiction.

We have proved that the centralizer of each element of order 4 is abelian. Let again A be any maximal normal abelian subgroup of G so that we have $\Omega_1(G) = \Omega_1(A) = Z(G)$ since for each $x \in G - A$, $C_A(x) = \Omega_1(A)$. Also, $\Omega_1(A) < A$ and $|A : \Omega_1(A)| = |\mathfrak{U}_1(A)|$. Let $x \in G - A$ and consider any element $y \in A$ with $y^2 \notin \langle x^2 \rangle$ and suppose that $y^x \neq y^{-1}$ so that (noting that $\langle x, y \rangle \cong \mathcal{H}_2$) $y^x = yx^2$. Assume further that there is $v \in A$ with $v^2 \notin \langle x^2, y^2 \rangle$. If $v^x \neq v^{-1}$, then $v^x = vx^2$ and $(vy)^x = (vx^2)(yx^2) = vy$, a contradiction since $o(vy) = 4$. Thus $v^x = v^{-1}$. Since $(vy)^2 \notin \langle x^2, y^2 \rangle$, we also get $(vy)^x = (vy)^{-1}$ and this implies $y^x = y^{-1}$, a contradiction. Hence, $y^x = y^{-1}$ for all $y \in A$ with $y^2 \notin \langle x^2 \rangle$ and so x inverts A . We have proved that in case $|A : \Omega_1(A)| \geq 8$, each element $x \in G - A$ inverts A and so $|G : A| = 2$ and $G = A\langle x \rangle$ which gives groups in part (b6).

Assume that $|A : \Omega_1(A)| = |\mathfrak{U}_1(A)| = 4$ so that $A = \langle y, z \rangle \Omega_1(A)$ with $\langle y, z \rangle \cong C_4 \times C_4$ and $\mathfrak{U}_1(A) = \langle y^2, z^2 \rangle$. Since $|\Phi(G)| > 4$, there is an element $u \in G - A$ such that $u^2 \notin \langle y^2, z^2 \rangle$. By the arguments of the previous paragraph, u inverts A and $A\langle u \rangle$ is a group in part (b6). Assume that $A\langle u \rangle \neq G$ and let $x \in G - (A\langle u \rangle)$. If $x^2 \notin \langle y^2, z^2 \rangle$, then x would invert A and then $xu \notin A$ and xu would centralize A , a contradiction. Hence $x^2 \in \langle y^2, z^2 \rangle$ and we may set (say) $x^2 = z^2$. If x inverts some element s of order 4 in $\langle y, z \rangle$, then xu centralizes s , a contradiction. Since $\langle y, x \rangle \cong \langle yz, x \rangle \cong \mathcal{H}_2$, we have $y^x = yz^2$, $(yz)^x = (yz)z^2$ and then $(yz)z^2 = (yz)^x = y^x z^x = yz^2 z^x$, which gives $z^x = z$, a contradiction.

It remains to consider the case where $|A : \Omega_1(A)| = 2$ for each maximal normal abelian subgroup A of G . We have $A = \langle y \rangle \Omega_1(A)$ and note that each maximal abelian subgroup of G is normal in G and so G does not possess a subgroup isomorphic to $C_4 \times C_4$. For each $x \in G - A$, we have $[x, y] \neq 1$. Suppose that each $x \in G - A$ inverts y . Then $|G : A| = 2$, $G = A\langle x \rangle$, $\langle x, y \rangle \cong Q_8$ or \mathcal{H}_2 and $\Phi(G) = \langle x^2, y^2 \rangle$ which is of order ≤ 4 , contrary to our assumption. Hence there is $x \in G - A$ such that $y^x \neq y^{-1}$ and so $\langle x, y \rangle \cong H_2$. If $x^2 = y^2$, then replacing x with $x' = xy$, we get $(x')^2 \neq y^2$ and x' does not invert y . Writing again x instead of x' , we may assume from the start that $x^2 \neq y^2$ and $y^x = yx^2$ and we have $\Phi(A\langle x \rangle) = \langle x^2, y^2 \rangle \cong E_4$. Since $|\Phi(G)| > 4$, there is $u \in G - (A\langle x \rangle)$ with $u^2 \notin \langle x^2, y^2 \rangle$. Then we have $y^u \in \{y^{-1}, yu^2\}$ since $u^2 \neq y^2$ and $\langle u, y \rangle \cong \mathcal{H}_2$. We have $[x, u] \neq 1$ and so

$\langle x, u \rangle \cong \mathcal{H}_2$ which gives $(xu)^2 \in \{u^2, x^2\}$ and so in any case $(xu)^2 \neq y^2$. First suppose $y^u = y^{-1}$. Then $y^{xu} = (yx^2)^u = y(y^2x^2)$. Since $\langle y, xu \rangle \cong \mathcal{H}_2$, we get $y^{xu} = yy^2$ or $y^{xu} = y(xu)^2$. But from the above, $y^{xu} = y(y^2x^2)$ and so we must have $(xu)^2 = y^2x^2$, contrary to the above result that $(xu)^2 \in \{u^2, x^2\}$. Hence we have the second possibility $y^u = yu^2$ and this gives $y^{xu} = (yx^2)^u = y(u^2x^2)$ and so $u^2x^2 = y^2$ (which is not possible since $u^2 \notin \langle x^2, y^2 \rangle$) or $u^2x^2 = (xu)^2$. But then we have $u^2x^2 = (xu)^2 = x^2u^2[u, x]$ which gives $[u, x] = 1$, a final contradiction. \square

Corollary 92.7 ([Bla7]). *Let G be a finite p -group which possesses nonnormal subgroups and let $R(G)$ be the intersection of all nonnormal subgroups. If $R(G) > \{1\}$, then $p = 2$, $|R(G)| = 2$ and G is one of the following groups:*

- (a) $G \cong Q_8 \times C_4 \times E_{2^s}$, $s \geq 0$,
- (b) $G \cong Q_8 \times Q_8 \times E_{2^s}$, $s \geq 0$,
- (c) G has an abelian maximal subgroup A of exponent > 2 and an element $x \in G - A$ of order 4 which inverts each element in A .

Proof. Let H be a minimal nonabelian subgroup of G which is not isomorphic to Q_8 . By Proposition 1.26, we get $p = 2$, $H \cong \mathcal{H}_2 = \langle a, b \mid a^4 = b^4 = 1, a^b = a^{-1} \rangle$ and so $R(G) = R(H) = \langle b^2 \rangle$ is of order 2. If all minimal nonabelian subgroups of G are isomorphic to Q_8 , then Corollary A.17.3 implies that $G = Q \times V$, where $Q \cong Q_{2^n}$ is generalized quaternion of order 2^n , $n \geq 4$, and $\exp(V) \leq 2$ and so again $R(G) = Z(Q)$ is of order 2.

We are in a position to use Theorem 92.6. Suppose that G is a group of part (a) of that theorem. For each $a \in A$, $o(ax) = 4$ ($x \in G - A$) and so $\langle ax \rangle$ is not normal in G (since $|G'| > 2$). This gives $x^2 = (ax)^2 = ax^2a^x$ and $a^x = a^{-1}$ and so we have obtained a group of part (a) of our corollary. If G is a group of Theorem 92.6(b2), then we have $\langle a \rangle \cap \langle b \rangle = \{1\}$, and $\langle a \rangle$ and $\langle b \rangle$ are nonnormal in K , a contradiction. If G is a group of Theorem 92.6(b7), then $\langle d \rangle \cap \langle ad \rangle = \{1\}$ and $\langle d \rangle$ and $\langle ad \rangle$ are nonnormal in K , a contradiction. Hence there remain groups given in parts (a), (b) and (c) of our corollary. \square

Appendix 16

Some central products

In this section we consider central products of some small 2-groups. Recall that a group G is a central product of its subgroups A and B , if $G = AB$ and $[A, B] = \{1\}$; we write $G = A * B$. In that case, $A \cap B \leq Z(G)$. If $A \cap B = \{1\}$, then $A * B = A \times B$. It is possible to define a central product of arbitrary number of groups. Central products of a finite number of groups have appeared in §4.

The following two exercises are cited many times in this book.

Exercise A. Suppose that a p -group $G = A * C$, where C is cyclic of order $> p$ and $A \cap C = \Omega_1(C)$. Let \mathcal{C} be the set of cyclic subgroups of A of order p^2 containing $\Omega_1(C)$ and \mathcal{K} the nonempty set of all subgroups of order p in G not contained in A . Write $|\mathcal{C}| = t$. Then $|\mathcal{K}| = tp$, and so

$$(A) \quad c_1(G) = |\mathcal{K}| + c_1(A) = tp + c_1(A).$$

In particular,

$$(B) \quad c_1(D_{2^n} * C) = 2 \cdot 1 + (2^{n-1} + 1) = 2^{n-1} + 3,$$

$$(C) \quad c_1(Q_{2^n} * C) = 2(2^{n-2} + 1) + 1 = 2^{n-1} + 3,$$

$$(D) \quad c_1(SD_{2^n} * C) = 2(2^{n-3} + 1) + 2^{n-2} + 1 = 2^{n-1} + 3.$$

We also have $c_1(M_{2^n} * C) = 2 \cdot 2 + 3 = 7$. If $A = \mathcal{H}_2 = \langle a, b \mid a^4 = b^4 = 1, a^b = a^3 \rangle$ and $\mathcal{H}_2 \cap C = \langle a^2b^2 \rangle$, then (A) is not applicable (in that case, $t = 0$). If $\mathcal{H}_2 \cap C = \langle b^2 \rangle$, then $c_1(G) = 2 \cdot 4 + 3 = 11$. If $\mathcal{H}_2 \cap C = \langle a^2 \rangle$, then $c_1(G) = 2 \cdot 2 + 3 = 7$.

Solution. Since G/A is cyclic, every element of G of order p is contained in $A\Omega_2(C)$, so one may assume from the start that $|C| = p^2$. Take $x \in G - A$ of order p . Then $x = ac$, where $a \in A - C$ and $\langle c \rangle = C$. It follows from $a^p c^p = (ac)^p = x^p = 1$ that $a^p = c^{-p}$ so $o(a) = p^2$. Therefore, every element $x \in G - A$ of order p is contained in ZC , where $\Omega_1(C) < Z < A$, Z is cyclic of order p^2 (in our concrete case, $Z = \langle a \rangle$). If $V < A$ is another cyclic subgroup of order p^2 with $\Omega_1(C) < V$, then $ZC \cap VC = C$ and VC has exactly p subgroups of order p not contained in C (note that $ZC \cong VC \cong C_{p^2} \times C_p$). If \mathcal{L}_1 be the set of subgroups of order p in ZC that are not contained in C , and let \mathcal{L}_2 be defined similarly for VC ; then

$|\mathcal{L}_1| = |\mathcal{L}_2| = p$, $\mathcal{L}_1 \cap \mathcal{L}_2 = \emptyset$ and members of sets \mathcal{L}_1 and \mathcal{L}_2 are not contained in A (indeed, $A \cap ZC = Z$ and $A \cap VC = V$). Let \mathcal{C} and \mathcal{K} be defined as in the statement of exercise. Then $|\mathcal{K}| = \sum_{Z \in \mathcal{C}} [c_1(ZC) - 1] = tp$, where $t = |\mathcal{C}|$. Thus, $c_1(G) = |\mathcal{K}| + c_1(A) = tp + c_1(A)$, where $t = |\mathcal{C}|$, and this proves formula (A).

In particular, if A of our exercise is irregular of order p^{p+1} , then $\Omega_1(C) = \mathfrak{V}_1(A)$ so

$$\begin{aligned} c_1(A * C) &= c_1(A) + pc_2(A) = c_1(A) + p \frac{p^{p+1} - (p-1)c_1(A) - 1}{p(p-1)} \\ &= \frac{p^{p+1} - 1}{p-1} = 1 + p + \dots + p^p, \end{aligned}$$

and this number is independent of the structure of A .

Exercise B. Let a 2-group $G = A * Q$, where $Q \cong Q_{2^n}$ and $A \cap Q = Z(Q)$. Find $c_1(G)$ if we know $c_1(A)$ and the number t of cyclic subgroups of A of order 4 containing $\Omega_1(Q)$.

Solution. Let T be a subgroup of order 2 of G not contained in A . Then $AT \cap Q = C \cong C_4$ since all subgroups of Q of order 4 are cyclic. Clearly, $T < AC$. By (A), AC contains exactly $2t$ subgroups of order 2 not contained in A . If C_1 is another cyclic subgroup of order 4 in Q , then $AC \cap AC_1 = A$. Since $c_2(Q) = 2^{n-2} + 1$, we get

$$(E) \quad c_1(G) = 2t(2^{n-2} + 1) + c_1(A).$$

Here t is the number of cyclic subgroups of A containing $Z(Q)$ (if $t = 0$, then $c_1(G) = c_1(A)$ which is obvious). In particular, we have

$$(F) \quad c_1(D_{2^m} * Q_{2^n}) = 2(2^{n-2} + 1) + 2^{m-1} + 1 = 2^{n-1} + 2^{m-1} + 3,$$

$$(G) \quad c_1(Q_{2^m} * Q_{2^n}) = 2(2^{m-2} + 1)(2^{n-2} + 1) + 1,$$

$$(H) \quad c_1(SD_{2^m} * Q_{2^n}) = 2(2^{m-3} + 1)(2^{n-2} + 1) + 2^{m-2} + 1.$$

From this we have $c_1(D_8 * D_8) = c_1(Q_8 * Q_8) = 2(2+1)(2+1) + 1 = 19$ (since $D_8 * D_8 \cong Q_8 * Q_8$) and $c_1(D_8 * Q_8) = 2(2+1) + 2^2 + 1 = 11$; both these results are known.

1°. Let $G = Q * C$, where $Q = \langle a, b \mid a^4 = 1, a^2 = b^2, a^b = a^{-1} \rangle \cong Q_8$ and $C = \langle c \mid c^4 = 1 \rangle \cong C_4$, $Q \cap C = Z(Q) = \langle a^2 \rangle = \langle c^2 \rangle$, Then $|G| = 2^4$, $\Phi(G) = G' = Q'$ is of order 2, $d(G) = 3$ so $\exp(G) = 4$ and $|\Gamma_1| = 7$. Next, $Z(G) = C$, $G/C \cong E_4$ so C is contained in exactly 3 members of the set Γ_1 , and all these members are abelian of type (4, 2). All other members of the set Γ_1 are nonabelian since G is nonabelian (see Exercise 1.6(a)). Set $ab = d$ and $A = \langle a \rangle$, $B = \langle b \rangle$, $D = \langle d \rangle$. The following seven distinct elements are involutions: a^2 , ac , a^3c , bc , b^3c , dc , d^3c . The cyclic subgroups A, B, D, C contain exactly 8 distinct

elements of order 4: $a, a^3, b, b^3, d, d^3, c, c^3$. It follows that all involutions of G have listed so that $c_1(G) = 7$. Since $\exp(G) = 4$, we get $c_2(G) = \frac{16-8}{2} = 4$. Next we list the set Γ_1 . As we know, there are exactly three distinct abelian maximal subgroups of G : $A_1 = \langle a, c \rangle$, $A_2 = \langle b, c \rangle$, $A_3 = \langle d, c \rangle$; all of them contain $C = Z(G)$. It remains to find $7 - 4 = 3$ nonabelian maximal subgroups of G . One of these is Q . Since $a^{bc} = a^b = a^{-1}$ and $o(bc) = 2$, the subgroup $D_1 = \langle a, bc \rangle \cong D_8$. Similarly, $D_2 = \langle d, bc \rangle \cong D_8$ and $D_3 = \langle b, dc \rangle \cong D_8$ are two remaining nonabelian members of the set Γ_1 . Since D_1, D_2 and D_3 are dihedral, it follows that Q is characteristic in G ; obviously, $C = Z(G)$ is also characteristic in G and it is the unique cyclic subgroup of order 4 not contained in Q . We have also $G = D_i * C$ for $i = 1, 2, 3$. In particular, $Q_8 * C_4 \cong D_8 * C_4$ if the both products are of order 16. It follows from $c_1(G) = 7$ that $\Omega_1(G) > D_1$ so $\Omega_1(G) = G$. Since $|G : Q| = 2$, G has no elementary abelian subgroups of order 8. It follows that all four-subgroups are G -invariant. Since all subgroups of order 4 contain $G' = \mathfrak{V}_1(G)$ and $c_2(G) = 4$, we conclude that G contains exactly $7 - 4 = 3$ normal four-subgroups.

2^o. In this subsection, $G = Q * C$, where $Q_{2^n} \cong Q = \langle a, b \mid a^{2^{n-1}} = 1, a^{2^{n-2}} = b^2, a^b = a^{-1} \rangle \cong Q_{2^n}$, $n > 3$, $C = \langle c \mid c^4 = 1 \rangle \cong C_4$ and $Q \cap C = Z(Q)$. Then $|G| = 2^{n+1}$, $\Phi(G) = G' = Q'$ so $d(G) = 3$ and $|\Gamma_1| = 7$. Set $A = \langle a \rangle$, $\beta = a^{2^{n-3}}$, $\alpha = \beta^2$; then $o(\alpha) = 2$, $o(\beta) = 4$. It follows from $(c\beta)^2 = c^2\beta^2 = c^4 = 1$ that $\gamma = c\beta$ is an involution. Set $A_1 = \langle a, c \rangle$; then $A_1 = \langle a \rangle \times \langle \gamma \rangle$ is abelian of type $(2^{n-1}, 2)$. Since $\text{cl}(G) = \text{cl}(Q) = n - 1 > 2$, A_1 is the unique abelian maximal subgroup of G .

Let us find the numbers of elements of given order in G . If u is a generator of A , then $(ub^3)^2 = (ub)^2 = ub^2u^b = ub^2u^{-1} = b^2$ so $o(ub) = o(ub^3) = 4$. Since all elements in $Q - A$ have order 4, $\beta, \beta^3, a^i b$, $i = 1, 2, \dots, 2^{n-1}$, are all $2^{n-1} + 2$ elements of order 4 in Q . Let $Z = \langle z \rangle < G$ be cyclic of order 4 such that $z \in G - (A \cup C)$. Then $QZ = G$ so $Z \cap Q = Z(Q)$. We have $z = uc$, where $u \in Q$ and $\langle c \rangle = C$. Then $\alpha = z^2 = u^2c^2 = u^2\alpha$ so $u^2 = 1$, $u = \alpha$ and $z \in C$, a contradiction. Thus, all cyclic subgroups of order 4 in G are contained in Q or C . There are two elements of order 4 in C . Thus, we obtained $2^{n-1} + 2 + 2 = 2^{n-1} + 4$ elements of order 4 so $c_2(G) = \frac{1}{2}(2^{n-1} + 4) = 2^{n-2} + 2$. By Exercise A (see formula (C)), $c_1(G) = 2^{n-1} + 3$. Next, A_1 contains exactly $|\Omega_k(A_1)| - |\Omega_{k-1}(A_1)| = 2^{k+1} - 2^k = 2^k$ elements of orders 2^k , $2 < k < n$. Since

$$\begin{aligned} 2^{n-1} + 3 + 2^{n-1} + 4 + (2^3 + \dots + 2^{n-1}) &= 2^n + 7 + 2^n - 8 \\ &= 2^{n+1} - 1 = |G^\#|, \end{aligned}$$

we conclude that $c_1(G) = 2^{n-1} + 3$, $c_2(G) = 2^{n-2} + 2$ and $c_k(G) = 2$ for $k = 3, \dots, n - 1$.

It remains to find five members of the set $\Gamma_1 - \{Q, A_1\}$, where $A_1 = \langle a, c \rangle$. We have $\Phi(G) = G' = \langle a^2 \rangle = \mathfrak{V}_1(A)$. Since $a^{bc} = a^b = a^{-1}$ and $(bc)^2 = 1$, we get $D = \langle a, bc \rangle \cong D_{2^n}$. The group D contains exactly $2^{n-1} + 1$ distinct involutions so

$G - D$ contains exactly two involutions hence D is the unique dihedral member of the set Γ_1 . Thus, Q , A_1 and D are all maximal subgroups of G containing A .

Let D_1 and D_2 be nonabelian maximal subgroups of D ; then $D_1, D_2 \in \Gamma_2$ so $G/D_1 \cong E_4 \cong D_2$. Then D_i ($i = 1, 2$) is contained in three maximal subgroups D, U_i, V_i . By Proposition 13.18(b), exactly two among subgroups D, U_i, V_i are of maximal class, say D, U_i ($i = 1, 2$). Since $G - D$ contains exactly two involutions and $D_i < U_i$, it follows that $U_i \cong SD_{2^n}$. We denote $U_i = SD_i$.

Next, $U = \langle ac \rangle$ is another cyclic subgroup of G of order 2^{n-1} . Since $c_{n-1}(G) = 2$ and $A \triangleleft G$, we get $U \triangleleft G$. Set $d = ac$. Since G/U is abelian of type $(2, 2)$, exactly three members of the set Γ_1 contain D , and one of them is A_1 . Thus, Q, D_1, SD_1 and SD_2 are of maximal class. By Theorem 5.4, all other maximal subgroups of G are not of maximal class. We see that Q and D_1 are characteristic in G . It remains to find yet two maximal subgroups of G . Set $M = D_1 * C$ and $N = D_2 * C$; then $M \neq N$. Clearly, $M \cong N$. Thus, $\Gamma_1 = \{Q, D, SD_1, SD_2, M, N, A_1\}$. Thus, we have proved the following

Proposition A.16.1. (a) $G = Q_8 * C_4 \cong D_8 * C_4$ if both these central products have order 2^4 . All proper subgroups of G are metacyclic. The subgroup of G isomorphic with Q_8 is characteristic. G has exactly three subgroups $\cong D_8$, $c_1(G) = 7$.

(b) Let $n > 3$; then $G = Q_{2^n} * C_4 \cong D_{2^n} * C_4 \cong SD_{2^n} * C_4$ provided $|G| = 2^{n+1}$. Exactly five members of the set Γ_1 have rank two, other two (namely, M and N) have rank three. Two members of the set Γ_1 that are isomorphic with Q_{2^n} and D_{2^n} , are characteristic in G . Exactly two members of the set Γ_1 are isomorphic with SD_{2^n} . Next, $c_1(G) = 2^{n-1} + 3$, $c_2(G) = 2^{n-2} + 2$, $c_k(G) = 2$ ($k = 3, \dots, n-1$).

Exercise 1. (a) Prove that $Q * C \cong D * C \cong SD * C$, where $Q \cong Q_{2^m}$, $D \cong D_{2^m}$, $SD \cong SD_{2^m}$, $C \cong C_{2^n}$, $m > 3$, $n > 2$, and all three central products have the same order 2^{m+n-1} .

(b) Find $c_k(G)$ for the group G from (a).

(c) List all maximal subgroups of the group G from (a).

Exercise 2. Let $G = Q_8 * Q_8$, $H = D_8 * D_8$, and $F = Q_8 * D_8$, $|G| = |H| = |F| = 32$. Let $L \in \{G, H, F\}$. (a) Prove that $G \cong H$ but $G \not\cong F$. (b) Find $c_k(L)$, $k = 1, 2$. (c) Find the number of nonabelian subgroups of order 8 in L . (d) Find the number of subgroups of L isomorphic with Q_8 . (e) List all maximal subgroups of L .

Exercise 3. Find $c_k(G)$, using the description of maximal subgroups of G from Proposition A.16.1.

Exercise 4. Let $G = M * N$, where M is a 2-group of maximal class and order $2^n > 8$ and N is nonabelian of order 8. Find the numbers of subgroups of maximal class and orders 8 and 2^n in G .

Exercise 5. Let G be the central product with amalgamated centers of m copies of a group of maximal class and order 2^n , $n > 3$. (i) Find $c_k(G)$ for all $k \in \mathbb{N}$. (ii) Describe all maximal abelian subgroups of G . (iii) Find the number of subgroups of maximal class and order 2^n in G .

Exercise 6. Let $H = Q * C$ be a subgroup of a 2-group G such that $Q \cong Q_{2^n}$, $C \cong C_4$, and $Q \cap C = Z(Q)$. Suppose that $G - H$ has no elements of order 4. Show that H and Q are characteristic in G . (Hint. $\Omega_2^*(H) = \langle x \in H \mid o(x) = 4 \rangle = H$ and Q is characteristic in H .)

Exercise 7. Prove that a 2-group $G = Q * C$, where Q is of maximal class, C is cyclic and $Q \cap C = Z(Q)$, has no elementary abelian subgroups of order 8.

Exercise 8. Let G be a 2-group of Proposition A.16.1(b). Is it true that the number of semidihedral subgroups of order 2^k , $k \in \{4, \dots, n-1\}$, in G is even?

Exercise 9. Let G be a group of Proposition A.16.1(b) with $n > 5$. Prove that the number of subgroups of maximal class and order 2^k in G equals 2^{n-k+2} .

Solution. Let $M < G$ be of maximal class and order 2^k . Then $C * M$ is of order 2^{k+1} and $CM = C * (CM \cap Q)$, where $CM \cap Q = Q_{2^k}$. Next, CM has exactly 4 subgroups of maximal class and order 2^k so every subgroup of Q of maximal class and order 2^k produces exactly three new subgroups of maximal class and order 2^k in G and these subgroups are not contained in Q . Since Q contains exactly 2^{n-k} subgroups of maximal class and order 2^k , the desired number is $2^{n-k} + 3 \cdot 2^{n-k} = 2^{n-k+2}$.

Exercise 10. Let a 2-group $G = QZ$, where $Q \cong Q_{2^n}$ is maximal in G , $Z \cong C_4$ is normal in G and $C_G(Z)$ is abelian. Prove that Q is a direct factor of G .

Solution. We proceed by induction on n . It suffices to show that $Z(G) \cong E_4$. Suppose that $n = 3$. Then $Z(G)$ is of order 4 (Proposition 10.17). If $Z(G)$ is cyclic, then $Z(G) = Z$ since Z is the only one cyclic subgroup of order 4 not contained in Q , and we get a contradiction. We are done if $n = 3$. Now suppose that $n > 3$. Let nonabelian $M < Q$ be maximal and set $H = MZ$. By induction, $Z(MZ) = R \cong E_4$. We have $C_G(Z) = AZ \in \Gamma_1$, where $A < Q$ is cyclic of index 2. In that case, AZ is abelian of type $(2^{n-1}, 2)$. Then $H \cap AZ$ is noncyclic (indeed, Z is maximal cyclic in H). Since $H \cap AZ$ is a maximal abelian subgroup of a nonabelian group H , we get $R = Z(H) \leq H \cap AZ$. Then $C_G(R) \geq HAZ = HA = G$, so $Z(G) = R \cong E_4$.

3^o. In this subsection we consider $G = Q_1 * Q_2$, where $|G| = 2^5$ and

$$Q_1 = \langle a, b \mid a^4 = 1, a^2 = b^2, a^b = a^{-1} \rangle \cong Q_8,$$

$$Q_2 = \langle c, d \mid c^4 = 1, c^2 = d^2, c^d = c^{-1} \rangle \cong Q_8.$$

Then G is extraspecial of order 2^5 , and $M_1 = \langle c, Q_1 \rangle$, $M_2 = \langle d, Q_1 \rangle$, $M_3 = \langle cd, Q_1 \rangle \in \Gamma_1$. For $k = 1, 2$, we have $c_k(G) = c_k(M_1) + c_k(M_2) + c_k(M_3) - 2$.

$c_k(Q_1)$. By 1^o , $c_1(M_i) = 7$ and $c_2(M_i) = 4$ for $i = 1, 2, 3$. Therefore, $c_1(G) = 7 + 7 + 7 - 2 = 19$ and $c_2(G) = 4 + 4 + 4 - 2 \cdot 3 = 6$. Thus, Q_1 and Q_2 contain all cyclic subgroups of order 4 from G .

All nonabelian subgroups of G of order 8 are contained in Γ_2 and all cyclic subgroups of order 4 are normal in G . Let $A < G$ be cyclic of order 4. Since $C_G(A)/A \cong E_4$, A is contained in exactly three abelian subgroups of order 8 so in $7 - 3 = 4$ nonabelian subgroups of order 8. By §76, G contains exactly 20 nonabelian subgroups of order 8. It follows from 1^o that G has exactly two subgroups $\cong Q_8$, namely Q_1 and Q_2 . By Lemma 64.1(q), G has no abelian subgroups of index 2.

Let D be a dihedral subgroup (of order 8) in G . Since $D' = G'$, we get $D \triangleleft G$. We have $G = DC_G(D)$ (Lemma 4.3). Since Q_1 and Q_2 are the only quaternion subgroups of G and they do not centralize D , we get $C_G(D) \cong D_8$. Thus, $Q_8 * Q_8 \cong D_8 * D_8$.

If $A < G$ is cyclic of order 4, then $C_G(A) \cong Q_8 * C_4 (\cong D_8 * C_4)$. Since $G = D * C_G(D)$ and $C_G(D) \cong D_8$, it follows that G contains a subgroup isomorphic with E_8 (such subgroup is contained in $D \times Z$, where Z is a noncentral subgroup of order 2 in $C_G(D)$). If A and C are cyclic subgroups of order 4 in Q_1 and Q_2 , respectively, then AC is abelian of type (4, 2). In such a way we obtain all 9 abelian subgroups of type (4, 2) in G . Since all subgroups of order 8 are members of the set Γ_2 , there are in G exactly $|\Gamma_2| - 20 - 9 = 6$ elementary abelian subgroups of order 8.

4^o . In this subsection $G = Q * D$, where $|G| = 2^5$, $Q \cong Q_8$ is as in 1^o and $D = \langle c, d \mid c^4 = d^2 = 1, c^d = c^{-1} \rangle \cong D_8$. Then G is extraspecial.

If $e \in D - \langle d \rangle$ is an involution and $M_1 = Q * \langle c \rangle$, $M_2 = Q \times \langle d \rangle$, $M_3 = Q \times \langle e \rangle$, then

$$c_1(G) = c_1(M_1) + c_1(M_2) + c_1(M_3) - 2c_1(Q) = 7 + 3 + 3 - 2 \cdot 1 = 11$$

so $c_2(G) = \frac{|G| - c_1(G) - 1}{\varphi(4)} = 10$ since $\exp(G) = 4$. The number of nonabelian subgroups of order 8 in G equals 20 (see §76). We have $Q_8 * Q_8 \not\cong Q_8 * D_8$ if both central products are of order 32 (indeed, these groups have different numbers of involutions). It follows that if $D < G$ is dihedral, then $C_G(D) \cong Q_8$ so the numbers of dihedral and quaternion subgroups in G are equal to 10.

Exercise 11. Let $G = Q_1 * Q_2$, where Q_1 and Q_2 are generalized quaternion groups. Find $c_k(G)$ for all $k \in \mathbb{N}$.

Exercise 12. Let $G = M_1 * M_2$, where $M_1 \cong M_{2^m}$, $M_2 \cong M_{2^n}$ and $|M_1 \cap M_2| = \min \{|Z(M_1)|, |Z(M_2)|\}$. Find $c_k(G)$ for all $k \in \mathbb{N}$.

Exercise 13. Let $G = R * S$, where R and S are 2-groups of maximal class and orders 2^m , 2^n , respectively, $m > 3, n > 3$, $|G| = 2^{m+n-1}$. Find the numbers of nonlinear irreducible characters of each possible degree. Find $k(G)$.

Solution. We have $|G : G'| = 2^4$, $G' = \Phi(G)$, $Z(G) = Z(R) = Z(S)$ is of order 2 so G has a faithful irreducible character. The number of non-faithful irreducible characters of G equals the number of irreducible characters of $G/Z(G) \cong (R/Z(G)) \times (S/Z(G))$, i.e., $(2^{m-3} + 3)(2^{n-3} + 3)$. Every faithful irreducible character of G is of degree 4 so the number of such characters equals $\frac{|G| - |G/Z(G)|}{4^2} = \frac{2^{m+n-1} - 2^{m+n-2}}{4^2} = 2^{m+n-6}$. Note that $k(G) = |\text{Irr}(G)|$.

Exercise 14. Let $G = R \times S$, where R, S are 2-groups of maximal class. Find the number of nonabelian subgroups of order 8 in G .

Exercise 15. Let a 2-group $G = QZ$, where Q is a normal subgroup of maximal class and Z is normal cyclic, $Z \cap Q = Z(Q)$ and $C_G(Z)$ is abelian. Is it true that $|Z(G)| > 2$?

Exercise 16. Let $G = HC$ be a p -group, where $C = \langle c \rangle \triangleleft G$ is cyclic of order p^2 and H is a subgroup of maximal class and order p^{p+1} , $|G : H| = p$. Find $c_1(G)$.

Appendix 17

Alternate proofs of characterization theorems of Miller and Janko on 2-groups, and some related results

G. A. Miller [Mil9] has classified the minimal non-Dedekindian 2-groups. We offer, in Theorem A.17.1, another proof of Miller's result. Then, in Theorem A.17.2, we classify the 2-groups all of whose nonabelian maximal subgroups are of the form $Q \times E$, where Q is generalized quaternion and $\exp(E) \leq 2$; our proof is based on Miller's theorem. Corollary A.17.3 is a partial case of Theorem 90.1 classifying the 2-groups all of whose minimal nonabelian subgroups have order 8.

A nonabelian 2-group G is said to be *generalized dihedral* if it is nonabelian and contains such subgroup A that all elements of the set $G - A$ are involutions. Then A is abelian, $|G : A| = 2$, all subgroups of A are G -invariant, $\Omega_1(A) = Z(G)$ and G/G' is elementary abelian since $\Omega_1(G) = G$ (Burnside). It is easy to check that A is the unique subgroup of G satisfying the above properties. Next, every minimal nonabelian subgroup of our group is isomorphic with D_8 . Nonabelian sections of generalized dihedral groups are generalized dihedral.

A p -group $M \times E$ is said to be an M^\times -group if M is of maximal class and E is elementary abelian (we consider the group $\{1\}$ as elementary abelian p -group). The above group is said to be an M_3^\times -group if, in addition, $|M| = p^3$. Nonabelian epimorphic images of M^\times -groups are M^\times -groups.

Suppose that a p -group $G = M \times E$, where M is nonabelian with cyclic center and $E > \{1\}$, is elementary abelian. Suppose that nonabelian $M_1 < G$ has no direct factors of order p . We claim that then M_1 is isomorphic to a subgroup of M . Indeed, it suffices to prove that $M_1 \cap E = \{1\}$. Assume, however, that $X = M_1 \cap E_1 > \{1\}$; then $|X| = p$ since $Z(M)$ is cyclic. Since $X \leq E$, we get $X \not\leq \Phi(G)$ so $G = X \times G_0$ for some $G_0 < G$. Then, by the modular law, $M_1 = X \times (M_1 \cap G_0)$, contrary to the hypothesis. In particular, if $|M_1| = |M|$, then $G = M_1 \times E$ and $M_1 \cong M$. Next, if $M_1 < G$ is minimal nonabelian, then M_1 is isomorphic to a subgroup of M . In what follows, we use these facts freely.

Remarks. 1. Let $G = M \times C$, where M is a p -group of maximal class and $C = \langle c \rangle$ is cyclic of order p^n , $n > 1$. We claim that G contains a nonmetacyclic \mathcal{A}_1 -subgroup H of order p^{n+2} with $|H \cap M| = p^2$, unless M is generalized quaternion.

Indeed, by Blackburn's theorem (see Theorem 9.6), M contains a nonabelian subgroup $D = \langle R, a \rangle$ of order p^3 , where $|R| = p^2$ and $o(a) \leq p^2$. Set $u = ac$; then $R \cap \langle u \rangle = \{1\}$, $o(u) = o(c)$. We assert that $L = \langle u, R \rangle = \langle u \rangle \cdot R$ is the desired subgroup. Indeed, $|L'| = p$ since L is nonabelian, and $d(L/L') = 2$ so L is minimal nonabelian, by Lemma 65.2(a); we also have $|L| = p^{n+2}$. If M is not generalized quaternion, one can take from the start $R \cong E_{p^2}$; in that case, L is not metacyclic since $E_{p^3} \cong R \times \Omega_1(C) < L$. (If M is generalized quaternion, then $|\Omega_1(G)| = 4$, so, by Lemma 65.1, all \mathcal{A}_1 -subgroups of G are metacyclic.)

2. Suppose that a group G of order $2^m > 2^4$ is not of maximal class. Let $H \in \Gamma_1$ be of maximal class. Then the set Γ_1 contains exactly four members, say $H = H_1, H_2, H_3, H_4$, of maximal class (Theorem 12.12(c)). Suppose that all nonabelian members of the set Γ_1 are M^\times -groups. We claim that then G itself is an M^\times -group. Assume that our claim is false. Let $Z < H$ be cyclic of index 2; then, since $|H| \geq 16$, Z (of order ≥ 8) is characteristic in H so normal in G . Next, G contains a normal abelian subgroup R of type $(2, 2)$ (Lemma 1.4); then $R \cap H = \Omega_1(Z)$. Since $A = RZ \in \Gamma_1$ is not an M^\times -group, it must be abelian, by hypothesis, and $|A : Z| = 2$. Let F be a nonabelian maximal subgroup of H . Then $RF \in \Gamma_1$ since $|RF| = |H|$, and RF is an M^\times -group which is not of maximal class since $|RF| \geq 16$. It follows that $R = Z(RF)$. Since $R < A$ (otherwise, $G = RA$ is of class $2 < 3 \leq \text{cl}(H)$, by Fitting's lemma; see Introduction, Theorem 21), we get $C_G(R) \geq A(RF) = AF = G$ so $R = Z(G)$. If $L < R$ is of order 2 and $L \not\leq H$, then $G = HL = H \times L$ is an M^\times -group.

3. Let G be a p -group which is not of maximal class and $A, H \in \Gamma_1$, where A is abelian and H is of maximal class. Then $|Z(G)| = p^2$ and $G = HZ(G)$. Indeed, $G' = H'$ has index p^3 in G (Theorem 12.12(a)). Then $|Z(G)| = \frac{1}{p}|G/G'| = p^2$ (Lemma 64.1(q) = Lemma 1.1) so $G = HZ(G)$.

Theorem A.17.1 ([Mil9]). *If G is a minimal non-Dedekindian 2-group, then G is either minimal nonabelian or isomorphic to Q_{16} .*

Proof. One may assume that G is not an \mathcal{A}_1 -group (= minimal nonabelian) so $|G| = 2^m > 2^3$. Let $H = Q \times E \in \Gamma_1$, where $Q \cong Q_8$ and $\exp(E) \leq 2$. Suppose that $E = \{1\}$; then $m = 4$. If $C_G(Q) \not\leq Q$, then $G = QZ(G)$ so $Z(G)$ is cyclic of order 4 since G is not Dedekindian. Then $G = Q * Z(G) \cong D_8 * Z(G)$ so G is not minimal non-Dedekindian since D_8 is non-Dedekindian. Thus, $C_G(Q) < Q$ so G is of maximal class (Proposition 10.17) hence $G \cong Q_{16}$. Next assume that $|G| > 2^4$ so $E > \{1\}$ for all nonabelian $H \in \Gamma_1$. We have $H' = Q' \triangleleft G$ and $H/Q' < G/Q'$ is elementary abelian. Assume that G/Q' is not an \mathcal{A}_1 -group. Then there is in G/Q' a nonabelian maximal subgroup $F/Q' = (Q_1/Q') \times (E_1/Q')$, where $Q_1/Q' \cong Q_8$ and $\exp(E_1/Q') \leq 2$. Then $(Q_1/Q') \cap (H/Q')$ is elementary abelian and maximal in Q_1/Q' , a contradiction. Thus, $\bar{G} = G/Q'$ is either abelian or minimal nonabelian.

(i) Let \bar{G} be minimal nonabelian; then $|G'| = 4$. Since $\exp(\bar{H}) = 2$ and $|\bar{H}| = 2$, we get $|\bar{H}| \leq 8$ (Lemma 65.1). If $\bar{H} \cong E_4$, then $|\bar{G}| = 8$ so $|G : G'| = 4$.

In that case, G is of maximal class (Taussky's theorem) so $G \cong Q_{16}$, contrary to $m > 4$. Now let $\bar{H} \cong E_8$. Since \bar{G} is generated by elements of order 4, it has two distinct maximal subgroups \bar{A} and \bar{B} of exponent 4. Then A and B are abelian (if, for example, A is nonabelian, then $A' = Q'$ and $\exp(A/A') = 2$, a contradiction). In that case, $A \cap B = Z(G)$ so $|G'| = 2$ (Lemma 1.1), a contradiction.

(ii) Let \bar{G} be abelian; then $G' = H' = Q'$ and $G = Q * C_G(Q)$ (Lemma 4.3). If $C_G(Q)$ has a cyclic subgroup L of order 4, then $Q * L$ is not Dedekindian. Thus, $\exp(C_G(Q)) = 2$ so $C_G(Q) = Z(G)$. If $Z(G) = Q' \times E_1$, then $G = Q \times E_1$ is Dedekindian, a final contradiction. \square

A 2-group G is said to be a Q^\times -group if $G = Q \times E$, where Q is generalized quaternion and E is elementary abelian.

Theorem A.17.2. *Suppose that all nonabelian maximal subgroups of a nonabelian 2-group G are Q^\times -groups, $|G| = 2^m$. Then G is either minimal nonabelian or a Q^\times -group.*

Proof. Assume that G is neither minimal nonabelian nor of maximal class (if G is of maximal class, it is generalized quaternion). We also may assume, in view of Lemma A.17.1, that $m > 4$. Then all proper nonabelian subgroups of G are Q^\times -groups. There is a nonabelian $H = Q \times E \in \Gamma_1$, where Q is generalized quaternion and E is elementary abelian. Suppose that $E = \{1\}$. Then, by Remark 2, G is a Q^\times -group. Next we assume that $E > \{1\}$ for every choice of nonabelian $H \in \Gamma_1$.

In view of Lemma A.17.1, one may assume that H is chosen so that $|Q| > 2^3$. Then $H' = Q'$ is cyclic of order > 2 and normal in G . In that case, $A = C_G(\Omega_2(Q')) \in \Gamma_1$ is abelian since $\exp(Z(A)) > 2$. Since $E < A$, we get $C_G(E) \geq HA = G$ so that $E < Z(G)$ ($<$, since $Z(Q) < Z(G)$ and $Z(Q) \not\leq E$). It follows from $|G'| > 2$ that A is the unique abelian member of the set Γ_1 (Lemma 65.2(c)). Take a nonabelian $F \in \Gamma_1 - \{H\}$ (F exists, by Exercise 1.6(a)) and assume that $E \not\leq F$. Then there is $X \leq E$ of order 2 such that $X \not\leq F$. In that case, $G = F \times X$ is a Q^\times -group, and we are done. Therefore, one may assume that $E < \Phi(G)$. Write $\bar{G} = G/E$. Note that if $L \in \Gamma_1$ is nonabelian, then \bar{L} is either elementary abelian or an M^\times -group (generally speaking, E is not a direct factor of L). By the above, \bar{G} contains a maximal subgroup \bar{H} , which is generalized quaternion of order > 8 . In view of Remark 2, the following two possibilities for \bar{G} must be considered.

(i) Let \bar{G} be not of maximal class. Then $\bar{G} = \bar{Q} \times \bar{C}$, where $|\bar{C}| = 2$ and \bar{G} has a subgroup $\bar{H} = \bar{Q}$ of maximal class and index 2 (Remark 2). Since $E < Z(G)$ and $|\bar{C}| = 2$, the subgroup $C \triangleleft G$ is abelian and $C \cap Q \leq E \cap Q = \{1\}$ so $G = Q \cdot C$, a semidirect product with kernel C . If F is a nonabelian maximal subgroup of Q (recall that $|Q| > 8$), then $F \cdot C \in \Gamma_1$ is an Q^\times -group so $FC = C \times F$ and hence $\exp(C) = 2$. Since Q is generated by its nonabelian maximal subgroups, we get $G = Q \times C$ so that G is a Q^\times -group.

