DE GRUYTER

Yakov Berkovich, Zvonimir Janko

GROUPS OF PRIME POWER ORDER

VOLUME 3

EXPOSITIONS IN MATHEMATICS 56

DE

Yakov Berkovich
Zvonimir Janko

Groups of Prime Power Order

Volume 3

De Gruyter

Mathematical Subject Classification 2010: 20-02, 20D15, 20E07.

ISBN 978-3-11-020717-0
e-ISBN 978-3-11-025448-8
ISSN 0938-6572

Library of Congress Cataloging-in-Publication Data

Berkovich, IA. G., 1938–
Groups of prime power order / by Yakov Berkovich, Zvonimir Janko.
p. cm. – (De Gruyter expositions in mathematics ; < >-56)
Description based on v. 3, copyrighted c2011.
Includes bibliographical references and index.
ISBN 978-3-11-020717-0 (v. 3 : alk. paper)
1. Finite groups. 2. Group theory. I. Janko, Zvonimir, 1932– II. Title.
QA177.B469 2011
512'.23–dc22
2011004438

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.

Typesetting: Dimler & Albroscheit, Müncheberg
Printing and binding: Hubert & Co. GmbH & Co. KG, Göttingen
∞ Printed on acid-free paper

Printed in Germany

www.degruyter.com

De Gruyter Expositions in Mathematics 56

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 $N \subset M$.

$\varnothing$ is the empty set.

N is called a nontrivial subset of M if $N \neq \varnothing$ 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.

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 if $\pi(m) \subseteq \pi$.

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

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

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

GF(p^m) is the finite field containing p^m elements.

F* is the multiplicative group of a field F.

$\mathfrak{L}(G)$ 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 few exceptions, by uppercase 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 $H = M$.

If H is a proper normal subgroup of G, then we write $H \lhd G$. Expressions 'normal subgroup of G' and 'G-invariant subgroup' are synonyms.

A normal subgroup of G is nontrivial provided $G > H > \{1\}$.

H is a minimal normal subgroup of G if (a) H is normal in G; (b) $H > \{1\}$; (c) $N \lhd G$ 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 $\mathrm{Sc}(G)$. We put, by definition, $\mathrm{Sc}(\{1\}) = \{1\}$.

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

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

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

If $A \leq B$ and A, B are normal in G, then $\mathrm{C}_G(B/A) = H$, where $H/A = \mathrm{C}_{G/A}(B/A)$.

A wr B (or $A \wr B$) 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 $|A|^{|B|}|B|$.

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

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

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

$\mathcal{N}(G)$ is the norm of G, the intersection of normalizers of all subgroups 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.

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

$\mathrm{Z}_i(G)$ is the i-th member of the upper central series of G; in particular, $\mathrm{Z}_0(G) = \{1\}$, $\mathrm{Z}_1(G) = \mathrm{Z}(G)$.

$\mathrm{K}_i(G)$ is the i-th member of the lower central series of G; in particular, $\mathrm{K}_2(G) = G'$. We have $\mathrm{K}_i(G) = [G, \ldots, G]$ ($i \geq 1$ times). We set $\mathrm{K}_1(G) = G$.

If G is nonabelian, then $\eta(G)/\mathrm{K}_3(G) = \mathrm{Z}(G/\mathrm{K}_3(G))$.

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

$\mathrm{Syl}_p(G)$ 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}.

$\mathrm{GL}(n, \mathrm{F})$ is the set of all nonsingular $n \times n$ matrices with entries in a field F, the n-dimensional general linear group over F, $\mathrm{SL}(n, \mathrm{F}) = \{A \in \mathrm{GL}(n, \mathrm{F}) \mid \det(A) = 1 \in \mathrm{F}\}$, 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, the intersection of all normal subgroups of G containing H, is the normal closure or normal hull of H in G. Obviously, H_G is normal in G.

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

If $H \leq G$ and $|G : \mathrm{N}_G(H)| = p^{\mathrm{sb}(H)}$, then $\mathrm{sb}(H)$ is said to be the subgroup breadth of H. Next, $\mathrm{sb}(G) = \max\{\mathrm{sb}(H) \mid H \leq G\}$.

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

$\Gamma_i = \{H < G \mid \Phi(G) \leq H, |G : H| = p^i\}, i = 1, \ldots, \mathrm{d}(G)$, 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 $\exp(G) = \max\{o(x) \mid x \in G\}$.

$\mathrm{k}(G)$ 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 $\mathrm{ccl}_G(x)$).

