Lecture Notes in Mathematics

Edited by A. Dold and B. Eckmann

1112

Products of Conjugacy Classes in Groups

Edited by Z. Arad and M. Herzog

Springer-Verlag
Berlin Heidelberg New York Tokyo

Lecture Notes in
Mathematics

Edited by A. Dold and B. Eckmann

1112

Products of Conjugacy Classes in Groups

Edited by Z. Arad and M. Herzog

Springer-Verlag
Berlin Heidelberg New York Tokyo

Editors

Zvi Arad
Department of Mathematics, Bar-Ilan University
Ramat-Gan, Israel

Marcel Herzog
School of Mathematical Sciences
Raymond and Beverly Sackler Faculty of Exact Sciences
Tel Aviv University, Tel Aviv, Israel

AMS Subject Classification (1980): 20-02, 20-04, 20A05, 20A15, 20B30, 20B99, 20C05, 20C07, 20C15, 20C30, 20C32, 20D05, 20D06, 20D08

ISBN 3-540-13916-8 Springer-Verlag Berlin Heidelberg New York Tokyo
ISBN 0-387-13916-8 Springer-Verlag New York Heidelberg Berlin Tokyo

Printed in Germany

Printing and binding: Beltz Offsetdruck, Hemsbach / Bergstr.
2146 / 3140-543210

Lecture Notes in Mathematics

For information about Vols. 1–898, please contact your bookseller or Springer-Verlag.

Vol. 899: Analytic Number Theory. Proceedings, 1980. Edited by M.I. Knopp. X, 478 pages. 1981.

Vol. 900: P. Deligne, J. S. Milne, A. Ogus, and K.-Y. Shih, Hodge Cycles, Motives, and Shimura Varieties. V, 414 pages. 1982.

Vol. 901: Séminaire Bourbaki vol. 1980/81 Exposes 561–578. III, 299 pages. 1981.

Vol. 902: F. Dumortier, P.R. Rodrigues, and R. Roussarie, Germs of Diffeomorphisms in the Plane. IV, 197 pages. 1981.

Vol. 903: Representations of Algebras. Proceedings, 1980. Edited by M. Auslander and E. Lluis. XV, 371 pages. 1981.

Vol. 904: K. Donner, Extension of Positive Operators and Korovkin Theorems. XII, 182 pages. 1982.

Vol. 905: Differential Geometric Methods in Mathematical Physics. Proceedings, 1980. Edited by H.-D. Doebner, S.J. Andersson, and H.R. Petry. VI, 309 pages. 1982.

Vol. 906: Séminaire de Théorie du Potentiel, Paris, No. 6. Proceedings. Edité par F. Hirsch et G. Mokobodzki. IV, 328 pages. 1982.

Vol. 907: P. Schenzel, Dualisierende Komplexe in der lokalen Algebra und Buchsbaum-Ringe. VII, 161 Seiten. 1982.

Vol. 908: Harmonic Analysis. Proceedings, 1981. Edited by F. Ricci and G. Weiss. V, 325 pages. 1982.

Vol. 909: Numerical Analysis. Proceedings, 1981. Edited by J.P. Hennart. VIi, 247 pages. 1982.

Vol. 910: S.S. Abhyankar, Weighted Expansions for Canonical Desingularization. VII, 236 pages. 1982.

Vol. 911: O.G. Jørsboe, L. Mejlbro, The Carleson-Hunt Theorem on Fourier Series. IV, 123 pages. 1982.

Vol. 912: Numerical Analysis. Proceedings, 1981. Edited by G. A. Watson. XIII, 245 pages. 1982.

Vol. 913: O. Tammi, Extremum Problems for Bounded Univalent Functions II. VI, 168 pages. 1982.

Vol. 914: M. L. Warshauer, The Witt Group of Degree k Maps and Asymmetric Inner Product Spaces. IV, 269 pages. 1982.

Vol. 915: Categorical Aspects of Topology and Analysis. Proceedings, 1981. Edited by B. Banaschewski. XI, 385 pages. 1982.

Vol. 916: K.-U. Grusa, Zweidimensionale, interpolierende Lg-Splines und ihre Anwendungen. VIII, 238 Seiten. 1982.