(ii) Now let \bar{G} be of maximal class. In that case, $d(G) = 2$ since $E < \Phi(G)$, and hence, by Schreier's Theorem A.25.1, we get $d(F) \leq 3$ for all $F \in \Gamma_1$. It follows that $|E| = 2$. Since $E \not\leq G'$ (otherwise, $|G : G'| = 4$ so, by Taussky's theorem, G is of maximal class), we get $E \cap G' = \{1\}$; then G' is cyclic of index 8 in G and G/G' is abelian of type $(4, 2)$ since $d(G) = 2$. Let A/G' and B/G' be two distinct cyclic subgroups of order 4 in G/G' . Since abelian epimorphic images of Q^\times -groups have exponent 2, it follows that A and B are abelian maximal subgroups of G so $A \cap B = Z(G)$. In that case, $|G'| = 2 < |H'|$, a final contradiction. \square

Corollary A.17.3 (Janko; see Theorem 90.1). *If all minimal nonabelian subgroups of a nonabelian 2-group G are isomorphic to Q_8 , then G is a Q^\times -group.*

Proof. We use induction on $|G|$. By induction, every proper nonabelian subgroup of G is a Q^\times -group. Now the result follows from Theorem A.17.2. \square

A 2-group G is said to be a D^\times -group if $G = D \times E$, where D is dihedral and E is elementary abelian. (Of course, Q^\times - and D^\times -groups are M^\times -groups.)

Proposition A.17.4. *Suppose that all nonabelian maximal subgroups of a nonabelian 2-group G are D^\times -groups. Then one of the following holds:*

- (a) G is a D^\times -group.
- (b) G is a generalized dihedral group of order 2^5 with abelian subgroup of type $(4, 4)$. The group G is special, $d(G) = 3$.

Proof. Suppose that G is neither minimal nonabelian nor a D^\times -group. All minimal nonabelian subgroups of G are isomorphic to D_8 so generated by involutions. Then, by Theorem 10.33, $G = C \cdot A$ is a generalized dihedral group; here A is abelian of index 2 in G and all elements of the set $G - A$ are involutions which invert A , and $\exp(A) > 2$. Since G is not dihedral, A is noncyclic. Let $A_2 \leq A$ be of type $(4, 4)$; then $A_1 = C \cdot A_2$ is neither dihedral nor a nontrivial direct product so $A_1 = A$. It follows that A has no proper subgroups of type $(4, 4)$. If $A = L \times A_0$, where $|L| = 2$, then L is a direct factor of G ; in that case G is a D^\times -group. Thus, assuming that all invariants of A are greater 2, we conclude that A is abelian of type $(4, 4)$. Next, $Z(G) = \Omega_1(A) \leq G'$. By Taussky's theorem, $|G : G'| > 4$, so $Z(G) = G'$. It follows from $\Omega_1(G) = G$ that $G' = \Phi(G)$ so G is special. \square

Lemma A.17.5. *Suppose that all nonabelian maximal subgroups of a nonabelian 2-group G are M_3^\times -groups and $|G| = 2^m$. Then one of the following holds:*

- (a) G is minimal nonabelian.
- (b) G is of maximal class and order 16.
- (c) The central product $G = M * C$, where M is nonabelian of order 8 and C is cyclic of order 4, $m = 4$.

- (d) G is generalized dihedral, $m = 5$, with abelian subgroup A of type $(4, 4)$ (as in Proposition A.17.4(b)).
- (e) G is an M_3^\times -group.

Proof. Groups (a–e) satisfy the hypothesis. One may assume that G is neither minimal nonabelian nor of maximal class; then $m > 3$. In that case, all proper nonabelian subgroups of G are M_3^\times -groups so all \mathcal{A}_1 -subgroups of G have the same order 8 (Remark 1). Next, it follows from Proposition 10.17(a) that, if $m = 4$, then G is one of groups of parts (a–c), (e). In what follows we also assume that $m > 4$ and G is not an M_3^\times -group.

Let $M < G$ be an \mathcal{A}_1 -subgroup; then $|M| = 8$. Let $M < H \in \Gamma_1$, where $H = M \times E$ and $\exp(E) = 2$ since $m > 4$. Set $D = \langle H' \mid H \in \Gamma_1 \rangle$. Then $D \leq G' \cap \Omega_1(\mathbf{Z}(G)) (\leq \Phi(G))$ is elementary abelian and all maximal subgroups of $\bar{G} = G/D$ are abelian. It follows that \bar{G} is either elementary abelian or minimal nonabelian generated by involutions so of order 8 hence, in the second case, $\bar{G} \cong D_8$ (Lemma 65.2(c)).

(i) Assume that $|D| = 2$; then $\exp(\bar{G}) = 2$ since $m > 4$, so $G' = D$ and all \mathcal{A}_1 -subgroups of G are normal. Let $M < G$ be an \mathcal{A}_1 -subgroup. Then $G = M * C_G(M)$ (Lemma 4.3). It is easily seen that, in view of $m > 4$, $\exp(C_G(M)) = 2$ so $C_G(M) = \mathbf{Z}(G)$. If $\mathbf{Z}(G) = \mathbf{Z}(M) \times E$, when $G = M \times E$ is an M_3^\times -group.

In what follows we assume that $|D| > 2$. If $U < G$ is nonabelian of order 2^n , then $d(U) = n - 1$ since $|\Phi(U)| = 2$.

(ii) Suppose that $\exp(\bar{G}) = 2$. Let $M < G$ be minimal nonabelian; then $H = MC_G(M) \in \Gamma_1$. It follows from $|D| > 2$ that there is an \mathcal{A}_1 -subgroup $M_1 < G$ such that $M'_1 \neq M'$. In view of Corollary A.17.3 and Proposition A.17.4, one may assume that there are in G two nonisomorphic minimal nonabelian subgroups. Therefore, one may assume from the start that $M \cong Q_8$. Then $M \cap M_1 = \{1\}$ so $|MM_1| = 2^6$, by the product formula. Set $U = \langle M, M_1 \rangle$; then $d(U) \leq d(M) + d(M_1) = 4 < 6 - 1$ so, by the previous paragraph, $U = G$. Using Remark 1, we get $[M, M_1] > \{1\}$ (otherwise, $M \times M_1$ contains an \mathcal{A}_1 -subgroup of order 2^4). Therefore, one may assume that M is not normal in U . Then some cyclic subgroup $C_1 < M_1$ does not normalize some cyclic subgroup $C < M$ (of order 4). Since $U_1 = \langle C, C_1 \rangle$ of order $\geq 2^4$ is generated by two elements and $2 < 4 - 1$, we get $U_1 = G$, and we conclude that $d(G) = 2$. It follows that G is minimal nonabelian (Lemma 65.2(a)), contrary to the assumption.

Now we assume that $\bar{G} \cong D_8$. Since $D < G'$, we get $|G : G'| = |\bar{G} : \bar{G}'| = 4$ so G is of maximal class (Taussky), a contradiction since $|D| > 2 = \exp(D)$. \square

Theorem A.17.6. *Suppose that all nonabelian maximal subgroups of a nonabelian 2-group G are M^\times -groups. Then one of the following holds:*

- (a) G is minimal nonabelian.
- (b) The central product $G = M * C$ is of order 16, M is nonabelian of order 8 and C is cyclic of order 4.

- (c) G is generalized dihedral of order 2^5 with abelian subgroup A of type $(4, 4)$ as in Proposition A.17.4.
- (d) G is an M^\times -group.

Proof. Groups (a–d) satisfy the hypothesis. The group $M * C$, where M is of maximal class and C is cyclic of order > 2 , satisfies the hypothesis if and only if $M \cap C = Z(M)$, $|M| = 8$ and $|C| = 4$.

Assume that the theorem is false. One may assume, in view of Lemma A.17.5, that G contains a maximal subgroup $H = M \times E$, where M is of maximal class and order > 8 and E is elementary abelian. Then $M' = H'$ is cyclic of order ≥ 4 and G -invariant. Let $V = \Omega_2(H')$; then $V \not\leq Z(M)$ so $C_G(V)$ is abelian of index 2 in G since the center of any M^\times -group is elementary abelian. It follows from $|G'| > 2$ that $C_G(V) = A$ is the unique abelian maximal subgroup of G (Lemma 65.2(c)). Since $E < A \cap H$, it follows that $E < Z(G)$ ($<$ since $\Omega_1(M') \leq Z(G)$ and $\Omega_1(M') \not\leq E$).

Assume that $E = \{1\}$ and G is not of maximal class. Then the set Γ_1 has exactly three members which are not of maximal class (Theorem 12.12(c)) so they are either abelian or M^\times -groups. If the set Γ_1 has three distinct abelian members, we get $|G : Z(G)| = 4$; then $|M| = 8$, $|G| = 16$ and G either an M^\times -group or as stated in (b). If $|G| > 16$, then, by Remark 2, G must be an M^\times -group; then $E > \{1\}$, contrary to the assumption. Next we assume that $E > \{1\}$ for every choice of H .

By Lemma 65.2(c), H has only one abelian maximal subgroup, say A_1 , since $|H'| > 2$ so $H \cap A = A_1$. If $E \not\leq \Phi(G)$, then $G = X \times G_0$, where $X \leq E$ is of order 2, $G_0 \in \Gamma_1$. However, by hypothesis, G_0 is an M^\times -group so G is also an M^\times -group. Next we assume that $E < \Phi(G)$.

Suppose that $\bar{G} = G/E$ is not of maximal class. Since $(\bar{H} \cong) \bar{M} < \bar{G}$, we get $\exp(\bar{G}) \geq \exp(\bar{M}) = \exp(M) \geq 8$. By Remark 2, we get $\bar{G} = \bar{M} \times \bar{C}$ where $|\bar{C}| = 2$. Also, $C \triangleleft G$ is abelian and $C \cap M = E \cap M = \{1\}$ so $G = M \cdot C$, a semidirect product with kernel C . If F is a nonabelian maximal subgroup of M , then $F \cdot C$ is an M^\times -group, by hypothesis, so $F \triangleleft FC$, and we conclude that $FC = C \times F$ hence C is elementary abelian. Since M is generated by its two distinct nonabelian maximal subgroups, we get $G = M \times C$ so that G is an M^\times -group.

Next we assume that \bar{G} is of maximal class. In that case, $d(G) = 2$ since $E < \Phi(G)$, and hence, by Schreier's Theorem A.25.1, we get $d(F) \leq 3$ for all $F \in \Gamma_1$. It follows that $|E| = 2$. Since $E \not\leq G'$ (otherwise, by Taussky's theorem, G is of maximal class), we get $E \cap G' = \{1\}$ and so G/G' is abelian of type $(4, 2)$ since $d(G) = 2$. Let $U/G', V/G' < G/G'$ be distinct cyclic of order 4. Then A, B are abelian since $\exp(X/X') = 2$ for any M^\times -group X . We have $A \cap B = Z(G)$ so $|G'| = 2, m = 4$, a final contradiction. \square

Theorem A.17.7. Suppose that all nonabelian maximal subgroups of a nonabelian p -group G , $p > 2$, are M_3^\times -groups. Then either G is an M_3^\times -group or one of the following holds:

- (a) G is minimal nonabelian.
- (b) G is of maximal class and order p^4 .
- (c) $G = M * C$ is of order p^4 , where M is nonabelian of order p^3 and exponent p and C is cyclic of order p^2 .
- (d) G is extraspecial of order p^5 and exponent p .
- (e) G is special of order p^5 , $d(G) = 3$.
- (f) G is special of order p^6 and exponent p , $d(G) = 3$.
- (g) G is of order p^5 , $|G'| = p^3$, $Z(G) < G'$ is abelian of type (p, p) . If $R < Z(G)$ is of order p , then $\text{cl}(G/R) = 3$, G has no abelian subgroups of index p .

Proof. Suppose that the theorem holds for all groups of order $< |G|$. Then all proper nonabelian sections of G are M_3^\times -groups. Groups (a–d), (f) and also groups of exponent p from parts (e) and (g) satisfy the hypothesis. Set $|G| = p^m$. One may assume that G is not minimal nonabelian; then $m > 3$.

Let $M < G$ be minimal nonabelian; then $|M| = p^3$. Assume that $C_G(M)$ has a cyclic subgroup C of order p^2 . Then $|M * C| = p^4$, by Remark 1 and we get $|M \cap C| = p$ and $Z(M * C) = C$ so $G = M * C$, the group of part (c). If $C_G(M) < M$, then G is of maximal class (Proposition 10.17). However, G has no proper subgroups of maximal class and order p^4 , by hypothesis, so $|G| = p^4$ (Theorems 9.5 and 9.6). In what follows we assume that $m > 4$.

Let D be generated by derived subgroups of all nonabelian members of the set Γ_1 ; then $D \leq G' \cap \Omega_1(Z(G)) \leq \Phi(G)$. If $M < G$ is minimal nonabelian, then $M < H \in \Gamma_1$, where H is an M_3^\times -subgroup so that $M' = H' \triangleleft G$. In that case, H/H' is elementary abelian. If a p -group G has a nonabelian maximal subgroup, it has at least p such subgroups (Exercise 1.6(a)). It follows that all maximal subgroups of G/D are abelian and at least p of them are elementary so G/D is either elementary abelian or minimal nonabelian generated by elements of order p (in the last case, G/D is nonabelian of order p^3 and exponent p by Lemma 65.1). By Lemma 65.1(u), $|G'| \leq p^3$.

(i) Suppose that $|D| = p$. Then G/D is elementary abelian so $G' = D$ since $m > 4$. Let $M < G$ be minimal nonabelian. Then, by Lemma 4.3, $G = MC_G(M)$ and $\exp(C_G(M)) = p$ (Remark 1). If $C_G(M)$ is abelian, then $C_G(M) = Z(G) = M' \times E$ so $G = M \times E$ is an M_3^\times -group.

Now assume that $C_G(M)$ is nonabelian (of exponent p). Let $N \leq C_G(M)$ be minimal nonabelian. Since $M' = D = N'$, we get $M \cap N = Z(M) = Z(N)$. Then MN is extraspecial so it is not an M_3^\times -group, and hence $G = MN$ is extraspecial of order p^5 and exponent p . In that case, G is as in (d).

(ii) Now let $|D| > p$. Then there are nonabelian $H, F \in \Gamma_1$ with $H' \neq F'$. The set Γ_1 has at most one abelian member since $|G'| \geq |D| > p$ (Lemma 64.1(u)). Then H/H' and F/F' are distinct elementary abelian so $\Omega_1(G/D) = G/D$. Since $p > 2$

and $\text{cl}(G/D) \leq 2$, we get $\exp(G/D) = p$. Therefore, if G/D is minimal nonabelian, then $|G/D| = p^3$ (Lemma 65.1). Next, $\exp(G) \leq \exp(D) \cdot \exp(G/D) = p^2$.

(ii1) Assume that the quotient group G/D is minimal nonabelian (of order p^3); then $d(G) = d(G/D) = 2$. Since $|G' : D| = p$, we get $|D| = p^2$ and $|G'| = p^3$ so $|G| = |D||G/D| = p^5$. Let F and H be such as in the previous paragraph. Then $F = M \times H'$ and $H = M_1 \times F'$, where M and M_1 are minimal nonabelian (note that $F'H' \leq \Phi(G)$ so $H' < F$ and $F' < H$). Since $F/H' < G/H'$ is nonabelian of order p^3 and $d(G/H') = 2$, it follows from Proposition 10.17 that G/H' is of maximal class. Similarly, G/F' is of maximal class. If G has an abelian subgroup of index p , then $p^5 = |G| = p|G'||Z(G)| = p^6$ (Lemma 1.1), a contradiction. Thus, all maximal subgroups of G are nonabelian and G is as in (g). It is easy to check that if $\exp(G) = p$, then G satisfies the hypothesis (see the last paragraph of (i)).

(ii2) Now let G/D be elementary abelian; then $G' = D = \Phi(G)$ and $\text{cl}(G) = 2$.

Assume that $\exp(Z(G)) > p$. Let $C \leq Z(G)$ be cyclic of order p^2 ; then C is not contained in any nonabelian $H \in \Gamma_1$. If $H = M \times E$ is as above, then $M * C$ is not a subgroup of an M_3^\times -group (Remark 1), and we conclude that $G = M * C$ is as in (c).

Now let $\exp(Z(G)) = p$. Assume, in addition, that a subgroup $X < Z(G)$ of order p is not contained in $\Phi(G)$. Then $G = X \times G_0$, where $G_0 \in \Gamma_1$, so $G_0 = M_0 \times E_0$, where E_0 is elementary abelian and M_0 is nonabelian of order p^3 . In that case, $G = M_0 \times (E_0 \times X)$ is an M_3^\times -group.

Let, in what follows, $Z(G) \leq \Phi(G)$; then $Z(G) = G' = \Phi(G) = D \leq Z(G)$ so G is special. Let $M < G$ be minimal nonabelian. Then $M\Phi(G)/\Phi(G) = MD/D \cong M/(M \cap D) \cong E_{p^2}$.

If $d(G) = 2$, then G is minimal nonabelian (Lemma 65.2(a)), a contradiction.

Suppose that $d(G) > 3$. Then MD/D is contained in two distinct maximal subgroups, say F/D and H/D , of G/D . Since M is a direct factor in F and H (see the paragraph preceding Remark 1), we get $N_G(M) \geq FH = G$ so $M \triangleleft G$. It follows that $G = MC_G(M)$ since $G' = \Phi(G) = D \leq C_G(M)$ and Sylow p -subgroups of $\text{Aut}(M)$ are nonabelian of order p^3 and exponent p . Assume that $C_G(M)$ has a minimal nonabelian subgroup N and suppose that $M \cap N = \{1\}$. It follows from Remark 1 that $\exp(M) = p = \exp(N)$. Let $T < M \times N$ be the diagonal subgroup; then $T \cong M$ is minimal nonabelian. However, $T \not\leq M \times N$, contrary to what has just been said. Now let $M \cap N = Z(M)$; then $M * N$ is extraspecial so is not an M_3^\times -subgroup, and we conclude that $G = MN$. Then $|G'| = p < p^2 \leq |D|$, a contradiction. Thus, N does not exist so $C_G(M)$ is elementary abelian (Remark 1). Since $G = MC_G(M)$, we get $C_G(M) = Z(G)$. If $Z(G) = Z(M) \times E$, then $G = M \times E$; in that case, $|G'| = p < |D|$ again, a contradiction.

Thus, $d(G) = 3$. In that case, $|G| = |G'||G/G'| \leq p^6$. Suppose that $|G'| = p^3$. Then $G' = D = F' \times H' \times L'$, where F, H and L are appropriate minimal nonabelian subgroups of G . As above, $\exp(G/F'H') = \exp(G/H'L') = \exp(G/L'F') = p$ so, since $F'H' \cap H'L' \cap L'F' = \{1\}$, we conclude that $\exp(G) = p$ and G is special.

Now let G be special of order p^5 or p^6 , $\exp(G) = p$, $|G'| = p^2$ or p^3 , respectively, and $d(G) = 3$. If $M < G$ is minimal nonabelian (in that case, $|M| = p^3$), then the M_3^\times -group $MG' = M \times E$ (here $G' = M' \times E$) is the unique maximal subgroup of G containing M . \square

Appendix 18

Replacement theorems

Thompson's replacement theorem (see Corollary A.18.3 below) received wide application in the study of arbitrary finite groups. Theorem A.18.4, which is due to Glauberman, is a deep generalization of Thompson's result. The proof of Theorem A.18.1 presents some ideas of the proof of Theorem A.18.4 in a more easy form.

Theorem A.18.1 (Isaacs [Isa2]). *Let G be a p -group and $A < G$ abelian. Suppose that $B < G$ is also abelian, $A \leq N_G(B)$ and $B \not\leq N_G(A)$. Then there exists an abelian subgroup $A^* < G$ such that*

- (a) $|A^*| = |A|$,
- (b) $A \cap B < A^* \cap B$,
- (c) $A^* \leq N_G(A)$,
- (d) $\exp(A^*)$ divides $2 \cdot \exp(A)$.

Proof. Without loss of generality, one may assume that $G = AB$; then $B \triangleleft G$ but A is not normal in G so G is not Dedekindian and $|G : A| > p$. We proceed by induction on $|G|$. Let $A < M < G$, where $M \in \Gamma_1$. Then $M = A(B \cap M)$ and $B \cap M \triangleleft G$ since $B, M \triangleleft G$. Suppose that $B \cap M \not\leq N_G(A)$. By induction, applied to the triple $\{A, B \cap M, M\}$, there is an abelian subgroup $A^* \leq M$ satisfying (a), (c) and (d) and such that $A \cap (B \cap M) < A^* \cap (B \cap M)$, and so $A \cap B < A^* \cap B$, and we are done in this case.

Therefore, one may assume that $B \cap M \leq N_G(A)$. Then $M = A(B \cap M) \leq N_G(A)$, i.e., $A \triangleleft M$ so $N_G(A) = M$ since $A \not\triangleleftharpoonup G$ and $M \in \Gamma_1$. Let $b \in B$ be such that $A \neq A^b$. Obviously, A^b is normal in $M^b = M$ so that $H = AA^b$ is normal in M . Since A and A^b are abelian, we get $Z = A \cap A^b \leq Z(H)$ and $\text{cl}(H) \leq 2$, by Fitting's lemma. By Exercise 1.18, $\exp(H)$ divides $2 \cdot \exp(A)$. Since B is abelian and $b \in B$, we get

$$A^b \cap B = (A \cap B)^b = A \cap B$$

and hence

$$(1) \quad Z \cap B = (A \cap A^b) \cap B = A \cap (A \cap B) = A \cap B.$$

Setting $A^* = (H \cap B)Z$, we see that $A^* \leq H$ and A^* is abelian since $H \cap B$ is abelian and $Z \leq Z(H)$. It remains to show that A^* satisfies conditions (a–d).

By the modular law, $H = A(H \cap B)$ and, since $A < H$, we have $H \cap B \not\leq A$. Next, $H \cap B = (AA^b) \cap B \geq A \cap B$. Hence,

$$A^* \cap B = [(H \cap B)Z] \cap B \geq H \cap B > A \cap B$$

($>$ since $A \cap B \leq H \cap B \not\leq A$), and (b) follows.

Since $A^* \leq M = N_G(A)$, i.e., (c) is true, it remains to prove (a). By (1), $Z \cap B = A \cap B$, and $H \cap Z \cap B = Z \cap B = A \cap B$. We have

$$|A^*| = |(H \cap B)Z| = \frac{|H \cap B| \cdot |Z|}{|H \cap Z \cap B|} = \frac{|H \cap B| \cdot |Z|}{|A \cap B|}.$$

Since $H = AA^b = A(H \cap B)$, we get

$$\frac{|A|^2}{|Z|} = \frac{|A|^2}{|A \cap A^b|} = |H| = \frac{|A| \cdot |H \cap B|}{|A \cap H \cap B|} = \frac{|A| \cdot |H \cap B|}{|A \cap B|}.$$

Therefore, $|A| = \frac{|Z| \cdot |H \cap B|}{|A \cap B|} = |A^*|$, proving (a). Since $\exp(H)$ divides $2\exp(A)$ and $\exp(Z)$ divides $\exp(A)$, condition (d) also holds. The proof is complete. \square

Corollary A.18.2 ([Isa2]). *Let G be a nonabelian p -group, $p > 2$, and let $B \triangleleft G$ be abelian. Suppose that $x \in C_G(\Omega_n(B))$ has order $\leq p^n$. Then $[B, x] \leq \Omega_n(B)$.*

Proof. The subgroup $A = \langle \Omega_n(B), x \rangle$ is abelian of exponent at most p^n . Assume that $B \not\leq N_G(A)$. Then, by Theorem A.18.1, there exists an abelian subgroup $A^* < G$ such that $\exp(A^*) \leq \exp(A) \leq p^n$ and $A^* \cap B > A \cap B$. However, $A^* \cap B \leq \Omega_n(B) \leq A \cap B$, a contradiction. Thus $B \leq N_G(A)$, and so $[B, x] \leq [B, A] \leq A \cap B = \Omega_n(B)$ ($=$ since $\exp(A \cap B) \leq p^n$). \square

Let $\mathcal{A}(G)$ be the set of all abelian subgroups of G of maximal order. If $A \in \mathcal{A}(G)$, then $Z(G) \leq C_G(A) = A$. We did not assume, in Theorem A.18.1, that $A \in \mathcal{A}(G)$.

Theorem A.18.3 (Thompson's replacement theorem [Tho3]). *Let G be a p -group and $B \triangleleft G$ abelian. If $A \in \mathcal{A}(G)$ is such that $B \not\leq N_G(A)$, then there exists $A^* \in \mathcal{A}(G)$ such that $A^* \cap B > A \cap B$, $A^* \leq N_G(A)$ and $B \leq N_G(A^*)$.*

Proof. Let $A^* \in \mathcal{A}(G)$ be such that $|A^* \cap B|$ is as large as possible. By Theorem A.18.1, the first two assertions hold. Assume that B does not normalize A^* . Then, by Theorem A.18.1 again, there exist $A^{**} \in \mathcal{A}(G)$ such that $A^* \cap B < A^{**} \cap B$, contrary to the choice of A^* . \square

Exercise 1. Let B be a subgroup of a p -group G and $A \in \mathcal{A}(G)$. Then B normalizes A if and only if $[B, A, A] = \{1\}$.

Solution. If $[B, A, A] = \{1\}$, then $[B, A] \leq C_G(A) = A$. If $B \leq N_G(A)$, then $[B, A, A] \leq [A, A] = \{1\}$.

Definition 1. Let G be a p -group. The (characteristic) subgroup $J(G) = \langle A \mid A \in \mathcal{A}(G) \rangle$ is called the *Thompson subgroup* of G (or *J -subgroup* of G).

If $J(G) \leq H < G$, then $J(H) = J(G)$ so $J(G)$ is a characteristic subgroup of any subgroup of G containing $J(G)$. Clearly, $Z(J(G)) \leq A$ for all $A \in \mathcal{A}(G)$. Therefore, $Z(J(G)) = \bigcap_{A \in \mathcal{A}(G)} A$. Next, $\mathcal{A}(J(G)) = \mathcal{A}(G)$.

Exercise 2. Let G be a nonabelian p -group. If $J(G)$ is cyclic, then G is a 2-group of maximal class so $|G : J(G)| = 2$. (*Hint.* Let $|J(G)| = p^n$; then $c_n(G) = 1 \not\equiv 0 \pmod{p}$. Use Theorems 1.10(b) and 1.17(b).)

Exercise 3. Let G be a p -group, $T \leq G$ and $\mathcal{A}(G) \cap \mathcal{A}(T) \neq \emptyset$. Then $Z(J(G)) \leq Z(J(T))$.

Theorem A.18.4 (Glauberman's replacement theorem). *Suppose that a p -group G , $p > 2$, has a normal subgroup B such that $B' \leq Z(J(G)) \cap Z(B)$. If $A \in \mathcal{A}(G)$ is such that B does not normalize A , then there is $A^* \in \mathcal{A}(G)$ such that $A \cap B < A^* \cap B$, $A^* \leq N_G(A)$ and $\exp(A^*)$ divides $\exp(A)$.*

Proof. In view of Theorem A.18.3, one may assume that B is nonabelian so $\text{cl}(B) = 2$. We proceed by induction on $|G|$. Set $T = AB(\leq G)$. Since $A \in \mathcal{A}(T)$, we have $J(T) \leq J(G)$ and $Z(J(G)) \leq Z(J(T))$ (Exercise 3). We also have $B' \leq Z(J(T)) \cap Z(B)$. Hence, if $T < G$, theorem follows by induction. We may, therefore, assume that $G = AB$; then $B \triangleleft G$, $A \not\triangleleftharpoonup G$ so $|G : A| > p$. We have

$$(1) \quad B' \leq Z(J(G)) \cap Z(B) \leq A \cap B \leq Z(G).$$

Let $A < M \in \Gamma_1$ and $B_1 = B \cap M$; then $J(M) \leq J(G)$, $M = AB_1$ and $B_1 \triangleleft G$ since $B, M \triangleleft G$. Next, we have $B'_1 \leq B' \leq Z(J(G)) \leq Z(J(M))$ (Exercise 3) and $B'_1 \leq Z(B_1)$. Therefore, $B'_1 \leq Z(J(M)) \cap Z(B_1)$. If $B_1 \not\leq N_M(A)$, then the triple $\{A, B_1, M\}$ satisfies the hypothesis, and, there is $A^* \in \mathcal{A}(M)$ such that

$$A \cap B_1 < A^* \cap B_1, \quad [A^*, A, A] = \{1\}, \quad \exp(A^*) \mid \exp(A),$$

by induction. In that case, we have $\mathcal{A}(M) \subseteq \mathcal{A}(G)$, and the theorem is true since $A \cap B_1 = A \cap (B \cap M) = A \cap B$ and $A^* \cap B_1 \leq A^* \cap B$.

Assume that $B_1 \leq N_M(A)$. We have $[B, A] \leq [B, M] \leq B \cap M = B_1$ so $[B, A, A] \leq [B_1, A] \leq A$, i.e., $[B, A]$ normalizes A . Since $B \triangleleft G$, we have $[B, A, A] \leq B \cap A$. Consider the quotient group $\bar{G} = G/B'$. Then $\bar{G} = \bar{A}\bar{B}$ (bar convention!) and $\bar{A} \cap \bar{B} \leq Z(\bar{G})$ since \bar{A} and \bar{B} are abelian. Therefore, $[\bar{B}, \bar{A}, \bar{A}] \leq \bar{B} \cap \bar{A} \leq Z(\bar{G})$. Since B does not normalize A , there is an element $b \in B$ such that $A^b \neq A$. Set $D = [b, A] = \langle [b, a] \mid a \in A \rangle$. Since $A, A^b \triangleleft M$, we have $AA^b \triangleleftharpoonup M$ so $D \leq AA^b$. Then we have $D \leq [B, A] \leq [B, M] \leq B \cap M = B_1$. We have $AA^b = DA$. Indeed,

$$AA^b = \langle aa_1^b \mid a, a_1 \in A \rangle = \langle aa_1[a_1, b] \mid a, a_1 \in A \rangle \subseteq AD,$$

and since $A, D \leq AA^b$, our claim follows. We have $D \not\leq A$ (otherwise, $AA^b = DA = A$ so $A^b = A$, which is not the case). Set

$$A^* = D(A \cap A^b).$$

We will prove that A^* has the required properties. We have $A^* = D(A \cap A^b) \leq DA = AA^b \leq M < G$. Since $\text{cl}(AA^b) \leq 2$ (Fitting's lemma) and $p > 2$, it follows that $\exp(AA^b) = \exp(A)$, and so $\exp(A^*)$ divides $\exp(AA^b) = \exp(A)$.

We have $B' \leq Z(\text{J}(G)) \leq A$ so $B' \leq B \cap A$; then $B \cap A \triangleleft B$. Hence $(A \cap B)^{b^{-1}} = A \cap B$, and so $A \cap B = A^b \cap B$ and $A^* = D(A \cap A^b) = D(A \cap B)$. Thus,

$$A \cap B \leq A \cap (A \cap B) = A \cap (A^b \cap B) = (A \cap A^b) \cap B \leq A^* \cap B.$$

Since $D = [b, A] \leq B \cap A^*$ but $D \not\leq A$, we have $A \cap B < A^* \cap B$. We have $A^* \leq M = N_G(A)$ and so $[A^*, A, A] = \{1\}$.

It remains to prove that $A^* \in \mathcal{A}(G)$. Set $Z = A \cap A^b (\leq Z(AA^b))$. We have (since $A^*A = D(A \cap A^b)A = DA$)

$$(2) \quad |A : Z| = |A^b : Z| = |AA^b : A| = |DA : A| = |A^*A : A| = |A^* : (A^* \cap A)|.$$

Next, $Z = A \cap A^b < D(A \cap A^b) = A^*$, and hence $Z \leq A^* \cap A$. Thus we get, by (2), $|A^*| \cdot |Z| = |A| \cdot |A^* \cap A| \geq |A| \cdot |Z|$ so $|A^*| \geq |A|$. If D is abelian, then $A^* = DZ = D * Z$ is abelian, and we get $A^* \in \mathcal{A}(G)$.

It remains to show that $D = [b, A]$ is abelian, i.e., $[[b, u], [b, v]] = 1$ for any $u, v \in A$. Setting $w = [b, v]$ and $s = u^{-1}$, we have, by the Hall–Witt identity,

$$[b, u, w]^s [s, w^{-1}, b]^w [w, b^{-1}, s]^b = 1.$$

Since $w \in B(\triangleleft G)$, we get

$$[w, b^{-1}, s]^b \in [B, B, A] = [B', A] \leq [Z(\text{J}(G)), A] = \{1\}.$$

The remaining factors of that formula are contained in $[B, B] \leq Z(G)$ (see (1)), hence the above identity gives us

$$[b, u, w] = [s, w^{-1}, b]^{-1} = [u^{-1}, w^{-1}, b]^{-1}.$$

Therefore, taking into account the inclusion $[u^{-1}, w^{-1}, b] \in Z(G)$, we get

$$[b, u, w] = [[u^{-1}, w^{-1}]^{-1}, b] = [w^{-1}, u^{-1}, b].$$

On the other hand, we have $[w^{-1}, u^{-1}] \in [b, A, A]$ since $w^{-1} = [b, v]^{-1} \leq [b, A]$. Thus, in $\bar{G} = G/B'$, $[w^{-1}, u^{-1}]$ corresponds to an element of the center (since $[\bar{B}, \bar{A}, \bar{A}] \leq Z(\bar{G})$). So, we get

$$[w^{-1}, u^{-1}] \equiv [w, u] \pmod{B'}.$$

Since $B' \leq Z(B)$, we have $[w^{-1}, u^{-1}, b] = [w, u, b]$ for any $b \in B$. By the above (recall that $[b, v] = w$),

$$(2) \quad [[b, u], [b, v]] = [b, u, w] = [w^{-1}, u^{-1}, b] = [w, u, b] = [b, v, u, b].$$

Applying the formula $[u, xy] = [u, y][u, x]^y$ to the equality $[b, uv] = [b, vu]$ ($uv = vu$ since A is abelian), we obtain

$$[b, uv] = [b, v][b, u][b, u, v] = [b, vu] = [b, u][b, v][b, v, u],$$

and so, since $[b, u], [b, v] \in B$,

$$[b, u, v] = [[b, v], [b, u]][b, v, u] \equiv [b, v, u] \pmod{B'}.$$

Since $B' \leq Z(G)$, we get $[b, u, v] = [b, v, u]z$ with $z \in B' = Z(B)$ so $[b, u, v, b] = [[b, v, u]z, b] = [b, v, u, b]^z[z, b] = [b, v, u, b]$, which proves (see (2)) that

$$[[b, u], [b, v]] = [[b, v], [b, u]] (= ([[b, u], [b, v]])^{-1}.$$

Since $p > 2$, we have $[[b, u], [b, v]] = 1$. Thus, D is abelian, and the proof is complete. \square

Appendix 19

New proof of Ward's theorem on quaternion-free 2-groups

Below we present a new proof of Ward's theorem (see Theorem 56.1) which is due to Z. Bozikov. Recall that Ward's theorem asserts that a nonabelian quaternion-free 2-group has a characteristic maximal subgroup. This proof is short but not so elementary as given in §56.

Proof of Ward's theorem. (i) First we assume that G is a Q_8 -free 2-group which is also D_8 -free; then G is modular (see §§43 and 73). We prove that then G has a characteristic maximal subgroup and use induction on $|G|$. By classification of nonabelian modular 2-groups (see §73), there is $A \triangleleft G$ abelian and such that $G/A \neq \{1\}$ is cyclic and there is $g \in G$ and an integer $s \geq 2$ so that $G = \langle A, g \rangle$ and $a^g = a^{1+2^s}$ for all $a \in A$.

We have $\{1\} \neq G' < A$. If $G' \not\leq Z(G)$, then $C_G(G') \geq A$, $G/C_G(G')$ is nontrivial cyclic and $C_G(G')$ is a characteristic subgroup in G . In that case G has a characteristic maximal subgroup containing $C_G(G')$. Hence we may assume that $G' \leq Z(G)$ and so G is of class 2.

Suppose that G' is not elementary abelian. Then $\Omega_1(G) < G'$ so $G/\Omega_1(G')$ is nonabelian of order $< |G|$. By induction, $G/\Omega_1(G')$ has a characteristic maximal subgroup. Hence, we may assume that G' is elementary abelian.

For any $x, y \in G$, $[x^2, y] = [x, y]^2 = 1$ since $\text{cl}(G) = 2$, so $\Phi(G) = \mathfrak{U}_1(G) \leq Z(G)$. In particular, $g^2 \in Z(G)$ and so the maximal subgroup $M = \langle g^2, A \rangle$ is abelian. If M is the unique abelian maximal subgroup of G , then M is characteristic in G , and we are done. Therefore we may assume that G has another abelian maximal subgroup $N \neq M$. We have $M \cap N = Z(G)$ and $|G : Z(G)| = 4$. Since $A \not\leq Z(G)$, $|A : (N \cap A)| = 2$ and therefore $NA = G$. Lemma 1.1 implies $|G'| = 2$. Also, we may assume that there is $\alpha \in \text{Aut}(G)$ such that $N = M^\alpha$ (otherwise, M is characteristic in G). Let $h \in N - A$ be such that $N = \langle h, N \cap A \rangle$, and so $G = NA = \langle h, N \cap A, A \rangle = \langle h, A \rangle$. Since $h^2 \in Z(G)$, we have $M = \langle h^2, A \rangle$ which is the unique abelian maximal subgroup of G containing A (recall that G/A is cyclic). We have $h = gm$ for some $m \in M$ and so h acts the same way on A as the element g . Since h centralizes $N \cap A$, we have $\exp(N \cap A) \leq 2^s$ and all elements in $A - (N \cap A)$ are of order 2^{s+1} , $s \geq 2$, which implies $\exp(N \cap A) = 2^s$, in view $|A : (N \cap A)| = 2$.

For any $a \in A - N$, $a^h = a^{1+2^s}$ and so $G' = [A, h] = \langle [a, h] \mid a \in A \rangle = \langle a^{2^s} \mid a \in A \rangle = \mathfrak{U}_s(A)$. Since $M \cap N = Z(G)$, we get $(M \cap N)^\alpha = M \cap N$. But $M^\alpha = N$

and so $\langle(A - N)^\alpha\rangle = \langle A^\alpha - M\rangle \leq N - M$. Let $a^\alpha = h_0$, where $a \in A - N$ so that $o(h_0) = 2^{s+1}$ and $\langle h_0 \rangle$ covers $N/(N \cap A)$ since $N/(N \cap A)$ is cyclic. It follows that $N = (N \cap A)\langle h_0 \rangle$ and $M \cap N = (N \cap A)\langle h_0^2 \rangle$ and therefore $\exp(M \cap N) = 2^s$, $\exp(N) = 2^{s+1}$, $\langle h_0^{2^s} \rangle = G'$ and $\mathfrak{V}_s(N) = G'$. This implies $\mathfrak{V}_s(M) = G'$ and $h^{2^s} = h_0^{2^s}$. We compute (noting that $[h^2, a^2] = 1$)

$$(ha)^2 = haha = h^2(a^h)a = h^2a^{1+2^s}a = h^2a^2a^{2^s},$$

$$(ha)^{2^s} = ((ha)^2)^{2^{s-1}} = (h^2a^2a^{2^s})^{2^{s-1}} = h^{2^s}a^{2^s} = 1$$

(note that $s \geq 2$ and $o(a) = 2^{s+1}$). This implies that the third abelian maximal subgroup $K = (M \cap N)\langle ha \rangle$ is of exponent 2^s . Since each abelian maximal subgroup of G contains $M \cap N = Z(G)$, it follows that G has exactly three abelian maximal subgroups M, N, K , where $\exp(M) = \exp(N) = 2^{s+1}$ and $\exp(K) = 2^s$ and therefore K is characteristic in G , and we are done.

(ii) We assume now that G is a quaternion-free 2-group which is not D_8 -free. By Main Theorem of §79, G is isomorphic to one of the groups of types (a), (b) or (c) of that theorem (these groups were named W_a -, W_b - and W_c -groups, respectively).

(ii)(a) Suppose that G is a W_a -group. Then G is a semidirect product $G = \langle x \rangle \cdot N$, where N is a maximal abelian normal subgroup of G with $\exp(N) > 2$ and, if t is the involution in $\langle x \rangle$, then every element in N is inverted by t .

Since $G/N > \{1\}$ is cyclic, we have $\Omega_1(G) = \Omega_1(\langle N, t \rangle) = N\langle t \rangle$. Note that all elements in Nt are involutions and each $y \in Nt$ inverts every element in N .

If N is not characteristic in G , then, since $\Omega_1(G)$ is characteristic in G and $|\Omega_1(G) : N| = 2$, there is $\alpha \in \text{Aut}(G)$ such that $\Omega_1(G) = NN^\alpha$, where $|\Omega_1(G) : N^\alpha| = 2$. Let $u \in N^\alpha - N$. Then u is an involution in Nt and so u inverts and centralizes each element in $N \cap N^\alpha$. This implies that $N \cap N^\alpha$ is elementary abelian. But then $N^\alpha = (N \cap N^\alpha)\langle u \rangle$ is elementary abelian contrary to $\exp(N^\alpha) = \exp(N) > 2$. Thus N is a characteristic subgroup of G with cyclic $G/N > \{1\}$. In that case, the maximal subgroup U/N of G/N is characteristic in G/N ; then U is characteristic in G since N is, and we are done.

(ii)(b) Let G be a W_b -group. Then $G = N\langle x \rangle$, where we may assume that N is a maximal normal elementary abelian subgroup of G and $\langle x \rangle$ is not normal in G .

If $\Omega_1(G) = N$, then, since G/N is cyclic $> \{1\}$, the maximal subgroup M of G containing N is characteristic in G , and we are done.

We may assume that $\Omega_1(G) > N$. Since G/N is cyclic, we have $|\Omega_1(G) : N| = 2$. If $G \neq \Omega_1(G)$, then, since $G/\Omega_1(G)$ is cyclic $> \{1\}$, the maximal subgroup M of G containing $\Omega_1(G)$ is characteristic in G , and we are done.

Assume, in addition, that $G = \Omega_1(G)$ with $|G : N| = 2$ and N is not characteristic in G (otherwise, we are done). There is $\alpha \in \text{Aut}(G)$ such that $G = NN^\alpha$, $|N : (N \cap N^\alpha)| = 2$, and $N \cap N^\alpha = Z(G)$ with $|G : Z(G)| = 4$. We note that N and N^α are elementary abelian maximal subgroups of G . On the other hand, each abelian

maximal subgroup of G contains $N \cap N^\alpha = Z(G)$, where $|G : Z(G)| \cong E_4$ and so G has exactly three abelian maximal subgroups. Let a be an element of order 4 in $G - (N \cup N^\alpha)$ so that $M = (N \cap N^\alpha)\langle a \rangle$ is the third abelian maximal subgroup of G . Since $\exp(M) = 4$, M is characteristic in G , and we are done.

(ii)(c) Suppose that G is isomorphic to a W_c -group. Then G has an elementary abelian normal subgroup N such that $G/N \cong M_{2^n}$, $n \geq 4$, and if $H/N = \Omega_1(G/N)$, then $H \cong D_8 \times E_{2^m}$ and $Z(H) = N$. Also, G/H is cyclic of order ≥ 4 . Since $H \cong D_8 \times E_{2^m}$, we have $H = \Omega_1(G)$. Therefore, if M is the maximal subgroup of G containing $\Omega_1(G)$, then M is characteristic in G and we are done. \square

Appendix 20

Some remarks on automorphisms

In this section we prove some results on automorphisms of finite groups. §§32, 33, 34 contain further information on automorphisms.