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 $[A, B] = \{1\}$.

$\mathrm{E}_{p^m} = \mathrm{C}_p^m$ 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).

$\mathrm{ES}(m, p)$ is an extraspecial group of order p^{1+2m} (a p-group G is said to be extraspecial if $G' = \Phi(G) = \mathrm{Z}(G)$ is of order p). Note that for each positive integer m, 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 $G' = \Phi(G) = \mathrm{Z}(G)$ 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.

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

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

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

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

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

A p-group G is said to be regular if for any $x, y \in G$ there exists $z \in \langle x, y \rangle'$ such that $(xy)^p = x^p y^p z^p$.

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

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 a normal subgroup N 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 group G is said to metacyclic if it contains a normal cyclic subgroup C such that G/C is cyclic.

A group G is said to be minimal nonmetacyclic if it is nonmetacyclic but all its proper subgroups are metacyclic.

A subgroup A of a group G is said to be soft if $\mathrm{C}_G(A) = A$ and $|\mathrm{N}_G(A) : A| = p$.

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

If $\mathrm{F} = \mathrm{GF}(p^n)$, then we may write $\mathrm{GL}(m, p^n), \mathrm{SL}(m, p^n), \ldots$ instead of $\mathrm{GL}(m, \mathrm{F})$, $\mathrm{SL}(m, \mathrm{F}), \ldots$.

$\mathrm{c}_n(G)$ is the number of cyclic subgroups of order p^n in a p-group G.

$\mathrm{s}_n(G)$ 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.

A group G is said to be minimal nonabelian if it is nonabelian but all its proper subgroups are abelian.

$\mathcal{A}_n$-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.

$\mathcal{MA}(G)$ is the set of minimal nonabelian subgroups of a p-group G.

$\mathcal{MA}_k(G) = \{H \in \mathcal{MA}(G) \mid \Omega_k(H) = H\}$.

$\mathrm{D}_k(G) = \langle \mathcal{MA}_k(G) \rangle = \langle H \mid H \in \mathcal{MA}_k(G) \rangle$.

$L_n = |\{x \in G \mid x^n = 1\}|$.

Characters and representations

$\mathrm{Irr}(G)$ is the set of all irreducible characters of G over complex numbers.

A character of degree 1 is said to be linear.

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

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

$\chi(1)$ 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: $\bar{\chi}(x) = \overline{\chi(x)}$ (here $\bar{w}$ is the complex conjugate of a complex number w).

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

1_G is the principal character of G.

$\mathrm{Irr}^{\#}(G) = \mathrm{Irr}(G) - \{1_G\}$.

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.

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

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

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

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

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

$\mathrm{M}(G)$ is the Schur multiplier of G.

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

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

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

Preface

This is the third volume of the book devoted to elementary parts of p-group theory. Sections 93–95, 98–102, 113, 117, 118, 120–123, 125–133, 137, 139, 140–142, 144 are written by the second author, Sections 107, 138 and Appendix 41 are jointly written by both authors, all other material, apart from Appendices 33 and 44, is written by the first author. All exercises and about all problems are due to the first author. All material of this part is appeared in the book form for the first time.

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

(i) classification of p-groups containing exactly one maximal subgroup which is neither abelian nor minimal nonabelian,
(ii) classification of groups all of whose nonnormal subgroups have the same order (independently, this result was obtained by Guido Zappa),
(iii) classification of p-groups all of whose nonnormal subgroups have normalizers of index p,
(iv) computation of the number of subgroups of given order in metacyclic p-groups (for $p > 2$ this was done by Avinoam Mann),
(v) computation of the order of the derived subgroup of a group with subgroup breadth 1,
(vi) classification of p-groups all of whose subgroups have derived subgroups of order $\leq p$ (so-called $\mathcal{A}_2$-groups satisfy this condition),
(vii) classification of p-groups G all of whose maximal abelian subgroups containing a non-G-invariant cyclic subgroup of minimal order, say p^v, have order $\leq p^{v+1}$.

