DE GRUYTER
EXPOSITIONS
IN
MATHEMATICS
47

Yakov Berkovich
Zvonimir Janko

Groups of Prime Power Order

Volume 2

W
DE
G

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.

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

de Gruyter Expositions in Mathematics 47

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. $N \subseteq M$ ($N \nsubseteq M$) 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.

$\mathbb{Z}$ 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.

$\mathrm{GF}(p^m)$ 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 $\mathrm{Sc}(G)$. 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 $A, B \trianglelefteq G$, then $\mathrm{C}_G(B/A) = H$, where $H/A = \mathrm{C}_{G/A}(B/A)$.

$A \operatorname{wr} B$ 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 $|A|^{|B|}|B|$.

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

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

$\operatorname{Out}(G) = \operatorname{Aut}(G)/\operatorname{Inn}(G)$, 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 $H \le G$ 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 $\mathrm{K}_i(G) = [G, \dots, G]$ ($i \ge 1$ 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}.

$\mathrm{GL}(n, F)$ is the set of all nonsingular $n \times n$ matrices with entries in a field F, the n-dimensional *general linear* group over F, $\mathrm{SL}(n, F) = \{A \in \mathrm{GL}(n, F) \mid \det(A) = 1 \in F\}$, 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), $\Phi(\{1\}) = \{1\}$, $p^{\mathrm{d}(G)} = |G : \Phi(G)|$.

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

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 $m \in \mathbb{N}$, 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 $G' = \Phi(G) = \mathrm{Z}(G)$ 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 $\mathrm{cl}(G) = m-1$.

$\Omega_m(G) = \langle x \in G \mid o(x) \le p^m \rangle$, $\Omega_m^*(G) = \langle x \in G \mid o(x) = p^m \rangle$ and $\mho_m(G) = \langle x^{p^m} \mid x \in G \rangle$.

A p-group is absolutely regular if $|G/\mho_1(G)| < p^p$.

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 $H \le G$ 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 $F = \mathrm{GF}(p^n)$, then we write $\mathrm{GL}(m, p^n), \mathrm{SL}(m, p^n), \dots$ instead of $\mathrm{GL}(m, F)$, $\mathrm{SL}(m, F), \dots$.

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

$\mathcal{A}_n$-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

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

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 $w \in \mathbb{C}$).

$\mathrm{Irr}(\chi)$ 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.

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

If $N \trianglelefteq G$, 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 $H \lhd G$.

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 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.

Contents

Appendix

§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: $\mathbb{F} = \mathrm{GF}(p^m)$, $m > 1$; 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 $\mathbb{F}_\theta$ 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 $\mathrm{Irr}_1(G)$ denote the set of all nonlinear irreducible characters of G. Put $\mathrm{cd}(G) = \{\chi(1) \mid \chi \in \mathrm{Irr}(G)\}$. Next, $\mathrm{Irr}_{(t)}(G)$ denotes the number of characters of degree t in $\mathrm{Irr}(G)$.

Definition. The Suzuki p-group $\mathrm{A}_p(m, \theta)$ 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 $G = \mathrm{A}_p(m, \theta)$; 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 $(c, d) \in \mathrm{Z}(G)$ 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, $\mathrm{Z}(G) = \{(0, d) \mid d \in \mathbb{F}\}$. We have $\mathrm{Z}(G) \cong \mathrm{E}_{p^m}$. 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 $(a, b)^p \in \mathrm{Z}(G)$; moreover, if $p > 2$, then $\exp(G) = p$.

1^o. Throughout this subsection $p = 2$ and $G = \mathrm{A}(m, \theta) = \mathrm{A}_2(m, \theta)$. Our aim is to find $\mathrm{cd}(G)$ and the number of irreducible characters of every degree $s \in \mathrm{cd}(G)$.

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

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

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

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

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 $\mathrm{C}_G((a,b)) = \{(az, u) \mid z \in \mathbb{F}_\theta, u \in \mathbb{F}\}$ so $|\mathrm{C}_G((a,b))| = 2^{m+n}$. 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 $\mathrm{Z}(G) = \Omega_1(G)$. Therefore, since $\exp(G) = 4$, we get $\Omega_1(G) = \mho_1(G) = \Phi(G)$.

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

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 $o(\varphi_\lambda) = d = o(\lambda)$. □

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 $d = a^\delta - 1$. □