Theorem A.20.1. *Let φ be an automorphism of a group G , N a φ -invariant normal subgroup of G . Then $|C_{G/N}(\varphi)| \leq C_G(\varphi)|$.*

Proof. Let W be the semidirect product of G and $\langle \varphi \rangle$, compatible with action of φ on G ; then $N \triangleleft W$. By the Second Orthogonality Relation,

$$|C_W(\varphi)| = \sum_{\chi \in \text{Irr}(W)} |\chi(\varphi)|^2 \geq \sum_{\chi \in \text{Irr}(W/N)} |\chi(\varphi)|^2 = |C_{W/N}(\varphi)|.$$

By the modular law, $C_W(\varphi) = \langle \varphi \rangle \cdot C_G(\varphi)$ and $C_{W/N}(\varphi) = \langle \varphi \rangle \cdot C_{G/N}(\varphi)$ (both products are semidirect), and now the result follows from the above long formula. \square

In the case where $(|N|, o(\varphi)) = 1$, the result may be strengthened.

Theorem A.20.2. *Let G, φ, N be as in Theorem A.20.1. If, in addition, $(|N|, o(\varphi)) = 1$, then $C_{G/N}(\varphi) = C_G(\varphi)N/N$.*

Corollary A.20.3. *Let G be a group and φ an $\pi(G)'$ -automorphism of G . Then (a) $G = C_G(\varphi)[G, \varphi]$ and (b) $[G, \varphi, \varphi] = [G, \varphi]$.*

Proof. (a) We know that $[G, \varphi] \triangleleft \langle G, \varphi \rangle$ so $[G, \varphi] \triangleleft G$. As $g^\varphi = g[g, \varphi]$, φ acts trivially on $G/[G, \varphi]$ so $G/[G, \varphi] = C_{G/[G, \varphi]}(\varphi) = C_G(\varphi)[G, \varphi]/[G, \varphi]$ (Theorem A.20.2), and hence $G = C_G(\varphi)[G, \varphi]$, as was to be shown.

(b) By (a), $[G, \varphi] = [C_G(\varphi)[G, \varphi], \varphi] = [[G, \varphi], \varphi] = [G, \varphi, \varphi]$. \square

Corollary A.20.4 (= Corollary 6.5 (Fitting)). *If a group G of Corollary A.20.3 is abelian, then $G = C_G(\varphi) \times [G, \varphi]$.*

Exercise 1. Let $\alpha \in \text{Aut}(G)$, where G is a p -group and $o(\alpha) = p$. If α has exactly p fixed points then one of the following holds: (a) G is of order $\leq p^p$ and exponent p , (b) G is absolutely regular, (c) G is irregular of maximal class. (*Hint.* By Proposition 1.8, $\langle G, \varphi \rangle$ is of maximal class. Use Theorems 9.5 and 9.6.)

Exercise 2. Let $p > 2$, $G = \langle a \rangle \cong C_{p^n}$, $n > 1$ and $\varphi \in \text{Aut}(G)$ be such that $\varphi : a \rightarrow a^{1+p}$. Then $|C_G(\varphi^{p^k})| = p^{k+1}$ for $k = 0, 1, \dots, n-1$. Hence, the class of the natural extension W of G by $\langle \varphi \rangle$, which is metacyclic, is n .

Exercise 3. Let G be a p -group and $\varphi \in \text{Aut}(G)^\#$, and suppose that φ fixes all elements of G of orders p and 4. Prove that $o(\varphi)$ is a power of p . (Hint. Use Lemma 10.8 and Frobenius' normal p -complement theorem.)

Exercise 4. Let $G = \langle a \rangle \cong C_{2^n}$, $n > 2$. Then $\text{Aut}(G)$ is an abelian group of type $(2^{n-2}, 2)$ with two independent generators $\sigma : a \rightarrow a^{-1}$ and $\tau : a \rightarrow a^5$. The group $\text{Aut}(G)$ has exactly three involutions: σ , $\tau^{2^{n-3}} : a \rightarrow a^{1+2^{n-1}}$ and $\rho = \sigma\tau^{2^{n-3}} : a \rightarrow a^{-1+2^{n-1}}$. Let W be the natural semidirect product of G and $\text{Aut}(G)$, the holomorph of G . Show that $D = \langle G, \sigma \rangle \cong D_{2^{n+1}}$, $M = \langle G, \tau^{2^{n-3}} \rangle \cong M_{2^{n+1}}$ and $S = \langle G, \rho \rangle \cong SD_{2^{n+1}}$. Check that $\text{cl}(G) = n$. Moreover, construct the upper and lower central series of W . Find $c_k(W)$.

Hint. The natural semidirect product $H = \Omega_1(\text{Aut}(G)) \cdot G$ has exactly three maximal subgroups containing G , namely, D, M, S . Clearly, $\Omega_1(H) = \Omega_1(W)$ so

$$\begin{aligned} c_1(W) &= c_1(H) = c_1(D) + c_1(S) + c_1(M) - 2c_1(G) \\ &= (2^n + 1) + (2^{n-1} + 1) + 3 - 2 = 2^n + 2^{n-1} + 3, \\ c_2(W) &= c_2(D) + c_2(S) + c_2(M) - 2c_2(G) \\ &= 1 + (2^{n-1} + 1) + 2 - 2 = 2^{n-1} + 2, \end{aligned}$$

and, for $k \in \{3, \dots, n\}$, we have $c_k(W) = c_k(D) + c_k(S) + c_k(M) - 2c_k(G) = 1 + 1 + 2 - 2 = 2$.

An automorphism $\varphi \in \text{Aut}(G)$ is said to be *fixed-point-free* (or *regular*) if $x^\varphi = x$ for $x \in G$ implies $x = 1$. If $G = F \cdot H$ is a Frobenius group with kernel H and complement F and $f \in F^\#$, then $h \mapsto h^f$ is a fixed-point-free automorphism of H .

Proposition A.20.5. Let $\varphi \in \text{Aut}(G)$ be fixed-point-free of order n .

- (a) If $x \in G$, then there exists exactly one $y \in G$ such that $x = y^{-1}y^\varphi$.
- (b) If $x \in G$, then $xx^\varphi \dots x^{\varphi^{n-1}} = 1$.
- (c) If $o(\varphi) = 2$, then $x^\varphi = x^{-1}$ (in that case, G is abelian).
- (d) If $N \triangleleft G$ is φ -invariant, then the automorphism induced by φ on G/N , is fixed-point-free.

Proof. (a) If $y^{-1}y^\varphi = z^{-1}z^\varphi$ for $y, z \in G$, then $zy^{-1} = (zy^{-1})^\varphi$, so $zy^{-1} = 1$ since φ is fixed-point-free. Then $y = z$ so $|\{y^{-1}y^\varphi \mid y \in G\}| = |G|$. It follows that $x = y^{-1}y^\varphi$ for exactly one $y \in G$, proving (a).

(b) Let $x \in G$. Then $x = y^{-1}y^\varphi$ for some $y \in G$, by (a), and so

$$xx^\varphi \dots x^{\varphi^{n-1}} = y^{-1}y^\varphi(y^{-1})^\varphi y^{\varphi^2} \dots (y^{-1})^{\varphi^{n-1}} y^{\varphi^n} = y^{-1}y = 1.$$

(c) If $o(\varphi) = 2$, then, by (b), $xx^\varphi = 1$ so $x^\varphi = x^{-1}$ for all $x \in G$. If $x, y \in G$, then $x^{-1}y^{-1} = x^\varphi y^\varphi = (xy)^\varphi = (xy)^{-1} = y^{-1}x^{-1}$ so $xy = yx$, and G is abelian.

(d) Assume that $(xN)^\varphi = xN$ for some $x \in G$. Then $x^{-1}x^\varphi \in N$. As φ_N is fixed-point-free, there exists $y \in N$ such that $x^{-1}x^\varphi = y^{-1}y^\varphi$. By (a), $x = y \in N$, so $xN = N$, i.e., φ induces a fixed-point-free automorphism on G/N . \square

Proposition A.20.6 ([Isa15, Lemma 3.2]). *Let $C = Z(G)$, where C is cyclic and G/C is abelian. Then every automorphism of G , which is trivial on C and G/C , is inner.*

Proof. Suppose that $\mathcal{A} = \{\sigma \in \text{Aut}(G) \mid [G, \sigma] \leq C \text{ and } [C, \sigma] = \{1\}\}$ and note that $\text{Inn}(G) \leq \mathcal{A}$. Since $|\text{Inn}(G)| = |G/C|$, it suffices to show that $|\mathcal{A}| \leq |G/C|$.

For each $\sigma \in \mathcal{A}$, there is a well-defined map $\theta_\sigma : G/C \rightarrow C$ defined by $(Cg)\theta_\sigma = [g, \sigma]$, and we have $\theta_\sigma \in \text{Hom}(G/C, C)$ (check!). The map $\mathcal{A} \rightarrow \text{Hom}(G/C, C)$ defined by $\sigma \rightarrow \theta_\sigma$ is injective since if $\theta_\sigma = \theta_\tau$, then $[g, \sigma] = [g, \tau]$ for all $g \in G$. It follows that $g^\sigma = g^\tau$ for all g and so $\sigma = \tau$. Thus, $|\mathcal{A}| \leq |\text{Hom}(G/C, C)|$. Since C is cyclic, it follows easily from the fundamental theorem on abelian groups applied to G/C , that $|\text{Hom}(G/C, C)| \leq |G/C|$, and the result follows. \square

Appendix 21

Isaacs' examples

1^o. Let $b = \frac{p^s - 1}{p - 1} = 1 + p + \cdots + p^{s-1}$; then \mathbb{F}^* , the (cyclic) multiplicative group of the field $\mathbb{F} = \text{GF}(p^s)$, has a unique subgroup C of order b . We define an action of C on $P = A_p(s, \theta)$, where θ is the Frobenius automorphism of \mathbb{F} (see §46), as follows: $(x, y)^c = (xc, yc^{p+1})$ ($c \in C$). Taking into account that $\theta(c) = c^p$ and writing $(x, y)^c = (xc, y\theta(c)c)$, it is easy to check that this is in fact an action. Indeed,

$$\begin{aligned} [(x, y)(u, v)]^c &= (x + u, y + v + x\theta(u))^c \\ &= ((x + u)c, (y + v + x\theta(u))\theta(c)c) \\ &= (xc, y\theta(c)c)(uc, v\theta(c)c) = (x, y)^c(u, v)^c. \end{aligned}$$

If $(x, y)^c = (x, y)$, then $c = 1$, i.e., every element of $C^\#$ induces a fixed-point-free automorphism of P . Therefore, $C \cdot P = (C, P)$ is a Frobenius group with kernel P and complement C . In what follows we retain the above notation.

We will construct a p -solvable group G such that $b(Q) = \max \{\phi(1) \mid \phi \in \text{Irr}(Q)\}$ does not divide $\chi(1)$ for all $\chi \in \text{Irr}(G)$, where $Q \in \text{Syl}_p(G)$. This example disproves one conjecture of the first author and is taken from Isaacs' note (unpublished).

Let $P = A_p(s, \theta)$. In what follows, we assume that $s = p > 2$; then $P = A_p(p, \theta)$ and $o(\theta) = p$. We define an action of $\mathcal{S} = \langle \theta \rangle$ on P as follows: $(x, y)^\theta = (\theta(x), \theta(y))$. Set $G = (\mathcal{S} \cdot C) \cdot P$. Next, $(x, y)^\theta = (x, y)$ if and only if $x, y \in \mathbb{F}_0$, the prime subfield of \mathbb{F} , and so $|C_P(\theta)| = |\mathbb{F}_0|^2 = p^2$, $|C_{Z(P)}(\theta)| = |\mathbb{F}_0| = p$. Thus, θ fixes exactly p classes of $Z(P)$ and p classes of $P/P' = P/Z(P)$. By Brauer's permutation lemma, θ fixes exactly p linear characters of both groups $Z(P)$ and P . If $\lambda \in \text{Lin}(Z(P)) - \{1_{Z(P)}\}$ is one of them and $H = \ker(\lambda)$, then θ fixes all linear characters of $Z(P)$ with kernel H . It follows that θ fixes exactly one maximal subgroup of $Z(P)$. We choose θ so that it raises every element of \mathbb{F} in power p (i.e., θ is a Frobenius automorphism of \mathbb{F}). If $c \in C$ and $\theta(c) = c$, then $c^{p-1} = 1$ so $c = 1$ since $(|C|, p - 1) = (b, p - 1) = (1 + p + \cdots + p^{p-1}, p - 1) = 1$ in view of

$$1 + p + \cdots + p^{p-1} = p + (p - 1) + (p^2 - 1) + \cdots + (p^{p-1} - 1) \equiv 1 \pmod{p - 1}$$

(recall that $p > 2$). Therefore, $\mathcal{S} \cdot C = (\mathcal{S}, C)$ is a Frobenius group with kernel C and complement \mathcal{S} , $|\mathcal{S} \cdot C| = pb$. The group $\mathcal{S} \cdot C$ has exactly $|C| = b$ subgroups of order p , and all these subgroups are conjugate in $\mathcal{S} \cdot C$ (Sylow). Then, if T is a

subgroup of order p in $\mathcal{S} \cdot C = T \cdot C$, then T fixes exactly one maximal subgroup H_T of $Z(P)$. Since b is the number of maximal subgroups of $Z(P)$, there is a one-to-one correspondence $T \leftrightarrow H_T$, where T is a subgroup of order p in $\mathcal{S} \cdot C$ and H_T is a maximal subgroup of $Z(P)$ fixed by T .

By the previous paragraph, \mathcal{S} fixes exactly $p^2 - p$ nonlinear irreducible characters of P (these characters are irreducible constituents of the induced character α^P , where α runs over all nonprincipal linear characters of $Z(P)/H_{\mathcal{S}}$ and $H_{\mathcal{S}}$ is a unique maximal subgroup of $Z(P)$ fixed by \mathcal{S}). It follows that $\alpha^{\mathcal{S} \cdot P}$ is the sum of p^2 irreducible characters of $\mathcal{S}P$ of degree $p^{(p-1)/2}$. In particular, the inertia subgroup $I_G(\alpha) = \mathcal{S} \cdot P$, and so all irreducible constituents of α^G have degree $bp^{(p-1)/2}$. If $T < \mathcal{S} \cdot C$ is of order p , then, if H_T is the maximal subgroup of $Z(P)$ fixed by T and β is a nonprincipal irreducible character of $Z(P)/H_T$, then $I_G(\beta) = T \cdot P$. If $\chi \in \text{Irr}_1(G/Z(P))$, then $\chi(1)$ divides $|G : P| = bp$, by Ito's theorem on degrees (see Introduction, Theorem 17). Therefore, the p -part of the degree of every irreducible character of G does not exceed $p^{(p-1)/2}$.

However, $\mathcal{S} \cdot P \in \text{Syl}_p(G)$ has an irreducible character of degree $p^{(p+1)/2}$. This is because \mathcal{S} definitely does not stabilize all nonlinear irreducible characters of P . This proves, that $b(P) = \max \{\psi(1) \mid \psi \in \text{Irr}_1(P)\} \nmid \chi(1)$ for all $\chi \in \text{Irr}(G)$. We do not know if there exists an analogous example for $p = 2$.

Isaacs [Isa4] proved that for every set \mathcal{S} of powers of a prime p such that $p^0 = 1 \in \mathcal{S}$, there exists a p -group P such that $\text{cd}(P) = \mathcal{S}$ (see Theorem A.21.2, below). Next, he showed (in the letter to the author) that for each p -group P there exists a group G with cyclic Sylow p -subgroup C such that $\text{cd}(G) = \text{cd}(P)$. We will prove this result. Moreover, we show that, for every set \mathcal{S} of powers of a prime p containing $1 = p^0$ and with maximum member p^a , there exists a group G having a cyclic Sylow p -subgroup C of order p^a such that $\text{cd}(G) = \mathcal{S}$. Let a prime $q \neq p$. For each member $p^e \in \mathcal{S}$, let V_e be an elementary abelian q -group on which a cyclic group of order p^e acts faithfully and irreducibly. Let C act on V_e with kernel of order p^{a-e} (in that case, C acts on V_e irreducibly), and let W be the direct product of the groups V_e for $p^e \in \mathcal{S}$, so that C acts on W . Let G be the semidirect product of W with C . We claim that $\text{cd}(G) = \mathcal{S}$. Obviously, it is enough to prove that $p^a \in \text{cd}(G)$; by Ito's theorem (Introduction, Theorem 17), the set $\text{cd}(G)$ contains only powers of p not exceeding $|C| = p^a$. Let $W = V_{e_1} \times \dots \times V_{e_s}$, where $\mathcal{S} = \{1, p^{e_1}, \dots, p^{e_s} = p^a\}$. Let $x_i \in V_{e_i}^\#$, $i = 1, \dots, s$ $x = x_1 \dots x_s$. Then the normal closure of $\langle x \rangle$ in G is W , the socle of G . Therefore, $\text{Irr}(G)$ has a faithful character χ (Gaschütz; see [BZ, Chapter 9]). We claim that $\chi(1) = p^{e_s} = p^a$. Note that $C \cdot V_a$ is a Frobenius group. Since $V_a \not\subseteq \ker(\chi)$, it follows that the restriction χ_{V_a} has a non-principal constituent, and so $\chi(1) \geq p^a$ in view of $\text{cd}(C \cdot V_a) = \{1, p^a\}$. Since $\chi(1)$ divides p^a , by Ito's theorem, we get $\chi(1) = p^a$.

It is not surprising that the subgroup W in the previous example is abelian. Indeed, if the degrees of all irreducible characters of G are powers of a fixed prime p , then G has an abelian normal p -complement (Ito).

2^o . Let \mathcal{S} be the set of powers of p such that $1 \in \mathcal{S}$. We will prove that there exists p -groups G such that $\text{cd}(G) = \mathcal{S}$. Moreover, Isaacs [Isa4] has showed that there exists a p -group G of class ≤ 2 such that $\text{cd}(G) = \mathcal{S}$.

Let U be an abelian group which acts on an abelian group A . Let $\tilde{A} = \text{Lin}(A)$ be the group of linear characters of A . As we know (see [BZ, §1.9]), there exists a natural isomorphism of \tilde{A} onto A . If $\alpha \in \tilde{A}$, $u \in U$ and $a \in A$, then, setting $\alpha^u(a) = \alpha(uau^{-1})$, we define the action of U on \tilde{A} .

Lemma A.21.1 ([Isa4]). *Let U be an abelian group acting on an abelian group A and \mathcal{S} the set of the sizes of the U -orbits in this action. Write $G = U \cdot A$, where the semidirect product is constructed with respect to the action of U on \tilde{A} , induced by the given action of U on A . Then $\text{cd}(G) = \mathcal{S}$. Furthermore, if $[A, U, U] = \{1\}$, then $\text{cl}(G) \leq 2$.*

Proof. Let $\lambda \in \text{Lin}(\tilde{A})$ and T the stabilizer of λ in U . Since the cyclic group $\tilde{A}/\ker(\lambda)$ is centralized by T , which is abelian, it follows that $\tilde{A}T/\ker(\lambda)$ is abelian and thus every $\psi \in \text{Irr}(\lambda^{\tilde{A}T})$ is linear. Obviously, $\tilde{A}T = \text{I}_G(\lambda)$, the inertia subgroup of λ in G , and thus every $\chi \in \text{Irr}(\lambda^G)$ has degree $|G : \tilde{A}T| = |U : T|$. Therefore, $\text{cd}(G) = \{|U : T| \mid T \text{ is a stabilizer in } U \text{ of some } \lambda \in \text{Lin}(\tilde{A})\}$. However, there is a natural correspondence between $\text{Lin}(\tilde{A})$ and A and this defines a permutation isomorphism of the actions of U on A and $\text{Lin}(\tilde{A})$, respectively, and we conclude that $\text{cd}(G) = \mathcal{S}$.

Now suppose that $[A, U, U] = \{1\}$. If $\alpha \in \tilde{A}$, we have for $u \in U$ and $a \in A$ that

$$[\alpha, u](a) = (\alpha^{-1}\alpha^u)(a) = \alpha(a^{-1})\alpha(uau^{-1}) = \alpha([a, u^{-1}]).$$

Therefore, if $v \in U$, we get

$$[\alpha, u, v](a) = [\alpha, u]([a, v^{-1}]) = \alpha([a, v^{-1}, u^{-1}]) = \alpha(1) = 1,$$

and so $[\tilde{A}, U, U] = \{1\}$. Since \tilde{A} is abelian and $[\tilde{A}, U] \leq \tilde{A}$, this yields $\text{C}_G([\tilde{A}, U]) \geq \tilde{A}U = G$, i.e., $[\tilde{A}, U] \leq Z(G)$. Since $G/[\tilde{A}, U] = \tilde{A}U/[\tilde{A}, U]$ is abelian, it follows that $\text{cl}(G) \leq 2$. \square

Now we are ready to prove the main result of this subsection.

Theorem A.21.2 ([Isa4]). *Let p be a prime and $0 = e_0 < e_1 < \dots < e_m$ integers. Then there exists a p -group that is generated by elements of order p and has nilpotence class ≤ 2 such that $\text{cd}(G) = \{p^{e_i} \mid 0 \leq i \leq m\}$.*

Proof. Let u_1, \dots, u_{e_m} be generators of $U \cong E_{p^{e_m}}$. Let A be an elementary abelian p -group with basis

$$a_1, z_{1,1}, \dots, z_{1,e_1}, a_2, z_{2,1}, \dots, z_{2,e_2}, \dots, a_m, z_{m,1}, \dots, z_{m,e_m},$$

and define an action of U on A as follows.

Put $(z_{i,\mu})^{u_v} = z_{i,\mu}$ for all i, μ, v and $(a_i)^{u_v} = a_i$ if $v > e_i$ and $(a_i)^{u_v} = a_i z_{i,v}$ if $v \leq e_i$. Since the automorphisms of A defined this way all have order p and commute pairwise, this does define an action of U on A .

Let us compute the sizes of the U -orbits of this action. Write $Z = \langle z_{i,\mu} \mid \mu \leq e_i \rangle \leq A$ and take $a \in A$. Then $Z \leq Z(G)$, where $G = U \cdot A$ is the natural semidirect product with kernel A . Assume that $a \in A - Z$. There exists, then, a unique subscript i such that $a = bcz$, where $b \in \langle a_j \mid j < i \rangle$, $1 \neq c \in \langle a_i \rangle$, $z \in Z$.

Suppose that $u \in U$. If (the expression of) u involves the generator u_μ with $\mu \leq e_i$, the exponents of $z_{i,\mu}$ in (expressions of) a and a^u will not be equal, and u does not centralize a . Thus $C_U(a) \leq \langle u_v \mid v > e_i \rangle$. Since the reverse inclusion is obvious, we get $C_G(a) = \langle u_v \mid v > e_i \rangle$.

We now have $|U : C_U(a)| = p^{e_i}$ and we see that the orbit sizes of the action of U on A are precisely the numbers p^{e_i} for $0 \leq i \leq m$. Since $[A, U] \leq Z \leq Z(G)$, we have $[A, U, U] = \{1\}$ and the result follows by Lemma A.21.1. \square

Appendix 22

Minimal nonnilpotent groups

A group G is said to be *minimal nonnilpotent* if it is not nilpotent but all its proper subgroups are nilpotent. In this section we present information on the structure of minimal nonnilpotent groups. The results of Theorem A.22.1 are due to O. Y. Schmidt [Sch2] and Y. A. Gol'dfand [Gol]; L. Rédei [Red] has classified such groups.

Theorem A.22.1. *Let G be a minimal nonnilpotent group. Then $|G| = p^a q^\beta$, where p and q are distinct primes. Let $P \in \text{Syl}_p(G)$, $Q \in \text{Syl}_q(G)$. Let b be the order of $q \pmod{p}$.*

- (a) *One of the subgroups P , Q (say Q) coincides with G' .*
- (b) *If Q is abelian, then $Q \cap Z(G) = \{1\}$ and $Q \cong E_{q^b}$.*
- (c) *P is cyclic and $|P : (P \cap Z(G))| = p$.*
- (d) *If Q is nonabelian, then it is special and $|Q/Q'| = q^b$, $Q \cap Z(G) = Z(Q)$. The number b is even.*

Proof. Let us show by induction on $|G|$ that G is solvable. Assuming that G is a minimal counterexample, we conclude that G is nonabelian simple.

Let H and F be different maximal subgroups of G whose intersection $D = H \cap F$ is as large as possible. Suppose that $D > \{1\}$. Since H, F are nilpotent, it follows that $N_H(D) > D$, $N_F(D) > D$, and therefore $N_G(D) \not\leq H$ and $N_G(D) \not\leq F$. Let $N_G(D) \leq R$, where R is maximal in G . Obviously, $H \neq R \neq F$. However $|H \cap R| > |N_H(D)| > |D|$, contrary to the choice of H and F . Hence $D = \{1\}$.

By Sylow's theorem, there exist in G two maximal subgroups H, F of different orders. Then

$$\begin{aligned} |G^\#| &= |G| - 1 \geq \sum_{x \in G} (H^\#)^x + (F^\#)^x \\ &= |G : H| \cdot |H^\#| + |G : F| \cdot |F^\#| = 2|G| - |G : H| - |G : F|, \end{aligned}$$

i.e., $|G : H| + |G : F| > |G|$, which is impossible. Hence, G is solvable.

Let $H \triangleleft G$ be of prime index p ; then $H = F(G)$, the Fitting subgroup of G , and H is the only normal subgroup of prime index in G . Let Q be a p' -Hall subgroup of H ; then Q is a normal p -complement in G . Let $P \in \text{Syl}_p(G)$, $|P| = p^a$. Then $G/Q \cong P$, and G/Q contains only one subgroup of index p . Therefore $P \cong C(p^a)$. If $P_0 = P \cap H$, then $C_G(P_0) \geq \langle P, Q \rangle = G$ and $P_0 \leq Z(G)$ so $P_0 = P \cap Z(G)$.

Assume that the p' -Hall subgroup Q of G is not primary. Then $Q = Q_1 \times Q_2$, where $\{1\} < Q_1 \in \text{Syl}(G)$ and $Q_2 > \{1\}$ is a Hall subgroup of G . By assumption, $PQ_1 < G$, $PQ_2 < G$; therefore, $PQ_1 = P \times Q_1$, $PQ_2 = P \times Q_2$, and so $C_G(P) = G$ and $G = P \times Q$ is nilpotent, a contradiction. Thus, $Q \in \text{Syl}_q(G)$, where $q \neq p$ is a prime. Since $G/Q \cong P$ is abelian, $G' \leq Q$. Since G contains only one normal subgroup of prime index, we get $Q = G'$.

Let $Q_0 \triangleleft G$ be such that $Q_0 < Q$ and $P, P_1 \in \text{Syl}_p(G)$ different. Since we have $PQ_0, P_1Q_0 < G$, it follows that $C_G(Q_0) \geq \langle P, P_1 \rangle = G$ (the subgroup $\langle P, P_1 \rangle$, which contains two different Sylow p -subgroups, is not nilpotent), and so $Q_0 \leq Z(G)$.

(i) Suppose that Q is abelian. Since G has no nontrivial direct factors, it follows from Corollary 6.5 that $Q \cap Z(G) = \{1\}$, and so, by the result of the previous paragraph, Q is a minimal normal subgroup of G so elementary abelian.

Let $|Q| = q^\beta$ and let b be the order of $q \pmod{p}$, $P = \langle x \rangle$; then $x^p \in Z(G)$. If $v_0 \in Q^\#$ and $v = v_0v_0^x \dots v_0^{x^{p-1}}$, then $v^x = v$. Since x normalizes $Q_1 = \langle v_0, v_0^x, \dots, v_0^{x^{p-1}} \rangle$, it follows that $Q_1 \triangleleft G$; therefore, by the previous paragraph, $Q_1 = Q$ and $\beta \leq p$. The equality $v^x = v$ implies that $v = 1$, since $v \in Z(G) \cap Q = \{1\}$. Therefore, $\beta < p$. Next, P does not normalize nontrivial subgroups of Q so the number s of subgroups of order q in Q is divisible by p . Let $\beta = kb + t$, $0 \leq t < b$. Assume that $t > 0$; then $b > 1$ so $p \nmid q - 1$. We have,

$$s = \frac{q^{kb+t} - 1}{q - 1} = q^t \cdot \frac{q^{kb} - 1}{q - 1} + \frac{q^t - 1}{q - 1}$$

so p divides $\frac{q^t - 1}{q - 1}$, a contradiction since $0 < t < b$. Thus, $t = 0$ so $\beta = kb$.

Assume that $k > 1$. The number of subgroups of order q^b in Q is

$$d = \frac{(q^{kb} - 1) \dots (q^{kb} - q^{b-1})}{(q^b - 1) \dots (q^b - q^{b-1})}.$$

Since $kb - i \not\equiv 0 \pmod{b}$ for $i \in \{1, \dots, b-1\}$, we get $q^{kb} - q^i = q^i(q^{kb-i} - 1) \not\equiv 0 \pmod{p}$. Since P does not normalize subgroups of Q of order q^b , it follows that p divides d so that p divides $\frac{q^{kb} - 1}{q^b - 1} = q^{b(k-1)} + \dots + q^b + 1 \equiv k \pmod{p}$ hence $k \geq p$. But then $\beta > p$, a contradiction. Thus, $k = 1$, $\beta = b$, $|Q| = q^b$.

(ii) Now suppose that Q is nonabelian. In that case, as we have proved, all G -invariant subgroups, properly contained in Q , lie in $Z(G) \cap Q = Z(Q)$. In particular, $\Phi(Q) \leq Z(Q)$. By (i), applied to G/Q' , we must have $Q' = Z(G)$, and we conclude that $Q' = \Phi(Q) = Z(Q)$, i.e., Q is special. Let $L < Z(Q)$ be maximal. Then by what has just been proved, Q/L is extraspecial of order q^{b+1} so b is even. \square

If G is the group of Theorem A.22.1 and $|Q \cap Z(G)| = q^c$, then G is called an $S(p^a, q^b, q^c)$ -group, where $|P| = p^a$, $|Q| = q^\beta = q^{b+c}$. As we saw, if $c > 0$, then b is even. Y. A. Gol'dfand [Gol] has shown that $c \leq b/2$, but we omit the proof.

Set $\text{mc}(G) = \frac{k(G)}{|G|}$ and $\text{f}(G) = \frac{1}{|G|} \sum_{\chi \in \text{Irr}(G)} \chi(1)$.

Theorem A.22.2 ([BZ, Chapter 11]). Let $G = PQ$ be an $S(p^a, q^b, q^c)$ -group, $P \in \text{Syl}_p(G)$, $Q = G' \in \text{Syl}_q(G)$ and $\chi \in \text{Irr}_1(G)$.

- (a) If $Q \cap Z(G) \leq \ker(\chi)$, then $\chi(1) = p$; if $Q \cap Z(G) \not\leq \ker(\chi)$, then $\chi(1) = q^{b/2}$.
- (b) $\text{mc}(G) = \frac{q^2 + p^2 q^c - 1}{p^2 q^{b+c}}$, $f(G) = \frac{q^b + pq^{c+b/2} + p - pq^{b/2} - 1}{pq^{b+c}}$.
- (c) If $H \leq Z(G)$, then $f(G/H) \geq f(G)$. If $c > 0$ and $\{1\} < H < Z(Q)$, then $f(G/H) = f(G)$ if and only if $p = 1 + q^{b/2}$, $q = 2$, $f(G) = 2^{-(b/2)}$.
- (d) If $p > q$ and $f(G) \geq \frac{1}{q}$, then $p = 3$, $q = 2$, $G/(P \cap Z(G)) \in \{\text{A}_4, \text{SL}(2, 3)\}$, $f(G) = \frac{1}{2}$.

Appendix 23

Groups all of whose noncentral conjugacy classes have the same size

In this section we prove some results from [Ito2]. For $x \in G$, we write $i_G(x) = |G : C_G(x)|$ and call that number the *index* of x in G . Recall that G is said to be *p -closed* (*p -nilpotent*) if Sylow p -subgroup is normal in G (G has a normal p -complement). Recall that $\pi(G)$ is the set of all prime divisors of $|G|$.

Theorem A.23.1. *Let $p, q \in \pi(G)$ be distinct and $pq \nmid i_G(x)$ for all $x \in G$. Then G is either p - or q -nilpotent. If G is p -nilpotent, then $N_G(P) = C_G(P)$ for $P \in \text{Syl}_p(G)$.*

Proof. Take $P \in \text{Syl}_p(G)$, $Q \in \text{Syl}_q(G)$ and let $x \in G$ with $p \nmid i_G(x)$. Then $P^y \leq C_G(x)$ for some $y \in G$ so $x \in C_G(P^y)$, i.e., any element of G whose index is prime to p , is contained in at least one conjugate subgroup of $C_G(P)$. Similarly, any element of G whose index is prime to q , is contained in at least one conjugate subgroup of $C_G(Q)$. Therefore, by hypothesis, we obtain the following inequality:

$$|G : N_G(C_G(P))|(|C_G(P)| - 1) + |G : N_G(C_G(Q))|(|C_G(Q)| - 1) + 1 \geq |G|.$$

Dividing the both sides by $|G|$, we obtain

$$\begin{aligned} & \frac{|C_G(P)|}{|N_G(C_G(P))|} + \frac{|C_G(Q)|}{|N_G(C_G(Q))|} \\ & \geq 1 + (|N_G(C_G(P))|^{-1} + |N_G(C_G(Q))|^{-1} - |G|^{-1}) > 1. \end{aligned}$$

At least one of two summands on the left hand side equals 1. Let, for definiteness, $\frac{|C_G(P)|}{|N_G(C_G(P))|} = 1$, or, what is the same, $C_G(P) = N_G(C_G(P))$. Since $C_G(P) \trianglelefteq N_G(P)$, we get $C_G(P) = N_G(C_G(P)) \geq N_G(P) (\geq C_G(P))$ so $N_G(P) = C_G(P)$. By Burnside's normal p -complement theorem, G is p -nilpotent. \square

Exercise 1. Study the structure of G such that, for some non-conjugate $A, B < G$, we have $\bigcup_{x \in G} (A \cup B)^x = G$.

Definition 1. The centralizer F of an element $x \in G - Z(G)$ is said to be *free* if there are no elements $y, z \in G - Z(G)$ such that $C_G(y) < F$ and $F < C_G(z)$.

Proposition A.23.2. Let F be a free centralizer in G . Then $F = P \times A$, where $P \in \text{Syl}_p(F)$ and A is abelian. If F contains two elements $x, y \in G$ such that $\pi(o(x)) = \{p\}$, $\pi(o(y)) = \{q\}$, $p \neq q$, and $C_G(x) = F = C_G(y)$, then F is abelian.

Proof. There are $p \in \pi(F)$ and a p -element $x \in G$ such that $F = C_G(x)$ since F is free. Let $y \in F$ with $\pi(o(y)) = \{q\}$, where $q \neq p$. Then $\langle xy \rangle = \langle x \rangle \times \langle y \rangle$ so $C_G(xy) \leq C_G(x) = F$. Since F is free, we get $C_G(xy) = F$ so $y = x^{-1}(xy) \in Z(F)$, and we conclude that $F = P \times A$, where $P \in \text{Syl}_p(F)$ and A is abelian (here we use Burnside's normal p -complement theorem). Assume, in addition, that $y \notin Z(G)$. Then $C_G(y) = F$ and $F = Q \times B$, where $Q \in \text{Syl}_q(F)$ and B is abelian, by the above. Since $Q \leq A$ so Q is abelian, we conclude that F is abelian. \square

Exercise 2. Let $H \triangleleft G$ be a π -Hall subgroup. Suppose that $i_G(x)$ is a π -number for all $x \in H$. Prove that then $G = F \times H$.

Solution. Let F be a π' -Hall subgroup of G (Schur–Zassenhaus). If $x \in H$, then $F^y \leq C_G(x)$ for some $y \in H$ so $x \in C_G(F^y) = C_G(F)^y$. Let $x_1, \dots, x_n \in H$ be representatives of the set of all H -classes such that $x_i \in C_G(F)$, $i = 1, \dots, n$, and set $D = \{x_1, \dots, x_n\}$; then $D = H$ (Burnside). It follows that $G = F \times D = F \times H$.

We say that a group G has an abelian partition with kernel K , if G is a set-theoretic union of some abelian subgroups each pair of which has intersection K ; then $K \leq Z(G)$.

Definition 2. A p -group G is said to be of type (F) if, for every $x \in G - Z(G)$, the centralizer $C_G(x)$ is free.

Exercise 3. If the centralizers of all noncentral elements of G are abelian, then G has an abelian partition with kernel $Z(G)$ and G is of type (F).

Exercise 4. Let $x \in N \triangleleft G$. Prove that $i_N(x)$ divides $i_G(x)$. (*Hint.* Let K be a G -class containing x . Then $\text{Inn}(G)$ permutes transitively the set of N -classes contained in K .)

Let $\text{cs}(G)$ be the set of class sizes of G . If $\text{cs}(G) = \{1, n\}$ with $n > 1$, then G is of type (F).

Lemma A.23.3. Suppose that $\text{cs}(G) = \{1, n\}$ and G is nonnilpotent. Then $F = C_G(x)$ is abelian for all $x \in G - Z(G)$.

Proof. Suppose that F is a p -subgroup for some $p \in \pi(G)$. Then all p' -elements of G lie in $Z(G)$ so G is nilpotent, a contradiction. Thus, $|\pi(F)| > 1$. By Lemma A.23.2, $F = P \times A$, where $F \in \text{Syl}_p(F)$ and $A > \{1\}$ is abelian. Assume that P is nonabelian so one may assume that $\pi(o(x)) = \{p\}$. By Lemma A.23.2, $A \leq Z(G)$. Since G is nonnilpotent, there is $y \in G - Z(G)$ with $\pi(o(y)) = \{q\}$, $q \neq p$. Set $F_1 = C_G(y)$; then $|F_1| = |F|$ and $F_1 = Q \times A_1$, where $Q \in \text{Syl}_q(F_1)$ and $A_1 > \{1\}$ is abelian. But $A \leq Z(G) < F_1$ so $A_1 = A$ since $|A_1| = |A|$. It follows that $P \leq A_1$ so P is abelian, contrary to the assumption. \square

Theorem A.23.4. *Let G be a group with $\text{cs}(G) = \{1, n\}$. Then $G = P \times A$ is nilpotent with $P \in \text{Syl}_p(G)$, $A \leq Z(G)$ and $\pi(n) = \{p\}$.*

Proof. Suppose that G is nonnilpotent. Then, by Lemma A.23.3, centralizers of noncentral elements of G are abelian so G admits an abelian partition $\Sigma = \{\text{C}_G(x_i)\}_{i=1}^m$ with kernel $Z(G)$ all of whose components are centralizers of noncentral elements of G and therefore have the same order $\frac{1}{n}|G|$ (Exercise 1). In that case, $G/Z(G)$ has a nontrivial abelian partition with kernel $\{1\}$ all of whose components have the same order $\frac{1}{n}|G : Z(G)|$ (i.e., $G/Z(G)$ is an equally partitioned group). By Isaacs' Theorem 68.4, there is a prime p such that $\exp(G/Z(G)) = p$; then G is nilpotent, i.e., G is not a counterexample. Clearly, $P \in \text{Syl}_p(G)$ is a unique nonabelian Sylow subgroup of G . Since $G = PZ(G)$, we get $\pi(n) = \{p\}$. \square

Proposition A.23.5. *Let G be a nonabelian p -group of type (F). Then there exists an abelian $A \triangleleft G$ such that $Z(G) \leq A$ and $\exp(G/A) = p$.*

Proof. This follows from Exercise 7.22. \square

A nonabelian p -group G in which $i_G(x) = p^e$ for all $x \in G - Z(G)$ is called an *Ito p -group*. Since an Ito p -group is of type (F), we deduce from Proposition A.23.5 the following

Corollary A.23.6. *If G is an Ito p -group, then $\exp(G/A) = p$ for a suitable abelian $A \triangleleft G$. In particular, if $p = 2$, then G/A is elementary abelian.¹*

Let G be an Ito p -group. It follows from Ito's proof of Proposition A.23.5 (see also the solution of Exercise 7.21) that, if $x \in Z_2(G) - Z(G)$, then $x^p \in Z(G)$ so $[x, y]^p = [x^p, y] = 1$ for all $y \in G$ hence $\{[x, y] \mid y \in G\} = L(x) \leq Z(G)$ and $\exp(L(x)) = p$ so $L(x)$ is elementary abelian. As we know, the map $y \mapsto [x, y]$ is the isomorphism $G/C_G(x) \cong L(x)$ so $|L(x)| = p^e$, where $p^e = i_G(x)$. Since $L(x) \cong E_{p^e}$, we conclude that $\Phi(G) \leq C_G(x)$. Thus, we have the following

Proposition A.23.7. *Let G be an Ito p -group with $i_G(x) = p^e$ for all $x \in G - Z(G)$. Then $d(G) \geq e$ and $|\Omega_1(Z(G))| \geq p^e$.*

Let $Z(G)$ be cyclic. Then $|\Omega_1(Z(G))| = p$ so, since $E_{p^e} \cong L(x) \leq Z(G)$, we get $e = 1$. In that case, by [Kno1] (see also Exercise 2.7), $|G'| = p$ so $\text{cl}(G) = 2$.

Ishikawa [Ish] has proved that if G is a group of Theorem A.23.5, then $\text{cl}(G) \leq 3$.

¹As A one can take a subgroup $\mathcal{M}(G) = \langle x \in G \mid C_G(x) = C_G(x^p) \rangle$ (see Exercise 7.22).

Appendix 24

On modular 2-groups

A p -group G is *modular* if every two subgroups of G are permutable (for arbitrary groups the definition is another). Sections of modular p -groups are modular. In this section we offer a generalization of a part of Iwasawa's theorem on modular 2-groups [Iwa] (see also §73).

Let $\mathcal{H}_2 = \langle a, b \mid a^4 = b^4 = 1, a^b = a^{-1} \rangle$ be the unique nonabelian metacyclic group of order 16 and exponent 4. The group \mathcal{H}_2 has exactly three (central) involutions a^2 , b^2 and a^2b^2 , the quotient group $\overline{\mathcal{H}_2} = \mathcal{H}_2/\langle a^2b^2 \rangle \cong Q_8$. Indeed, the group $\overline{\mathcal{H}_2} = \langle \bar{a}, \bar{b} \rangle$ has three distinct cyclic subgroups of index 2, namely $\langle \bar{a} \rangle$, $\langle \bar{b} \rangle$, $\langle \bar{a}\bar{b} \rangle$ of order 4, and our claim follows. Since $\exp(\mathcal{H}_2) = 4$, a^2b^2 is not a square. Since $\langle a^2 \rangle = \mathcal{H}'_2$, it follows that $\langle a^2 \rangle$, $\langle b^2 \rangle$ and $\langle a^2b^2 \rangle$ are characteristic in \mathcal{H}_2 . Note that \mathcal{H}_2 is nonmodular since $\mathcal{H}_2/\langle b^2 \rangle \cong D_8$ is nonmodular.

We define the 2-group \mathcal{F} as follows:

- (\mathcal{F}_1) $\mathcal{F} = \langle Q, Z \rangle$, where $Q \cong Q_8$, $Z \cong C_8$, $|Q \cap Z| = 4$.
- (\mathcal{F}_2) $|\mathcal{F}| = 2^5$.
- (\mathcal{F}_3) $C_{\mathcal{F}}(Q) \cong E_4$.
- (\mathcal{F}_4) $\Omega_2(\mathcal{F}) = QC_{\mathcal{F}}(Q)$.