Some results proved in this part have no analogs in existing books devoted to finite p-groups. We list only a few such results:

(a) study the p-groups G all of whose minimal nonabelian subgroups have exponent $< \exp(G)$,
(b) study the groups admitting an irredundant covering by few proper subgroups,
(c) study of some 2-groups with sectional rank 4,
(d) study the p-groups which do not generated by certain minimal nonabelian subgroups,
(e) study the p-groups, $p > 3$, in which certain nonabelian subgroups are generated by two elements,
(f) study the p-groups with nonnormal maximal elementary abelian subgroup of order p^2 (this is a continuation of the paper of Glauberman–Mazza),
(g) classification of p-groups with exactly one maximal subgroup which is neither abelian nor minimal nonabelian,

(h) classification of p-groups all of whose proper subgroups have derived subgroups of orders $\leq p$,
(i) classification of p-groups all of whose nonnormal cyclic subgroups of minimal possible order have index p is their normalizers,
(j) classification of p-groups G all of whose maximal abelian subgroups containing non-G-invariant cyclic subgroup of minimal order, say p^v, have order $\leq p^{n+1}$,
(k) classification of p-groups all of whose maximal subgroups have cyclic derived subgroups,
(l) characterizations of abelian and minimal nonabelian groups,
(m) describing all possible sets of numbers of generators of maximal subgroups of two-generator 2-groups,
(n) study the equilibrated p-groups,
(o) classification of nonabelian 2-groups in which any two distinct minimal nonabelian subgroups have cyclic intersection,
(p) study the p-groups of breadth 2,
(q) study groups containing a soft subgroup,
(r) proof of the Schenkman theorem on the norm of a finite group and a new proof of Baer's theorem on an arbitrary 2-group with nonabelian norm.

For further information, see the Contents.

Essential part of this volume is devoted to investigation of impact of minimal nonabelian subgroups on the structure of a p-group.

Some appendices are devoted to nilpotent subgroups of nonnilpotent groups.

The section 'Research problems and themes III', written by the first author, contains about 900 research problems and themes some of which are solved by the second author. There are in the text approximately 200 exercises most of which are solved.

Avinoam Mann (Hebrew University of Jerusalem) analyzed the list of problems and made a great number of constructive comments and corrections. He also read a number of sections and made numerous useful remarks. Moshe Roitman (University of Haifa) wrote Appendix 44 and helped with LaTeX. Noboru Ito wrote Appendix 33. We are indebted to these three mathematicians.

We are grateful to the publishing house of Walter de Gruyter and all its workers for supporting and promoting the publication of our book and especially to Simon Albroscheit and Kay Dimler.

Prerequisites from Volumes 1 and 2

In this section we state some results from Volumes 1 and 2 which we use in what follows. If we formulate Lemma 1.4 from Volume 1, then it is named below also as Lemma 1.4.

Lemma INTR. (a) *If $M, N \lhd G$, then the quotient group $G/(M \cap N)$ is isomorphic to a subgroup of $G/M \times G/N$.*

(b) *If Z is a cyclic subgroup of maximal order in an abelian p-group, then Z is a direct factor of G. In particular, an abelian p-group is a direct product of cyclic subgroups.*

(c) (Fitting's lemma) *If M and N are nilpotent normal subgroups of a group G, then* $\mathrm{cl}(MN) \leq \mathrm{cl}(M) + \mathrm{cl}(N)$.

(d) *If G is a p-group, then $G/\Phi(G)$ is elementary abelian of order, say d. Every minimal set of generators of G contains exactly d members.*

(e) *If G is a p-group, then $\Phi(G) = G'\mho_1(G)$.*

Lemma 1.1. *If A is an abelian subgroup of index p in a nonabelian p-group G, then* $|G| = p|G'||\mathrm{Z}(G)|$.

Theorem 1.2. *Suppose that a nonabelian p-group has a cyclic subgroup of index p. Then one of the following holds:*

(a) $G = \langle a, b \mid a^{2^{n-1}} = b^2 = 1, a^b = a^{-1}\rangle \cong \mathrm{D}_{2^n}$ *is of class $n-1$, all elements of the set $G - \langle a\rangle$ are involutions.*

(b) $G = \langle a, b \mid a^{2^{n-1}} = 1, a^{2^{n-2}} = b^2, a^b = a^{-1}\rangle \cong \mathrm{Q}_{2^n}$ *is of class $n-1$, all elements of the set $G - \langle a\rangle$ have the same order* 4.

(c) $G = \langle a, b \mid a^{2^{n-1}} = 1, a^{2^{n-2}} = b^2, a^b = a^{-1}\rangle \cong \mathrm{SD}_{2^n}$ *is of class $n-1$,* $\Gamma_1 = \{D \cong \mathrm{D}_{2^{n-1}}, Q \cong \mathrm{Q}_{2^{n-1}}, \langle a\rangle \cong \mathrm{C}_{2^{n-1}}\}$, $\Omega_1(G) = D$, $\Omega_2^*(G) = Q$.

(d) $G = \langle a, b \mid a^{p^{n-1}} = b^p = 1,\ a^b = a^{1+p^{n-2}}\rangle \cong \mathrm{M}_{p^n}$ *is of class* 2, *where $n > 3$ if $p = 2$,* $\mathrm{Z}(G) = \langle a^p\rangle$, $\Omega_1(G) = \langle a^{p^{n-2}}, b\rangle \cong \mathrm{E}_{p^2}$.

The groups D_{2^n}, Q_{2^n}, SD_{2^n} are called dihedral, generalized quaternion, semidihedral, respectively.

Proposition 1.3. *If a p-group has only one subgroup of order p, then it is either cyclic or a generalized quaternion group.*

Lemma 1.4. *Let N be a normal subgroup of a p-group G. If N has no G-invariant abelian subgroup of type (p, p), then it is either cyclic or a 2-group of maximal class.*

It follows from Lemma 1.4 that if $\mathrm{Z}_2(G)$ is cyclic, then G is either cyclic or a 2-group of maximal class.

Lemma 1.6 (Taussky). *If a nonabelian 2-group G satisfies $|G : G'| = 4$, then it is a 2-group of maximal class.*

Exercise 1.6(a). The number of abelian maximal subgroups in a nonabelian p-group G is either 0 or 1 or $p + 1$.

Exercise P1. If a nonabelian p-group G has two distinct abelian maximal subgroups, then $|G'| = p$.

Proposition 1.8 (Suzuki). *If a nonabelian p-group G has a self-centralizing abelian subgroup of order p^2, then G is of maximal class. (For the converse assertion, see Theorem 9.6(c).)*

Exercise 1.8(a). If a p-group G is minimal nonabelian, then

$$|G'| = p, \quad \mathrm{d}(G) = 2, \quad |G : \mathrm{Z}(G)| = p^2,$$

and one of the following holds:

(a) $G = \langle a, b \mid a^{p^m} = b^{p^n} = 1, a^b = a^{1+p^{m-1}} \rangle$ is metacyclic.

(b) $G = \langle a, b \mid a^{p^m} = b^{p^n} = 1, [a, b] = c, c^p = 1, [a, c] = [b, c] = 1 \rangle$ is nonmetacyclic. In that case, $\mathfrak{V}_1(G) = \langle a^p \rangle \times \langle b^p \rangle$, $G/\mathfrak{V}_1(G)$ is nonabelian of order p^3 and exponent p unless $p = 2$ (if $p = 2$, then $G/\mathfrak{V}_1(G) \cong \mathrm{E}_4$).

(c) $G \cong \mathrm{Q}_8$.

Next, a group G is nonmetacyclic if and only if G' is a maximal cyclic subgroup of G. The group G is metacyclic if and only if $|\Omega_1(G)| \leq p^2$. No noncentral cyclic subgroup is normal in G.

Theorems 1.10 and 1.17. *Suppose that a p-group G is neither cyclic nor a 2-group of maximal class. Then*

(a) $\mathrm{c}_1(G) \equiv 1 + p \pmod{p^2}$.

(b) *If $k > 1$, then* $\mathrm{c}_k(G) \equiv 0 \pmod{p}$.

Theorem 1.20. *If all subgroups of a nonabelian p-group G are normal, then we have $G = Q \times E$, where $Q \cong \mathrm{Q}_8$ and* $\exp(E) \leq 2$.

Exercise 1.69(a). Let G be a p-group and let $H \neq K$ be two distinct maximal subgroups of G. Then $|G' : H'K'| \leq p$. In particular, if G' is cyclic, there is $A \in \Gamma_1$ such that $|G' : A'| \leq p$.

Lemma 4.2. *Let G be a p-group with $|G'| = p$. Then $G = (A_1 * A_2 * \cdots * A_s)\mathrm{Z}(G)$, the central product, where $A_1, \ldots, A_s$ are minimal nonabelian, so $G/\mathrm{Z}(G)$ is elementary abelian of even rank. In particular, if G/G' is elementary abelian, then we have $|A_1| = \cdots = |A_s| = p^3$, $E = A_1 * \cdots * A_s$ is extraspecial and $G = E\mathrm{Z}(G)$.*

Lemma 4.3. *Let E be a subgroup of a p-group G with $|E'| = p$ and $\mathrm{Z}(E) = \Phi(E)$. If $[G, E] = E'$, then $G = E * \mathrm{C}_G(E)$.*