We have $N_{\mathcal{F}}(Q \cap Z) \geq \langle Q, Z \rangle = \mathcal{F}$ so $Q \cap Z \triangleleft \mathcal{F}$. By (\mathcal{F}_1) and (\mathcal{F}_2), $QZ \neq ZQ$ so \mathcal{F} is not modular, and $\mathcal{F}/(Q \cap Z) \cong D_8$. By (\mathcal{F}_3) and (\mathcal{F}_4), $\Omega_2(\mathcal{F}) \cong Q \times C_2$ hence $c_1(\mathcal{F}) = 3$, $c_2(\mathcal{F}) = 6$ so $c_3(\mathcal{F}) = \frac{|\mathcal{F}|-|\Omega_2(\mathcal{F})|}{\varphi(8)} = 4$ and \mathcal{F} is not of maximal class. By (\mathcal{F}_1) and (\mathcal{F}_2), $Z \not\leq \mathcal{F}$. Let $U/(Q \cap Z)$ be the cyclic subgroup of order 4 in $\mathcal{F}/(Q \cap Z)$. Then U is nonabelian (otherwise, $C_{\mathcal{F}}(Q \cap Z) \geq UZ = \mathcal{F}$ so $Q \cap Z \leq Z(\mathcal{F})$, a contradiction since $|Q : (Q \cap Z)| = 2$ and Q is nonabelian). If $\exp(U) = 4$, then $U \cong \mathcal{H}_2$ is minimal nonabelian so $c_2(U) = 6 = c_2(\mathcal{F})$, $c_1(U) = 3 = c_1(\mathcal{F})$ so $U = \Omega_2(\mathcal{F})$, a contradiction since $\Omega_2(\mathcal{F}) (> Q)$ is not minimal nonabelian. Thus, $\exp(U) = 8$ so $U \cong M_{24}$.

The group \mathcal{F} is uniquely determined. This follows from §52. Let G be a 2-group of order $> 2^4$ with $\Omega_2(G) = Q_8 \times C_2$. Then $|G| = 2^5$ and G is uniquely determined: $G = \langle w, y \rangle$, where

$$\begin{aligned} w^4 &= y^8 = 1, & [w, y] &= t, & y^2 &= tv, & w^2 &= v^2 = u, \\ v^2 &= t^2 = [t, w] = 1, & [t, y] &= [v, w] = u, & v^y &= v^{-1}. \end{aligned}$$

Here $Z(G) = \langle u \rangle$ is of order 2, $C_G(t) = \langle t \rangle \times \langle v, w \rangle$, where $\langle v, w \rangle \cong Q_8$.

In Theorem A.24.1 we offer another approach to the proof of the following assertion from [Iwa]: If a modular 2-group has a section $\cong Q_8$, it is Dedekindian. In fact, Theorem A.24.1 is a generalization of the above assertion since in that theorem we do not assume that G is modular.

Theorem A.24.1. *A 2-group G is Dedekindian if it satisfies the following conditions:*

- (i) *Every two subgroups of G of order ≤ 4 are permutable.*
- (ii) *G has a section isomorphic to Q_8 .*
- (iii) *G is \mathcal{H}_2 -free.*
- (iv) *G has no subgroups isomorphic to \mathcal{F} .*

We first prove the following

Lemma A.24.2. *Suppose that a 2-group G is \mathcal{H}_2 -free and such that $G/N \cong Q_8$ for some $N \triangleleft G$. Then $G = Q \cdot N$ with $Q \cap N = \{1\}$ and $Q \cong Q_8$.*

Proof. We use induction on $|G|$. One may assume that $|G| > 2^3$. First let $|N| = 2$. Since G is not of maximal class, it has no cyclic subgroups of index 2 (Lemma 64.1(t)). If $N \not\leq \Phi(G)$, we get $G = N \times Q$, and we are done. Now let $N < \Phi(G)$. In that case, all maximal subgroups of G are abelian of type $(4, 2)$ so G is minimal nonabelian, and $\Omega_1(G) \cong E_4$. Then, by Lemma 65.1, G is metacyclic of exponent 4 so $G \cong \mathcal{H}_2$, contrary to the hypothesis.

Now suppose that $|N| > 2$. Let L be a G -invariant subgroup of index 2 in N . By the previous paragraph, $G/L = (Q/L) \times (N/L)$, where $Q/L \cong Q_8$. By induction applied to Q , we have $Q = Q_1 \cdot L$, where $Q_1 \cap L = \{1\}$ and $Q_1 \cong Q_8$. We have

$$Q_1 \cap N = (Q_1 \cap Q) \cap N = Q_1 \cap (Q \cap N) = Q_1 \cap L = \{1\}$$

so $G = Q_1 \cdot N$ is a semidirect product. □

Proof of Theorem A.24.1. We use induction on $|G|$. The hypothesis is inherited by subgroups. All subgroups of G of exponent ≤ 4 are modular, by (iii), so $\exp(\Omega_1(G)) = 2$. By hypothesis, there is a chain $L \trianglelefteq K \leq G$ such that $K/L \cong Q_8$. Since K is \mathcal{H}_2 -free, we get $K = Q \cdot L$, where $Q \cap L = \{1\}$ and $Q \cong Q_8$ (Lemma A.24.2). Set $Q = \langle a, b \mid a^4 = b^4 = 1, a^b = a^{-1} \rangle$, $A = \langle a \rangle$, $B = \langle b \rangle$. Let $Q \leq H \in \Gamma_1$. By induction, $H = Q \times E$, where $\exp(E) \leq 2$. Let $z \in G - H$, where $o(z)$ is as small as possible. Set $Z = \langle z \rangle$. We get $\exp(H) \leq 4$ so $|Z| \leq 2\exp(H) = 8$.

Let $|Z| = 2$. Then $ZA = AZ$ and $BZ = ZB$ are abelian of type $(4, 2)$ since G has no subgroups $\cong D_8$. If $y \in E$, then $\langle z, y \rangle \cong E_4$ since $\langle z \rangle \langle y \rangle < G$. Then $G = H \times Z = (Q \times E) \times Z = Q \times (E \times Z)$ is Dedekindian.

Let $|Z| = 4$. Then Z is permutable with all subgroups of H , by (i). Set $M = QZ$; then $M \leq G$. Assume that $Q \cap Z = Z(Q)$; then $|M| = 2^4$. Since a 2-group of maximal class and order $\geq 2^4$ has two non-permutable subgroups of order 4, M is not

of maximal class. Therefore, by Lemma 64.1(i) (= Proposition 1.17), $M = Q * Z(M)$. Next, $Z(M) \cong E_4$ (otherwise, $\Omega_1(M) = M$ is not elementary abelian, by Appendix 16). It follows that $M = Q \times L$, where $|L| = 2$. Then $L \not\leq H$ and $|L| = 2 < |Z|$, contrary to the choice of z . Thus, $Q \cap Z = \{1\}$. By the previous paragraph, $\Omega_1(Z) < Z(M)$. If $D = Z(Q) \times \Omega_1(Z)$ ($\cong E_4$), then $D \triangleleft M$ and $M/D \cong E_8$ so $\exp(M) = 4$ and M is modular, by (i). Then, by the previous paragraph, $M/\Omega_1(Z) = (Q\Omega_1(Z)/\Omega_1(Z)) \times (Z/\Omega_1(Z))$ so $Z \triangleleft M$. Since $A \cdot Z \not\cong \mathcal{H}_2$, it follows that AZ is abelian of type (4, 4). Similarly, $B \cdot Z \cong A \times Z$. It follows that Z centralizes $AB = Q$ so $M = Q \times Z$. Let $T = \langle a^2 z^2 \rangle$. Then $M/T \cong Q_8 * C_4$ is of order 16 so $Q_8 * C_4 \cong D_8 * C_4$ (Appendix 16). The inverse image of D_8 of exponent 4 is not modular since D_8 is not modular, a contradiction.

It remains to consider the case $|Z| = 8$. Then $H \cap Z$ is cyclic of order 4. Since $\mathcal{V}_1(H) = Z(Q)$, we get $Z(Q) < Z \cap H < Z$. Since $C_H(Q) = Z(H)$ is elementary abelian, we may assume that $Z \cap H$ does not centralize a subgroup A of order 4 in Q . Then $A(H \cap Z) = (H \cap Z)A$ and $\Omega_1(H \cap Z) = \Omega_1(A) (= Z(Q))$ so $A(H \cap Z) = Q_1 \cong Q_8$. Since every nonabelian subgroup of order 8 is a direct factor of H , one may assume from the start that $|Q \cap Z| = 4$. Set $D = \langle Q, Z \rangle$. Assume that $|D| = 2^4$; then $D = QZ = ZQ$ has the cyclic subgroup Z of index 2 so D is of maximal class (Lemma 64.1(t)). Since D has two non-permutable subgroups of order 4, we get a contradiction. Thus, $|D| > 2^4$ so Z does not normalize Q . Then $D/(Q \cap Z) \cong D_{2^n}$ for $n > 2$ since $D/(Q \cap Z)$ is generated by two non-permutable subgroups $Q/(Q \cap Z)$ and $Z/(Q \cap Z)$ of order 2. Since $\exp(H/(Q \cap Z)) = 2$, we get $\exp(G/(Q \cap Z)) \leq 4$ so $n = 3$. We conclude that $D/(Q \cap Z) \cong D_{2^3}$ so $|D| = |Q \cap Z||D/(Q \cap Z)| = 2^5$. As above, D is not of maximal class so $C_D(Q) \not\leq Q$ (Lemma 64.1(i)). Since $QC_D(Q)$ is modular, $C_D(Q) \cong E_4$ (Appendix 16). In that case, $QC_D(Q) = Q \times L$, where $|L| = 2$. Clearly, $QC_D(Q) = D \cap H$. Take $y \in D - QC_D(Q)$ and set $Y = \langle y \rangle$. Since $y \notin H$, we get $|Y| = 8$, by the choice of z . Then $c_3(D) = 4$, $c_2(D) = c_2(QC_D(Q)) = 6$, $c_1(D) = c_1(QC_D(Q)) = 3$. It follows that $D \cong \mathcal{F}$, contrary to the hypothesis. Thus, G has no cyclic subgroups of order 8. The proof is complete. \square

Thus, the classification of modular 2-groups G is reduced to the case where G is quaternion-free. If G of Theorem A.24.1 is a minimal counterexample, it is minimal non-Dedekindian so the result follows from Theorem A.17.3. However, the proof of Theorem A.24.1 presents independent interest.

Corollary A.24.3. *A 2-group G is Dedekindian if it satisfies the following conditions:* (i) *Whenever $U, V \leq G$ with $|U| \leq 4$, $|V| \leq 8$, then U and V are permutable.* (ii) Q_8 *is involved in G .* (iii) G *is \mathcal{H}_2 -free.*

Indeed, G has no subgroups $\cong \mathcal{F}$ so G is Dedekindian, by Theorem A.24.1.

Corollary A.24.4 ([Iwa]). *Suppose that a 2-group G is modular. If Q_8 is involved in G , then G is Dedekindian.*

Indeed, \mathcal{H}_2 and \mathcal{F} are nonmodular since they have epimorphic image $\cong D_8$. Now the result follows from Theorem A.24.1.

Corollary A.24.5. *Let a non-Dedekindian 2-group G be \mathcal{H}_2 -free and let $\Omega_2(G) < G$ be nonabelian Dedekindian. Then G has a subgroup $\cong \mathcal{F}$.*

Indeed, if G has no subgroups isomorphic to \mathcal{F} , it satisfies the hypothesis of Theorem 24.1 (see Theorem 1.20) so G is Dedekindian.

Now we state an analog of Lemma A.24.2 for $p > 2$. Suppose that a p -group G , $p > 2$, has no sections of order p^4 which are either of maximal class or nonmetacyclic minimal nonabelian of order p^4 . Let $N \triangleleft G$ be such that $G/N \cong S(p^3)$, the nonabelian group of order p^3 and exponent p . Then $G = S \cdot N$, where $S \cap N = \{1\}$. Assume that our assertion is false. As in the proof of Lemma A.24.2, one may confine to the case $|N| = p$. Then $d(G) = 2$. Since G is not of maximal class, we get $|Z(G)| = p^2$. In that case, however, G is a nonmetacyclic \mathcal{A}_1 -group, a contradiction.

Appendix 25

Schreier's inequality for p -groups

If $d(G)$ is the minimal number of generators of (not necessarily prime power) group G , $H < G$, then the following inequality due to O. Schreier holds:

$$(1) \quad d(H) \leq 1 + (d(G) - 1)|G : H|.$$

Consider the regular wreath product $G_0 = E_{p^{d-1}} \text{wr } C_n$, where $p \in \pi(n), n, d > 1$. Let H_0 be the base subgroup of G_0 ; then $H_0 \cong E_{p^{(d-1)n}}$. Let $C_n = \langle x \rangle$; then $G_0 = \langle x, H_0 \rangle$. Define the group $G = \langle y, H_0 \rangle$ as follows: $\langle y \rangle \cap H_0 = \{1\}$, $o(y) = pn$, $y^n \in Z(G)$, $h^y = h^x$ for all $h \in H_0$. Set $H = \langle y^n, H_0 \rangle$; then $H = \langle y^n \rangle \times H_0 \cong E_{p^{1+(d-1)n}}$. Since $y^n \leq \Phi(\langle y \rangle) \cap Z(G)$, we get $\langle y^n \rangle \leq \Phi(G)$. Since $G/\langle y^n \rangle \cong G_0$, we have $d(G) = d(G_0)$. Since $G_0 = \langle x, E_{p^{d-1}} \rangle$, we get $d(G) \leq d$. Since $d(H) = 1 + (d - 1)n$, we get $d(G) = d$, by (1), so estimate (1) is attained. We offer another proof of (1) for p -groups.

Theorem A.25.1. *Let H be a subgroup of index p^m in a p -group G . Then $d(H) \leq 1 + p^m(d(G) - 1)$.*

Proof. We use induction on m .

(i) Let $m = 1$. Then $\Phi(H) \triangleleft G$ and $\Phi(H) \leq \Phi(G)$. Hence $d(G/\Phi(H)) = d(G)$, $d(H/\Phi(H)) = d(H)$ so, without loss of generality, one may assume that $\Phi(H) = \{1\}$. Then $H \cong E_{p^{d(H)}}$.

Take $x \in G - H$; then $G = \langle x \rangle H$, $x^p \in Z(G) \cap \Phi(G)$. Setting $\bar{G} = G/\langle x^p \rangle$, we get $d(\bar{G}) = d(G)$. It follows from $\Omega_1(\bar{G}) = \bar{G}$ that $\bar{G}' = \Phi(\bar{G})$.

Let, in addition, $d(G) = 2$. Then $|\bar{G} : \bar{G}'| = p^2$ so $d(G) = d(\bar{G}) = 2$ and \bar{G} is either abelian of order p^2 or of maximal class. In the first case, $|G| = p^3$ so (1) is true. If \bar{G} is of maximal class, the $d(\bar{H}) \leq p$ (Theorems 9.5 and 9.6) so $d(H) \leq p + 1$, and (1) holds again. (If, in addition, $o(x) = p$, then $|G| \leq p^{p+1}$ so $d(H) \leq p$.)

Next suppose that $d = d(G) > 2$. Then $G = \langle x, x_2, \dots, x_d \rangle$ where $x_2, \dots, x_d \in H$. Set $A_i = \langle x, x_i \rangle$ ($i = 2, \dots, d$). Since $d(A_i) = 2$ and $H \cap A_i$ is elementary abelian of index p in A_i , we have $|A_i| \leq p^{2+p}$, $i = 2, \dots, d$, by the previous paragraph. Since $N_G(H \cap A_i) \geq HA_i = G$, $H \cap A_i$ is normal in G . Next, $A_2(H \cap A_3) \dots (H \cap A_d) \geq \langle x, x_2, \dots, x_d \rangle = G$ and the factors $A_2, H \cap A_3, \dots, H \cap A_d$ are pairwise permutable. Now, for $i = 2, \dots, d$, we get

$$|A_i/\langle x^p \rangle| \leq p^{1+p}, \quad |(H \cap A_i)/\langle x^p \rangle| \leq p^p, \quad |\bar{G}| = |G/\langle x^p \rangle| \leq p^{1+(d-1)p},$$

and

$$|G| \leq p|\bar{G}| \leq p^{2+(d-1)p}, \quad |H| \leq p^{1+(d-1)p}, \quad d(H) \leq 1 + (d-1)p,$$

proving (1) for G and H in the case $m = 1$.¹

(ii) Let $m > 1$. Take in G a maximal subgroup F containing H . By induction, $d(H) \leq 1 + p^{m-1}(d(F) - 1)$. By (1), $d(F) - 1 \leq p(d(G) - 1)$ so

$$d(H) \leq 1 + p^{m-1} \cdot p(d(G) - 1) = 1 + p^m(d(G) - 1),$$

and (1) is also proved for $m > 1$. □

Definition. A p -group G is said to be *generalized regular* if $\exp(\Omega_1(H)) = p$ for every nontrivial section H of G .

Generalized regular p -groups coincide with \mathcal{P}_2 -groups (see §11). The group Q_8 is generalized regular but irregular.

Theorem A.25.2. *Let H be a maximal subgroup of a p -group G .*

(a) *If $\exp(G) = p$, then $d(H) \leq (p-1)(d(G)-1)$.*

(b) *If G is generalized regular, then $d(H) \leq 1 + (p-1)(d(G)-1)$.*

Proof. We may assume that G is nonabelian and, as before, $\Phi(H) = \{1\}$; then $H \cong E_{p^{d(H)}}$. Set $d = d(G)$.

(a) Let $\exp(G) = p$; then $\Phi(G) = G'$ so $|G : G'| = p^d$ and, by Lemma 64.1(q), $|\mathrm{Z}(G)| = p^{d-1}$.

(i) Let $d = 2$. Then G is of maximal class so $|G| \leq p^p$ (Theorem 9.5) and $|H| \leq p^{p-1}$, $d(H) \leq p-1 = (d-1)(p-1)$.

(ii) Let $d > 2$. Take $x = x_1 \in G - H$; then $G = \langle x_1, x_2, \dots, x_d \rangle$, where $x_2, \dots, x_d \in H$. For $i = 2, \dots, d$, consider the subgroup $A_i = \langle x_1, x_i \rangle$; then, by (i), $|A_i| \leq p^p$. We have $\mathrm{N}_G(H \cap A_i) \geq HA_i = G$ so $H \cap A_i$ is G -invariant of order $\leq p^{p-1}$ for $i > 1$. It follows from

$$A_2(H \cap A_3) \dots (H \cap A_d) \geq \langle x_1, x_2, \dots, x_d \rangle = G$$

that $|G| \leq p^{1+(p-1)(d-1)}$, $|H| \leq p^{(p-1)(d-1)}$ so $d(H) \leq (d-1)(p-1)$.

(b) Let $H \in \Gamma_1$ and, as above, $\Phi(H) = \{1\}$, i.e., H is elementary abelian. If $x = x_1 \in G - H$, then $x^p \in \mathrm{Z}(G)$, $G = \langle x \rangle \cdot H$. As above, $G = \langle x_1, x_2, \dots, x_d \rangle$, where $x_2, \dots, x_d \in H$, $x_1 = x$. Let $G_0 = G/\langle x^p \rangle$, $H_0 = H/\langle x^p \rangle$. If $y_i = x_i \langle x^p \rangle$, then $G_0 = \langle y_1, \dots, y_d \rangle$, $y_2, \dots, y_d \in H_0$. Since G_0 is generalized regular and $\Omega_1(G_0) = G_0$, we have $\exp(G_0) = p$. By (a), $d(H_0) \leq (d-1)(p-1)$. Hence, $d(H) \leq 1 + d(H_0) \leq 1 + (d-1)(p-1)$, completing the proof of (b). □

¹If $\exp(x) = p$, then, as we know, $|A_i| \leq p^{p+1}$ for all $i = 2, \dots, d$ so $|G| \leq p^{1+p(d-1)}$ and $d(H) \leq p(d-1)$. Thus, if $d(H) = 1 + p(d-1)$, then $x^p \neq 1$ for $x \in G - H$ or, what is the same, $\Omega_1(G) = H$.

It is possible to show that estimates of Theorem A.25.2 are best possible.

Let G be a generalized regular p -group and let $H < G$ be of index $p^m > p$. Using Theorem A.25.2(b) and induction on m , it is easy to show that $d(H) \leq 1 + (p - 1)^m(d(G) - 1)$. In particular, if $p = 2$, then $d(H) \leq d(G)$.

Appendix 26

p -groups all of whose nonabelian maximal subgroups are either absolutely regular or of maximal class

In this section we prove the following

Theorem A.26.1. *Let a nonabelian p -group G be neither minimal nonabelian nor absolutely regular, $p > 2$ and $|G| > p^{p+1}$. If all nonabelian maximal subgroups of G are either absolutely regular or of maximal class, then one of the following holds:*

- (a) *G is of maximal class.*
- (b) *$G = B \times C$ where B is absolutely regular, $|C| = p$, $|\Omega_1(G)| = p^p$, $\Omega_1(G) \leq Z(G)$, $d(G/\Omega_1(G)) = 2$. All maximal subgroups of B containing $\Omega_1(B)$, are abelian.*
- (c) *G is an L_p -group (see §§17, 18), $|G : C_G(\Omega_1(G))| = p$.*

Groups (a)–(c) satisfy the hypothesis.

Proof. The last assertion is checked easily as will be clear from the proof. It remains to show that if G satisfies the hypothesis, it is one of groups (a)–(c).

If G is of maximal class (of order $> p^{p+1}$), then all maximal subgroups of G are either absolutely regular or of maximal class (Theorem 9.6) so G satisfies the hypothesis. In what follows we assume that G is not of maximal class.

Suppose that $\exp(G) = p$. Then G has no absolutely regular maximal subgroups. By Theorem 9.5, G has no subgroups of maximal class and index p . Since G is not minimal nonabelian, we get a contradiction. Thus, $\exp(G) > p$.

Let G be regular. Then, by Theorem 9.5, G has no subgroups of maximal class and index p . Assume that $|\Omega_1(G)| > p^p$. Then the set Γ_1 has no absolutely regular members. Since G is not minimal nonabelian. we get a contradiction. Now let $|\Omega_1(G)| = p^p$. Then all maximal subgroups of G , containing $\Omega_1(G)$, are abelian (Theorem 9.5). If $G/\Omega_1(G)$ is cyclic, then G is an L_p -group. Now assume that $G/\Omega_1(G)$ is noncyclic. Then there are in G two distinct maximal subgroups A and B that contain $\Omega_1(G)$; moreover, $d(G/\Omega_1(G)) = 2$ (Exercise 1.6(a)). In that case, $\Omega_1(G) \leq A \cap B = Z(G)$ so $|G'| = p$. If $\Omega_1(G) \leq \Phi(G)$, then $d(G) = 2$ so G is minimal nonabelian, contrary to the hypothesis. Otherwise, there is $X < \Omega_1(G)$ of

order p such that $G = X \times M$, where $M \in \Gamma_1$ is absolutely regular. In that case, G is as in (b).

Next we assume that G is irregular. Since G is not of maximal class, it contains a normal subgroup R of order p^p and exponent p .

(i) Suppose that $|G| > p^{p+2}$. Then all maximal subgroups of G containing R are neither absolutely regular nor of maximal class (Lemma 64.1(f)). Therefore, if $R < A$, where A is maximal in G , then A is abelian. Assume that $R < \Omega_1(G)$. Let $x \in G - R$ be of order p ; then $L = \langle x, R \rangle$ is elementary abelian of order p^{p+1} . Consideration of intersection of a maximal subgroup, say H , with L shows that H is neither of maximal class nor absolutely regular. Then all maximal subgroups of G are abelian, a contradiction since G is not minimal nonabelian. Thus, $R = \Omega_1(G)$. Therefore, if G/R is cyclic, then G is an L_p -group so it is as in (c). Suppose that G/R is noncyclic. Since all maximal subgroups of G , containing R , are abelian, it follows that $R \leq Z(G)$ and $|G : Z(G)| = p^2$ so $\text{cl}(G) = 2$ and G is regular, contrary to the assumption.

(ii) Let $|G| = p^{p+2}$.

(ii1) Suppose that G/R is cyclic (of order p^2). Let $D < R$ be G -invariant of index p^2 and $C = C_G(R/D)$; then $|G : C| \leq p$. Since $\text{cl}(G) \geq p > 2$, it follows that $C \in \Gamma_1$ is not of maximal class so abelian. If $\Omega_1(G) = R$, then G is an L_p -group. Assume that $|\Omega_1(G)| = p^{p+1}$; then $\Omega_1(G)$ is regular so elementary abelian. In that case, all maximal subgroups of G are abelian, a contradiction.

Now let $G/R \cong E_{p^2}$.

(ii2) Suppose that all $M < G$ such that $R < M$, are abelian. Then $R = Z(G)$ and $\text{cl}(G) = 2$ so G is regular, contrary to the assumption.

(ii3) Now suppose that there is nonabelian $M < G$ such that $R < M$. Then M is of maximal class so the number of subgroups of maximal class and index p in G is exactly p^2 (Theorem 12.12(c)). Since $d(G) = 3$ and G has no absolutely regular maximal subgroups (Theorem 12.12(b)), the number of abelian subgroups of index p in G is exactly $p + 1$. In that case, $\text{cl}(G) = 2$ so G is regular, a final contradiction. \square

Since absolutely regular 2-groups are cyclic, similar result for $p = 2$ gives the following

Exercise 1. If all nonabelian maximal subgroups of a nonabelian 2-group G are of maximal class, then one of the following holds:

- (a) G is minimal nonabelian.
- (b) G is of maximal class.
- (c) $G = DZ(G)$ is of order 16, where G is nonabelian of order 8.

Exercise 2. Classify the nonabelian p -groups of order p^{p+1} , $p > 2$, all of whose nonabelian maximal subgroups are either absolutely regular or of maximal class.

Research problems and themes II

This is the second part of the list written by the first author.

701. Study the irregular p -groups, $p > 2$, all of whose metabelian subgroups are regular.
702. Classify the minimal non-quaternion-free 2-groups. (For a solution, see §80.)
703. Study the p -groups G such that all elements of the set $G - G'$ ($G - \mathfrak{U}_1(G)$) have the same order $> p$ and $< \exp(G)$.
704. Describe the p -groups with cyclic subgroup of index p^3 acting as in §74.
705. Classify the U_3 -groups (see §64).
706. Classify the p -groups G such that for every (i) $H < G$ there exists $R \triangleleft G$ with $G/R \cong H$, (ii) $R \triangleleft G$ there exists $H \leq G$ such that $G/R \cong H$.
707. Construct a p -group $G = XY$ ($X, Y < G$) such that $C_Y(x) = \{1\}$ for all $x \in X$.
708. Set $\alpha(G) = \max \{d(A) \mid A \leq G, A' = \{1\}\}$, $\tau(G) = \max \{d(H) \mid H \leq G\}$. Produce a good estimate of $\tau(G)$ in terms of $\alpha(G)$.
709. Does there exist special p -groups all of whose maximal subgroups are special? If so, classify such groups.
710. Let $|\Phi(G)| = p^n$. Study the structure of $G = G_n$ provided $\text{cl}(G) = n + 1$. Find the minimal n such that all G_n ($p > 2$) are irregular.
711. Does there exist p -groups of order $> p^2$ and exponent $> p$, all of whose maximal subgroups are generated by elements of order p ? If so, study their structure.
712. Study the p -groups G of exponent p such that $|Z_p(G)| = p^p$.
713. Classify the p -groups which are lattice isomorphic to p -groups with abelian subgroup of index p .
714. Is it true that a p -group with a subgroup of order p^{p+2} and exponent p has a normal subgroup of order p^{p+1} and exponent p ?
715. Study the p -groups G such that $\text{Aut}(G)$ is an extraspecial p -group.
716. Classify the p -groups G such that G/R is special for all $R \leq Z(G)$ of order p .

717. Let $\Phi(G) < N < G$. Study the structures of N and G provided all maximal subgroups of G not containing N , are metacyclic.

718. Let $M \in \Gamma_1$. Classify the p -groups G all of whose nonabelian $L \in \Gamma_1 - \{M\}$ are minimal nonabelian.

719. Study the p -groups G such that for every $x \in \Phi(G)$ there is a minimal basis a_1, \dots, a_d with $x \in \langle a_1 \rangle$.

720. Is it true that the derived length of a p -group G is bounded provided that $\exp(\text{Aut}(G))_p = p$? Study the p -groups G satisfying the last condition.

721. Let G be group of order p^m with exactly p^{m-2} minimal nonabelian subgroups. Is it true that $|G'|$ is bounded?

722. (Old problem) Study the p -groups with elementary abelian $\text{Aut}(G)$.

723. Study the pairs $H < G$ of p -groups, if they exist, with $\text{cd}(G) = \text{cd}(H)$ and $|\text{Irr}(G)| = |\text{Irr}(H)|$.

724. Classify the p -groups with self centralizing abelian subgroup A of order p^3 . (For $p = 2$ and noncyclic A , see §§51, 77.)

725. Study the p -groups all of whose maximal subgroups are either metacyclic or have derived subgroup of order $\leq p$.

726. Classify the p -groups G such that $\text{Aut}(G) \in \{\Sigma_{p^n}, \text{UT}(n, p)\}$ for some n .

727. Does there exist a 2-group G such that $\Phi(G)$ is isomorphic to a Sylow 2-subgroup of some Suzuki simple group $\text{Sz}(2^m)$? If so, find all such m .

728. (i) Study the p -groups G , $p > 2$, such that $G/\mathfrak{U}_1(G)$ is extraspecial. (ii) Does there exist among groups satisfying (i), irregular p -groups?

729. Study the p -groups G with a minimal basis a_1, \dots, a_d such that every element of G can be presented in the unique way in the form $a_1^{\mu_1} \dots a_d^{\mu_d}$ with $0 \leq \mu_i < o(a_i)$, $i = 1, \dots, d$.

730. Classify the p -groups whose nonabelian subgroups of index p^2 are metacyclic.

731. Classify the p -groups all of whose two-generator subgroups are metacyclic.

732. Study the p -groups G with equal numbers of principal series in G and G/G' .

733. (Passman [Pas]) Classify the 2-groups all of whose nonnormal subgroups are cyclic. (This problem is solved in §16.)

734. Classify the p -groups G such that, whenever nonabelian $H \in \Gamma_1$, then $H = EZ(H)$, where E is extraspecial.

735. (Isaacs–Slattery) Given $p > 2$, does there exist a p -group G of class $p + 1$ with $\text{cd}(G) = \{1, p^2, p^4\}$?

736. Classify the p -groups G such that, whenever $H \leq G$ is nonabelian, then $C_G(H) = Z(H)$.

737. Classify the p -groups G all of whose maximal cyclic subgroups coincide with their centralizers.

738. For definition of an \mathcal{A}_n -group, see §§65, 71, 72. There exists $\alpha(n)$ such that $|G'| \geq p^{\alpha(n)}$ for all \mathcal{A}_n -groups G , and for some \mathcal{A}_n -group H we have $|H'| = p^{\alpha(n)}$. Give good estimate for $\alpha(n)$. Even $\alpha(4)$ is not known (it is known only that $\alpha(4) \leq 6$; see §72). Is it true that $\alpha(n+1) > \alpha(n)$ for all n ? Janko conjectured that $\alpha(n) \leq n+1$.

739. (i) Study the \mathcal{A}_n -groups G satisfying $|G'| = p^{\alpha(n)}$. (ii) Is it true that $\alpha(4) = 6$? (See #738.)

740. Study the p -groups G such that $G/\mathfrak{U}_2(G)$ is special.

741. Classify the p -groups G with $|G : Z(\chi)| \leq p^5$ for all $\chi \in \text{Irr}_1(G)$. (Here $Z(\chi) = \langle x \in G \mid |\chi(x)| = \chi(1) \rangle$.)

742. Classify the p -groups in which every nonabelian two-generator subgroup is either metacyclic or minimal nonabelian. (See #699.)

743. Study the 2-groups G such that every proper nonabelian subgroup of G has a section (i) $\cong Q_8$, (ii) $\cong D_8$.

744. Study the p -groups G with $H' = G'$ for all $H \in \Gamma_1$. (As Mann proved [Man12], these groups coincide with groups without irreducible characters of degree p .)

745. Classify the \mathcal{A}_n -groups G , $n > 1$ (see #738), with cyclic G' of order p^{n-1} (see §72).

746. Study the 2-groups G satisfying (i) $\Omega_1(G) \cong D_{2^n} * C_4$ (for $n = 3$, see Theorem 43.9), (ii) $\Omega_1(G) = D_{2^n} \times E_{2^m}$.

747. Let a p -group G be an \mathcal{A}_n -group. Is it true that $\exp(G') \leq p^n$.

748. Let G be a p -group of maximal class and $\max \{\chi(1) \mid \chi \in \text{Irr}(G)\} = p^b$. Is it true that (i) $\text{cd}(G) = \{1, p, p^2, \dots, p^b\}$? (ii) all faithful irreducible characters have the same degree p^b ?

749. Classify the p -groups G of coclass 2 without subgroups of maximal class and index p . (For such G , either $|G : G'| = p^2$, and then $p > 2$, or $G/K_3(G)$ is minimal nonabelian of order p^4 .)

750. Study the nonabelian p -groups G such that $H' = \Phi(H)$ for all nonabelian $H \leq G$. Moreover, study the nonabelian p -groups G such that, whenever $H \leq G$ is nonabelian, then H/H' is homocyclic.

751. Study the p -groups G with $Z(H) = Z(G)$ for any \mathcal{A}_1 -subgroup $H < G$.

752. Study the p -groups all of whose maximal subgroups have trivial Schur multipliers.

753. (Ito) Let a p -group G have a faithful irreducible character of degree p^2 . Study the abelian subgroups of G .

754. Study the p -groups with an automorphism $\neq \text{id}$ leaving unchanged all maximal abelian subgroups.

755. (Old problem) Classify the 2-groups containing exactly three involutions. (This is solved in §83.)

756. Describe the group of all automorphisms ϕ of the abelian p -group G such that $\phi_{\Omega_1(G)} = \text{id}$.

757. Study the p -groups G with $C_G(x) \leq H$ for all A_1 -subgroups $H < G$ and $x \in H - Z(G)$. (For a solution, see Theorem 92.1.)

758. Classify the p -groups all of whose maximal subgroups are of the form $M \times E$, where M is metacyclic and E is abelian.

759. Is it true that if G is irregular of order p^m with $c_1(G) = 1 + p + \dots + p^{m-2}$, then either $\exp(G) = p^2$ or $|G : \Omega_1(G)| \leq p$?

760. Classify the p -groups all of whose nonabelian maximal subgroups are either class 2 or of maximal class.

761. Find the greatest $s \in \mathbb{N}$ such that, whenever G is an irregular L_s -group (see §17), then $\mathcal{V}_1(G)$ is cyclic. (I think that $s = p$.)

762. Classify the p -groups G containing an element t of order p such that $C_G(t) = \langle t \rangle \times M$, where $M \cong M_{p^n}$.

763. Let G be a p -group and $M < G$ be of maximal class with $C_G(M) < M$. Estimate ranks of abelian subgroups, abelian normal subgroups, subgroups, normal subgroups of G in terms of M .

764. Study the p -groups G containing an extraspecial subgroup E such that $C_G(E) < E$.

765. Classify the nonabelian p -groups such that the orders of elements of any their minimal basis are pairwise distinct. (The group SD_{2^n} , $n > 3$, satisfies the above property.)

766. (i) (Blackburn) Study the p -groups G , $p > 2$, with $|G/K_3(G)| = p^3$. (ii) Moreover, classify the p -groups G such that $G/K_3(G)$ is extraspecial (minimal non-abelian).

767. Classify the two-generator p -groups, $p > 2$, all of whose maximal subgroups are two-generator. (See §70 and Theorem 71.7.)

768. Classify the p -groups all of whose nonnormal subgroups are abelian.
769. Study the p -groups G such that $Z(H)$ is either cyclic or $\cong E_{p^2}$ for all nonabelian $H < G$.
770. Construct, for each $p > 2$, a p -group G all of whose maximal regular subgroups are not normal.
771. Study the p -groups G with $d(G) < d(H)$ for $H \in \Gamma_1$.
772. Study the p -groups G such that $A \cap B$ is cyclic for all distinct \mathcal{A}_1 -subgroups $A, B < G$.
773. Let $G \triangleleft W$, where W is a 2-group and let all W -invariant maximal subgroups of G be metacyclic (two-generator). Study the structure of G .
774. Does there exist a p -group H such that $H \cong G'$ for some p -group G but $H \not\cong \Phi(W)$ for all p -groups W ?
775. Does there exist a p -group H such that $H \cong \Phi(G)$ for some p -group G but $H \not\cong W'$ for all p -groups W ?
776. (Ito–Ohara) Classify the nonmetacyclic 2-groups $G = AB$, where A and B are cyclic. (For a solution, see §87.)
777. Study the p -groups containing only one non-two-generator maximal subgroup.
778. Classify the p -groups all of whose nonabelian maximal subgroups are either minimal nonabelian or metacyclic.
779. Study the p -groups with metacyclic $G/Z(G)$. (It follows from Theorem 36.1 that if, in addition, $Z(G) < G'$, then G is metacyclic.)
780. Study the p -groups G such that all nonidentity cyclic direct factors of maximal abelian subgroups of G are maximal cyclic subgroups of G .
781. Let $\mathcal{H}_2 = \langle a, b \mid a^4 = b^4 = 1, a^b = a^{-1} \rangle$. Study the 2-groups G such that (i) G is \mathcal{H}_2 -free, (ii) $C_G(H) = Z(H)$ for some $H \cong \mathcal{H}_2$.
782. Study the p -groups all of whose normal non-characteristic subgroups have the same order.
783. Classify the nonabelian p -groups covered by nonabelian subgroups of order p^3 .
784. Classify the p -groups G without special sections.
785. Study the p -groups G such that $N_G(H) \leq H^G$ ($H^G \leq N_G(G)$) for all nonnormal $H < G$.
786. (Old problem) Classify the p -groups G with $\Phi(G) \cong E_{p^2}$. (By Proposition 4.9, if $p = 2$, then $\Phi(G) \leq Z(G)$.)

787. Classify the p -groups all of whose nonnormal subgroups have exponent p (elementary abelian).
788. Study the p -groups in which every two noncommuting elements generate a p -group of maximal class. (A solution in case $p = 2$ follows from Theorem 90.1.)
789. Study the p -groups, $p > 2$, all of whose irregular sections are two-generator.
790. Study the 2-groups G such that $C_G(t)/\langle t \rangle$ is of maximal class for an involution $t \in G$.
791. Classify the p -groups all of whose nonabelian maximal subgroups are two-generator. (See §70.)
792. Let $\delta(G)$ be the minimal degree of faithful representation of a group G by permutations (the degree of G). For p -groups A, B , find $\delta(A * B)$, where $A \cong B$ and $A \cap B = Z(A)$.
793. Classify the p -groups G , $p > 2$, such that, whenever $A < H \leq G$, where A is a maximal abelian subgroup of G , then H is irregular.
794. Study the p -groups all of whose maximal regular subgroups have the same order.
795. Study the p -groups all of whose subgroups of fixed order p^r , $r > 3$, are two-generator.
796. Let G be a group of order p^m with exactly p^{m-3} minimal nonabelian subgroups. Is it true that the set Γ_1 has an abelian member?
797. Study the p -groups G such that $Z(G/H_G)$ is cyclic for every nonnormal $H < G$.
798. Classify the 2-groups with exactly two involutions which are squares.
799. Classify the p -groups with minimal nonabelian $G/Z(G)$.
800. Does there exist a p -group such that every its maximal subgroup is a direct product of nonabelian groups of order p^3 ?
801. Classify the p -groups all of whose \mathcal{A}_1 -subgroups are of order $\leq p^4$.
802. Estimate the order of a p -group $G = \Omega_2^*(G)$ in terms of $c_2(G)$. (See §64.)
803. Let G be a p -group with $|\Omega_1(G)| = p^n$. Does there exist a constant $c = c(p, n)$ such that $|G/\mathfrak{U}_1(G)| \leq p^c$? Moreover, if $\Omega_1(G)$ is of order p^n and exponent p , does there exist a constant $f = f(p)$ such that $|G/\mathfrak{U}_1(G)| \leq p^{f^n}$? (See the Remark in §15 where this problem is solved by Mann for $p > 2$. See also [Man5, II].)
804. Does there exist an \mathcal{A}_n -group G with metacyclic G' and $|G'| = p^{\alpha(n)}$ (see #738)? If so, classify such groups.
805. Study the p -groups G such that A^G is minimal nonabelian for all nonnormal abelian $A < G$.

806. Find a necessary and sufficient condition for a p -group to have a p -admissible Hall chain (see §§24, 88).
807. Classify the p -groups G such that $|C_G(Z)/Z| = |\text{Aut}(Z)|_p$ for all cyclic $Z < G$.
808. Study the p -groups G containing $H \in \Gamma_1$ such that each maximal cyclic subgroup of H is a maximal cyclic subgroup of G .
809. Does there exist an \mathcal{A}_4 -group G with nonabelian G' ? (See §72.)
810. Study the p -groups G such that, whenever $A < G$ is not normal and $x \in G - N_G(A)$, then $A \cap A^x = A_G$.
811. Study the p -groups in which normalizers of all subgroups are two-generator.
812. Classify the p -groups G such that $|N_G(Z) : Z| = p$ for all maximal cyclic $Z < G$.
813. Describe the one-stepped maximal subgroups of the following groups: $\Sigma_{p^n} \in \text{Syl}_p(\text{S}_{p^n})$ and $\text{UT}(n, p) \in \text{Syl}_p(\text{GL}(n, p))$ (see §64).
814. Is it true that $G \cong \Sigma_{p^2}$ if $s_k(G) = s_k(\Sigma_{p^2})$ for $k = 1, 2$?
815. Let $A \in \{\Sigma_{p^n}, \text{UT}(m, p^n)\}$ (see #813). Classify the p -groups G with $c_k(G) = c_k(A)$ for all k .
816. Let $1 < k < m$ and let G be a group of order p^m satisfying $s_k(G) \geq \varphi_{m-1,k}$, where $\varphi_{m,k} = s_k(E_{p^m})$. Study the structure of G . (See Theorem 5.17.)
817. Classify the p -groups G in which the intersection of all \mathcal{A}_1 -subgroups is not contained in $Z(G)$.
818. Suppose that the lattices of normal subgroups of p -groups G and H are isomorphic. Describe the structure of H if $G \cong \Sigma_{p^n}$.
819. Classify the p -groups in which the normalizer of every nonnormal abelian subgroup is either abelian or an \mathcal{A}_1 -subgroup.
820. Study the p -groups G such that $\Phi(A) \leq Z(G)$ for all minimal nonabelian subgroups $A < G$ but $\Phi(G) \not\leq Z(G)$.
821. Improve the estimate given in Theorem 15.4.
822. (Roitman) Let $A \triangleleft G$ be p -groups, let $|A : C_A(g)| \leq p^p$ for all $g \in G - A$. Study the structure and embedding of A in G . (See Appendix 7.)
823. Study the p -groups G in which each $M \in \Gamma_1$ equals $C_G(x)$ for some $x \in G$.
824. Classify the metacyclic p -groups all of whose maximal subgroups are characteristic.

825. Let $|G| = p^m$, let $H < G$ be of order p^h and $1 < k < m - h$. Set $\mathfrak{M} = \{F < G \mid H < F, |F| = p^{h+k}\}$. Is it true that if $|\mathfrak{M}| = \varphi_{m-h,k}$, then $H \triangleleft G$?

826. Classify the p -groups all of whose minimal nonabelian subgroups have cyclic subgroups of index p .

827. Study the p -groups $G = \langle a, b, c \rangle$ such that $\langle a, b \rangle, \langle b, c \rangle, \langle a, c \rangle \in \Gamma_1$.

828. Study the p -groups G covered by normal abelian subgroups.

829. Study the p -groups with exactly $p + 1$ subgroups of order p^p and exponent p in detail. (See Theorem 13.23.)

830. Is it true that $|G : Z(G)|$ is bounded provided $|G : N_G(H)| \leq p$ for all $H < G$? (Reported by Mann: According to results of Mann and Vaughan-Lee, in that case $|G/Z(G)| \leq p^6$.)

831. Find $\alpha_1(H * C)$ in terms of H , where C is cyclic. $H \cap C = Z(H)$ of order p .

832. Classify the p -groups G with $\alpha_1(G) < |\Gamma_1|$. (For $\exp(G) = p$, see §76.)

833. Estimate $|G'|$ in terms of $\alpha_1(G)$.

834. Study the p -groups, $p > 2$, all of whose sections of exponent p are abelian.

835. Study the p -groups G of class $c > p$ such that $Z_{c-1}(G)$ is of exponent p .

836. Is it true that for each p -group H there exists a p -group G such that $H \cong H_1 \leq \Phi(G)$ and $\Omega_1(\Phi(G)) = \Phi(G)$?

837. (Kazarin) For each abelian p -group G we can determine the parameter $t(G)$ as a minimal n such that G is a subgroup of $\mathrm{GL}(n, p)$. How to calculate $t(G)$?

838. (Kazarin) Let R be an associative nilalgebra over the field of characteristic p . Determine the “circle” operation as follows (N. Jacobson): $a \circ b = ab + a + b$ and obtain the p -group R^* , the adjoint group of R . What is the structure of the adjoint group of a finite nilpotent algebra?

839. (Kazarin) Is it true that if the minimal number of generators of the adjoint group R^* is bounded (R is a nilpotent algebra over the field of characteristic p), then $|R|$ is also bounded? This problem is connected with Golod’s examples of infinite finitely generated groups.

840. Let $G = \mathrm{ES}(m, p)$ be an extraspecial group of order p^{2m+1} . Find the number of extraspecial subgroups of given order in G . Find $s_n(G)$ for all n .

841. Classify the 2-groups G with $|\mathrm{C}_G(B)| = 4$ for a nonabelian $B < G$, $|B| = 8$.

842. Study the p -groups G with $|\mathrm{Z}(M)| \leq p^2$ for all $M \in \Gamma_1$.

843. Study the p -groups G with $|M : \mathrm{Z}(M)| \leq p^2$ for all $M < G$ with $|G : M| = p^2$.

844. Let $N > \{1\}$ be a subgroup of a p -group G . Study the structure of G if, whenever $x \in G - N$, then $\text{cl}(\langle N, x \rangle) = \text{cl}(N)$.
845. Study the p -groups G such that Sylow p -subgroups of $\text{Aut}(G)$ are \mathcal{A}_1 -groups.
846. Classify the p -groups in which any two distinct \mathcal{A}_1 -subgroups have cyclic intersection.
847. Study the p -groups G such that, for some $N \triangleleft G$ and all abelian $A < G$, we have $|AN : N| \leq p$.
848. Find all minimal nonabelian p -groups with trivial Schur multiplier.
849. Let A be a maximal abelian normal subgroup of a p -group G . Suppose that for every $a \in A - Z(G)$ there is $x \in G$ such that $\langle a, x \rangle$ is minimal nonabelian. Study the structure of G .
850. Classify the non-Dedekindian p -groups G such that, whenever $F < G$ is non-normal, then $|G : F^{\text{Aut}(G)}| \leq p$.
851. Study the p -groups G such that $\exp(H^G) = \exp(H)$ for all minimal nonabelian $H \leq G$.
852. Study the p -groups G in which all \mathcal{A}_1 -subgroups are isomorphic. (For the case, where, in addition, all \mathcal{A}_1 -subgroups have exponent 4, see §57.)
853. Classify the p -groups G such that $C_G(C_G(H)) = H$ for all nonabelian (minimal nonabelian) $H \leq G$.
854. Classify the p -groups G in which every nonnormal subgroup is either abelian or minimal nonabelian.
855. Classify the pairs $H < G$ of p -groups with $\beta_1(G, H) \in \{p - 1, p, p + 1\}$ (see §76).
856. Study the p -groups, $p > 2$, with exactly one minimal irregular subgroup. Moreover, study the p -groups G with exactly one irregular member of the set Γ_1 .
857. Find the least upper bound of orders of \mathcal{A}_1 -subgroups of Σ_{p^n} and $\text{UT}(n, p)$.
858. Classify the p -groups G such that $\ker(\chi) \leq Z(G)$ for all $\chi \in \text{Irr}_1(G)$.
859. Study the p -groups which are generated by centers of their \mathcal{A}_1 -subgroups.
860. Classify the p -groups covered by \mathcal{A}_1 -subgroups.
861. Classify the p -groups all of whose maximal subgroups, but one, are either abelian or minimal nonabelian.
862. Study the p -groups in which every subgroup is generated by its elements of maximal order. (Regular p -groups satisfy this property, however, p -groups of maximal class and exponent $> p^2$ does not satisfy).

863. Classify the p -groups G with two maximal subgroups which are special.
864. Let $i \in \{1, \dots, d(G) - 1\}$. Is it true that the number of subgroups H of maximal class and such that $H \in \Gamma_i$, is divisible by p ? (This is true if $i = 1$, by Theorem 12.12(c)).
865. Does there exist a p -group H of maximal class, of order p^P and exponent $p > 3$ such that for every irregular p -group G of maximal class, we have $G/\mathcal{U}_1(G) \not\cong H$?
866. Classify the 2-groups G all of whose proper nonabelian subgroups are of the form $\mathcal{H}_2 \times E$, where $\mathcal{H}_2 = \langle a, b \mid a^4 = b^4 = 1, a^b = a^{-1} \rangle$ and E is elementary abelian. (The solution follows from Theorem 57.3.)
867. Study the p -groups G such that $p^2 \nmid |\text{Aut}(G)/\text{Inn}(G)|$.
868. Study the p -groups all of whose \mathcal{A}_1 -subgroups have the same exponent p^2 .
869. Study the p -groups G with $|\text{N}_G(F)| = |\text{N}_G(H)|$ for any $F, H \trianglelefteq G$.
870. Classify the special p -groups possessing an abelian maximal subgroup.
871. Study the groups G of exponent p having exactly one normal subgroup of index p^i for $i = 2, \dots, p - 1$.
872. Study the p -groups such that the normal closure of each their abelian subgroup is either abelian or an \mathcal{A}_1 -subgroup.
873. Study the irregular p -groups, $p > 2$, such that the normal closure of each their nonnormal cyclic subgroup is regular.
874. Study the p -groups all of whose metacyclic subgroups are abelian.
875. Study the p -groups G such that their holomorph is nilpotent of the same class as G .
876. Study the p -groups G with $\text{N}_G(A) = A\text{C}_G(A)$ for all nonabelian $A < G$.
877. Study the p -groups G with $\text{cl}(B^G) = \text{cl}(B)$ for all nonabelian $B \leq G$.
878. Construct a p -group G such $\Phi(G) = M \times N$ and M, N of maximal class.
879. Study the normal and power structures of an irregular p -group, $p > 3$, which is a product of two metacyclic subgroups.
880. Let $G = \Sigma_{p^n}$. Describe all $H < G$ such that $d(H) = p^{n-1}$.
881. Study the p -groups G with $\text{Aut}(G) \cong \text{Aut}(A)$ for some abelian p -group A .
882. Is it true that for each p -group G with trivial multiplier there is a p -group W with $d(W) = d(G)$ and $W/N \cong G$ for some $\{1\} < N \triangleleft W$?
883. Study the p -groups G with abelian $\Omega_n^*(G)$ of type (p^n, p, \dots, p) , $n > 1$.

884. Study the 2-groups G with $C_G(t) \cong C_{2^n} \times E_{2^m}$, $n > 1$, for some involution $t \in G$.
885. Study the 2-groups G with $C_G(t) = M \times E$, where M is of maximal class and E is elementary abelian. (For $|E| = 2$, see §§49, 51.)
886. Study the 2-groups $G = C_1 \dots C_d$, where C_1, \dots, C_d are cyclic not necessarily pairwise permutable and $d = d(G)$.
887. Let G be an abelian 2-group of exponent ≤ 4 and $d(G) = n$. Find the maximum of ranks of subgroups of $\text{Aut}(G)$. The same question for arbitrary abelian p -group.
888. Classify the 2-groups G with G/Z of maximal class for some cyclic $Z \triangleleft G$.
889. Classify the p -groups G such that all maximal subgroups of its \mathcal{A}_1 -subgroups are maximal abelian subgroups of G . (For a solution, see §92.)
890. Classify the p -groups which are not generated by noncyclic subgroups of index p^3 .
891. Classify the metacyclic p -groups with trivial Schur multiplier.
892. Does there exist an \mathcal{A}_n -group, with noncyclic derived subgroup of exponent $> p^{n-1}$? If so, classify such groups.
893. Describe the set $\{\alpha_1(G) \mid G \text{ is an } \mathcal{A}_3\text{-group}\}$.
894. Give an upper estimate of the number $|G : Z(G)|$, where G runs over the set of \mathcal{A}_n -groups.
895. Classify the p -groups G with $\alpha_2(G) = 1$ ($\alpha_n(G)$ is the number of \mathcal{A}_n -subgroups in a p -group G).
896. Classify the 2-groups all of whose \mathcal{A}_1 -subgroups are isomorphic to (i) M_{2^n} or Q_8 , (ii) M_{2^n} or D_8 , (iii) M_{2^n} or Q_8 or D_8 , (iv) M_{2^n} or $\mathcal{H}_2 = \langle a, b \mid a^4 = b^4 = 1, a^b = a^3 \rangle$.
897. Study the p -groups G such that $\Omega_1(A) \leq Z(G)$ for all minimal nonabelian subgroups $A < G$ but $\Omega_1(G) \not\leq Z(G)$.
898. Classify the nonabelian groups G of exponent p such that, whenever $A, B \leq G$ are minimal nonabelian, then $A \cap B > \{1\}$.
899. Study the 3-groups, all of whose minimal nonabelian subgroups are maximal regular.
900. Classify the 2-groups G such that $\Omega_2(G)$ is abelian of type $(4, 2, \dots, 2)$.
901. Describe the structure of $\text{Aut}(G)$, where $G = \text{ES}(m, p) \times C_{p^n}$ ($G = \text{ES}(m, p) * C_{p^n}$ is of order p^{2m+n}); here $\text{ES}(m, p)$ is extraspecial of order p^{2m+1} .
902. Study the p -groups G such that $[\Omega_i(G), \mathfrak{U}_i(G)] = \{1\}$ for all i .

903. Find $\alpha_1(A \times C)$, where A is a minimal nonabelian p -group and $C \cong C_{p^n}$, $n > 1$.
904. Study the p -groups G such that, whenever $A, B < G$ are distinct minimal non-abelian, then $|A \cap B| \leq p^2$. (Such G contains an \mathcal{A}_1 -subgroup of order p^3 .)
905. Classify the irregular p -groups of order p^m with maximal possible number of solutions of equation $x^p = 1$. (For $p = 2$, see Exercise 10.20.)
906. Classify the p -groups having a representation group of exponent p . (According to D.L. Johnson, the multipliers of noncyclic groups of exponent p are nontrivial.)
907. Let $\mathcal{H}_2 = \langle a, b \mid a^4 = b^4 = 1, a^b = a^{-1} \rangle$. Classify minimal non- \mathcal{H} -free 2-groups. (See §§78, 80.)
908. Describe the representation groups of extraspecial p -groups.
909. Study the structures of representation groups of homocyclic p -groups.
910. Classify the p -groups whose \mathcal{A}_2 -subgroups H satisfy (i) $\alpha_1(H) = p$, (ii) $\alpha_1(H) = p + 1$, (iii) $\alpha_1(H) \leq p + 1$.
911. Classify the \mathcal{A}_1 -groups (\mathcal{A}_2 -groups), isomorphic to G -invariant subgroups of Φ -subgroup of a p -group G . (The group \mathcal{H}_2 from #907 does not satisfy the above condition.)
912. Study the p -groups in which the centralizer of every noncentral element is (i) an \mathcal{A}_1 -subgroup; (ii) either abelian or an \mathcal{A}_1 -subgroup, (iii) of class ≤ 2 .
913. Classify the p -groups in which the normalizer of every nonnormal cyclic subgroup is such as in #912.
914. Study the 2-groups G satisfying $G' = \mathfrak{O}_3(G)$.
915. Study the p -groups G of order p^m and class $m - 2$ satisfying one of the following conditions: (i) $d(G) = 2$ and $|G : G'| = p^3$, (ii) $|Z(G)| = p^2$.
916. (i) Does there exist a p -group all of whose maximal subgroups are direct products of extraspecial (special) groups? If so, classify such groups. (ii) Study the p -groups all of whose nonabelian maximal subgroups are special.
917. Classify the p -groups all of whose irreducible characters are induced from abelian subgroups (from \mathcal{A}_1 -subgroups).
918. Study the p -groups G such that, whenever $A < G$, then G contains a normal subgroup $B \cong A$.
919. Given $n > 3$, does there exist a 2-group, which is not of maximal class, containing exactly one proper subgroup isomorphic with D_{2^n} (Q_{2^n} , SD_{2^n})?
920. Classify the p -groups all of whose \mathcal{A}_1 -subgroups are of order p^3 . (See also #115. For $p = 2$, this problem is solved in §90.)

921. Let G, G_0 be p -groups of the same order containing, for each n , the same number of conjugacy classes of size p^n . Is it true that G_0 is special if G is?

922. Given a group Γ , find a group G such that Γ is a representation group of G or prove that such G does not exist.

923. Suppose that a p -group G contains a subgroup $H = M \times C$, where M is irregular of maximal class and $|C| = p$. Describe the structure of G if it has only one subgroup $\cong H$.

924. Study the p -groups G such that, whenever its nonabelian epimorphic image H has cyclic center, then $|\mathrm{Z}(H)| = p$.

925. Find the representation groups of $M \times N$, where M and N are 2-groups of maximal class.

926. Classify the 2-groups G such that whenever $H \in \Gamma_1$ is nonabelian, then $H = M \times E$, where M is minimal nonabelian and E is abelian.

927. Study the representation groups of p -groups of maximal class, $p > 2$.

928. (I. D. Macdonald) Let $n > 2$. Classify the p -groups G of class $2n$ all of whose maximal subgroups are of class n .

929. Given a nonabelian group G of exponent p , does there exist a p -group W such that $W/S \cong G$, where S is the socle of W ?

930. Does there exist a group of exponent p and order $> p^p$ such that it has only one normal subgroup of order p^i , $i = 1, 2, \dots, p$?

931. Given $k \in \mathbb{N}$, let a p -group G be such that, for every abelian group A of order p^k , there is $A_1 \leq G$ isomorphic with A . Give a realistic upper bounds of $p^{nk} = \min |G|$.

932. Classify the non- p -abelian p -groups all of whose proper subgroups (sections) are p -abelian.

933. Classify the p -groups G satisfying the following condition. Whenever $H < G$ is nonnormal, there exists exactly one maximal subgroup of G containing H . (This problem was solved in §84.)

934. Does there exist a p -group with two representation groups of different classes?

935. Study the p -groups having the same class as all their representation groups.

936. Let $p > 3$, let G be a p -group of maximal class and order $> p^{p+1}$ and $H < G$, $H \not\leq G_1$. Is it true that if $|H| = p^{p-2}$ and p is large, then $H_G > \{1\}$?

937. Study the p -groups all of whose noncyclic (nonabelian) subgroups of the same order are isomorphic.

938. Study the 2-groups $G = \langle x_1, x_2, \dots, x_n \rangle$, where x_1, x_2, \dots, x_n are involutions such that $|\langle x_i, x_j \rangle| \leq 8$ for all $i \neq j$.

939. Find all $n \in \mathbb{N}$ such that there exists an \mathcal{A}_n -group G with $\alpha_1(G) \leq p^3$.
940. Find all k such that the groups Σ_{p^n} and $\text{UT}(n, p)$ have \mathcal{H}_k -chains. (See §88.)
941. Classify the powerful p -groups with abelian subgroup of index p .
942. Study the regular p -groups all of whose proper subgroups are powerful.
943. Study the regular p -groups G all of whose proper subgroups containing G' ($\Phi(G)$), are powerful.
944. Classify the p -groups all of whose powerful sections are abelian.
945. Classify the p -groups G such that $\alpha_1(H) = p^{d(H)-1}$ for all $H \leq G$ which are neither abelian nor minimal nonabelian.
946. Classify the p -groups all of whose \mathcal{A}_1 -subgroups are characteristic.
947. Classify the p -groups in which any two nonnormal abelian subgroups of the same order are conjugate.
948. Find all $n \in \mathbb{N}$ such that there exists a nonabelian p -group G all of whose subgroups of order (index) p^n are isomorphic.
949. Find $\alpha_{m,e} = \max \{\alpha_1(G) \mid |G| = p^m, \exp(G) = p^e\}$. Is it true that $\alpha_{m,1} \geq \alpha_{m,e}$?
950. Classify the p -groups in which any two nonnormal subgroups of the same order are contained in the same number of maximal subgroups.
951. Classify the p -groups G admitting an automorphism α of order p such that $C_G(\alpha)$ is cyclic. (See §48 and [Bla13].)
952. Classify the 2-groups G possessing an automorphism α of order 2 such that $C_G(\alpha)$ is of maximal class. (See §49.)
953. Classify the p -groups all of whose \mathcal{A}_1 -subgroups have normal complements.
954. Let a p -group $G = A \wr B$ be a standard wreath product. Study the structure of $G/Z(G)$.
955. Study the pairs $H < G$ of p -groups such that $|G : H| = p$, $\exp(H) > p$ and $C_H(x)$ is of exponent p for all $x \in G - H$.
956. Study the p -groups G such that G/G'' is special.
957. Study the p -groups whose Φ -subgroup is special. (The Burnside group $B(4, 2)$ of order 2^{12} satisfies the above condition; see §60.)
958. Classify the 2-groups with exactly eight \mathcal{A}_1 -subgroups. Moreover, classify the p -groups G with $\alpha_1(G) = (p^2 + p + 1) + 1$. (See §76.)
959. Classify the p -groups of maximal class, $p > 2$, whose representation groups are also of maximal class.

960. Classify the representation groups of Suzuki 2-groups $A(m, \theta)$ (see §46).
961. Describe the representation groups of abelian p -groups.
962. Study the p -groups all of whose subgroups (nonabelian subgroups) of index p^2 are isomorphic.
963. Classify the p -groups G such that G has a representation group with cyclic center.
964. Classify the minimal M_{24} -free 2-groups.
965. Classify (i) the minimal non- F -free 2-groups, where $F \in \{D_8 \times C_2, Q_8 \times C_2, D_8 * C_4\}$.
966. Classify the 2-groups containing a nonabelian subgroup of order 8, all of whose nonabelian subgroups of order 16 are of the form $M * C$, where C is cyclic of order 4.
967. Study the p -groups G with an element x of order p which is contained in only one maximal subgroup of G .
968. (Zhmud) Study the p -groups G such that, whenever $x, y \in G$ have the same normal closures, then they are conjugate.
969. Find the least upper bound of ranks of E_{p^4} -free p -groups.
970. Given a 2-group G and $n > 3$, let $sd_n(G)$ be the number of proper subgroups of G isomorphic with SD_{2^n} . Which members of the set $\{1, 2, 3\}$ may be values of the function $sd_n(*)$?
971. Study the p -groups G such that $|H : H'| \leq p^3$ for all nonabelian $H \leq G$.
972. Study the pairs $H < G$ of 2-groups such that $|G : H| = 2$ and $G - H$ is the union of at most four conjugacy classes.
973. Let p^n be the minimal order of \mathcal{A}_1 -subgroups of a p -group G . Study the structure of G if the number of \mathcal{A}_1 -subgroups of order p^n in G is $\leq p + 1$.
974. Classify the groups G of exponent p such that $|G/K_3(G)| = p^3$.
975. Study the structure of Φ -subgroups of quaternion-free 2-groups.
976. Suppose that N is a proper G -invariant subgroup of $\Phi(G)$, where G is a p -group. Does there exist a p -group W such that $N \cong \Phi(W)$?
977. (Mann) Classify the p -groups with exactly $p^2 - p$ minimal characters (see Appendix 10).
978. (Mann) Classify the p -groups with exactly $p^2 - 1$ minimal characters.
979. Classify the p -groups G such that G has a subgroup H of index p^n with $H_G = \{1\}$ and G contains a subgroup E with $d(E) = 1 + p + \cdots + p^{n-1}$.

980. Let G be a p -group such that $\{1\} < \mathrm{H}_p(G) < G$. Is it true that the class of $G/\mathrm{H}_p(G)$ is bounded?

981. Classify the two-generator 2-groups containing exactly one maximal subgroup that is not two-generator. (See [BJ2].)

982. Study the 2-groups such that $\Omega_2(G)$ is extraspecial (special).

983. Classify the p -groups which are not generated by minimal nonmetacyclic subgroups.

984. Classify the p -groups G with nonabelian derived subgroup (Φ -subgroup) such that all proper subgroups of G have abelian derived subgroups (Φ -subgroups).

985. Classify the p -groups G with non-absolutely regular derived subgroup (Φ -subgroup) such that all proper subgroups of G have absolutely regular derived subgroups (Φ -subgroups).

986. Classify the p -groups G with nonmetacyclic derived subgroup (Φ -subgroup) such that all proper subgroups of G have metacyclic derived subgroups (Φ -subgroups).

987. Study the p -groups all of whose sections of exponent $\leq p^2$ are abelian.

988. Study the p -groups G such that $\Phi(G) = E \times C_{p^n}$, where E is extraspecial.

989. Study the p -groups all of whose maximal nonnormal subgroups have cyclic intersection.

990. Study the p -groups all of whose Thompson critical subgroups are special (see §14).

991. Does there exist a nonmetacyclic 2-group with exactly one proper subgroup isomorphic with $\mathcal{H}_2 = \langle a, b \mid a^4 = b^4 = 1, a^b = a^{-1} \rangle$. If so, classify all such G .

992. Study the 2-groups G in which the centralizer of every element of order 4 is abelian.

993. Study the p -groups G such that $\Phi(G)$ and G' are special and $G' < \Phi(G)$.

994. Study the 2-groups G such that $\Phi(G)$ is nonabelian of order 2^4 . (For a solution, see Theorem 85.1.)

995. Classify p -groups all of whose nonnormal subgroups are either abelian or extraspecial.

996. Study the p -groups G with $n(G) = |\mathrm{Irr}_1(G)| = k_G(G')$ (here $k_G(G')$ is the number of G -classes contained in $(G')^\#$). (If G is a normal Sylow 2-subgroup of minimal nonnilpotent subgroup of order $5 \cdot 2^6$, then $k_G(G') = 3 = n(G)$.)

997. Study the 2-groups G containing an abelian subgroup A of type $(4, 4)$ (of type $(4, 2, 2)$) with $C_G(A) = A$.

998. Study the p -groups G such that (i) $|\mathrm{N}_G(H) : H| = p$ for all \mathcal{A}_1 -subgroups $H < G$, (ii) $\mathrm{N}_G(H)$ is an \mathcal{A}_2 -group for every \mathcal{A}_1 -subgroup $H < G$. (iii) Classify the 2-groups G containing a subgroup $\mathcal{H}_2 = \langle a, b \mid a^4 = b^4 = 1, a^b = a^3 \rangle$ and such that $|\mathrm{N}_G(\mathcal{H}_2) : \mathcal{H}_2| = 2$.

999. Classify the 2-groups G , containing the subgroup $A = D_8 * C_4$ such that (i) $\mathrm{C}_G(A) = Z(A)$, (ii) $|\mathrm{N}_G(A) : A| = 2$.

1000. Let a p -group $G = A \text{ wr } B$, where the active factor B is a regular permutation group. Find the structure of the multiplier of G in terms of A and B .

1001. Study the structure of the p -groups with exactly two class sizes (see [Ish]).

1002. Study the p -groups G such that a Sylow p -subgroup of $\mathrm{Aut}(G)$ is isomorphic to (i) Σ_{p^n} , (ii) $\mathrm{UT}(n, p)$.

1003. (Old problem) Classify the p -groups G such that $|G| \nmid |\mathrm{Aut}(G)|$.

1004. (Old problem) Study the p -groups G such that $|\mathrm{Aut}(G) : \mathrm{Inn}(G)|_p = p$.

1005. Let $k > 1$ be fixed. Study the p -groups G such that $\mathrm{Aut}(G)$ acts on the set of all subgroups of G of order p^k transitively.

1006. Study the p -groups G such that A/A_G is cyclic for all $A \leq G$.

1007. Study the p -groups G with $|\mathrm{C}_G(H) : Z(H)| \leq p$ for all nonabelian $H \leq G$.

1008. Compute the groups of central automorphisms of Σ_{p^n} and $\mathrm{UT}(n, p)$.

1009. Study the p -groups G such that $\mathrm{Aut}(G)$ acts transitively on the set of all \mathcal{A}_1 -subgroups of G .

1010. Study the p -groups G such that all p -automorphisms of G fix all G -classes.

1011. Study the p -groups G , $p > 2$, with $|G/G''| = p^5$.

1012. Does there exist a p -group G of exponent $> p > 2$, such that all elements of the set $G - \Phi(G)$ have the same order p ? (According to Khukhro, such 7-groups exist.)

1013. Find the set $\{\mathrm{d}(A)\}$, where A runs through all maximal abelian subgroups of Σ_{p^n} ($\mathrm{UT}(n, p)$).

1014. Study special quotient groups of representation groups of E_{p^n} .

1015. Classify the p -groups all of whose nonnormal subgroups are metacyclic.

1016. Classify the p -groups all of whose two distinct \mathcal{A}_1 -subgroups generate an \mathcal{A}_2 -subgroup.

1017. Study the p -groups G such that, for all minimal nonabelian $A < G$, (i) $\mathrm{C}_G(A) = Z(G)$, (ii) $\mathrm{C}_G(A) = Z(A)$.

1018. Study the p -groups G such that, whenever $F, H < G$ and $F^G = H^G$, then F and H are conjugate in G .

1019. Study the p -groups G of class 2 with $k(G) = |\text{Z}(G)| + k(G/\text{Z}(G)) - 1$.
1020. Classify the p -groups G such that $\text{Aut}(G)$ is a p -group which is (i) metacyclic, (iii) of maximal class, (iv) extraspecial.
1021. Classify the p -groups G with $C_G(A) \neq C_G(B)$ if $A, B < G$ and $|A| \neq |B|$.
1022. Study the structure of the Φ -subgroup of a p -group G provided $\Phi(G)$ is non-abelian and $|\Phi(G) : \Phi(G)'| = p^3$.
1023. Study the structure of the Φ -subgroup of a p -group G provided $\Phi(G)$ is non-abelian and $|\text{Z}(\Phi(G))| = p^2$.
1024. Is it true that $\lim_{|\text{cd}(G)| \rightarrow \infty} (|\text{cd}(G)| - \text{dl}(G)) = \infty$, where G runs over all p -groups and $\text{dl}(G)$ is the derived length of G , $\text{cd}(G) = \{\chi(1) \mid \chi \in \text{Irr}(G)\}$?
1025. Study the structure of the Φ -subgroup of a p -group G provided $\Phi(G)$ contains a subgroup B of order p^3 such that $C_{\Phi(G)}(B) = B$.
1026. Classify the 2-groups such that, whenever $A, B \in \Gamma_1$ are distinct, then $A \cap B$ is metacyclic.
1027. Let $N \triangleleft G$ be the union of $k_G(N)$ conjugacy classes of G . Classify the p -groups G satisfying $k(G) \leq k_G(N) + k(G/N) + p - 2$.
1028. Study the p -groups all of whose Thompson critical subgroups have cyclic centers.
1029. Classify the irregular p -groups with exactly one k -admissible Hall chain (see §88).
1030. Classify the p -groups G with $\Omega_1(H) = H$ for all nonmetacyclic $H \leq G$. (For solution, see [Ber33] and [BozJ4].)
1031. Does there exist p -groups G such that, whenever $A, B \in \Gamma_1$ are distinct, then $A \cap B$ is an \mathcal{A}_1 -subgroup? If so, classify these groups.
1032. Study the structure of a p -group G if $C_G(x) \leq \Phi(G)$ for all $x \in \Phi(G) - \text{Z}(G)$.
1033. Describe the p -groups G with $|\Gamma : \text{Z}(\Gamma)| < |G|$, where Γ is a representation group of G .
1034. Study the p -groups covered by nonabelian metacyclic subgroups.
1035. Study the p -groups all of whose two-generator subgroups are of order $\leq p^4$.
1036. Classify the p -groups all of whose normal nonabelian subgroups have index $\leq p^2$.
1037. Let $G \in \{\Sigma_{p^n}, \text{UT}(m, p^n)\}$. Describe $\mathcal{M}(G)$, where $\mathcal{M}(G) = \langle x \in G \mid C_G(x^p) = C_G(x) \rangle$ is the Mann subgroup of G .

1038. Let $n < m$. Classify the groups G of order p^m with $s_n(G) < s_n(E_{p^m})$ and such that there does not exist a group H of order p^m with $s_n(G) < s_n(H) < s_n(E_{p^m})$.

1039. Let S be a p -group. Does there exist a p -group G such that S is isomorphic to a direct factor of $\Phi(G)$? The same problem for $\mathcal{U}_1(G)$ and G' instead of $\Phi(G)$.

1040. Let $J(G)$ be the subgroup generated by all abelian subgroups of maximal order in a p -group G . Study the p -groups G such that $J(G) \leq G'$.

1041. Does there exist 2-groups containing exactly one proper U_2 -subgroup (see §67) of given order?

1042. Study the p -groups G , $p > 2$, with G/G'' of maximal class.

1043. (Old problem) Estimate the number of p -groups of maximal class and given order.

1044. Let G be a p -group and $\mathcal{M}(G)$ its Mann subgroup. Classify the p -groups G such that the cyclic subgroup $\mathcal{M}(G) > Z(G)$.

1045. Let all members of the set Γ_1 be irregular p -groups. Find the least upper bound for $|G|$.

1046. Study the irregular p -groups with exactly two nontrivial characteristic subgroups.

1047. Let $\mathcal{M}_1(G)$ be the subgroup generated by all cyclic subgroups $C < G$ such that $N_G(\mathcal{U}_1(C)) = N_G(C)$. Study the structure of $\mathcal{M}_1(G)$.

1048. Study the p -groups all of whose cyclic subgroups of order $> p$ are characteristic.

1049. Study the p -groups having only one Thompson critical subgroup (see §14).

1050. Find $\mathcal{M}(G)$, where p -group $G = A \text{ wr } B$ is the standard wreath product (here $\mathcal{M}(G)$ is the Mann subgroup of G).

1051. Let $G = A \cdot B$ be a semidirect product with kernel B . Consider the following situations: (i) $\mathcal{M}(G) = \mathcal{M}(B)$, (ii) $\mathcal{M}(G) = \mathcal{M}(A) \times \mathcal{M}(B)$.

1052. Study the p -groups with $\mathcal{M}(G) > Z(G)$ and $\mathcal{M}(H) = Z(H)$ for all $H < G$.

1053. Study the p -groups G with $C_G(x) < C_G(x^p)$ for all $x \in G - \Phi(G)$.

1054. Let $G = \Omega_1(G)$ be a p -group of class > 2 . Describe the structure of G provided $|\langle x, y \rangle| \leq p^3$ for all elements $x, y \in G$ of order p .

1055. Study the p -groups G such that $\langle x, y \rangle$ is either regular or of maximal class for all $x, y \in G$.

1056. Study the p -groups in which any two distinct maximal abelian subgroups have distinct orders (exponents).

1057. Study the 2-groups G of exponent > 4 containing a maximal subgroup H such that all minimal nonabelian subgroups of G not contained in H have order 8. (See §90.)

1058. Classify the 2-groups G containing an involution t such that $C_G(t)/\langle t \rangle$ has a cyclic subgroup of index 2.

1059. Study the 2-groups G satisfying $\Omega_1(G) = \text{ES}(m, 2) \times E_{2^n}$, where $\text{ES}(m, 2)$ is an extraspecial group of order p^{1+2m} .

1060. Study the p -groups G with an involution t such that $C_G(t) \cong \text{ES}(m, 2) \times C_2$.

1061. Describe the non-Dedekindian p -groups G such that, whenever $H \not\trianglelefteq G$, then G/H^G has exactly one subgroup of order p .

1062. Let $A < G$ be a maximal abelian subgroup of a p -group G , $|G : A| > p$. Study the structure of G if, whenever $A < H \in \Gamma_1$, then $|H'| = p$.

1063. Let Γ^1 be a representation group of G , Γ^2 a representation group of Γ^1 , and so on. Such a series we call a Γ -series of G . Is it true that each p -group has a finite Γ -series? (We do not assert that all Γ -series are finite.)

1064. Construct all Γ -series for E_{p^k} , $p > 2$, $k \in \{2, 3\}$.

1065. Construct all Γ -series for nonabelian metacyclic p -groups. (By Theorem 47.4, all members of these series are metacyclic.)

1066. Construct all Γ -series for groups (i) $A_p(m, \theta)$ (see §46), (ii) for nonabelian Sylow subgroups of minimal nonnilpotent groups, (iii) for all minimal nonabelian p -groups.

1067. Construct all Γ -series for 2-groups $M \times C_2$ (where M is of maximal class).

1068. Let G be a p -group, $p > 2$. Study the structure of $\Phi(G)$ if it is irregular of order p^{2+p} .

1069. Construct all Γ -series for all 14 groups of order 2^4 .

1070. Given a p -group G , let G_0 be a group containing a normal subgroup N of order p such that $G_0/N \cong G$ and $N \leq \Phi(G_0)$. Such G_0 we call a Φ -extension of G if it exists. Study the p -groups which have no nontrivial Φ -extensions.

1071. Classify the p -groups G of exponent p^e such that the subgroup $\Omega_e^*(G) = \langle x \in G \mid o(x) = p^e \rangle$ is abelian.

1072. Classify the 2-groups all of whose subgroups of order 2^5 are two-generator.

1073. Study the p -groups G such that $C_G(x)$ is an \mathcal{A}_1 -subgroup of order p^4 for some $x \in G$ of order p .

1074. Classify the p -groups G with $\mathfrak{U}_1(G)' > \{1\}$ and $\mathfrak{U}_1(H)' = \{1\}$ for all $H < G$.

1075. Study the p -groups with abelian Thompson critical subgroups for all $H < G$ but nonabelian Thompson critical subgroups for G (see §14).
1076. Study the p -groups G such that (i) $\mathcal{M}(G) = \Phi(G)$, (ii) $\mathcal{M}(G) = \mathfrak{U}_1(G)$.
1077. For all k , find the minimal $m = m_{k,p}$ such that each group of order p^m has an abelian subgroup of order p^k .
1078. Study the pairs $H < G$ of p -groups such that H is a nonabelian normal subgroup of G and all characters in $\text{Irr}_1(H)$ are not G -invariant.
1079. Let \mathcal{N} be the set of all $n \in \mathbb{N}$ such that there does not exist a 2-group G with $|\text{Irr}_1(G)| = n$. Is it true that the set \mathcal{N} is nonempty and finite?
1080. Give a realistic estimate of $|G'|$, where G is a 2-group with $|\text{Irr}_1(G)| \leq n$.
1081. Does there exist a p -group H with $G/\mathcal{M}(G) \not\cong H$ for all p -groups G ?
1082. Study the pairs $N < G$ of p -groups such that all elements of the coset xN have the same order for all $x \in G - N$.
1083. Study the p -groups, all of whose maximal subgroups are nontrivial central products.
1084. Classify the 2-groups G such that $G - Z(G)$ is the union of ≤ 12 conjugacy classes.
1085. Is it true that $\alpha_1(G) \geq \alpha_1(G/N)$ for $\{1\} < N \triangleleft G$?
1086. Classify the p -groups $G = \Omega_1(G)$ of order p^n with minimal possible $c_1(G)$.
1087. Classify the special p -groups G with $|Z(G)| = p^2$.
1088. Classify the p -groups, $p > 2$, all of whose nonabelian maximal subgroups are of the form $M \times E$, where M is of maximal class and E is elementary abelian.
1089. Let G be an abelian p -group. Find the class of a Sylow p -subgroup (i) of $\text{Aut}(G)$, (ii) of the holomorph of G .
1090. Does there exist a p -group G of arbitrary large order with $\text{dl}(P) = \text{dl}(G)$, where P is a Sylow p -subgroup of the holomorph of G ?
1091. Classify the 2-groups G with $|\text{C}_G(\alpha)| = 2$ for $\alpha \in \text{Aut}(G)$ of order 4. (See §77.)
1092. Suppose that $M < G$ is metacyclic and, whenever $M < N \leq G$, when $\exp(N) > \exp(M)$. Study the structure of G .
1093. Classify the 2-groups containing exactly three subgroups $\cong D_8$. (There is only one 2-group containing exactly one proper subgroup $\cong D_8$, namely SD_{16} .)
1094. Classify the 2-groups containing exactly one proper subgroup $\cong Q_{2^n}$.
1095. Let Γ be a representation group of E_{p^n} . Find all possible values of $|\text{Aut}(\Gamma)|$.

1096. Let $k > 3$ be fixed. Study the 2-groups all of whose normal subgroups of order 2^k are two-generator.

1097. Classify the p -groups G such that there exists a pair $R \triangleleft H$ such that $|R| = p$, $H/R \cong G$ and $n(H) - n(G) = p - 1$. (Here $n(G) = |\text{Irr}_1(G)|$.)

1098. Classify the groups G of order 2^{2n+1} such that there exists a pair $R \triangleleft H$ with $|R| = 2$, $H/R \cong G$ and $n(H) - n(G) = 2$.

1099. Study the pairs of p -groups $N \triangleleft G$ such that $|N| = p^3$ and $n(G) - n(G/N) = p^2 + p - 2$.

1100. Classify the special p -groups G all of whose maximal abelian subgroups have order $p|G'|$, $p > 2$.

1101. Classify the p -groups G with $U \cap V \triangleleft G$ for any distinct $U, V < G$ of the same order.

1102. Study the p -groups $G = A \cdot \mathcal{M}(G)$ with $A \cap \mathcal{M}(G) = \{1\}$ (here $\mathcal{M}(G)$ is the Mann subgroup of G).

1103. Study the p -groups G with $\mathcal{M}(A) \leq \mathcal{M}(G)$ for all nonabelian $A < G$.

1104. Classify the 2-groups containing a normal subgroup of maximal class and index 4.

1105. Suppose that $H \in \Gamma_1$ and all cyclic subgroups that are not contained in H , are normal in G . Study the structure of G .

1106. Suppose that G is a p -group with $|\mathfrak{U}_{i-1}(G) : \mathfrak{U}_1(\mathfrak{U}_{i-1}(G))| \leq p^p$ for some $i \in \mathbb{N}$. Is it true that then $|\mathfrak{U}_{i-1}(G) : \mathfrak{U}_i(G)| \leq p^p$?

1107. Classify the p -groups G such that $|C_G(H)| \leq p^2$ for all nonabelian $H \leq G$.

1108. Classify the p -groups having only one $(p-1)$ -admissible Hall chain (see §§24, 88).

1109. Let G run over all groups of exponent p^e , $e > 2$. Does there exist $c = c(e)$ such that $\exp(\mathfrak{U}^c(G)) < p^e$ for all such G ? (For definition, see §23. For $p > 2$, see [Wil2].)

1110. For $G \in \{\Sigma_{p^n}, \text{UT}(n, p^k)\}$, study the structures of the following quotient groups: $\mathfrak{U}^{n-1}(G)$, $\mathfrak{U}_{n-1}(G)$, $G/\mathfrak{U}^2(G)$ and $G/\mathfrak{U}_2(G)$.

1111. Find $\pi(\text{Aut}(G))$ for $G \cong \text{UT}(n, p^k)$.

1112. (N. Ito) Let $B_0 = B(d, p^e)$ be the maximal finite group of exponent p^e with d generators, $d > 1$, $p > 2$. Set $G = B_0/K_3(B_0)$. (i) Find $\text{cd}(G)$ and the number of characters of each degree n in $\text{Irr}(G)$. (For $e = 1$, see [IM].) (ii) Find the class sizes vector of G .

1113. Let G be a p -group. A series $\mathcal{E} : \{1\} = E_0 < E_1 < \dots < E_n = G$ is said to be an E-series of G of length $l(\mathcal{E}) = n$, if E_{i+1}/E_i is a normal subgroup of exponent p and maximal order in G/E_i , $i = 0, 1, \dots, n - 1$. Does there exist a p -group G which has two E-series of different lengths?

1114. Study the 2-groups G with abelian $G/\mathfrak{U}_1(\mathfrak{U}_1(G))$.

1115. Describe all \mathcal{A}_1 -subgroups of a p -group $G = M \times C$ ($M = M * C$ with $M \cap C = \Omega_1(C)$), where M is minimal nonabelian and C is cyclic.

1116. Study the p -groups G such that $\mathfrak{U}_1(G)$ is powerful.

1117. Study the p -groups G , $p > 2$, such that $|\Phi(G) : \mathfrak{U}_1(G)| = p$.

1118. Define the series $G = \Phi_0(G) > \Phi_1(G) > \Phi_2(G) > \dots > \Phi_n(G) > \dots$ as follows. $\Phi_0(G) = G$, $\Phi_1(G) = \Phi(G)$, $\Phi_{i+1}(G) = \Phi(\Phi_i(G))$. Study the p -groups G such that the above series is lower central.

1119. Given a p -group G , let $E_i(G)$ be least normal subgroups of G such that $G/E_i(G)$ is generated by elements of order p , $i = 1, 2$. Does there exist a p -group G such that $|E_1(G)| \neq |E_2(G)|$.

1120. Study the p -groups G with $H' = \mathfrak{U}_1(H)$ for all nonabelian $H < G$ but $G' \neq \mathfrak{U}_1(G)$.

1121. Study the p -groups G with $G/\mathcal{M}(G) \in \{\mathbf{M}_{p^n}, \mathbf{C}_{p^n} \times \mathbf{C}_p\}$.

1122. Classify the p -groups G such that H/H_G is cyclic for all $H < G$.

1123. Let G be a nonabelian p -group, $d(G) = 3$. Study the structure of G if $A\Phi(G) \in \Gamma_1$ ($AG' \in \Gamma_1$) for all \mathcal{A}_1 -subgroups $A < G$.

1124. Classify the 2-groups, all of whose nonabelian maximal subgroups are of the form $T * C$, where T has a cyclic subgroup of index 2 and C is cyclic.

1125. Given a p -group G , is it true that there exists a p -group H such that (i) $\Phi(H) \cong \mathfrak{U}_1(G)$, (ii) $\mathfrak{U}_1(H) \cong \Phi(G)$, (iii) $H' \cong \Phi(G)$, (iv) $\Phi(H) \cong G'$?

1126. Let the Burnside 2-group $G = B(2^m, n)$, $m, n > 1$. Study the structures of subgroups $\Omega_1(G)$, $\Omega_2(G)$ and $\Omega_2^*(G)$, $\Phi(G)$, G' . Find $k(G)$, $cd(G)$ and $cl(G)$. (For $m = 2 = n$, see §60.)

1127. Does there exist, for each $e > 1$, a p -group G of exponent p^e such that $\exp(\mathfrak{U}^{e-1}(G)) = p$ and $\mathfrak{U}_{e-1}(G) < \mathfrak{U}^{e-1}(G)$?

1128. Study the regular p -groups, $p > 2$, which are also powerful.

1129. Study the 2-groups G with $\Phi(G)$ elementary abelian and squares constitute a basis of $\Phi(G)$.

1130. Classify the 2-groups all of whose nonabelian maximal subgroups are of the form $T \times E$, where $T \cong \mathbf{M}_{2^n}$ and E is elementary abelian.