Theorem 5.2 (Hall's enumeration principle). *Let G be a p-group and $\mathcal{M}$ be a set of proper subgroups of G. Given $H \leq G$, let $\alpha(H)$ be the number of members of the set $\mathcal{M}$ contained in H. Then*

$$\alpha(G) \equiv \sum_{H \in \Gamma_1} \alpha(H) \pmod{p}.$$

Theorems 5.3 and 5.4. *Suppose that a p-group G of order p^m is neither cyclic nor a 2-group of maximal class and $1 \leq n < m$. Then $\mathrm{s}_n(G) \equiv 1 + p \pmod{p^2}$.*

Theorem 5.8. *Let G be a group of order $p^m > p^3$ and exponent p, $2 < n < m$. Let $\mathcal{M}$ denote the set of all 2-generator subgroups of order p^n in G and $\alpha(K)$ the number of elements of the set $\mathcal{M}$ contained in $K \leq G$.*

(a) *If $n = m - 1$, then $\alpha(G) \in \{0, p, p^2\}$.*

(b) *p divides $\alpha(G)$.*

Theorem 7.1. *Let G be a p-group.*

(a) *Regularity is inherited by sections.*

(b) *If $\mathrm{cl}(G) < p$ or $|G| \leq p^p$ or $\exp(G) = p$, then G is regular.*

(c) *If $\mathrm{K}_{p-1}(G)$ is cyclic, then G is regular.*

Theorem 7.2. *Suppose that G is a regular p-group.*

(b) $\exp(\Omega_n(G)) \leq p^n$.

(c) $\mathfrak{V}_n(G) = \{x^{p^n} \mid x \in G\}$.

(d) $|\Omega_n(G)| = |G : \mathfrak{V}_n(G)|$.

Theorem 9.5. *Let G be a group of maximal class and order p^m, $m \leq p+1$. Then $\Phi(G)$ and $G/\mathrm{Z}(G)$ have exponent p. If $m = p + 1$, then G is irregular and $|\mathfrak{V}_1(G)| = p$.*

Theorem 9.6. *Let G be a group of maximal class and order p^m, $p > 2$, $m > p + 1$. Then G is irregular and*

(a) *$|G : \mathfrak{V}_1(G)| = p^p$. In particular, $\mathfrak{V}_1(G) = \mathrm{K}_p(G)$.*

(b) *There is $G_1 \in \Gamma_1$ such that $|G_1 : \mathfrak{V}_1(G_1)| = p^{p-1}$.*

(c) *G has no normal subgroups of order p^p and exponent p (here the condition that $m > p+1$ is essential). Moreover, if $N \lhd G$ and $|G:N| > p$, then N is absolutely regular since $N < G_1$. Next, if $N \lhd G$ of order p^{p-1}, then $\exp(N) = p$. In particular, G has no normal cyclic subgroups of order p^2.*

(d) *Let $Z_2 = Z_2(G)$ be a normal subgroup of order p^2 in G, $G_0 = C_G(Z_2)$. Then G_0 is regular such that $|\Omega_1(G_0)| = p^{p-1}$.*

(e) *Let $\Gamma_1 = \{M_1 = G_0, M_2, \ldots, M_{p+1}\}$, where G_0 is defined in* (d). *Then the subgroups $M_2, \ldots, M_{p+1}$ are of maximal class (and so irregular; see Theorem 9.5). Thus the subgroups G_1 from* (b) *and G_0 from* (d) *coincide. In what follows we call G_1 the fundamental subgroup of G.*

(f) *In this part, $m \geq 3$ (i.e., we do not assume as in other parts that $m > p+1$). The group G has an element a such that $|C_G(a)| = p^2$, i.e., $C_G(a) = \langle a, K_{m-1}(G)\rangle$.*

Theorem 9.7. *A nonabelian p-group G is of maximal class if and only if $G/K_{p+1}(G)$ is of maximal class.*

Theorem 9.8. (a) *Absolutely regular p-groups G (i.e., G with $|G/\mho_1(G)| < p^p$) are regular.*

(b) *If a p-group G is such that $|G'/\mho_1(G')| < p^{p-1}$, then G is regular.*

(c) *Any irregular p-group G has a characteristic subgroup R of order $\geq p^{p-1}$ and exponent p such that $R \leq G'$.*

Theorem 9.11. *A p-group G, $p > 2$, is metacyclic if and only if $|G/\mho_1(G)| \leq p^2$.*

Exercise 9.13. Let G be a p-group of maximal class, $p > 2$, and $H < G$. Then $d(H) \leq p$. If $d(H) = p$, then $G \cong \Sigma_{p^2} \in \mathrm{Syl}_p(S_{p^2})$. In particular (Blackburn), if G is a p-group of maximal class, $p > 2$, $N \lhd G$ and $G/N \cong \Sigma_{p^2}$, then $N = \{1\}$.