1131. Does there exist an \mathcal{A}_4 -group G , $p > 2$, such that $\alpha_1(G) = 1 + (p^2 + p + 1)$?
1132. Let a p -group $G = A_1 * \cdots * A_n$, where A_1, \dots, A_n are minimal nonabelian and $A_i \cap A_j = Z(A_i) = Z(A_j)$ for all $i \neq j$. Describe (i) maximal abelian subgroups of G , (ii) degrees of irreducible characters of G and the number of irreducible characters of each degree.
1133. Study the powerful p -groups all of whose maximal subgroups are powerful.
1134. Classify the p -groups G in which any nonnormal subgroup is contained in exactly one maximal subgroup of G . (This problem was solved in §28.)
1135. Describe the structures of Φ -subgroups having derived subgroup of order p .
1136. Let $\{1\} < H < G$. Suppose that, whenever $K \triangleleft H$, then $H \cap K^G = K$. Study the embedding of H in G and the structure of H/H_G .
1137. Study the p -groups G satisfying $\Omega_i(H) = \mathfrak{U}_{e-i}(H)$, $i = 1, \dots, e-1$, for all its sections H of exponent p^e , where $p^e \in \{p, \dots, \exp(G)\}$.
1138. Let G be an irregular p -group such that the indices of the chain $\mathcal{C} : G > \mathfrak{U}_1(G) > \mathfrak{U}_2(G) > \dots$ are $\leq p^p$ and suppose that the length of \mathcal{C} is n . Estimate the length of the chain $G > \mathfrak{U}^1(G) > \mathfrak{U}^2(G) > \dots$ (see §24).
1139. Study the p -groups G of exponent p^e such that the length of the chain $G > \mathfrak{U}^1(G) > \mathfrak{U}^2(G) > \dots$ equals $e+1$.
1140. Give an algorithm for construction of a k -admissible Hall chain for an arbitrary abelian p -group (see §24).
1141. Find the number of k -admissible Hall chains in a homocyclic p -group.
1142. Classify the p -groups, all of whose \mathcal{A}_1 -subgroups have the same order p^n . Consider case $n = 3$ in detail,
1143. Let G be a special group with $d(G) = d$. Suppose that G/M is extraspecial for all maximal subgroups M of G' . Estimate $|G'|$.
1144. Let G be a special group with $d(G) = d$. Suppose that G/M is extraspecial for all maximal subgroups M of G' . Estimate $|G'|$.
1145. Classify the p -groups of maximal class and order p^{p+1} such that $|\Omega_1(G)| = p^p$. (As Mann showed, the set of such G is nonempty.)
1146. Classify the p -groups G with $M \cap H \triangleleft G$ for all $M \not\leq H \in \Gamma_1$.
1147. Study the p -groups G with $e_p(G) = 2p + 1$, where $e_p(G)$ is the number of subgroups of order p^p and exponent p in G .
1148. Let $1 < k < p$. Does there exist a p -group G of order p^{p+1} with $e_p(G) = k$? (As Mann [Man5] has showed, there is irregular G of order p^{p+1} , $p > 2$, with $e_p(G) = 1$.)

1149. Let $M \in \Gamma_1$. Suppose that $|G : H^G| = p$ for all subgroups (cyclic subgroups) $H < G$ not contained in M . Study the structure of G .
1150. Classify the subgroups of class 2 of maximal order in Σ_{p^m} and $\mathrm{UT}(n, p)$.
1151. Find the orders of $\mathrm{Aut}(\Sigma_{p^n})$ and $\mathrm{Aut}(\mathrm{UT}(n, p))$.
1152. Find the character degrees vectors for Σ_{p^n} and $\mathrm{UT}(n, p)$.
1153. Study the p -groups G such that, whenever $\chi, \tau \in \mathrm{Irr}(G)$ with $\chi(1)\tau(1) \leq b(G) = \max\{\theta(1) \mid \theta \in \mathrm{Irr}(G)\}$, then $\chi\tau \in \mathrm{Irr}(G)$.
1154. Study the p -groups without subgroups of maximal class.
1155. Find for $G \in \{\Sigma_{p^n}, \mathrm{UT}(n, p)\}$ such number k_n that G has an irregular subgroup of order p^{k_n} but all subgroups of G of order $< p^{k_n}$ are regular. Find $\max\{|R| \mid R < G \text{ is regular}\}$.
1156. Study the 2-groups G with (i) $G/\mathcal{M}(G)$ of maximal class, (ii) cyclic $G/\mathcal{M}(G)$ (here $\mathcal{M}(G)$ is the Mann subgroup of G).
1157. Does there exist, for each $n > 1$, a p -group G with abelian $\mathfrak{U}_n(G)$ and irregular $\mathfrak{U}^n(G)$?
1158. Does there exist a p -group G such that, for some $n \in \mathbb{N}$, the subgroups $\mathfrak{U}_n(G)$ and $\mathfrak{U}^n(G)$ are abelian but different?
1159. Let G be a p -group, P is a Sylow p -subgroup of the holomorph of G . Study the structure of G provided $|G : [G, P]| = p$.
1160. Study the p -groups whose Φ -subgroups are irregular of order p^{p+2} .
1161. Does there exist a p -group G such that any two different maximal subgroups of exponent p in G have distinct orders?
1162. Classify the 2-groups all of whose minimal nonabelian subgroups are isomorphic to (i) $\mathcal{H}_2 = \langle a, b \mid a^4 = b^4 = 1, a^b = a^3 \rangle$ or Q_8 , (ii) \mathcal{H}_2 or D_8 , (iii) \mathcal{H}_2 or Q_8 or D_8 . (Problem (i) was solved by Janko; see §92. If the intersection of all nonnormal subgroups of G is $> \{1\}$, then G satisfies (i). Janko also deduced the last result from (i); see §92.)
1163. Study the p -groups G with special $\Omega_1(G)$ ($\Omega_2(G)$).
1164. Classify the p -groups G such that $|G : H^G| = p$ for all nonnormal $H < G$. (For a solution, see §62.)
1165. Study the p -groups, $p > 2$, in which the number of subgroups of maximal class and order p^p is not a multiple of p .
1166. Does there exist a \mathcal{P} -group G (see §11) with non-powerful $\mathfrak{U}_1(G)$?

1167. Study the structure of a p -group $G = \Omega_1(G)$ if it has no subgroups of order p^{p+1} and exponent p .
1168. Classify the 2-groups containing a U_2 -subgroup of index 2 (see §67).
1169. Estimate $a_n = \max \{\alpha_1(G) \mid |G| = p^n\}$. Is it true that if n large and G of order p^n is such that $\alpha_1(G) = a_n$, then $\exp(G) = p$?
1170. Study the p -groups G such that, in all sections of G , upper and lower central series coincide.
1171. Find $\exp(\text{Aut}(G))$, where G is abelian of given type.
1172. Study the p -groups G with extraspecial (special) $N_G(H)$ for some $H < G$.
1173. Describe abelian subgroups in the holomorph of a 2-group of maximal class.
1174. Let G be an abelian group of type (p^n, p, \dots, p) , $n > 1$. Describe the structure of a Sylow p -subgroup of $\text{Aut}(G)$.
1175. Classify the 2-groups G with nonabelian $\Omega_1(G)$ of order 2^4 .
1176. Study the p -groups all of whose maximal regular subgroups are isomorphic.
1177. Let $R < G$ be abelian of type (p, p) . Study the structure of G provided $C_G(R)$ is metacyclic.
1178. Study the p -groups generated by normal subgroups of order p^3 .
1179. Study the p -groups generated by normal A_1 -subgroups.
1180. Study the p -groups G such that $\text{Aut}(G)$ acts transitively on the set of elementary abelian subgroups of G of order p^2 .
1181. Classify the p -groups all of whose A_2 -subgroups are metacyclic.
1182. Does there exist a p -admissible Hall chain in $\Sigma_{p^n} \in \text{Syl}_p(S_{p^n})$, $\text{UT}(n, p) \in \text{Syl}_p(\text{GL}(n, p))$?
1183. Study the p -groups all of whose proper nonabelian epimorphic images are special.
1184. Study the p -groups in which any two non-conjugate maximal abelian subgroups have distinct orders.
1185. Study the p -groups that have maximal regular subgroup of order p^{p+1} .
1186. Study the p -groups G such that H^G is irregular of maximal class for some nonnormal absolutely regular $H < G$.
1187. Classify the p -groups, $p > 2$, with exactly one 2-admissible Hall chain.
1188. Find $\max \{m \mid \exp(G)_p = \exp(E_{p^m})\}$, where G runs over all nonabelian groups of order p^m and exponent p .

1189. Study the p -groups of exponent p^e all of whose metacyclic subgroups have order $\leq p^{e+1}$.

1190. Study the p -groups G with cyclic $\mathcal{M}(G)/\mathbb{Z}(G) > \{1\}$ (here $\mathcal{M}(G)$ is the Mann subgroup of G).

1191. Study the nonabelian p -groups $G = \Omega_1(G)$, $p > 2$, in which every two noncommuting elements of order p generate a p -group of maximal class.

1192. Let P be a Sylow p -subgroup of the holomorph of C_{p^n} . Study the structure of $\text{Aut}(P)$.

1193. Study the structure of $\text{Aut}(P)$, where P is a Sylow p -subgroup of the holomorph of a p -group with cyclic subgroup of index p .

1194. Study the p -groups G with $\mathcal{M}(G) = G'$.

1195. Study the p -groups G such that, whenever $H \trianglelefteq G$ is of order p^p and exponent p , then H^G is of maximal class.

1196. Study the p -groups of exponent $p^e > p$, all of whose cyclic subgroups of order p^e are normal.

1197. Find $c_k(G)$ for all k , where $G \in \{\Sigma_{p^n}, \text{UT}(n.p)\}$.

1198. Given $e > 2$, does there exist a p -group G of exponent p^e such that the quotient group $\mathfrak{U}_i(G)/\mathfrak{U}_{i+1}(G)$ is irregular for $i = 1, \dots, e-1$?

1199. Classify the p -groups, $p > 2$, all of whose nonabelian two-generator subgroups are absolutely regular.

1200. Let G be of exponent $p^e > p^2$ and suppose that $\mathfrak{U}^e(G) = \{1\}$. Is it true that then $\mathfrak{U}^i(G) = \mathfrak{U}_i(G)$ for all i ?

1201. Does there exist a constant C such that, for each $e \geq C$ and each p -group G of exponent p^e , the subgroup $\mathfrak{U}^n(G) > \{1\}$ is regular? (The answer is ‘no’, by [Wil2].)

1202. Classify the p -groups in which any two noncommuting elements generate either \mathcal{A}_1 -subgroup or subgroup of maximal class.

1203. Study the nonabelian p -groups all of whose nonabelian epimorphic images have cyclic centers.

1204. Study the p -groups G in which each characteristic subgroup equals $\Omega_i(G) \cap \mathfrak{U}_j(G)$ for some $i, j \in \mathbb{N}$.

1205. Classify the p -groups possessing a subgroup Z of order p which is contained in only one abelian subgroup of type (p, p) .

1206. Classify the 2-groups G with $H < G$ such that $N_G(H)$ is a U_2 -group.

1207. Classify the p -groups G possessing a subgroup A of order p^2 such that the centralizer of A in G has order p^3 . (For $p = 2$, see §§51, 77.)

1208. Classify the 2-groups G possessing a subgroup H of order 8 such that the normalizer of H in G has order 16.

1209. Let G be a two-generator p -group. Suppose that exactly p maximal subgroups F of G satisfy $|Z(F)| = p$ and exactly p maximal subgroups H of G satisfy $|H : H'| = p^2$. Is it true that G is of maximal class. (The answer is ‘yes’ for $p = 2$, by Taussky’s theorem and Theorem 5.4.)

1210. Given k , let a p -group G contain all types of groups of order p^k . Give a realistic upper bound of $|G|$. (See also #931.)

1211. Study the p -groups of class > 3 covered (generated) by normal subgroups of class ≤ 2 .

1212. Classify the p -groups G with metacyclic $N_G(M)$ for some $M < G$.

1213. Let $\kappa_1(G)$ be the number of conjugate classes of \mathcal{A}_1 -subgroups of G . Classify the p -groups G with $\kappa_1(G) \in \{p - 1, p, p + 1\}$ (see Proposition 76.15).

1214. Let a p -group $G = A \cdot B$ be a semidirect product with kernel B , the subgroups A and B are abelian. Estimate $\text{cl}(G)$ in terms of A, B and action of A on B .

1215. Study the p -groups G such that $d(G) < d(H)$ for all $H \in \Gamma_1$. (Almost all nonmetacyclic \mathcal{A}_1 -groups satisfy this condition.)

1216. Study the p -groups G with $\ker(\chi) \cap \ker(\tau) = \{1\}$ provided $\chi, \tau \in \text{Irr}_1(G)$ and $\chi(1) \neq \tau(1)$.

1217. Study the nonabelian p -groups G all of whose characters from $\text{Irr}_1(G)$ have kernels of the same order.

1218. (Old problem) Classify the p -groups with cyclic derived subgroup.

1219. Find $\max\{|G'|\}$, where G runs over all \mathcal{A}_n -groups with (i) abelian G' , (ii) metacyclic G' .

1220. Study the p -groups whose cyclic subgroups are characteristic in their centralizers.

1221. Study the p -groups G with $N_G(H) = HC_G(H)$ for all \mathcal{A}_1 -subgroups $H < G$.

1222. Let G be a 2-group of order $2^{2(e+1)+1}$ and exponent 2^e , $e > 1$, such that $|\mathfrak{U}_{e-1}(G)| = 2^5$. Study the structure of $\mathfrak{U}_{e-1}(G)$ provided it is nonabelian.

1223. Let G be a p -group of order $p^{p(e+1)}$ and exponent p^e , $p > 2$, $e > 1$, such that $|\mathfrak{U}_{e-1}(G)| = p^{2p}$. Study the structure of $\mathfrak{U}_{e-1}(G)$ provided it is irregular (see §23.)

1224. Study the p -groups G containing only one maximal subgroup with center of order $> p$.

1225. Let $R \leq \Phi(G)$ be a G -invariant nonabelian subgroup of order $\leq p^6$. Describe the structure of R .

1226. Let $R \leq \Phi(\Phi(G))$ be a G -invariant nonabelian subgroup of order p^5 or p^6 . Describe the structure of R .
1227. Does there exist a nonabelian p -group G that is generated by kernels of its nonlinear irreducible characters. If answer is ‘yes’, classify such groups.
1228. Study the finite 2-groups generated by two elements x and y of order 2 and 4, respectively. Describe the structures of Φ -subgroups of such groups.
1229. Describe the structures of G' , where G is as in #1228.
1230. Suppose that G is a nonabelian p -group of exponent p^e such that $\Omega_e^*(G) = \langle x \in G \mid o(x) = p^e \rangle$ is abelian. Is it true that the $\text{dl}(G)$ is bounded?
1231. A group G is said to be a Q -group if, whenever $a, b \in G$ generate the same subgroup, then a and b are conjugate in G . Classify the Q -groups of exponent ≤ 8 .
1232. Study the p -groups G with $\text{Aut}_c(G) = \text{Z}(\text{Aut}(G))$. (Here $\text{Aut}_c(G)$ is the group of central automorphisms of G .)
1233. Study the p -groups G such that, for every $H < G$ of index at most p^2 , one has $\text{Z}(H) \leq \text{Z}(G)$.
1234. Study the p -groups in which the centralizer of each noncentral element of composite order has cyclic subgroup of index p .
1235. Study the p -groups G containing only one maximal subgroup, say A , such that $|A : A'| > p^2$. (If $p = 2$, then G is of maximal class by Taussky’s theorem and Theorem 5.4.)
1236. (This problem was inspired by Mann’s paper [Man32] on skew 2-groups.) Let G be a 2-group and $t(G)$ the number of involutions in G . Study the 2-groups G such that, whenever N is a nonidentity G -invariant subgroup in $\Phi(G)$, then (i) $t(G) < t(G/N)$, (ii) $t(G) > t(G/N)$.
1237. Does there exist a p -group G of order p^{p+2} , $p > 2$, which is not of maximal class and such that G/N is of maximal class for each minimal normal subgroup N of G .
1238. Study the irregular p -groups G such that $\text{K}_p(G) = \mathfrak{U}_1(G)$ and $G/\mathfrak{U}_1(G)$ is of maximal class.
1239. Classify the p -groups G such that $\delta(H) \geq \frac{1}{p}|H|$ for all $H < G$. Here $\delta(G)$ is the minimal degree of representation of G by permutations.
1240. Let $\mathfrak{N}(X)$ be the set of nonnormal subgroups of a p -group X . Let G and H be non-Dedekindian p -groups. Suppose that there is a 1 – 1-correspondence between $\mathfrak{N}(G)$ and $\mathfrak{N}(H)$ such that corresponding subgroups and their normalizers are isomorphic. Is it true that G and H are not necessarily isomorphic?
1241. Classify the p -groups G in which all members of the set Γ_2 are \mathcal{A}_1 -groups.

1242. Classify the p -groups all of whose maximal subgroups are either abelian or special.

1243. Study the 2-groups G without normal subgroup $\cong E_{2^4}$, but all of whose maximal subgroups have normal subgroups $\cong E_{2^4}$.

1244. Study the structure of a p -group G if for any \mathcal{A}_1 -subgroup $A < G$ we have $|G : A^G| = p$.

1245. Study the p -groups G such that, whenever $A, B < G$ are distinct maximal abelian, then (i) $N_G(A \cap B) = \langle A, B \rangle$; (ii) $A \cap B \triangleleft G$.

1246. Study the p -groups G such that, whenever U, V are distinct \mathcal{A}_1 -subgroups of G , then $U \cap V$ is maximal either in U or in V .

1247. Let $d > k > 2$ be fixed. Find the minimal number of nonabelian members in the set Γ_k , where G is a nonabelian p -group with $d(G) = d$. (See §76.)

1248. Study the p -groups G such that, whenever $A < G$ is minimal nonabelian, then there is in G only one subgroup of order $p|A|$ containing A .

1249. Let G be a p -group with $c_1(G) = 1 + p + \dots + p^{p-1} + kp^p$, where $k > 1$. Let $e_p(G)$ be the number of subgroups of order p^p and exponent p in G . Estimate $e_p(G)$ in terms of k .

1250. Study the irregular p -groups G with $\text{cl}(H) \leq \frac{1}{2}(p+1)$ for all $H < G$.

1251. Study the p -groups without normal cyclic subgroups of order p^2 .¹

1252. Study the p -groups G such that for any nonabelian $H \in \Gamma_1$, all \mathcal{A}_1 -subgroups in H are conjugate in G . (In that case, H has a G -invariant abelian subgroup of index p , by Theorem 10.28.)

1253. A p -group G is said to be *generalized metacyclic* with respect to its cyclic subgroup C if there exists only one maximal chain of subgroups connecting C and G . Classify the p -groups which are generalized metacyclic with respect to all their maximal cyclic subgroups. (Such group must be two-generator.)

1254. Study the p -groups with only one abelian subgroup of type (p^n, p) , $n > 1$.

1255. Study the p -groups G such that all members of the set $\Gamma_1 \cup \Gamma_2$ are two-generator. (See §70.)

¹The group $\Sigma_{p^n} \in \text{Syl}_p(\text{S}_{p^n})$, $n > 1$, has no normal cyclic subgroups of order p^2 , unless $p^n = 4$. Indeed, assume that $p^n > 4$ and let L be a normal cyclic subgroup of order p^2 in $G_n = \Sigma_{p^n}$. Since G_2 is of maximal class, it has a normal abelian subgroup of type (p, p) so it has no normal cyclic subgroups of order p^2 , hence $n > 2$. Let $B = H_1 \times \dots \times H_p$, where $H_i \cong \Sigma_{p^{n-1}}$ is the i th coordinate subgroup of the base B of the wreath product $G_n = G_{n-1} \text{ wr } C_p$. Then $\Omega_1(L) = Z(G)$ and $L \cap H_i = \{1\}$ for all i . Assume that $L < B$; then $C_G(L) \geq H_1 \times \dots \times H_p = B$, a contradiction, since $Z(B)$ is elementary abelian. Thus, $L \not\leq B$. Since $Z(H_i)$ centralizes L (consider the centralizer of L in semidirect product $H_i \cdot L$ and take into account that $Z(H_i)$ is of order p) so $C_G(Z(H_i)) \geq BL = G$, we get $Z(H_i) \leq Z(G)$ for all i , a contradiction since $|Z(G)| = p$.

1256. Classify the p -groups G such that all members of the set Γ_2 are metacyclic.
1257. Study the p -groups G such that all members of the set Γ_2 are centralizers of appropriate elements.
1258. Estimate the number $\max |\{k(G) \mid |G| = p^n\}|$ (see [BI]).
1259. Study the p -groups G with $c_1(G) = 1 + p + \dots + p^k$ and exactly $k + 1$ conjugate classes of subgroups of order p .
1260. Study the 2-groups with exactly two conjugate classes of four-subgroups. (This problem was solved by Janko, according to his letter at 16/05/07.)
1261. Study the p -groups all of whose nonnormal subgroups of the same order are conjugate. (For a solution, see §58.)
1262. Does there exist an universal constant $C = C(p)$ such that, whenever $G/\Omega_C(G)$ is regular for a p -group G , then G is also regular?
1263. Study the nonabelian p -groups all of whose nonabelian subgroups have centers of orders at most p^2 .
1264. Is it true that $\{\alpha_1(G) \mid G \text{ is a nonabelian 2-group}\} = \mathbb{N}$? (See §76.)
1265. Is it true that for each n there exists k with $\alpha_1(G) \notin \{k+1, \dots, k+n\}$ for all p -groups G ?
1266. Classify the p -groups G with minimal nonabelian $\text{Aut}(G)$.
1267. Study the p -groups G such that all members of the set Γ_2 are special.
1268. Study the p -groups, in which each 4-fold commutator $[x, y, x, y]$ equals 1 for all $x, y \in G$.
1269. Study the p -groups G such that $C_G(x)$ is absolutely regular for all $x \in G - Z(G)$.
1270. Study the p -groups without subgroups of order p^{p+1} and exponent p that contain a subgroup $\cong E_{p^p}$.
1271. Classify the p -groups G of exponent $> p$ such that $\Omega_1(\Phi(G)) = \Phi(G)$ but $\Omega_1(\Phi(H)) < \Phi(H)$ for all $H \in \Gamma_1$.
1272. Study the p -groups G of exponent p^e , $e > 1$, with $c_1(G) > \sum_{i=2}^e c_i(G)$.
1273. Classify the pairs $H \triangleleft G$ of p -groups such that there exists only one 1-admissible chain in H (see §88).
1274. Study the p -groups G such that whenever H is a nonnormal subgroup of G , then $\exp(N_G(H)) = \exp(H)$.
1275. Let a p -group G be neither abelian nor an \mathcal{A}_1 -group. Study the structure of the group $A = \{\alpha \in \text{Aut}(G) \mid M^\alpha = M \text{ for all nonabelian subgroups } M < G\}$.

1276. Study the p -groups G containing a minimal nonabelian subgroup H such that H is the unique minimal nonabelian subgroup of its order in G .

1277. Classify the groups that are not generated by their noncyclic subgroups of index p^4 .

1278. (Old problem) Classify \mathcal{A}_3 -groups.

1279. Let Γ be the representation group of the restricted Burnside group $B(d, p)$. Find the maximum of ranks of proper subgroups (of abelian subgroups) of Γ .

1280. Classify the p -groups covered by normal extraspecial (special) subgroups.

1281. Classify the p -groups that are not generated by minimal nonmetacyclic subgroups. In particular, classify the p -groups G such that all subgroups of G not contained in a fixed $H \in \Gamma_1$, are metacyclic.

1282. Study the p -groups containing exactly one subgroup of order $p^{(p-1)k+2}$ and exponent $\leq p^k$.

1283. Let G be a p -group of maximal class and order $> p^{p+1}$ and $t = |\{H \in \Gamma_1 \mid e_p(H) > 0\}|$. Find all possible values of t . (Here $e_p(G)$ is the number of subgroups of order p^p and exponent p in G .)

1284. Study \mathcal{A}_n -groups G , $n > 2$, with $\alpha_{n-1}(G) = 1$.

1285. Suppose that a p -group G is neither abelian nor an \mathcal{A}_1 -group. Classify the p -groups G such that $\alpha_1(G) = p^{d(G)-1}$ (see §76, Theorem B).

1286. Classify the 2-groups with exactly one subgroup of order 2 which is not maximal cyclic.

1287. Study the p -groups G such that $U = Z(C_G(U))$ for all cyclic subgroups $U < G$ of orders $> p$.

1288. Classify the p -groups in which the number of \mathcal{A}_1 -subgroups of index p is $> p$.

1289. Study the p -groups G with $|N_G(A)| \neq |N_G(B)|$ for all non-conjugate nonnormal subgroups A and B of the same order.

1290. Study the p -groups in which any abelian subgroup is contained in a two-generator subgroup.

1291. Classify the p -groups of class > 2 in which any two subgroups of the same order have the same class.

1292. Study a pair $H \triangleleft G$ of p -groups such that $Z_p(G)$ is regular but $Z_p(H)$ is irregular.

1293. Study the p -groups G with $\text{cl}(N_G(A)) = \text{cl}(A)$ for all nonnormal nonabelian $A < G$.

1294. Study the p -groups G with (a) $\Phi(\mathrm{N}_G(A)) = \Phi(A)$, (b) $\mathrm{N}_G(A)' = A'$, (c) $\mathfrak{U}_1(\mathrm{N}_G(A)) = \mathfrak{U}_1(A)$ for all $A \not\trianglelefteq G$.
1295. Study the structure of the subgroup $\bigcap_H \mathrm{N}_G(H)$, where H runs over the set of subgroups of G of class 2.
1296. Study the p -groups all of whose two-generator subgroups are \mathcal{P} -groups. (See §11.)
1297. Study the irregular p -groups with regular normalizers of nonnormal subgroups.
1298. Study the irregular p -groups with regular centralizers of noncentral elements.
1299. Let G be a p -group of order p^{n+2} with $|G'| = p^2$. Find all possible degrees vectors of G .
1300. Find the degrees vector of $P_{d,n}$, a Sylow p -subgroup of $\mathrm{Aut}(H_{d,n})$, where $H = H_{d,n}$ is homocyclic with $d(H) = d$ and $\exp(H) = p^n$.
1301. Let $D_1(p^e)$ be the set of all possible values of $k(G)$ provided G runs over all groups of order p^e and exponent p . Find the minimal value of e (or prove that it does not exist) such that $\lim_{p \rightarrow \infty} D_1(p^e) = \infty$.
1302. Compute $d(A)$ and $\exp(A)$, where $A \in \mathrm{Syl}_p(\mathrm{Aut}(G))$ and G is abelian of given type.
1303. Study the p -groups G , $p > 2$, such that $H_p(G) < G$ is special (minimal nonabelian).
1304. Study the p -groups G all of whose subgroups of index p^2 that are not members of the set Γ_2 , are not G -invariant.
1305. Study the minimal non- p -abelian p -groups.
1306. Study the p -groups G such that $\mathrm{Inn}(G)$ is not characteristic in $\mathrm{Aut}(G)$.
1307. Classify the p -groups lattice isomorphic with \mathcal{A}_2 -groups.
1308. Study the p -groups G all of whose \mathcal{A}_1 -subgroups H satisfy $|H/H_G| \leq p$.
1309. Study the 2-groups all of whose minimal nonmetacyclic sections are $\cong E_8$.
1310. Study the nonmetacyclic 2-groups, all of whose minimal nonmetacyclic subgroups are isomorphic.
1311. Study the p -groups G such that whenever $\chi, \tau \in \mathrm{Irr}(G)$ have the same degree, then all nonlinear irreducible constituents of their product $\chi\tau$ have the same degree.
1312. Study the p -groups G such that, for each $\chi \in \mathrm{Irr}_1(G)$, the set $\mathrm{Lin}(G)\chi$ contains all irreducible characters of G of degree $\chi(1)$.
1313. (Old problem) Characterize the p -groups Φ such that there exists a p -group G with $\Phi(G) \cong \Phi$.

1314. Give a condition sufficient for the set \mathcal{R} of elements $x \in G$ such that $\langle x, y \rangle$ is regular for all $y \in G$.

1315. Let G be a p -group such that $d(\text{Aut}(G)) = 2$. Estimate $d(G)$. Is it possible to estimate $d(G)$ in terms of $d(\text{Aut}(G))$?

1316. Classify the p -groups such that $\text{Aut}(G)$ acts transitively on every set of nonnormal subgroups of G of the same order.

1317. Find all p -groups H with $\Omega_1(H) = H$ and such that there is no p -group G of order $> |H|$ satisfying $\Omega_1(G) \cong H$?

1318. (Janko) Let a nonabelian 2-group G possess a cyclic subgroup L of order 4 such that $C_G(L)$ is abelian of type $(4, 2)$. Is it true that G is of coclass 2?

1319. Study the 2-groups G containing an element t such that $C_G(t)$ is (i) abelian of type $(4, 4)$, (ii) metacyclic. (See §§48, 49.)

1320. Study the p -groups G such that $\mathfrak{U}_1(G)$ is nonabelian of order p^4 .

1321. Study the 2-groups all of whose \mathcal{A}_1 -subgroups are isomorphic with M_{2^n} . (For $n = 4$, see Theorem 57.6.)

1322. Describe $\text{Aut}(G)$ for all \mathcal{A}_2 -groups.

1323. Study the 2-groups G with $C_G(x) \cong A(m, \theta)$ for some $x \in G$, $o(x) = 2$ (see §46).

1324. Describe the automorphism groups of nonabelian Sylow subgroups of all minimal nonnilpotent groups.

1325. Suppose that G is a p -group, $p > 2$, which is neither abelian nor an \mathcal{A}_1 -group and α an automorphism of G of order 2. Is it true that G contains an α -invariant \mathcal{A}_1 -subgroup? (For more general result, see Lemma 31.4(c).)

1326. Given a nonabelian p -group H with center of order $> p$ and $k \in \mathbb{N}$, does there exist a p -group G of order $p^k |H|$ such that $C_G(x) \cong H$ for some $x \in G$?

1327. Let $\alpha \in \text{Aut}(G)$ be of order 2, where G is a nonabelian p -group, $p > 2$. Study the structure of G if it has no α -invariant nonnormal subgroup.

1328. (Old problem) Study the irregular p -groups all of whose proper subgroups are regular.

1329. Study the p -groups without minimal nonabelian epimorphic images.

1330. Find $\max \{d(G)\}$, where G runs over all 2-groups with $\Omega_1(G) \cong E_{2^n}$, n is fixed.

1331. Let G be a p -group, $p > 2$, with $|\Omega_1(G)| = p^n$ and $\exp(\Omega_1(G)) = p$. Is it true that $|G/\mathfrak{U}_1(G)|$ is bounded?

1332. Classify the groups of exponent p whose Schur multipliers have order p . (According to D.L. Johnson, all noncyclic groups of exponent p have nontrivial Schur multipliers.)

1333. Let G be a p -group of maximal class and order $p^m > p^3$. Find lower and upper estimates for $\beta_1(G, G_1)$. (See §76.)

1334. Study the p -groups G such that $\exp(N_G(H)) = \exp(H)$ for all nonnormal (nonnormal abelian) $H < G$.

1335. Let $A, B \in \Gamma_1$ be distinct. Suppose that $|A'| = p^n = |B'|$ and $|G'| = p^{2n+1}$. Study the structure of G' . Is n bounded?

1336. Let M be a p -group of maximal class and order $p^n > p^{p+1}$ with $e_p(M) = p^{n-p}$. Does there exist a p -group G of maximal class and order $p|M|$ that contains a subgroup isomorphic to M ?

1337. Classify the metacyclic p -groups M such that there does not exist a metacyclic p -group containing a maximal subgroup isomorphic to M . (If $M \cong \text{SD}_{2^n}$, then there does not exist a metacyclic 2-group containing a maximal subgroup isomorphic to M .)

1338. Let \mathfrak{R}_d be the set of all representation groups of E_{p^d} . Find (i) the orders of normal subgroups N of G such that G/N is extraspecial of order p^{2n+1} ($G \in \mathfrak{R}_d$), (iii) $|\text{Aut}(G)|$ for all $G \in \mathfrak{R}_d$.

1339. Let $H = H(d, p^e)$ be a homocyclic group of rank $d > 1$ and exponent $p^e > p$, let \mathfrak{R}_H be the set of all representation groups of H . Consider for $G \in \mathfrak{R}_H$ the same questions as in #1338.

1340. Let $G = \text{UT}(n, p) \in \text{Syl}_p(\text{GL}(n, p))$. Study the p -groups which are lattice isomorphic with G .

1341. Classify the p -groups G of exponent $> p^2$ such that $\Omega_3^*(G)$ is an L_p -group.

1342. Classify the p -groups G with $N_G(A \cap B) \geq \langle A, B \rangle$ for any two nonincident $A, B < G$.

1343. Study the 2-groups G containing an abelian subgroup of type $(4, 2)$ such that $N_G(A)$ is abelian of type $(4, 4)$.

1344. Let \mathfrak{R}_d be the set of representation groups of E_{p^d} , $d > 1$. Find $\{\alpha_1(G) \mid G \in \mathfrak{R}_d\}$.

1345. Let G and G_0 be lattice isomorphic p -groups. Suppose that there is in G a normal subgroup of order p^n and exponent p . Is it true that G_0 contains a normal subgroup of order p^n and exponent p ?

1346. Find a realistic upper bound for $\alpha_1(G)$, where $|G| = p^m$ and $\exp(G) = p$.

1347. Classify the nonabelian groups of exponent p all of whose two-generator subgroups have order p^3 ($\leq p^4$).

1348. Let $3 < n < m$ and let G be a group of order p^m and exponent p with a two-generator subgroup of order p^n . Study the structure of G if it has at most p^2 two-generator subgroups of order p^n .

1349. (Isaacs) Let a q -group Q act on a 2-group G so that Q -orbits have pairwise distinct sizes. Describe the structure of G . (See Appendix 3.)

1350. Study the p -groups G such that all its \mathcal{A}_2 -subgroups have exponent $< \exp(G)$.

1351. Classify the p -groups with homocyclic maximal subgroup.

1352. Classify the p -groups G such that $N_G(H) \trianglelefteq G$ for all $H \leq G$.

1353. Let $k_2(G)$ denote the number of conjugacy classes of abelian subgroups of type (p, p) in a p -group G . Classify the p -groups G with $k_2(G) = 3$.

1354. Study the p -groups in which all maximal subgroups of exponent p are maximal regular.

1355. Let a p -group $G = E_0 E_1$, where E_0 and E_1 are elementary abelian, $E_0 \cap E_1 = \{1\}$. Find $\min \{c_1(G)\}$ in terms of E_0 and E_1 .

1356. (This problem was inspired by Mann's letter in June 2006.) Present a two-generator p -group G , $p > 2$, with irregular (i) $\Phi(G)$, (ii) $\mathfrak{U}_1(G)$, (iii) $\mathfrak{U}^2(G)$, (iv) G' , (v) G'' .

1357. Study the structure of $G = AB$, where $\text{cl}(A), \text{cl}(B) \leq 2$ and $A_G B_G = \{1\}$.

1358. Study the \mathcal{A}_n -groups G with $d(G) = n + 1$.

1359. Classify the nonabelian p -groups G such that any two its subgroups of the same index p^k ($k = 1, 2$) are isomorphic.

1360. Let $A < G$ be p -groups with $|A| = p^{(p-1)k+2}$, $\exp(A) = p^k > p$. Suppose that $A < A_1 \leq G$ implies $\exp(A_1) > p^k$. Study the structure of G . (See §24.)

1361. Study the p -groups G such that for every minimal basis $\{a_1, \dots, a_d\}$ we have $\prod_{i=1}^d o(a_i) = |G|$.

1362. Classify the p -groups R of order p^P , $p > 2$, such that there exists an irregular p -group G of maximal class such that: (i) $R \cong R_1 < G$, however (ii) $R_1 \not\leq G_1$.

1363. (Ito) Let $n > 1$ be odd. Is the group $G = \langle a, b \mid a^{4n} = 1, b^2 = a^{2n}, a^b = a^{-1} \rangle$ Hadamard (see #247)?

1364. Study the 2-groups G such that $\Omega_2(G)$ is an U_2 -group (see §§18, 67).

1365. Study the 2-groups G such that $\Omega_2(G) \cong D_{2^m} \times D_{2^n}$.

1366. Let a p -group G be irregular but not of maximal class. Then $c_2(G) \equiv kp^{p-1} \pmod{p^P}$ (Theorem 13.2(b)). Find all possible values of k .

1367. Study the p -groups G such that whenever Z is a nonnormal maximal cyclic subgroup of G then G/Z^G is cyclic.

1368. Let G be a representation group of an elementary abelian p -group of rank d . Find the class of a Sylow p -subgroup of $\text{Aut}(G)$.

1369. Let \mathfrak{R}_d be the set of all representation groups of E_{p^d} . Find $|A|$, where A is the group of all automorphisms of $G \in \mathfrak{R}_d$ fixing all elements of $Z(G)$.

1370. Let $A = \langle \mu \in \text{Aut}(G) \mid M^\mu = M \text{ for all } \mathcal{A}_1\text{-subgroups } M < G \rangle$. Study the structure of A .

1371. Study the p -groups G containing a special subgroup E such that, whenever $E < M \leq G$, then $\exp(M) > \exp(E)$. (See §83.)

1372. Let $G = B(4, n)$ be the free group of exponent 4 and rank n . (i) Find $\max \{d(M) \mid M < G\}$. (ii) (Old problem) Compute $|G|$. (iii) Describe the lower and upper central series of G . (iv) Describe the members of the derived series of G . (v) Find $\max \{d(A) \mid A < G, A' = \{1\}\}$. (vi) Find $c_1(G)$. (vii) Does there exist a 2-admissible Hall chain in G ? Find the number of principal series in $B(4, 2)$. (viii) Find $cd(G)$ and the number of irreducible characters of G of given degree. (See §60.)

1373. Let H be a p -group. Find a p -group G of minimal possible order such that H is isomorphic to a subgroup of $\Phi(G)$.

1374. Find the number of maximal series in the abelian p -group of given type.

1375. Let G be a two-generator nonmetacyclic p -group of order $> p^4$, $p > 2$. Is it true that the number of two-generator members of the set Γ_1 is a multiple of p ?

1376. Classify the p -groups G such that $\Omega_2(G) = E \times E_1$, where E is extraspecial and E_1 is elementary abelian.

1377. For groups of order p^4 describe (i) automorphism groups, (ii) holomorphs, (iii) representation groups.

1378. Study the irregular p -groups, $p > 2$, all of whose regular subgroups are of class ≤ 2 . (In that case, $p = 3$.)

1379. Study the p -groups all of whose cyclic subgroups of some fixed order are conjugate. (For a solution, for order 4, see Theorem 89.8.)

1380. Suppose that a p -group $G = \Omega_e(G)$ is of order p^{pe} . Describe the structure of G provided $\exp(G) > p^e$.

1381. Does there exist a special p -group such that all its maximal subgroups are characteristic?

1382. Let G be a p -group of exponent $> p$ and $R < G$ a fixed subgroup of order p^p and exponent p . Suppose that if $Z < G$ is arbitrary cyclic of order $> p$, then $R \cap Z = \{1\}$. Describe the structures of R and G .

1383. Let A be an \mathcal{A}_1 -subgroup of a p -group G such that there is in G only one subgroup of order $p|A|$ containing A . Describe the structure of G .

1384. Study the irregular p -groups G such that $\exp(\Omega_1(Z^G)) = p$ for all cyclic $Z < G$.

1385. Describe maximal subgroups of standard wreath product $G = A * B$, where A and B are irregular p -groups of maximal class.

1386. Study the structure of an irregular p -group G such that, whenever $H < G$ is maximal abelian and $H < F < G$ with $|F : H| = p$, then $\exp(F) > \exp(H)$.

1387. Study the noncyclic p -groups G possessing only one normal subgroup of order p^i for $i = 1, \dots, p$. Is it true that G is irregular?

1388. Study the p -groups G such that (i) $|\Omega_2^*(G)| = p^{p+1}$, (ii) $\Omega_2^*(G)$ is irregular of order p^{p+2} .

1389. Determine the structure of the Schur multiplier and representation group of $\mathrm{UT}(n, p)$.

1390. Let Γ be a representation group of E_{p^n} . Determine the structure of the Schur multiplier of Γ .

1391. Does there exist a p -group G of exponent $> p$ satisfying $H_p(G) = \mathfrak{U}_1(G)$?

1392. Does there exist a p -group G such that $A \cap Z(G) = \{1\}$ for all minimal nonabelian $A < G$?

1393. Let G be an irregular p -group satisfying $\Omega_1(G) = G$. Study the structure of G provided all maximal subgroups of exponent p in G have the same order p^p .

1394. Study the p -groups G such that, whenever $H < G$ is nonnormal of exponent p , then $\exp(\Omega_1(N_G(H))) = p$ but $\exp(\Omega_1(G)) > G$.

1395. Classify the 2-groups G such that $\Omega_3^*(G)$ is a U_2 -group. (Note that if $n > 3$, then $\Omega_n^*(G)$ is not an U_2 -group.)

1396. Study the p -groups G such that $[\Omega_i(G), \mathfrak{U}_i(G)] = \{1\}$ for all i .

1397. Study the nonabelian p -groups G such that $|G/\ker(\chi)| = p\chi(1)^2$ for all $\chi \in \mathrm{Irr}_1(G)$. For partial case of this problem, see #1.

1398. Find a sufficient condition for existence of 3-admissible Hall chains in a 2-group (see §88).

1399. Let G be a p -group and $N \leq \Phi(\Phi(G))$ be G -invariant. Describe the structure of N if it is nonabelian of order $\leq p^6$.

1400. Let G be a p -group such that $\Phi(G) = E \times E_1$, where E and E_1 are extraspecial. Describe the structure of G .

Bibliography

- [Alp1] J. L. Alperin, On a special class of regular p -groups, *Trans. Amer. Math. Soc.* **106** (1963), 77–99.
- [Alp2] J. L. Alperin, Large abelian subgroups of p -groups, *Trans. Amer. Math. Soc.* **117** (1965), 10–20.
- [Alp3] J. L. Alperin, Centralizers of abelian normal subgroups of p -groups, *J. Algebra* **1** (1964), 110–113.
- [AlpG] J. L. Alperin and G. Glauberman, Limits of abelian subgroups of finite p -groups, *J. Algebra* **203** (1998), 533–566.
- [AlpK] J. L. Alperin and Kuo Tzee-Nan, The exponent and the projective representations of a finite group, *Illinois J. Math.* **11** (1967), 410–414.
- [AK1] B. Amberg and L. Kazarin, On the rank of a finite product of two p -groups, in: *Groups – Korea 94*, pp. 1–8, W. de Gruyter, Berlin, 1995.
- [AK2] B. Amberg and L. Kazarin, On the rank of a product of two finite p -groups and nilpotent p -algebras, *Comm. Algebra* **27**(8) (1999), 3895–3907.
- [Arg] D. E. Arganbright, The power-commutator structure of finite p -groups, *Pacific J. Math.* **29** (1969), 11–17.
- [Bae1] R. Baer, Groups with abelian central quotient groups, *Trans. Amer. Math. Soc.* **44** (1938), 357–386.
- [Bae2] R. Baer, Partitionen endlicher Gruppen, *Math. Z.* **75** (1961), 333–372.
- [Bae3] R. Baer, Gruppen mit Hamiltonschem Kern, *Comp. Math.* **2** (1935), 241–246.
- [Bae4] R. Baer, Group elements of prime power index, *Trans. Amer. Math. Soc.* **75** (1953), 20–47.
- [BM1] C. Baginski and I. Malinowska, On groups of order p^n with automorphism of order p^{n-2} , *Demonstr. Math.* **23** (1996), 565–575.
- [BM2] C. Baginski and I. Malinowska, On finite 2-groups with many involutions, *Arch. Math.* **81** (2003), 241–244.
- [Bal] F. Balogh, Finite groups in which different conjugacy classes have different cardinalities, *J. Algebra* **181** (1996), 286–287.
- [Ban] W. Bannisher, Über Gruppen mit genau zwei irreduziblen Charaktergraden I, II, *Math. Nachr.* **154** (1991), 253–563.
- [BarI] Y. Barnea and I. M. Isaacs, Lie algebras with few centralizer dimensions, *J. Algebra* **259** (2003), 284–299.
- [Bec] H. Bechtell, Frattini subgroups and Φ -central groups, *Pacific J. Math.* **18** (1966), 15–23.
- [Bei1] B. Beisiegel, Semi-extraspezielle p -Gruppen, *Math. Z.* **156** (1976), 247–254.

- [Bei2] B. Beisiegel, Die Automorphismengruppen homozyklischer p -Gruppen, *Arch. Math.* **29**, 4 (1977), 363–366.
- [Ben1] H. A. Bender, A determination of the groups of order p^5 , *Ann. Math.* (2) **29** (1927), 61–72.
- [Ben2] H. A. Bender, Determination of all prime power groups containing only one invariant subgroup of every index which exceeds this prime number, *Trans. Amer. Math. Soc.* **26**, 4 (1924), 427–434.
- [BenG] H. Bender and G. Glauberman, *Local Analysis for the Odd Order Theorem*, London Math. Soc. Lect. Note Series 188, Cambridge Univ. Press, Cambridge, 1994.
- [BKN] T. R. Berger, L. G. Kovacs and M. F. Newman, Groups of prime power order with cyclic Frattini subgroup, *Nederl. Akad. Wetensch. Indag. Math.* **42** (1980), no. 1, 13–18.
- [Ber0] V. G. Berkovich, Groups of order p^n possessing an automorphism of order p^{n-1} , *Algebra i Logika* **9** (1970), no. 1, 4–8 (in Russian).
- [Ber1] Y. Berkovich, On p -groups of finite order, *Siberian Math. Zh.* **9** (1968), 1284–1306 (in Russian).
- [Ber2] Y. Berkovich, Subgroups, normal divisors and epimorphic images of a finite p -group, *Soviet Math. Dokl.* **10** (1969), 878–881.
- [Ber3] Y. Berkovich, A generalization of theorems of Ph. Hall and Blackburn and an application to non-regular p -groups, *Math. USSR Izv.* **35** (1971), 815–844.
- [Ber4] Y. Berkovich, Some consequences of Maschke's theorem, *Algebra Coll.* **5**, 2 (1998), 143–158.
- [Ber5] Y. Berkovich, Alternate proofs of some basic theorems of finite group theory, *Glas. Mat.* **40** (2005), no. 2, 207–233.
- [Ber6] Y. Berkovich, Finite metacyclic groups, *Soobsch. Akad. Nauk Gruzin. SSR* **68** (1972), 539–542 (in Russian).
- [Ber7] Y. Berkovich, On finite metacyclic groups, in: *Structural Properties of Algebraic Systems*, pp. 12–19, Nalchik, 1985 (in Russian).
- [Ber8] Y. Berkovich, Relations between some invariants of finite solvable groups, *Soobsch. Akad. Nauk Gruzin. SSR* **123** (1986), no. 3, 469–472 (in Russian).
- [Ber9] Y. Berkovich, On subgroups of finite p -groups, *J. Algebra* **224** (2000), 198–240.
- [Ber10] Y. Berkovich, Alternate proofs of two theorems of Philip Hall on finite p -groups, and related results, *J. Algebra* **294** (2005), no. 2, 463–477.
- [Ber11] Y. Berkovich, On abelian subgroups of p -groups, *J. Algebra* **199** (1998), 262–280.
- [Ber12] Y. Berkovich, On the order of the commutator subgroup and the Schur multiplier of a finite p -group, *J. Algebra* **144** (1991), no. 2, 269–272.
- [Ber13] Y. Berkovich, On the number of subgroups of given order in a finite p -group of exponent p , *Proc. Amer. Math. Soc.* **109** (1990), no. 4, 875–879.
- [Ber14] Y. Berkovich, On the number of elements of given order in a finite p -group, *Israel. J. Math.* **73** (1991), 107–112.
- [Ber15] Y. Berkovich, On the number of subgroups of given order and exponent p in a finite irregular p -group, *Bull. London Math. Soc.* **24** (1992), 259–266.
- [Ber16] Y. Berkovich, Counting theorems for finite p -groups, *Arch. Math.* **59** (1992), 215–222.

- [Ber17] Y. Berkovich, On the number of solutions of equation $x^{p^k} = a$ in a finite p -group, *Proc. Amer. Math. Soc.* **116** (1992), no. 3, 585–590.
- [Ber18] Y. Berkovich, On p -subgroups of finite symmetric and alternating groups, *Contemporary Mathematics* **93** (1989), 67–76.
- [Ber19] Y. Berkovich, On the number of solutions of equation $x^{p^k} = 1$ in a finite group, *Rendiconti Lincei, Matematica e applicazioni Ser. 9* **6** (1995), 5–12.
- [Ber20] Y. Berkovich, On the number of subgroups of a given structure in a finite p -group, *Arch. Math.* **63** (1994), 111–118.
- [Ber21] Y. Berkovich, Normal subgroups in a finite group, *Soviet Math. Dokl.* **9** (1968), 1117–1120.
- [Ber22] Y. Berkovich, Short proofs of some basic characterization theorems of finite p -group theory, *Glas. Mat.* **41**(61) (2006), 239–258.
- [Ber23] Y. Berkovich, On an irregular p -group, *Siberian J. Math.* **12** (1971), no. 4, 907–911.
- [Ber24] Y. Berkovich, On subgroups and epimorphic images of finite p -groups, *J. Algebra* **248** (2002), 472–553.
- [Ber25] Y. Berkovich, Selected Topics of Finite Group Theory, Parts I, II, in preparation.
- [Ber26] Y. Berkovich, Nonnormal and minimal nonabelian subgroups of a finite group, *Glas. Mat.*, to appear.
- [Ber27] Y. Berkovich, Hall chains in finite p -groups, *Israel J. Math.*, to appear.
- [Ber28] Y. Berkovich, Alternate proofs of characterization theorems of Miller and Zvonimir Janko on p -groups, and some related results, *Glas. Math.* **43**(62) (2007), 319–343.
- [Ber29] Y. Berkovich, On the metacyclic epimorphic images of a finite p -group, *Glas. Mat.* **41**(61) (2007), 259–269.
- [Ber30] Y. Berkovich, Finite p -groups with few minimal nonabelian subgroups. With an appendix by Z. Janko, *J. Algebra* **297** (2006), no. 1, 62–100.
- [Ber31] Y. Berkovich, Alternate proofs of some basic theorems of finite group theory, *Glas. Mat.* **40** (2005), no. 2, 207–233.
- [Ber32] Y. Berkovich, A property of p -groups of order $p^{p(e+1)}$ and exponent p^e , *Glas. Mat.* **40**(60) (2005), 51–58.
- [Ber33] Y. Berkovich, *Groups of Prime Power Order*, Volume 1, Walter de Gruyter, Berlin, 2008.
- [Ber34] Y. Berkovich, p -groups in which some subgroups are generated by elements of order p , submitted.
- [BFP] Y. Berkovich, G. Freiman and C. E. Praeger, Small squaring and cubing properties for finite groups, *Bull. Aust. Math. Soc.* **44** (1991), no. 3, 429–450.
- [BIK] Y. Berkovich, I. M. Isaacs and L. S. Kazarin, Distinct monolithic character degrees, *J. Algebra* **216** (1999), 448–480.
- [BJ1] Y. Berkovich and Z. Janko, Structure of finite p -groups with given subgroups, *Contemporary Mathematics* **402** (2006), 13–93.
- [BJ2] Y. Berkovich and Z. Janko, On subgroups of finite p -groups, *Israel J. Math.*, to appear.
- [BerM] Y. Berkovich and A. Mann, On sums of degrees of irreducible characters, *J. Algebra* **199** (1998), 646–665.

- [BZ] Y. Berkovich and E. M. Zhemud, *Characters of Finite Groups*, Parts 1, 2, Translations of Mathematical Monographs 172, 181, American Mathematical Society, Providence, RI, 1998, 1999.
- [Bert] E. A. Bertram, Large centralizers in finite solvable groups, *Israel J. Math.* **47** (1984), 335–344.
- [BEOB1] H. U. Besche, B. Eick and E. A. O’Brien, The groups of order at most 2000, *Electronic Research Announcements of AMS* **7** (2001), 1–4.
- [BEOB2] H. U. Besche, B. Eick and E. A. O’Brien, A millennium project: Constructing small groups, *Internat. J. Algebra and Comp.* **12** (2002), 623–644.
- [Bey] F. R. Beyl, The Schur multiplicator of metacyclic groups, *Proc. Amer. Math Soc.* **40** (1973), 413–418.
- [BeyT] F. R. Beyl and J. Tappe, *Group Extensions, Representations and the Schur Multiplicator*, Lect. Notes in Math. 958, Springer, Berlin, 1982.
- [Bla1] N. Blackburn, On prime-power groups in which the derived group has two generators, *Proc. Cambridge Phil. Soc.* **53** (1957), 19–27.
- [Bla2] N. Blackburn, On prime power groups with two generators, *Proc. Cambridge Phil. Soc.* **54** (1958), 327–337.
- [Bla3] N. Blackburn, On a special class of p -groups, *Acta Math.* **100** (1958), 45–92.
- [Bla4] N. Blackburn, Über das Produkt von zwei zyklischen Gruppen, *Math. Z.* **68** (1958), 422–427.
- [Bla5] N. Blackburn, Generalizations of certain elementary theorems on p -groups, *Proc. London Math. Soc.* **11** (1961), 1–22.
- [Bla6] N. Blackburn, Automorphisms of finite p -groups, *J. Algebra* **3** (1966), 28–29.
- [Bla7] N. Blackburn, Finite groups in which the nonnormal subgroups have nontrivial intersection, *J. Algebra* **3** (1966), 30–37.
- [Bla8] N. Blackburn, Note on a paper of Berkovich, *J. Algebra* **24** (1973), 323–334.
- [Bla9] N. Blackburn, Some homology groups of wreath products, *Illinois J. Math.* **16** (1972), 116–129.
- [Bla10] N. Blackburn, Über Involutionen in 2-Gruppen, *Arch. Math.* **35** (1980), 75–78.
- [Bla11] N. Blackburn, The derived group of a 2-group, *Math. Proc. Camb. Phil. Soc.* **101** (1987), 193–196.
- [Bla12] N. Blackburn, On centralizers in p -groups, *J. London Math. Soc. (2)* **9**, (1975), 478–482.
- [Bla13] N. Blackburn, Groups of prime-power order having an abelian centralizer of type $(r, 1)$, *Mh. Math.* **99** (1985), 1–18.
- [Bla14] N. Blackburn, Conjugacy in nilpotent groups, *Proc. Amer. Math. Soc.* **16** (1965), 143–148.
- [Bla15] N. Blackburn, Nilpotent groups in which the derived group has two generators, *J. London Math. Soc.* **35** (1960), 33–35.
- [BlaDM] N. Blackburn, M. Deaconescu and A. Mann, Equilibrated groups, *Proc. Cambridge Philos. Soc.* **120** (1996), no. 2, 579–588.
- [BlaEs] N. Blackburn, A. Espuelas, The power structure of metabelian p -groups, *Proc. Amer. Math. Soc.* **92** (1984), 478–484.

- [BlaEv] N. Blackburn and L. Evens, Schur multipliers of p -groups, *J. reine angew. Math.* **309** (1979), 100–113.
- [Blac1] S. R. Blackburn, Enumeration within isoclinism classes of groups of prime power order, *J. London Math. Soc.* **50** (1994), 293–304.
- [Blac2] S. R. Blackburn, Groups of prime power order with derived subgroup of prime order, *J. Algebra* **219** (1999), 625–657.
- [BDM] H. F. Blichfeldt, L. E. Dickson and G. A. Miller, *Theory and Applications of Finite Groups*, New York, Stechert, 1938.
- [BosI] N. Boston and I. M. Isaacs, Class numbers of p -groups of given order, *J. Algebra* **279** (2004), 810–819.
- [BosW] N. Boston and J. L. Walker, 2-groups with few conjugacy classes, *Proc. Edinburgh Math. Soc. (2)* **43** (2000), no. 1, 211–217.
- [BozJ1] Z. Bozikov and Z. Janko, Finite 2-groups G with $|\Omega_3^*(G)| = 2^5$, *J. Group Theory* **7** (2004), 65–73.
- [BozJ2] Z. Bozikov and Z. Janko, On a question of N. Blackburn about finite 2-groups, *Israel J. Math.* **147** (2005), 329–331.
- [BozJ3] Z. Bozikov and Z. Janko, On finite p -groups in which the centralizer of each element is a normal subgroup, manuscript.
- [BozJ4] Z. Bozikov and Z. Janko, Finite p -groups all of whose nonmetacyclic subgroups are generated by involutions, *Arch. Math.* **90** (2008), 14–17.
- [BozJ5] Z. Bozikov and Z. Janko, A complete classification of finite p -groups all of whose noncyclic subgroups are normal, *Math. Z.*, to appear.
- [Bran] A. Brandis, Beweis einer Satzes von Alperin und Kuo Tzee-Nan, *Illinois J. Math.* **13** (1969), 275.
- [Bro] J. Brodkey, A note on finite groups with an abelian Sylow group, *Proc. Amer. Math. Soc.* **14** (1963), 132–133.
- [Bur1] W. Burnside, *The Theory of Groups of Finite Order*, Dover. Publ., N.Y., 1955.
- [Bur2] W. Burnside, On some properties of groups whose orders are powers of primes I, *Proc. London. Math. Soc. (2)* **11** (1912), 225–245; II. *ibid* **13** (1913), 6–12.
- [Bur3] W. Burnside, On the outer automorphisms of a group, *Proc. London Math. Soc. (2)* **11** (1913), 40–42.
- [Bur4] W. Burnside, On an unsettled question in the theory of discontinuous groups, *Quarterly J. Math.* **33** (1902), 230–238.
- [Bus] K. Buzasi, On the structure of the wreath product of a finite number of cyclic groups of prime order, *Publ. Math. Debrecen* **15** (1968), 107–129.
- [Ca] A. Caranti, Projectivity of p -groups of maximal class, *Rend. Sem. Mat. Padova* **61** (1979), 393–404 (in Italian).
- [Cha] E. I. Chankov, p -groups with five nonlinear irreducible characters, manuscript.
- [Che] Y. Cheng, On finite p -groups with cyclic commutator subgroups, *Arch. Math.* **39** (1982), 295–298.
- [CHe] D. Chillag and M. Herzog, Finite groups with almost distinct character degrees, to appear.

- [CI] M. D. E. Conder and I. M. Isaacs, Derived subgroups of products of an abelian and a cyclic subgroup, *J. London Math. Soc.* **69** (2004), no. 2, 333–348.
- [Con] S. B. Conlon, p -groups with an abelian maximal subgroup and cyclic centre, *J. Aust. Math. Soc. Ser. A* **22** (1976), no. 2, 221–233.
- [Cor] G. Corsi Tani, Automorphisms fixing every normal subgroup of a p -group, *Bull. Un. Mat. Ital. B* (6) **4** (1985), 245–252.
- [CHa] J. Cossey and T. Hawkes, Sets of p -powers as conjugacy classes sizes, *Proc. Amer. Math. Soc.* **128** (2000), 49–51.
- [CHM] J. Cossey, T. Hawkes and A. Mann, A criterion for a group to be nilpotent, *Bull. London Math. Soc.* **24** (1992), 267–270.
- [Cut] G. Cutolo, On a question about automorphisms of finite p -groups, *J. Group Theory* **9** (2006), 231–250.
- [Dad] E. C. Dade, Products of orders of centralizers, *Math. Z.* **96** (1967), 223–225.
- [DS] R. Dark and C. Scoppola, On Camina groups of prime power order, *J. Algebra* **181** (1996), 787–802.
- [Dav1] R. M. Davitt, The automorphism group of finite p -abelian p -groups, *Illinois J. Math.* **16** (1972), 76–85.
- [Dav2] R. M. Davitt, The automorphism group of a finite metacyclic p -group, *Proc. Amer. Math. Soc.* **25** (1970), 876–879.
- [Dav3] R. M. Davitt, On the automorphism group of a finite p -group with a small central quotient, *Can. J. Math.* **32** (1980), 1168–1176.
- [DO] R. M. Davitt and A. D. Otto, On the automorphism group of a finite p -group with the central quotient metacyclic, *Proc. Amer. Math. Soc.* **30** (1971), 467–472.
- [DO2] R. M. Davitt and A. D. Otto, On the automorphism group of a finite modular p -group, *Proc. Amer. Math. Soc.* **35** (1972), 399–404.
- [Ded] R. Dedekind, Über Gruppen, deren sämtliche Teiler Normalteiler sind, *Math. Ann.* **48** (1897), 548–561.
- [Del] P. Deligne, Congruences sur le nombre de sous-groupes d'ordre p^k dans un groupe fini, *Bull. Soc. Math. Belg.* **18** (1966), 129–132.
- [Die] J. Dietz, Automorphisms of p -groups given as cyclic-by-elementary abelian extensions, *J. Algebra* **242**, (2001), 417–432.
- [DdSMS] J. Dixon, M. P. F. du Sautoy, A. Mann and D. Segal, *Analytic Pro- p -Groups*, London Math. Soc. Lecture Notes Series 157, Cambridge University Press, 1991.
- [Dol] S. Dolfi, Arithmetical conditions on the length of the conjugacy classes of a finite group, *J. Algebra* **174** (1995), 753–771.
- [Dra] S. V. Draganyuk, On the structure of finite primary groups all 2-maximal subgroups of which are abelian, in: *Complex Analysis, Algebra and Topology*, pp. 42–51, Kiev, 1990.
- [Eas] T. E. Easterfield, The orders of products and commutators in prime-power groups, *Proc. Cambridge Philos. Soc.* **36** (1940), 14–26.
- [ENOB] B. Eick, M. F. Newman, and E. A. O'Brien. The class-breadth conjecture revisited. *J. Algebra* **300** (2006), 384–393.

- [ELGOB] B. Eick, C. R. Leedham-Green and E. A. O'Brien, Constructing automorphism groups of p -groups, *Comm. Algebra* **30** (2002), no. 5, 2271–2295.
- [Fal] K. Faltings, Automorphismengruppen endlicher abelscher p -Gruppen, in: *Studies on Abelian Groups* (Symposium, Montpellier, 1967), pp. 101–119, Springer, Berlin, 1968.
- [Fan] Y. Fan, A characterization of elementary abelian p -groups by counting subgroups, *Math. Practice Theory* **1** (1988), 63–65 (in Chinese); MR 89h: 20030.
- [Fei] W. Feit, Theory of finite groups in the twentieth century, *Amer. Math. Heritage: Algebra and Applied Math.* **13** (1881), 37–60.
- [FT] W. Feit and J. G. Thompson, Solvability of groups of odd order, *Pacific J. Math.* **13** (1963), 775–1029.
- [Fer] G. A. Fernandez-Alcober, An introduction to finite p -groups: regular p -groups and groups of maximal class, *Math. Contemp.* **20** (2001), 155–226.
- [F-AM] G. A. Fernandez-Alcober and A. Moreto, Groups with two extreme character degrees and their normal subgroups, *Trans. Amer. Math. Soc.* **353** (2001), 2271–2292.
- [Fitt] H. Fitting, Die Gruppe der zentralen Automorphismen einer Gruppe mit Hauptreihe, *Math. Ann.* **114** (1937), 355–372.
- [FMHOBS] J. Flynn, D. MacHale, E. A. O'Brien and R. Sheely, Finite groups whose automorphism groups are 2-groups, *Proc. Roy. Ir. Acad.* **94A** (2) (1994), 137–145.
- [Fom] A. N. Fomin, Finite 2-groups in which the centralizer of a certain involution is of order 8, *Ural Gos. Univ. Mat. Zap.* **8** (1972), no. 3, 122–132 (in Russian).
- [For] C. E. Ford, Characters of p -groups, *Proc. Amer. Math. Soc.* **101** (1987), 595–601.
- [FrT] J. S. Frame und O. Tamaschke, Über die Ordnungen der Zentralizatoren der Elemente in endlichen Gruppen, *Math. Z.* **83** (1964), 41–45.
- [FS] G. Frobenius and L. Stickelberger, Über Gruppen von vertauschbaren Elementen, *J. reine angew. Math.* **86** (1879), 217–262.
- [Gag] S. M. Gagola, Jr., A character theoretic condition for $F(G) > 1$, *Comm. Algebra* **33** (2005), 1369–1382.
- [GL] S. M. Gagola and M. L. Lewis, A character theoretic condition characterizing nilpotent groups, *Comm. Algebra* **27** (3) (1999), 1053–1056.
- [Gal] J. A. Gallian, Finite p -groups with homocyclic central factors, *Can. J. Math.* **26** (1974), 636–643.
- [Gas1] W. Gaschütz, Über die Φ -Untergruppe endlicher Gruppen, *Math. Z.* **58** (1953), 160–170.
- [Gas2] W. Gaschütz, Kohomologische Trivialitäten und äußere Automorphismen von p -Gruppen, *Math. Z.* **88** (1965), 432–433.
- [Gas3] W. Gaschütz, Nichtabelsche p -Gruppen besitzen äußere p -Automorphismen, *J. Algebra* **4** (1966), 1–2.
- [GNY] W. Gaschütz, J. Neubüser and Ti Yen, Über den Multiplikator von p -Gruppen, *Math. Z.* **100** (1970), 93–96.
- [GMMPS] N. Gavioli, A. Mann, V. Monti, A. Previtali and C. Scoppola, Groups of prime power order with many conjugacy classes, *J. Algebra* **202** (1998), 129–141.

- [GMS] N. Gavioli, A. Mann, and C. Scoppola, Two applications of the Hedges subgroup of finite group, in: *Ischia Group Theory 2006*, pp. 138–146, World Scientific Books, Singapore, 2007.
- [Gil] J. D. Gillam, A note on finite metabelian p -groups, *Proc. Amer. Math. Soc.* **25** (1970), 189–190.
- [Gla1] G. Glauberman, Large abelian subgroups of finite p -groups, *J. Algebra* **196** (1997), 301–338.
- [Gla2] G. Glauberman, Large abelian subgroups of groups of prime exponent, *J. Algebra* **237** (2001), 735–768.
- [Gla3] G. Glauberman, On Burnside's other $p^a g^b$ -theorem, *Pacific J. Math.* **56**, (1975), 469–476.
- [Gla4] G. Glauberman, Isomorphic subgroups of finite p -groups, I, II, *Canad. J. Math.* **23** (1971), 983–1022, 1023–1039.
- [Gla5] G. Glauberman, Large subgroups of small class in finite p -groups, *J. Algebra* **272** (2004), 128–153.
- [Gla6] G. Glauberman, Centrally large subgroups of finite p -groups, *J. Algebra* **300** (2006), 480–508.
- [Gla7] G. Glauberman, Existence of normal subgroups in finite p -groups, *J. Algebra* **319** (2008), 800–805.
- [Gol] Y. A. Gol'fand, On groups all of whose subgroups are nilpotent, *Dokl. Akad. Nauk SSSR* **125** (1948), 1313–1315.
- [Gor1] D. Gorenstein, *Finite Groups*, Harper and Row, N.Y., 1968.
- [Gor2] D. Gorenstein, On a theorem of Philip Hall, *Pacific J. Math.* **19** (1966), 77–80.
- [Gor3] D. Gorenstein (Editor), *Reviews on Finite Groups*, Amer. Math. Soc., Providence, RI, 1974.
- [GLS] D. Gorenstein, R. Lyons and R. Solomon, *The Classification of the Finite Simple Groups*, Part 1, Chapter G: General Group Theory, AMS, Providence, RI, 1995.
- [Gre] J. A. Green, On the number of automorphisms of a finite group, *Proc. Roy. Soc. London A* **237** (1956), 574–580.
- [Gro] F. Gross, 2-automorphic 2-groups, *J. Algebra* **40** (1976), 348–353.
- [Gro2] F. Gross, Automorphisms of permutational wreath products, *J. Algebra* **117** (1988), 472–493.
- [Grov] L. C. Grove, *Groups and Characters*, Pure and Applied Mathematics, John Wiley and Sons, New York, 1997.
- [Grov1] J. R. J. Groves, On minimal irregular p -groups, *J. Aust. Math. Soc.* **16** (1973), 78–89.
- [Grov2] J. R. J. Groves, On direct products of regular p -groups, *Proc. Amer. Math. Soc.* **37** (1973), 377–379.
- [Grov3] J. R. J. Groves, Some criteria for the regularity of a direct product of regular p -groups, *J. Aust. Math. Soc. Ser. A* **24** (1977), 35–49.
- [Gr1] O. Grün, Beiträge zur Gruppentheorie. V, Über endliche p -Gruppen, *Osaka Math. J.* **5** (1953), 117–146.

- [Gr2] O. Grün, Über das direkte Produkt regulärer p -Gruppen, *Arch. Math.* **5** (1954), 241–243.
- [Gr3] O. Grün, Eine obere Grenze für die Klasse einer h -stufigen p -Gruppe, *Abh. Math. Sem. Univ. Hamburg* **21** (1957), 90–91.
- [Gr4] O. Grün, Einige Sätze über Automorphismen abelscher p -Gruppen, *Abh. Math. Sem. Univ. Hamburg* **24** (1960), 54–58.
- [HalM] M. Hall, *The Theory of Groups*, Macmillan, New York, 1959.
- [HS] M. Hall and J. K. Senior, *On Groups of Order 2^n , ($n \leq 6$)*, Macmillan, New York, 1964.
- [Hall1] P. Hall, A contribution to the theory of groups of prime power order, *Proc. London Math. Soc.* **36** (1933), 29–95.
- [Hall2] P. Hall, On a theorem of Frobenius, *Proc. London Math. Soc.* **40** (1936), 468–501.
- [Hall3] P. Hall, The classification of prime power groups, *J. reine angew. Math.* **182** (1940), 130–141.
- [Hall4] P. Hall, *Nilpotent Groups*, Can. Math. Congr., Alberta, 1957.
- [Hall5] P. Hall, On groups of automorphisms, *J. Math.* **182** (1940), 194–204.
- [Hall6] P. Hall, Some sufficient conditions for a group to be nilpotent, *Illinois J. Math.* **2** (1958), 787–801.
- [Hall7] P. Hall, Verbal and marginal subgroups, *J. reine angew. Math.* **182** (1940), 156–167.
- [HH] P. Hall and G. Higman, On the p -length of p -solvable groups and the reduction theorems for Burnside's problem, *Proc. London Math. Soc.* **(3) 6** (1956), 1–42.
- [Han] A. Hanaki, A condition on lengths of conjugacy classes and character degrees, *Osaka J. Math.* **33** (1996), 207–216.
- [Har] K. Harada, On some 2-groups of normal 2-rank 2, *J. Algebra* **20** (1972), no. 1, 90–93.
- [Harr] M. E. Harris, On decomposing an abelian p -group under a p' -operator group, *Algebra Colloquium* **7** (2000), 291–294.
- [Haw] T. O. Hawkes, On the automorphism group of a 2-group, *Proc. London Math. Soc.* **26** (1973), 207–225.
- [HMH] P. Hegarty and D. MacHale, Two-groups in which an automorphism inverts precisely half of elements, *Bull. London Math. Soc.* **30** (1998), 129–135.
- [Hei1] H. Heineken, Gruppen mit kleinen abelschen Untergruppen, *Arch. Math.* **29** (1977), 20–31.
- [Hei2] H. Heineken, Über ein Levisches Nilpotenzkriterium, *Arch. Math.* **12** (1961), 176–178.
- [Hei3] H. Heineken, Nilpotente Gruppen, deren sämtliche Normalteiler charakteristisch sind, *Arch. Math.* **33** (1979/80), 497–503.
- [Hei4] H. Heineken, Bounds for the nilpotency class of a group, *J. London Math. Soc.* **37** (1962), 456–458.
- [HL1] H. Heineken and H. Liebeck, On p -groups with odd order automorphism groups, *Arch. Math.* **24** (1973), 465–471.
- [Hel1] G. T. Helleloid, A survey of automorphism groups of finite p -groups, arXiv.mathGR/0610294 v2 25 Oct 2006, 1–20.

- [Hel2] G. T. Helleloid, *Automorphism groups of finite p -groups: structure and applications*, PhD Thesis, Stanford Univ., 2007.
- [HelM] G. T. Helleloid and U. Martin, The automorphism group of a finite p -group is almost always a p -group, *J. Algebra* **312** (2007), 294–329 (see also arXiv.mathGR/0602039 v5 Oct 2006, 1–38).
- [Herz] M. Herzog, Counting group elements of order p modulo p^2 , *Proc. Amer. Math. Soc.* **66** (1977), 247–250.
- [HK] M. Herzog and G. Kaplan, Large cyclic subgroups contain non-trivial normal subgroups, *J. Group Theory* **4** (2001), 247–253.
- [HKL] M. Herzog, G. Kaplan and A. Lev, On the commutator and the center of finite groups, *J. Algebra* **278** (2004), 494–501.
- [HLMM] M. Herzog, P. Longobardi, M. Maj and A. Mann, On generalized Dedekind groups and Tarski super monsters, *J. Algebra* **226** (2000), 690–613.
- [Het] L. Hethelyi, On powerful normal subgroups of a p -group, *Monatsh. Math.* **130** (2000), 201–209.
- [HL] L. Hethelyi and L. Levai, On elements of order p in powerful p -groups, *J. Algebra* **270** (2003), 1–6.
- [Hig1] G. Higman, Suzuki 2-groups, *Illinois J. Math.* **7** (1963), 79–96.
- [Hig2] G. Higman, Enumerating p -groups, I, inequalities, *Proc. London Math. Soc.* **10** (1960), 24–30.
- [Hig3] G. Higman, Enumerating p -groups, II, Problems whose solution is PORC, *Proc. London Math. Soc.* **10** (1960), 566–582.
- [Hob1] C. Hobby, The Frattini subgroup of a p -group, *Pacific J. Math.* **10** (1960), 209–211.
- [Hob2] C. Hobby, A characteristic subgroup of a p -group, *Pacific J. Math.* **10** (1960), 853–858.
- [Hob3] C. Hobby, Generalizations of a theorem of N. Blackburn on p -groups, *Illinois J. Math.* **5** (1961), 225–227.
- [Hob4] C. Hobby, The derived series of a finite p -group, *Illinois J. Math.* **5** (1961), 228–233.
- [Hob5] C. Hobby, Nearly regular p -groups, *Can. J. Math.* **19** (1967), 520–522.
- [HW] C. Hobby and C. R. B. Wright, A generalization of a theorem of N. Ito on p -groups, *Proc. Amer. Math. Soc.* **1** (1960), 707–709.
- [HogK] G. T. Hogan and W. P. Kappe, On the H_p -problem for finite p -groups, *Proc. Amer. Math. Soc.* **20** (1969), 450–454.
- [Hop1] C. Hopkins, Metabelian groups of order p^m , $p > 2$, *Trans. Amer. Math. Soc.* **37** (1935), 161–195.
- [Hop2] C. Hopkins, Non-abelian groups whose groups of automorphisms are abelian, *Ann. Math.* **29** (1927/28), 508–520.
- [Hua] L. K. Hua, Some “Anzahl” theorems for groups of prime power order, *Sci. Rep. Nat. Tsing Hua Univ.* **4** (1947), 313–327.
- [HT1] L. K. Hua and H. F. Tuan, Determination of the groups of odd-prime-power order p^n which contain a cyclic subgroup of index p^2 , *Sci. Rep. Nat. Tsing. Hua Univ. A* **4** (1940), 145–154.

- [HT2] L. K. Hua and H. F. Tuan, Some “Anzahl” theorems for groups of prime-power orders, *J. Chinese Math.* **2** (1940), 313–319.
- [HT] D. R. Hughes and J. G. Thompson, The H_p -problem and the structure of H_p -groups, *Pacif. J. Math.* **9** (1959), 1097–1101.
- [Hug] N. J. S. Hughes, The structure and order of the group of central automorphisms of a finite group, *Proc. London Math. Soc.* **53** (1951), 377–385.
- [Hum] K. Hummel, The order of the automorphism group of a central product, *Proc. Amer. Math. Soc.* **47** (1975), 37–40.
- [Hup1] B. Huppert, *Endliche Gruppen*, Band 1, Springer, Berlin, 1967.
- [Hup2] B. Huppert, Über das Produkt von paarweise vertauschbaren zyklischen Gruppen, *Math. Z.* **58** (1953), 243–264.
- [HupB] B. Huppert and N. Blackburn, *Finite Groups II*, Springer, Berlin, 1982.
- [HupM] B. Huppert and O. Manz, Orbit sizes of p -groups, *Arch. Math.* **54** (1990), 105–110.
- [Isa1] I. M. Isaacs, *Character Theory of Finite Groups*, Acad. Press, N.Y., 1976.
- [Isa2] I. M. Isaacs, An alternate proof of the Thompson replacement theorem, *J. Algebra* **15** (1970), 149–150.
- [Isa3] I. M. Isaacs, The number of generators of a linear p -group, *Can. J. Math.* **24** (1972), 852–858.
- [Isa4] I. M. Isaacs, Sets of p -powers as irreducible character degrees, *Proc. Amer. Math. Soc.* **96** (1986), 551–552.
- [Isa5] I. M. Isaacs, *Algebra: A Graduate Course*, Brooks/Cole, 1994.
- [Isa6] I. M. Isaacs, Commutators and commutator subgroup, *Amer. Math. Monthly* **84** (1977), 720–722.
- [Isa7] I. M. Isaacs, Automorphisms fixing elements of prime order in finite groups, *Arch. Math.* **68** (1997), 359–366.
- [Isa8] I. M. Isaacs, Equally partitioned groups, *Pacific J. Math.* **49** (1973), 109–116.
- [Isa9] I. M. Isaacs, Normal subgroups and nonabelian quotients in p -groups, *J. Algebra* **247** (2002), 231–243.
- [Isa10] I. M. Isaacs, Recovering information about a group from its complex group algebra, *Arch. Math.* **47** (1986), 293–295.
- [Isa11] I. M. Isaacs, Characters of groups associated with finite algebras, *J. Algebra* **177** (1995), 708–730.
- [Isa12] I. M. Isaacs, Groups with many equal classes, *Duke Math. J.* **37** (1970), 501–506.
- [Isa13] I. M. Isaacs, Coprime group actions fixing all nonlinear irreducible characters, *Can. J. Math.* **41**, **1** (1989), 68–82.
- [Isa14] I. M. Isaacs, Large orbits in nilpotent action, *Proc. Amer. Math. Soc.* **127** (1999), 45–50.
- [IsM] I. M. Isaacs and A. Moreto, The character degrees and nilpotence class of a p -group, *J. Algebra* **238** (2001), 827–842.
- [INW] I. M. Isaacs, G. Navarro, T. R. Wolf, Finite group elements where no irreducible character vanishes, *J. Algebra* **222** (1999), 413–423.

- [IsP1] I. M. Isaacs and D. S. Passman, A characterization of groups in terms of the degrees of their characters I, *Pacific J. Math.* **15** (1965), 877–903; II, ibid. **24** (1968), 467–510.
- [IsP2] I. M. Isaacs and D. S. Passman, Half-transitive automorphism groups, *Can. J. Math.* **18** (1966), 1243–1250.
- [IsR] I. M. Isaacs and G. R. Robinson, On a theorem of Frobenius: solutions of $x^n = 1$ in finite groups, *Amer. Math. Monthly* **99** (1992), 352–354.
- [IsS] I. M. Isaacs and M. C. Slattery, Character degree sets that do not bound the class of a p -group, *Proc. Amer. Math. Soc.* **129** (2002), 119–123.
- [Ish] K. Ishikawa, On finite p -groups which have only two conjugacy lengths, *Isr. J. Math.* **129** (2002), 119–123.
- [Ito1] N. Ito, On the degrees of irreducible representations of a finite group, *Nagoya Math. J.* **3** (1951), 5–6.
- [Ito2] N. Ito, On finite groups with given conjugate types, I, *Nagoya Math. J.* **6** (1953), 17–28.
- [Ito3] N. Ito, *Lectures on Frobenius and Zassenhaus Groups*, Chicago, 1969.
- [Ito4] N. Ito, On a theorem of L. Rédei and J. Szep concerning p -groups, *Acta Sci. Math. Szeged* **14** (1952), 186–187.
- [Ito5] N. Ito, Note on p -groups, *Nagoya Math. J.* **1** (1950), 113–116.
- [Ito6] N. Ito, Über das Produkt von zwei zyklischen 2-Gruppen, *Publ. Math. Debrecen* **4** (1956), 517–520.
- [Ito7] N. Ito, Über das Produkt von zwei abelschen Gruppen, *Math. Z.* **62** (1955), 400–401.
- [Ito8] N. Ito, A conjecture on p -groups, manuscript.
- [Ito9] N. Ito, On Hadamard 2-groups, manuscript.
- [IM] N. Ito and A. Mann, Counting classes and characters of groups of prime exponent, *Israel J. Math.* **156** (2006), 205–220.
- [IO] N. Ito and A. Ohara, Sur les groupes factorisables par deux 2-groupes cycliques, I, II, *Proc. Japan Acad.* **32** (1956), 736–743.
- [Iwa] K. Iwasawa, Über die endlichen Gruppen und die Verbände ihrer Untergruppen, *J. Univ. Tokyo* **4** (1941), 171–199.
- [Jai] A. Jaikin-Zapirain, On almost regular automorphisms of finite p -groups, *Adv. Math.* **153** (2000), 391–402.
- [JNOB] R. James, M. F. Newman and E. A. O'Brien, The groups of order 128, *J. Algebra* **129** (1990), 136–158.
- [Jam] R. James, 2-groups of almost maximal class, *J. Austral. Math. Soc. (Ser. A)* **19** (1975), 343–357; corrigendum, ibid **35** (1983), 307.
- [Jan1] Z. Janko, Finite 2-groups with small centralizer of an involution, *J. Algebra* **241** (2001), 818–826.
- [Jan2] Z. Janko, Finite 2-groups with small centralizer of an involution, 2, *J. Algebra* **245** (2001), 413–429.
- [Jan3] Z. Janko, Bemerkung über eine Arbeit von N. Ito, *Glasnik Mat.-Fiz. Astronom. Drustvo Mat. Fiz. Hrvatske Ser. II* **11** (1961), 75–77.

- [Jan4] Z. Janko, A theorem on nilpotent groups, *Glasnik Mat.-Fiz. Astronom. Drustvo Mat. Fiz. Hrvatske Ser. II* **115** (1960), 247–249.
- [Jan5] Z. Janko, Finite 2-groups with no normal elementary abelian subgroups of order 8, *J. Algebra* **246** (2001), 951–961.
- [Jan6] Z. Janko, Finite 2-groups with a self centralizing elementary abelian subgroup of order 8, *J. Algebra* **269** (2003), 189–214.
- [Jan7] Z. Janko, Finite 2-groups G with $|\Omega_2(G)| = 16$, *Glas. Mat.* **40**(60) (2005), 71–86.
- [Jan8] Z. Janko, Finite 2-groups with exactly four cyclic subgroups of order 2^n , *J. reine angew. Math.* **566** (2004), 135–181.
- [Jan9] Z. Janko, Minimal nonmodular p -groups, *Glas. Mat.* **39** (2004), 221–233.
- [Jan10] Z. Janko, 2-groups with self-centralizing subgroup of type (4, 2), *Glas. Mat.* **39** (2004), 235–243.
- [Jan11] Z. Janko, Elements of order at most 4 in finite 2-groups, *J. Group Theory* **7** (2004), 431–436.
- [Jan12] Z. Janko, The structure of the Burnside group of order 2^{12} , manuscript.
- [Jan13] Z. Janko, Nonmodular quaternion-free 2-groups, *Israel J. Math.* **154** (2006), 157–184.
- [Jan14] Z. Janko, On maximal cyclic subgroups in finite p -groups, *Math. Z.* **254** (2006), 29–31.
- [Jan15] Z. Janko, Minimal non-quaternion-free finite 2-groups, *Israel J. Math.* **154** (2006), 185–189.
- [Jan16] Z. Janko, A classification of finite 2-groups with exactly three involutions, *J. Algebra* **291** (2005), 505–533.
- [Jan17] Z. Janko, Elements of order at most 4 in finite 2-groups 2, *J. Group Theory* **8** (2005), 683–686.
- [Jan18] Z. Janko, Finite p -groups with a uniqueness condition for non-normal subgroups, *Glas. Mat.* **40**(60) (2005), 235–240.
- [Jan19] Z. Janko, Finite 2-groups all of whose nonabelian subgroups are generated by involutions, *Math. Z.* **252** (2006), 419–420.
- [Jan20] Z. Janko, On finite 2-groups generated with three involutions, manuscript.
- [Jan21] Z. Janko, Finite p -groups with $\Omega_2^*(G)$ is metacyclic, *Glas. Mat.* **41**(61) (2006), 71–76.
- [Jan22] Z. Janko, New results in the theory of finite p -groups, *Cont. Math.* **402**, 193–195.
- [Jan23] Z. Janko, Nonabelian 2-groups in which any two noncommuting elements generate a group of maximal class, *Glas. Mat.* **41**(61) (2006), 271–274.
- [Jan24] Z. Janko, On maximal abelian subgroups in finite p -groups, *Math. Z.* **258** (2008), 629–635.
- [Jan25] Z. Janko, Finite nonabelian 2-groups all of whose minimal nonabelian subgroups are of exponent 4, *J. Algebra* **315** (2007), 801–808.
- [Jan26] Z. Janko, Finite 2-groups with exactly one nonmetacyclic maximal subgroup, *Israel J. Math.* (2008), to appear.
- [Jan27] Z. Janko, Finite 2-groups all of whose maximal cyclic subgroups of composite order are self-centralizing, *J. Group Theory* **10** (2007), 1–4.

- [Jan28] Z. Janko, Cyclic subgroups of order 4 in finite 2-groups, *Glas. Mat.* **46**(62) (2007), 345–355.
- [Jan29] Z. Janko, Some peculiar minimal situations by finite p -groups, *Glas. Mat.* (2008), to appear.
- [Jan30] Z. Janko, On minimal nonabelian subgroups of p -groups, *J. Group Theory* (2008), to appear.
- [Jan31] Z. Janko, Some exceptional minimal situations by finite p -groups, in: *Ischia Group Theory 2008*, to appear.
- [Joh] D. L. Johnson, A property of finite p -groups with trivial multiplicator, *Amer. J. Math.* **98** (1976), 105–108.
- [JonK1] D. Jonah and M. W. Konvisser, Abelian subgroups of p -groups, an algebraic approach, *J. Algebra* **34** (1975), 386–402.
- [JKon2] D. Jonah and M. W. Konvisser, Some nonabelian p -groups with abelian automorphism groups, *Arch. Math.* **26** (1975), 131–133.
- [Jon1] M. R. Jones, Multiplicators of p -groups, *Math. Z.* **127** (1972), 165–166.
- [Jon2] M. R. Jones, A property of finite p -groups with trivial multiplicators, *Trans. Amer. Math. Soc.* **210** (1975), 179–183.
- [Kal] L. Kaloujnine, La structure des p -groupes de Sylow des groupes symétriques finis, *Ann. Sci. Ecole Norm. Supér.* **65** (1968), 239–276.
- [Kal2] L. Kaloujnine, Zum Problem der Klassifikation der endlichen metabelschen p -Gruppen, *Wiss. Z. Humboldt-Univ. Berlin, Math.-Nat. Reihe* **4** (1955), 1–7.
- [Kar] G. Karpilovsky, *Group Representations*, vol. 2, North-Holland, Amsterdam, 1993.
- [Kaz1] L. S. Kazarin, Groups with certain conditions for normalizers of subgroups, *Uchen. zapiski Perm Univ.* **218** (1969), 268–279 (in Russian).
- [Kaz2] L. S. Kazarin, On some classes of finite groups, *Soviet Math. Dokl.* **12** (1971), no. 2, 549–553 (in Russian).
- [Kaz3] L. S. Kazarin, Groups with restrictions on normalizers of subgroups, *Izv. vuzov (mathematics)*, **2** (1973), 41–50 (in Russian).
- [Kaz4] L. S. Kazarin, On product of two nilpotent groups, *Questions of group theory and homological algebra* (1981), 62–66; II, ibid (1982), 47–49 (in Russian).
- [Kaz5] L. S. Kazarin, On groups with factorization, *Soviet Math. Dokl.* **23** (1981), no. 1, 19–22 (in Russian).
- [Keg] O. H. Kegel, Die Nilpotenz der H_p -Gruppen, *Math. Z.* **75** (1960), 373–376.
- [Khu] E. I. Khukhro, *Nilpotent Groups and their Automorphisms*, Walter de Gruyter, Berlin, 1993.
- [Kim1] I. Kiming, Some remarks on a certain class of finite p -groups, *Math. Scand.* **76** (1995), 35–49.
- [Kim] I. Kiming, Structure and derived length of finite p -groups possessing an automorphism of p -power order having exactly p fixed points, *Math. Scand.* **62** (1988), 153–172.
- [Kin1] B. W. King, Normal subgroups of groups of prime-power order, in: *Proc. 2nd Int. Conf. Theory Groups*, pp. 401–408, Lecture Notes in Math. 372, Springer, Berlin, 1973.