Theorem 10.1. *Let $p^n > 2$ and let $A < G$ be abelian of exponent p^n. Then the number of abelian subgroups $B \leq G$ of order $p|A|$ that contain A is congruent to* 1 *modulo p.*

Corollary 10.2. *Let N be a normal subgroup of a p-group G and let $A < N$ be a maximal G-invariant abelian subgroup of exponent $\leq p^n$, where $p^n > 2$. Then we have $\Omega_n(C_N(A)) = A$.*

Theorems 10.4 and 10.5. *Suppose that G is a p-group, $p > 2$. Let $\epsilon_n(G)$ be the number of elementary abelian subgroups of order p^n in G. If $k \in \{3, 4\}$ and $\epsilon_k(G) > 0$, then we have $\epsilon_k(G) \equiv 1 \pmod{p}$.*

Exercise P2. Let G and k be such as in the previous theorem.

(a) If $Z_k(G)$ has no G-invariant elementary abelian subgroup of order p^k, then we have $\epsilon_k(G) = 0$.

(b) If a G-invariant subgroup N of G has no G-invariant elementary abelian subgroup of order p^k, then $\epsilon_k(N) = 0$.

Lemma 10.8. *Suppose that G is a minimal nonnilpotent group. Then $G = PQ$, where $P \in \mathrm{Syl}_p(G)$, $Q = G' \in \mathrm{Syl}_q(G)$ and*

(a) *P is cyclic, $|P : (P \cap \mathrm{Z}(G)| = p$.*

(b) *Q is either elementary abelian or special, $|Q/\Phi(Q)| = q^b$, where b is the order of q modulo p.*

(c) *If Q is special, then b is even and $\Phi(Q) = \mathrm{Z}(Q) \leq \mathrm{Z}(G)$, $|\Phi(Q)| \leq p^{b/2}$.*

Theorem (Frobenius' normal p-complement theorem). *If a group G has no p-closed minimal nonnilpotent subgroup of order divisible by p, then G has a normal p-complement ($= p$-nilpotent).*

Theorem (Burnside's normal p-complement theorem). *If a Sylow p-subgroup of a group G is contained in the center of its normalizer, then G is p-nilpotent.*

Proposition 10.17. *If $B \leq G$ is a nonabelian subgroup of order p^3 in a p-group G and $C_G(B) < B$, then G is of maximal class.*

Remark 10.5. Let $H < G$ and assume that $\mathrm{N}_G(H)$ is of maximal class. Then G is also of maximal class.

Proposition 10.19. *Suppose that H is a nonabelian subgroup of order p^3 in a metacyclic p-group G. If $p > 2$, then $G = H$. If $p = 2$, then G is of maximal class.*

Proposition 10.28. *A nonabelian p-group G is generated by minimal nonabelian subgroups. In particular, if, in addition, G is not minimal nonabelian, it contains two nonconjugate minimal nonabelian subgroups.*

Theorem 10.33. *If all minimal nonabelian subgroups of a nonabelian 2-group G are generated by involutions, then $G = \langle x \rangle \cdot A$, where $A \in \Gamma_1$ is abelian and all elements in $G - A$ are involutions (such G is said to be* generalized dihedral*).*

Theorem 12.1. (a) *If a p-group G has no normal subgroup of order p^p and exponent p, then G is either absolutely regular or irregular of maximal class.*

(b) *If an irregular p-group G has an absolutely regular maximal subgroup H, then it is either of maximal class or $G = H\Omega_1(G)$, where $\Omega_1(G)$ is of order p^p (and, of course, of exponent p).*

Exercise P3. If $\Omega_p(G)$ has no G-invariant subgroup of order p^p and exponent p, then G is either absolutely regular or of maximal class.

Theorem 12.12. *Let a group G of order p^m be neither absolutely regular nor of maximal class and suppose that $H \in \Gamma_1$ is of maximal class. Then*

(a) $\mathrm{d}(G) = 3$.

(b) *Set $v = m - 2$ if $m \leq p + 1$ and $v = p$ if $m > p + 1$. Then $G/\mathrm{K}_v(G)$ is of order p^{v+1} and, if $m > 4$, it is of exponent p.*