- [Kin2] B. W. King, Normal structure of p -groups, *Bull. Aust. Math. Soc.* **10** (1974), 317–318.
- [Klu] F. L. Kluempen, The power structure of 2-generator 2-groups of class two, *Algebra Colloq.* **9**, 3 (2002), 287–302.
- [Kno] H. G. Knoche, Über den Frobeniusschen Klassenbegriff in nilpotenten Gruppen, I,II, *Math. Z.* **55** (1951), 71–83; ibid **59** (1953), 8–16.
- [Kon1] M. W. Konvisser, Embedding of abelian subgroups in p -groups, *Trans. Amer. Math. Soc.* **153** (1971), 469–481.
- [Kon2] M. W. Konvisser, 2-groups which contain exactly three involutions, *Math. Z.* **130** (1973), 19–30.
- [Kon3] M. W. Konvisser, Metabelian p -groups which contain a self-centralizing element, *Illinois J. Math.* **14** (1970), 650–657.
- [KonJ] M. W. Konvisser and D. Jonah, Counting abelian subgroups of p -groups. A projective approach, *J. Algebra* **34** (1975), 309–330.
- [KovN] L. G. Kovacs and M. F. Newman, Direct complementation in groups with operators, *Arch. Math.* **13** (1962), 427–433.
- [KLG] L. G. Kovacs and C. R. Leedham-Green, Some normally monomial p -groups of maximal class and large derived length, *Quart. J. Math. (2)* **37** (1986), 49–54.
- [KM] J. Krempa and I. Malinowska, Groups of p -automorphisms for finite p -groups, *Publ. Math. Debrecen* **61** (2002), no. 3–4, 495–509.
- [Kul] A. Kulakoff, Über die Anzahl der eigentlichen Untergruppen und der Elemente von gegebener Ordnung in p -Gruppen, *Math. Ann.* **104** (1931), 779–793.
- [KS] H. Kurzweil und B. Stellmacher, *Theorie der endlichen Gruppen. Eine Einführung*, Springer, 1998.
- [Laf1] T. J. Laffey, The minimum number of generators of a finite p -group, *Bull. London Math. Soc.* **5** (1973), 288–290.
- [Laf2] T. J. Laffey, Bounding the order of a finite p -group, *Proc. R. Ir. Acad. 80a* **2** (1980), 131–134.
- [Laf3] T. J. Laffey, A lemma on finite p -groups and some consequences, *Proc. Camb. Philos. Soc.* **75** (1974), 133–137.
- [Laf4] T. J. Laffey, Centralizers of elementary abelian subgroups in finite p -groups, *J. Algebra* **51** (1978), 88–96.
- [Laf5] T. J. Laffey, The number of solutions of $x^3 = 1$ in a 3-group, *Math. Z.* **149** (1976), no. 1, 43–45.
- [Lam1] T.-Y. Lam, Artin exponent of finite groups, *J. Algebra* **9** (1968), 94–119.
- [Lam2] T.-Y. Lam, On the number of solutions of $x^{p^k} = a$ in a p -group, *Illinois J. Math.* **32** (1988), 575–583.
- [Lan] G. L. Lange, Two-generator Frattini subgroups of finite groups, *Israel J. Math.* **29** (1978), 357–360.
- [LGMK] C. R. Leedham-Green and S. McKay, *The Structure of Groups of Prime Power Order*, London Mathematical Monographs, New Series, Oxford Science Publications, Oxford Univ. Press, Oxford, 2002.

- [LGNW] C. R. Leedham-Green, P. M. Neumann and J. Wiegold, The breadth and the class of a finite p -group, *J. London Math. Soc.* (2) **1** (1969), 409–420.
- [Leo] A. Leone, Finite minimal non-KC-groups, *Matematiche* **38** (1987), 191–200.
- [Leong1] Y. K. Leong, Finite 2-groups of class two with cyclic centre, *J. Aust. Math. Soc. Ser. A* **27** (1979), 125–140.
- [Leong2] Y. K. Leong, Odd order nilpotent groups of class two with cyclic centre, *J. Aust. Math. Soc.* **17** (1974), 142–153.
- [Lev] F. W. Levi, Groups in which the commutator operations satisfy certain algebraic conditions, *J. Indian Math. Soc.* **6** (1942), 87–97.
- [Li1] Li Shirong, The structure of NC-groups, *J. Algebra* **241** (2001), 611–619.
- [Li2] Li Shirong, Finite 2-groups with large centralizers of abelian subgroups, *Math. Proc. Roy. Irish Acad.* **A104** (2004), no. 2, 191–197.
- [Li3] Li Shirong, The number of conjugacy classes of nonnormal cyclic subgroups in nilpotent groups of odd order, *J. Group Theory* **1** (1998), 165–171.
- [Lie1] H. Liebeck, A note on prime-power groups with symmetrical generating relations, *Proc. Cambridge Philos. Soc.* **51** (1955), 594–595.
- [Lie2] H. Liebeck, The automorphism group of a finite p -group, *J. Algebra* **4** (1966), 426–432.
- [Lie3] H. Liebeck, Outer automorphisms in nilpotent groups of class 2, *J. London Math. Soc.* **40** (1965), 268–275.
- [LM] P. Longobardi and M. Maj, On p -groups of breadth two, *Algebra Colloq.* **6** (1999), 121–124.
- [LMM] P. Longobardi, M. Maj and A. Mann, Minimal classes and maximal class in p -groups, *Israel J. Math.* **110** (1999), 93–102.
- [LubM] A. Lubotzky and A. Mann, Powerful p -groups 1, *J. Algebra* **105** (1987), 484–505.
- [Macd1] I. D. Macdonald, Generalizations of a classical theorem on nilpotent groups, *Illinois J. Math.* **8** (1964), 556–570.
- [Macd2] I. D. Macdonald, A question of C.R. Hobby on regular p -groups, *Proc. Edin. Math. Soc.* (2) **18** (1973), 207–208.
- [Macd3] I. D. Macdonald, Commutators and their products, *Amer. Math. Monthly* **93** (1986), 440–444.
- [Macd4] I. D. Macdonald, Finite p -groups with unique maximal classes, *Proc. Edinburgh Math. Soc.* **26** (1983), 233–239.
- [Macd5] I. D. Macdonald, The breadth of finite p -groups. I, *Proc. Roy. Soc. Edinburgh* **A78** (1978), 1–39.
- [Macd6] I. D. Macdonald, Groups of breadth four have class five, *Glasgow Math. J.* **19** (1978), 141–148.
- [Macd7] I. D. Macdonald, Computer results on Burnside groups, *Bull. Aust. Math. Soc.* **9** (1973), 433–438.
- [Macd8] I. D. Macdonald, Solution of the Hedges problem for finite groups of class $2p - 2$, *Proc. Amer. Math. Soc.* **27** (1971), 39–42.

- [Macd9] I. D. Macdonald, Some examples in the theory of groups, in: *Mathematical Essays dedicated to A. J. Macintyre*, pp. 263–269, Ohio Univ. Press, Athens, Ohio, 1970.
- [Macd10] I. D. Macdonald, On cyclic commutator subgroups, *J. London Math. Soc.* **38** (1963), 419–422.
- [Macd12] I. D. Macdonald, On central series, *Proc Edinburgh Math. Soc. (2)* **3** (1962/63), 175–178.
- [MacW] A. R. MacWilliams, On 2-groups with no normal abelian subgroup of rank 3 and their occurrence as Sylow 2-subgroups of finite simple groups, *Trans. Amer. Math. Soc.* **150** (1970), 345–408.
- [Mal1] I. Malinowska, Finite p -groups with few automorphisms, *J. Group Theory* **4** (2001), 395–400.
- [Mal2] I. Malinowska, p -automorphisms of finite p -groups: problems and questions, in: *Advances in Group Theory* (2002), pp. 111–127, Napoli, Italy, 2002.
- [Mal3] I. Malinowska, On quasi-inner automorphisms of a finite p -group, *Publ. Math. Debrecen* **41** (1992), 73–77.
- [Mal4] I. Malinowska, On automorphism groups of finite p -groups, *Rend. Sem. Mat. Univ. Padova* **91** (1994), 265–271.
- [Man1] A. Mann, Generators of 2-groups, *Israel J. Math.* **10** (1971), 158–159.
- [Man2] A. Mann, Regular p -groups, I, *Israel J. Math.* **10** (1971), 471–477.
- [Man3] A. Mann, Regular p -groups, II, *Israel J. Math.* **14** (1973), 294–303.
- [Man4] A. Mann, Regular p -groups, III, *J. Algebra* **70** (1981), 89–101.
- [Man5] A. Mann, The power structure of p -groups I, *J. Algebra* **42** (1976), 121–135; II, ibid **318** (2007), 953–956.
- [Man6] A. Mann, Regular p -groups and groups of maximal class, *J. Algebra* **42** (1976), 136–141.
- [Man7] A. Mann, Conjugacy classes in finite groups, *Israel J. Math.* **31** (1978), 78–84.
- [Man8] A. Mann, Groups with small abelian subgroups, *Arch. Math.* **50** (1988), 210–213.
- [Man9] A. Mann, Extreme elements of finite p -groups, *Rend. Sem. Mat. Univ. Padova* **83** (1990), 45–54.
- [Man10] A. Mann, On p -groups whose maximal subgroups are isomorphic, *J. Aust. Math. Soc. A* **59** (1995), 143–147.
- [Man11] A. Mann, The number of generators of finite p -groups, *J. Group Theory* **8** (2005), 317–337.
- [Man12] A. Mann, Minimal characters of p -groups, *J. Group Theory* **2** (1999), 225–250.
- [Man13] A. Mann, On the splitting of extensions by a group of prime order, *Arch. Math.* **56** (1991), 105–106.
- [Man14] A. Mann, Some finite groups with large conjugacy classes, *Israel J. Math.* **71** (1990), 55–63.
- [Man15] A. Mann, Generators of p -groups, in: *Proceedings of Groups – St. Andrews 1985*, pp. 273–281, Cambridge, 1986.
- [Man16] A. Mann, Some applications of powerful p -groups, *Proceedings of Groups – St. Andrews 1989*, pp. 370–385, Cambridge, 1991.

- [Man17] A. Mann, A transfer result for powerful Sylow subgroups, *J. Algebra* **178** (1995), 299–301.
- [Man18] A. Mann, Finite groups with maximal normalizers, *Illinois J. Math.* **12** (1968), 67–75.
- [Man19] A. Mann, Enumerating finite groups and their defining relations, *J. Group Theory* **1** (1998), 59–64.
- [Man20] A. Mann, Some questions about p -groups, *J. Aust. Math. Soc. (Series A)* **67** (1999), 356–379.
- [Man21] A. Mann, The derived length of p -groups, *J. Algebra* **224** (2000), 263–267.
- [Man22] A. Mann, Finite p -Groups, in preparation.
- [Man23] A. Mann, Groups generated by elements of small breadth, *J. Group Theory* **4** (2001), 241–246.
- [Man24] A. Mann, On the power structure of some p -groups, *Circ. Mat. Palermo II* **23** (1990), 227–235.
- [Man25] A. Mann, Groups with few class sizes and the centralizer equality subgroup, *Isr. J. Math.* **142** (2004), 367–380.
- [Man26] A. Mann, Philip Hall’s ‘rather curious’ formula for abelian p -groups, *Israel J. Math.* **96B** (1996), 445–448.
- [Man27] A. Mann, An inequality for group presentations, *Bull. Aust. Math. Soc.* **62** (2000), 467–469.
- [Man28] A. Mann, A remark on class sizes in 2-groups, manuscript.
- [Man29] A. Mann, On characters-classes duality and orders of centralizers, *Cont. Math.* **402** (2006), 215–217.
- [Man30] A. Mann, Normally monomial p -groups, *J. Algebra* **300** (2006), 2–9.
- [Man31] A. Mann, On the exponent of the product of two groups, *Rend. Sem. Mat. Univ. Padova* **115** (2006), 205–207.
- [Man32] A. Mann, Elements of minimal breadth in finite p -groups and Lie algebras, *J. Aust. Math. Soc.* **81** (2006), 209–214.
- [MM] A. Mann and C. Martinez, The exponent of finite groups, *Arch. Math.* **67** (1996), 8–10.
- [MS] A. Mann and C. Scoppola, On p -groups of Frobenius type, *Arch. Math.* **56** (1991), 320–332.
- [Mat] S. Mattarei, An example of p -groups with identical character tables and different derived lengths, *Arch. Math.* **62** (1994), 12–20.
- [Maz] V. D. Mazurov, 2-groups with an automorphism of odd order fixing all involutions, *Algebra and Logika* **8** (1969), no. 6, 874–885 (in Russian).
- [McK] S. McKay, *Finite p -Groups*, Queen Mary Math. Notes 18, London, 2000.
- [McKel] A. M. McKelven, Groups of order 2^m that contain cyclic subgroups of order 2^{m-3} , *Amer. Math. Monthly* **13** (1906), 121–136.
- [Men] F. Menegazzo, Automorphisms of p -groups with cyclic commutator subgroup, *Rend. Sem. Mat. Padova* **90** (1993), 81–101.
- [Mie1] R. J. Miech, Metabelian p -groups of maximal class, *Trans. Amer. Math. Soc.* **152** (1970), 331–373.

- [Mie2] R. J. Miech, On p -groups with a cyclic commutator subgroup, *J. Aust. Math. Soc.* **20** (1975), 178–198.
- [Mie3] R. J. Miech, The metabelian p -groups of maximal class, *Trans. Amer. Math. Soc.* **236** (1978), 93–119.
- [Mie4] R. J. Miech, The metabelian p -groups of maximal class, II, *Trans. Amer. Math. Soc.* **272** (1982), 465–484.
- [Mil1] G. A. Miller, An extension of Sylow's theorem, *Proc. London Math. Soc. (2)* **2** (1904), 142–143.
- [Mil2] G. A. Miller, Number of abelian subgroups in every prime power group, *Amer. J. Math.* **51** (1929), 31–34.
- [Mil3] G. A. Miller, A nonabelian group whose group of isomorphisms is abelian, *Messenger Math.* **43** (1913), 124–125 (or G. A. Miller, *Collected Works*, vol. 5, 415–417).
- [Mil4] G. A. Miller, On the groups of order p^m which contain operators of order p^{m-2} , *Trans. Amer. Math. Soc.* **26** (1902), 383–387.
- [Mil5] G. A. Miller, Isomorphisms of a group whose order is a power of a prime, *Trans. Amer. Math. Soc.* **12** (1911), 387–402.
- [Mil6] G. A. Miller, The groups of order p^m which contain exactly p cyclic subgroups of order p^α , *Trans. Amer. Math. Soc.* **7** (1906), 228–232.
- [Mil7] G. A. Miller, Determination of all the groups of order 2^m which contain an odd number of cyclic subgroups of composite order, *Trans. Amer. Math. Soc.* **6** (1905), 58–62.
- [Mil8] G. A. Miller, On the holomorph of the cyclic group of order p^m , *Trans. Amer. Math. Soc.* **9** (1908), 232–236.
- [Mil9] G. A. Miller, The groups in which every subgroup is either abelian or Hamiltonian, *Trans. Amer. Math. Soc.* **8** (1907), 25–29.
- [MilM] G. A. Miller and H. Moreno, Non-abelian groups in which every subgroup is abelian, *Trans. Amer. Math. Soc.* **4** (1903), 398–404.
- [Mill] W. H. Mills, The automorphisms of the holomorph of a finite abelian group, *Trans. Amer. Math. Soc.* **85** (1956), 1–34.
- [MLC] E. Morgado Morales and M. Lazo Cortis, On the Sylow p -groups of the automorphism group of a finite homocyclic p -group, *Rev. Cienc. Mat.* **6** (1985), 35–44 (in Spanish).
- [Mori1] M. Morigi, A note on factorized (finite) p -groups, *Rend. Sem. Math. Univ. Padova* **98** (1997), 101–105.
- [Mori2] M. Morigi, Power automorphisms of finite p -groups, *Comm. Algebra* **70** (1999), 4853–4877.
- [Mori3] M. Morigi, On the minimal number of generators of finite non-abelian p -groups having an abelian automorphism group, *Comm. Algebra* **23** (1995), 2045–2064.
- [Mori4] M. Morigi, On p -groups with abelian automorphism group, *Rend. Sem. Mat. Univ. Padova* **92** (1994), 47–58.
- [Nak1] K. Nakamura, Über den Quasinormalteiler der regulären p -Gruppe von der Klasse 2, *Nagoya Math. J.* **26** (1966), 61–67.
- [Nak2] K. Nakamura, Über einige Beispiele der Quasinormalteiler einer p -Gruppe, *Nagoya Math. J.* **31** (1968), 97–103.

- [Nap1] F. Napolitani, Sui p -gruppi modulari finiti, *Rend. Sem. Mat. Univ. Padova* **39** (1967), 296–303.
- [Nap2] F. Napolitani, Gruppi finite minimal non-modulari, *Rend. Sem. Mat. Univ. Padova* **45** (1971), 229–248.
- [Nei] L. I. Neikirk, Groups of order p^m which contain cyclic subgroups of order p^{m-3} , *Trans. Amer. Math. Soc.* **6** (1905), 316–325.
- [Nek1] K. G. Nekrasov, On finite 2-groups with small Frattini subgroup, in: *Logical-Algebraic Constructions*, pp. 75–82, Tver, 1992 (in Russian).
- [Nek2] K. G. Nekrasov, On some 2-groups with a small noncyclic Frattini subgroup, in: *Algebraic and Logical Constructions*, pp. 53–65, Tver, 1994 (in Russian).
- [NekB] K. G. Nekrasov and Y. Berkovich, Necessary and sufficient condition for cyclicity of the Frattini subgroup of a finite p -group, in: *Questions of Group Theory and Homological Algebra*, pp. 35–37, Yaroslavl, 1985 (in Russian).
- [Neu] B. H. Neumann, On some finite groups with trivial multiplicator, *Publ Math. Debrecen* **4** (1955), 190–194.
- [NO] M. F. Newman and E. A. O'Brien, Classifying 2-groups by coclass, *Trans. Amer. Math. Soc.* **351** (1999), 131–169.
- [Nin] Y. Ninomiya, Finite p -groups with cyclic subgroups of index p^2 , *Math. J. Okayama Univ.* **36** (1994), 1–21.
- [Ols] A. Y. Olshanski, The number of generators and orders of abelian subgroups of finite p -groups, *Math. Notes* **23** (1978), 183–185.
- [Ott] A. D. Otto, Central automorphisms of a finite p -group, *Trans. Amer. Math. Soc.* **125** (1966), 280–287.
- [PS] P. P. Palfy and M. Szalay, The distribution of the character degrees of the symmetric p -groups, *Acta Math. Hung.* **41** (1983), 137–150.
- [PR] C. Parker and P. Rowley, *Symplectic Amalgams*, Springer, Berlin, 2002.
- [PS1] G. Parmeggiani and B. Stellmacher, p -groups of small breadth, *J. Algebra* **213** (1999), 52–68.
- [Pas] D. S. Passman, Nonnormal subgroups of p -groups, *J. Algebra* **15** (1970), no. 3, 352–370.
- [Pat1] A. R. Patterson (=MacWilliams), On Sylow 2-subgroups with no normal Abelian subgroups of rank 3, in finite fusion-simple groups, *Trans. Amer. Math. Soc.* **187** (1974), 1–67.
- [Pat2] A. R. Patterson, The minimal number of generators for p -subgroups of $\mathrm{GL}(n, p)$, *J. Algebra* **32** (1974), 132–140.
- [Paz] G. Pazdersky, Prime power groups which are cyclic extensions of elementary Abelian groups, *Math. Nachr.* **97** (1980), 57–68.
- [Pet] J. Petrescu, Sur les commutateurs, *Math. Z.* **61** (1954), 348–356.
- [Pol] J. Poland, Two problems on finite groups with k conjugate classes, *J. Aust. Math. Soc.* **8** (1968), 49–55.
- [Red1] L. Redei, Das schiefe Produkt in der Gruppentheorie, *Comment. Math. Helvet.* **20** (1947), 225–267.

- [Red2] L. Rédei, Die endlichen einstufig nichtnilpotenten Gruppen, *Publ. Math. Debrecen* **4** (1956), 303–324.
- [Rie] J. M. Riedl, Character degrees, class sizes and normal subgroups of a certain class of p -groups, *J. Algebra* **218** (1999), 190–215.
- [Rocc] N. R. Rocco, On weak commutativity between finite p -groups, *J. Algebra* **76** (1982), 471–488.
- [Rock] D. M. Rocke, p -groups with abelian centralizers, *Proc. London Math. Soc. (3)* **30** (1975), 55–75.
- [Rod] E. Rodemich, The groups of order 128, *J. Algebra* **67** (1980), 129–142.
- [Ron] C. Ronse, On centralizers of involutions in 2-groups, *Math. Ser. Cambridge Philos. Soc.* **86** (1979), 199–204.
- [Roi] M. Roitman, Relative indices of elements of finite p -groups, manuscript.
- [Roq] P. Roquette, Realisierungen von Darstellungen endlicher nilpotenter Gruppen, *Arch. Math.* **9** (1958), 241–250.
- [Rus] D. J. Rusin, What is the probability that two elements of a finite group commute, *Pacific J. Math.* **82** (1979), 237–247.
- [Sag1] I. A. Sagirov, Degrees of irreducible characters of 2-groups of Suzuki, *Math. Notes* **66** (1999), 258–263.
- [Sag2] I. A. Sagirov, Degrees of irreducible characters of p -groups of Suzuki $A_p(m, \theta)$, $p > 2$, to appear.
- [Sag3] I. A. Sagirov, Finite groups having exactly two degrees of monolithic characters, in: *Questions of Group Theory and Homological Algebra*, pp. 1–8, Univ. Yaroslavl, Yaroslavl, 1998.
- [Sak] A. I. Saksonov, Answer on a Brauer question, *Izv. Akad. Nauk BSSR, fiz.-mat. nauki* **1** (1967), 129–130.
- [San] P. J. Sanders, The coexponent of a regular p -group, *Comm. Algebra* **28** (2000), 1309–1333.
- [SanW] P. J. Sanders and T. S. Wilde, The class and coexponent of a finite p -group, manuscript.
- [Sand] P. R. Sanders, The central automorphisms of a finite group, *J. London Math. Soc.* **44** (1969), 225–228.
- [Sano] I. N. Sanov, Solution of Burnside's problem for exponent four, *Leningrad State Univ. Ann. Math. Ser.* **10** (1940), 166–170.
- [Schm1] P. Schmid, Normal p -subgroups in the group of outer automorphisms of a finite p -group, *Math. Z.* **147** (1976), 271–277.
- [Schm2] P. Schmid, Frattinan p -groups, *Geom. Dedicata* **6**, (1990), 359–364.
- [Schm3] P. Schmid, On the automorphism group of extraspecial 2-groups, *J. Algebra* **234** (2000), 492–506.
- [Sch1] O. Y. Schmidt, A new proof of the theorem of A. Kulakoff in group theory, *Mat. Sb.* **39** (1932), 66–71 (in Russian).
- [Sch2] O. Y. Schmidt, Groups all whose subgroups are nilpotent, *Mat. Sb.* **31** (1924), 366–372.
- [Scm3] O. Y. Schmidt, Groups having only one class of nonnormal subgroups (Russian), *Mat. Sb.* **33** (1926), 161–172.

- [Sch4] O. Y. Schmidt, Groups with two classes of nonnormal subgroups (Russian), *Proc. Seminar on Group Theory* (1938), 7–26.
- [Schn1] C. Schneider, On the derived subgroup of a finite p -group, *Austral. Math. Soc. Gaz.* **26** (1999), 232–237.
- [Schn2] C. Schneider, Groups of prime-power order with a small second derived quotient, *J. Algebra* **286** (2003), 539–551.
- [Schr] O. Schreier, Über die Erweiterung von Gruppen, I, *Monatsh. Math., Physik* **34** (1926), 165–180; II, *Abh. Math. Sem. Univ. Hamburg* **4** (1926), 321–346.
- [Sco] C. M. Scoppola, Groups of prime power order as Frobenius-Wielandt complements, *Trans. Amer. Math. Soc.* **325** (1991), 855–874.
- [Scot] W. R. Scott, *Group Theory*, Prentice Hall, 1964.
- [Sei1] G. Seitz, Finite groups having only one irreducible representation of degree greater than one, *Proc. Amer. Math. Soc.* **19** (1968), 459–461.
- [Sha1] A. Shalev, The structure of finite p -groups: effective proof of coclass conjectures, *Invent. Math.* **115** (1994), 315–345.
- [Sha2] A. Shalev, Finite p -groups, in: *Finite and locally finite groups*, pp. 401–450, Kluwer Acad. Publ., Dordrecht, 1995.
- [She] V. A. Sheriev, A description of the class of finite p -groups whose 2-maximal subgroups are abelian, in: *Proc. Sem. Algebraic Systems* **2**, pp. 25–76, Krasnoyarsk, 1970 (in Russian).
- [Shu] P. Shumyatsky, Involutory automorphisms of finite groups and their centralizers, *Arch. Math.* **71** (1998), 425–432.
- [Sim] C. C. Sims, Enumerating p -groups, *Proc. London Math. Soc.* **15** (1965), 151–166.
- [Sla1] M. C. Slattery, Character degrees of finite p -groups, in: *The Arcata Conf. on Representations of Finite Groups*, pp. 89–92, Proc. Symp. Pure Math. 47, Part 2, Amer. Math. Soc., Providence, RI, 1987.
- [Sla2] M. C. Slattery, Character degrees and nilpotent class in p -groups, *J. Aust. Math. Soc. (Series A)* **57** (1994), 76–80.
- [Sla3] M. C. Slattery, Character degrees and derived length in p -groups, *Glasgow Math. J.* **30** (1988), 221–230.
- [Sla4] M. C. Slattery, Computing character degrees in p -groups, *J. Symb. Comput.* **2** (1986), 51–58.
- [Spe] W. Specht, Isomorphic subgroups of finite p -groups revisited, *Canad. J. Math.* **26** (1974), 574–579.
- [SS] E. G. Straus and G. Szekeres, On a problem of D. R. Hughes, *Proc. Amer. Math. Soc.* **9** (1958), 157–158.
- [Str] R. R. Struik, Some nonabelian 2-groups with abelian automorphism groups, *Arch. Math.* **39** (1982), 299–302.
- [Suz1] M. Suzuki, *Group Theory I, II*, Springer, Berlin, 1982, 1986.
- [Suz2] M. Suzuki, *Structure of a Group and the Structure of its Lattice of Subgroups*, Ergebnisse der Mathematik und ihrer Grenzgebiete 10, Springer, Berlin, 1956.
- [Tau] O. Taussky, Remark on the class field tower, *J. London Math. Soc.* **12** (1937), 82–85.

- [Tes] L. Teschke, Über die Normalteiler der p -Sylowgruppe der symmetrischen Gruppe vom Grade p^m , *Math. Nachr.* **87** (1979), 197–212.
- [Tho1] J. G. Thompson, A replacement theorem for p -groups and a conjecture, *J. Algebra* **13** (1969), 149–151.
- [Tho2] J. G. Thompson, Finite groups with fixed-point-free automorphisms of prime order, *Proc. Nat. Acad. Sci. USA* **45** (1959), 578–581.
- [Tho3] J. G. Thompson, Nonsolvable finite groups all of whose local subgroups are solvable, I, *Bull. Amer. Math. Soc.* **74** (1968), 383–437.
- [Tho4] J. G. Thompson, Fixed points of p -groups acting on p -groups, *Math. Z.* **86** (1964), 12–13.
- [Tho5] J. G. Thompson, Centralizers of elements in p -groups, *Math. Z.* **96** (1967), 292–293.
- [Tow] M. J. Towers, *Modular Representations of p -Groups*, PhD Thesis, Hertford College, University of Oxford, 2005.
- [Tua1] H. F. Tuan, A theorem about p -groups with abelian subgroup of index p , *Acad. Sinica Science Record* **3** (1950), 17–23.
- [Tua2] H. F. Tuan, An Anzahl theorem of Kulakoff's type for p -groups, *Sci. Rep. Nat. Tsing-Hua Univ. A* **5** (1948), 182–189.
- [Ust] A. D. Ustjuzaninov, Finite 2-groups in which the set of self-centralizing abelian normal subgroups of rank ≥ 3 is empty ($SCN_3(2) = \emptyset$), *Izv. Akad. Nauk SSSR* **37** (1973), 251–283 (in Russian).
- [Ust2] A. D. Ustjuzaninov, Finite 2-groups with three involutions, *Sibirsk. Mat. Z.* **13** (1972), 182–197.
- [VL] M. R. Vaughan-Lee, Breadth and commutator subgroups of p -groups, *J. Algebra* **32** (1976), 278–285 (in Russian).
- [VLW1] M. R. Vaughan-Lee and J. Wiegold, Breadth, class and commutator subgroups of p -groups, *J. Algebra* **32** (1974), 268–277.
- [Ver] L. Verardi, A class of finite groups of exponent p in which every normal subgroup is characteristic, *Boll. Un. Mat. Ital. B* (6) **4** (1988), 307–317.
- [Waa] R. W. van der Waall, On finite p -groups whose commutator subgroups are cyclic, *Indag. Math.* **35** (1973), 342–345.
- [Wal] G. E. Wall, On Hughes' H_p -problem, in: *Proc. Internat. Conf. Theory of Groups (Canberra, 1965)*, pp. 357–362, Gordon and Breach, New York 1967.
- [Wal2] G. E. Wall, Finite groups with class-preserving outer automorphisms, *J. London Math. Soc.* **22** (1947), 315–320.
- [Wal3] G. E. Wall, Secretive prime-power groups of large rank, *Bull. Austral. Math. Soc.* **12** (1975), 963–969.
- [War] H. N. Ward, Automorphisms of quaternion-free 2-groups, *Math. Z.* **112** (1969), 52–58.
- [Web1] U. H. M. Webb, An elementary proof of Gaschütz theorem, *Arch. Math.* **35** (1980), 23–26.
- [Web2] U. H. M. Webb, The number of stem covers of an elementary abelian p -group, *Math. Z.* **182** (1983), no. 3, 327–337.
- [Web3] U. H. M. Webb, On the rank of a p -group of class 2, *Canad. Math. Bull.* **26** (1983), 101–105.

- [Web4] U. H. M. Webb, The Schur multiplier of a nilpotent group, *Trans. Amer. Math. Soc.* **291** (1985), 755–763.
- [Wei] P. M. Weichsel, On isoclinism, *J. London Math. Soc.* **38** (1963), 63–65.
- [Weir1] A. Weir, Sylow p -subgroups of the classical groups over finite fields with characteristic prime to p , *Proc. Amer. Math. Soc.* **6** (1955), 529–533.
- [Weir] A. Weir, The Sylow subgroups of the symmetric groups, *Proc. Amer. Math. Soc.* **6** (1955), 534–541.
- [Wie1] J. Wiegold, Multiplicators and groups with finite central factor-groups, *Math. Z.* **89** (1965), 245–247.
- [Wie2] J. Wiegold, The Schur multiplier: an elementary approach, in: Groups – St. Andrews, 1981, pp. 137–154, London Math. Soc. Lect. Notes 71, Cambridge, 1982.
- [Wie3] J. Wiegold, Commutator subgroups of finite p -groups, *J. Aust. Math. Soc.* **10** (1969), 480–484.
- [Wil1] B. Wilkens, On quaternion-free 2-groups, *J. Algebra* **258** (2002), 477–492.
- [Wil2] B. Wilkens, On the upper exponent of a finite p -group, *J. Algebra* **277** (2004), 249–263.
- [Wil3] B. Wilkens, 2-groups of breadth 3, *J. Algebra* **318** (2007), 202–224.
- [Wilk] D. F. Wilkinson, The groups of order p^7 (p any prime), *J. Algebra* **118** (1988), 109–119.
- [Wils] L. Wilson, On the power structure of powerful p -groups, *J. Group Theory* **5** (2002), no. 2, 129–144.
- [Xu] M. Y. Xu, Regular p -groups and their generalizations, manuscript.
- [XZA] M. Y. Xu, Q. Zhang and L.-J. An, Finite p -groups all of whose nonabelian subgroups are generated by two elements, in preparation.
- [Zap] G. Zappa, Finite groups in which all nonnormal subgroups have the same order II (Italian), *Atti Accad. Naz. Lincei Cl. Sci. Fiz. Mat. Natur. Rend. Lincei (9) Mat. Appl.* **14** (2003), no. 1, 13–21.
- [ZAX] Q. Zhang, L.-J. An and M. Y. Xu, Finite p -groups all of whose non-abelian proper subgroups are metacyclic, *Arch. Math.* **87** (2006), 1–5.
- [Zha] J. P. Zhang, Finite groups with many conjugate elements, *J. Algebra* **170** (1994), 608–624.
- [Zhm1] E. M. Zhmud, Finite groups with uniquely generated normal subgroups, *Mat. Sb.* **72** (114) (1967), 135–147 (in Russian).
- [Zhm2] E. M. Zhmud, On the multiplier of a finite group with nontrivial center, *Ukrainian Math. J.* **47** (1995), 546–550 (in Russian).
- [Zhm3] E. M. Zhmud, Symplectic geometries and projective representations of finite abelian groups, *Mat. Sb.* **87** (129) (1971) 3–17 (in Russian).
- [Zhm4] E. M. Zhmud, Symplectic geometries on finite abelian groups, *Math. Sb.* **86** (1972), 9–33 (in Russian).
- [Zhm5] E. M. Zhmud, The isomorphisms of the lattice of normal subgroups of a finite nilpotent group, *Vestnik Kharkov Univ.* **26** (1967), 3–17 (in Russian).
- [Zho] X. Zhou, On the order of Schur multipliers of finite p -groups, *Comm. Algebra* **22** (1994), 1–8.

Author index

A

An, L.-J., §65

B

Berkovich, Y., §§47, 48, 55, 58, 59,
62–65, 69, 72, 76, 88,

Appendices 16, 17, 21, 24, 27

Blackburn, N., §§66, 69

Bozikov, Z., §§52, 85, Appendix 19

Burnside, W., §§60, 61

C

Cepulic, V., §65

Cossey, J., Appendix 26

G

Glauberman, G., Appendix 18

Golfand, Y. A., Appendix 22

H

Hall, P., §88

I

Isaacs, I. M., §§47, 68, Appendices 18, 20,
21

Ito N., §64

Iwasawa, K., §§73, 79

J

Janko, Z., §§48–56, 60–63, 64–67, 70–87,
89–92, Appendix 17, Problems

K

Kazarin, L. S., §§58, 65, 71

L

Li Shirong, §63

M

Mann, A., §§64, 65, 76

Miller, G. A., Appendix 17

N

Napolitani, F., §73

P

Pyliavska, O., §65

R

Redei, L., §65, Appendix 22

S

Sagirov, I. A., §46

Sanov, I. N., §60

Schmidt, O. Y., §59, Appendix 22

Schreier, O., Appendix 25

Sheriev, V. A., §65

Suzuki, M., §48

T

Thompson, J. G., Appendix 18

Tobin, S. J., §60

V

Vishnevetsky, A., §46

X

Xu, M. Y., §65

W

Ward, H. N., §56, Appendix 19

Wilkens, B., §79

Z

Zhang, Q., §65

Subject index

A

- abelian subgroups of small index, §76
absolutely regular p -groups, §§88
 $\alpha_n(G)$, §76
 \mathcal{A}_n -groups, §72
 \mathcal{A}_2 -groups, properties, defining relations of §§65, 71
 \mathcal{A}_n -groups, $n = 3, 4$, derived subgroup of, §72
 \mathcal{A}_n -groups with cyclic derived subgroup of order p^n , §72
 \mathcal{A}_n -groups with cyclic derived subgroup of order p^{n-1} , $p > 2$, §72
artificial square, §56
automorphism group, Appendix 20

B

- $\beta_1(G, H)$, §76
 $\bar{\beta}_1(G, H)$, §76
Blackburn's theorems, §§66, 69
Burnside group $B(4, 2)$ of order 2^{12} , structure of, §60

C

- centralizer of involution, §§48, 49
central products of some 2-groups, Appendix 16
central products of 2-groups of maximal class with cyclic subgroup of order 4, Appendix 16
characteristic maximal subgroup in quaternion-free 2-groups, §56
characterization of groups of exponent p , §68
characterizations of p -groups of maximal class, §69
characters of Suzuki p -groups $A_p(m, \theta)$, §46
classification of \mathcal{A}_2 -groups, §71
classification of modular p -groups, §73

D

- Dedekindian groups, §73
derived subgroups of \mathcal{A}_n -groups, $n = 2, 3, 4$, §72
dominating chain, §88

E

- elements of order ≤ 4 in 2-groups, §75
estimate of $|\Omega_k(G)|$ and $|\Omega_k^*(G)|$ in terms of $c_k(G)$, §64
extraspecial p -groups, §83

F

- free centralizer, Appendix 23

G

- generators of p -groups, the number of, Schreier's theorem, Appendix 25
 $\Gamma_1(H)$, §76
 Γ_1^H , §76
group of type (F), Appendix 23
groups all of whose nonabelian maximal subgroups are either absolutely regular or of maximal class, Appendix 26
groups all of whose subgroups of index p^2 are abelian (= \mathcal{A}_2 -groups), §§65, 71
groups G of exponent p and order p^m satisfying $\alpha_1(G) = p^{m-3}$, §76
groups without normal elementary abelian subgroups of order p^3 , §§50, 69

H

- Hall chains (p -admissible and k -admissible = \mathcal{H}_k -chains), §88

I

- Isaacs' examples, Appendix 21

- Ito k -series, §64
- Iwasawa's theorem on modular p -groups,
new proof due to Janko, §73,
Appendix 24
- J**
- Janko's theorems on 2-groups with small
centralizer of an involution,
§§48, 49
- Janko's theorem on 2-groups without
normal elementary abelian
subgroup of order 8, §50
- Janko's theorem on 2-groups with
selfcentralizing elementary
abelian subgroup of order 8, §51
- Janko's theorem on 2-groups G with
 $|\Omega_2(G)| = 2^4$, §52
- Janko's theorems on 2-groups G with
 $c_n(G) = 4, n > 1$, §§53, 54
- Janko's theorem on 2-groups G in which
the subgroup generated by all
elements of order 4, is of order
4, §55
- K**
- $\kappa_1(G)$, §76
- $\kappa_1(\mathfrak{M})$, §76
- k -stepped p -groups, §64
- M**
- maximal abelian subgroups, §§91, 92
- maximal centralizers of p -groups,
Appendix 23
- \mathcal{M}_3 -groups, §76.
- metacyclic \mathcal{A}_n -groups with derived
subgroup of order p^n , §§65
- metacyclic groups, §§65, 66, 69
- metacyclic p -groups with derived
subgroup of order p^n are
 \mathcal{A}_n -groups, §65
- minimal nonabelian subgroups, the
number of, §§65, 76, 90, 92
- minimal nonmetacyclic p -groups, §§66,
69
- minimal nonmodular p -groups, §78
- minimal nonnilpotent groups, Appendix
22
- minimal non-quaternion-free 2-groups,
§§80
- modular p -groups, Iwasawa's
classification of, §73
- N**
- nonmodular quaternion-free 2-groups,
structure of, §79
- number of cyclic subgroups of given order
in some central and wreath
products, Appendix 16
- O**
- $\Omega_n^*(G)$, §55
- one-stepped p -groups, §64
- P**
- pairs $H < G$ with $\beta_1(G, H) = p - 1$, §76
- pairs $H < G$ with $\beta_1(G, H) = p$, §76
- p -groups all of whose nonnormal
subgroups are conjugate, §59
- p -groups all of whose cyclic subgroups of
composite orders are normal,
§63
- p -groups generated by elements of given
order, §64
- p -groups G satisfying $\alpha_1(G) \geq p^{d(G)-3}$,
§76
- p -groups G with $1 < \alpha_1(G) < p^2$ are
 \mathcal{A}_2 -groups, §76
- p -groups G with $\alpha_1(G) = p^2$, §76
- p -groups G with $\alpha_1(G) = p^2 + p + 1$,
§76
- p -groups G with $d(G) > 2$ all of whose
maximal subgroups are
two-generator, §70
- p -groups with abelian subgroups of index
 p^2 , §§65, 71
- p -groups with abelian n -th maximal
subgroups, $n = 3, 4$, §72
- p -groups with a cyclic subgroup of index
 p^2 , Janko's proof, §74
- p -groups with extraspecial $\Omega_1(G)$ or
 $\Omega_2^*(G)$, §83
- p -groups G , $p > 2$, with $c_1(G) = p + 1$,
§69
- p -groups G with metacyclic $\Omega_2^*(G)$, §86
- p -groups G with $\kappa_1(G) = p - 1$, §76
- p -groups G with $\kappa_1(G) = p$, §76
- p -groups without normal subgroup
 $\cong E_{p^3}$, $p > 2$, §69

- p*-groups, $p > 2$, without normal subgroup of order p^3 and exponent p , §69
- p*-groups with a uniqueness condition for nonnormal subgroups, §84
- p*-groups with few minimal nonabelian subgroups, §76
- p*-groups with large normal closures of nonnormal cyclic subgroups, §62
- p*-groups G with $|\Omega_2^*(G)| = p^{p+1}$, §55
- p*-groups G with $\Omega_2^*(G)$ extraspecial, §83
- p*-groups G with $\Omega_2^*(G)$ metacyclic, §86
- p*-groups G with $\Omega_n^*(G)$ metacyclic, $n > 2$, §86
- Q**
- quaternion-free 2-groups, structure of, Janko–Wilkins theorem, §79
- S**
- Schreier's inequality for *p*-groups, Appendix 25
- subgroup structure of A_2 -groups, §65
- T**
- two-generator modular *p*-groups are metacyclic, §73
- 2-groups all of whose minimal normal subgroups are of order 8, §90
- 2-groups all of whose minimal normal subgroups are isomorphic and have exponent 4, §57
- 2-groups in which the centralizer of an involution is abelian of type $(2, 2^m)$, §48
- 2-groups in which the centralizer of an involution is $C_2 \times Q_{2^m}$, §49
- 2-groups G with an involution t such that $C_G(t) \cong C_2 \times M$, where M is of maximal class, §51
- 2-groups with exactly four cyclic subgroups of order 4, §54
- 2-groups with exactly four cyclic subgroups of order 2^n , $n > 2$, §55
- 2-groups with exactly one nonmetacyclic maximal subgroup, §87
- 2-groups with exactly three involutions, §82
- 2-groups with nonabelian Frattini subgroup of order 16, §85
- 2-groups G with $|\Omega_2(G)| = 16$, §52
- 2-groups G with $|\Omega_3(G)| = 2^5$, §52
- 2-groups with 7 and 11 involutions, §64
- 2-groups G with $|\Omega_2^*(G)| = |\{x \in G \mid o(x) = 4\}| = 16$, §55
- 2-groups G with $\Omega_2^*(G) = Q_{2^n} \times C_2$, §75
- 2-groups without elementary abelian subgroups of order 8, §49
- 2-groups without normal elementary abelian subgroup of order 8, §50
- 2-groups with selfcentralizing abelian subgroup of type $(4, 2)$, §77
- 2-groups with selfcentralizing elementary abelian subgroup of order 8, §51
- U**
- unitriangular group, Problems
- U_2 -groups, determination, defining relations of, §§64, 67
- W**
- Ward's theorem on quaternion-free 2-groups, §56, Appendix 17
- Wilkins 2-groups (W_a -, W_b - and W_c -groups), §79