Vol. 917: Brauer Groups in Ring Theory and Algebraic Geometry. Proceedings, 1981. Edited by F. van Oystaeyen and A. Verschoren. VIII, 300 pages. 1982.

Vol. 918: Z. Semadeni, Schauder Bases in Banach Spaces of Continuous Functions. V, 136 pages. 1982.

Vol. 919: Séminaire Pierre Lelong – Henri Skoda (Analyse) Années 1980/81 et Colloque de Wimereux, Mai 1981. Proceedings. Edite par P. Lelong et H. Skoda. VII, 383 pages. 1982.

Vol. 920: Seminaire de Probabilites XVI, 1980/81. Proceedings. Edite par J. Azema et M. Yor. V, 622 pages. 1982.

Vol. 921: Seminaire de Probabilites XVI, 1980/81. Supplement: Géométrie Différentielle Stochastique. Proceedings. Edité par J. Azéma et M. Yor. III, 285 pages. 1982.

Vol. 922: B. Dacorogna, Weak Continuity and Weak Lower Semicontinuity of Non-Linear Functionals. V, 120 pages. 1982.

Vol. 923: Functional Analysis in Markov Processes. Proceedings, 1981. Edited by M. Fukushima. V, 307 pages. 1982.

Vol. 924: Séminaire d'Algèbre Paul Dubreil et Marie-Paule Malliavin. Proceedings, 1981. Edité par M.-P. Malliavin. V, 461 pages. 1982.

Vol. 925: The Riemann Problem, Complete Integrability and Arithmetic Applications. Proceedings, 1979-1980. Edited by D. Chudnovsky and G. Chudnovsky. VI, 373 pages. 1982.

Vol. 926: Geometric Techniques in Gauge Theories. Proceedings, 1981. Edited by R. Martini and E.M.de Jager. IX, 219 pages. 1982.

Vol. 927: Y. Z. Flicker, The Trace Formula and Base Change for GL (3). XII, 204 pages. 1982.

Vol. 928: Probability Measures on Groups. Proceedings 1981. Edited by H. Heyer. X, 477 pages. 1982.

Vol. 929: Ecole d'Eté de Probabilités de Saint-Flour X – 1980. Proceedings, 1980. Edited by P.L. Hennequin. X, 313 pages. 1982.

Vol. 930: P. Berthelot, L. Breen, et W. Messing, Théorie de Dieudonné Cristalline II. XI, 261 pages. 1982.

Vol. 931: D.M. Arnold, Finite Rank Torsion Free Abelian Groups and Rings. VII, 191 pages. 1982.

Vol. 932: Analytic Theory of Continued Fractions. Proceedings, 1981. Edited by W.B. Jones, W.J. Thron, and H. Waadeland. VI, 240 pages. 1982.

Vol. 933: Lie Algebras and Related Topics. Proceedings, 1981. Edited by D. Winter. VI, 236 pages. 1982.

Vol. 934: M. Sakai, Quadrature Domains. IV, 133 pages. 1982.

Vol. 935: R. Sot, Simple Morphisms in Algebraic Geometry. IV, 146 pages. 1982.

Vol. 936: S.M. Khaleelulla, Counterexamples in Topological Vector Spaces. XXI, 179 pages. 1982.

Vol. 937: E. Combet, Integrales Exponentielles. VIII, 114 pages. 1982.

Vol. 938: Number Theory. Proceedings, 1981. Edited by K. Alladi. IX, 177 pages. 1982.

Vol. 939: Martingale Theory in Harmonic Analysis and Banach Spaces. Proceedings, 1981. Edited by J.-A. Chao and W.A. Woyczynski. VIII, 225 pages. 1982.

Vol. 940: S. Shelah, Proper Forcing. XXIX, 496 pages. 1982.

Vol. 941: A. Legrand, Homotopie des Espaces de Sections. VII, 132 pages. 1982.

Vol. 942: Theory and Applications of Singular Perturbations. Proceedings, 1981. Edited by W. Eckhaus and E.M. de Jager. V, 363 pages. 1982.

Vol. 943: V. Ancona, G. Tomassini, Modifications Analytiques. IV, 120 pages. 1982.

Vol. 944: Representations of Algebras. Workshop Proceedings, 1980. Edited by M. Auslander and E. Lluis. V, 258 pages. 1982.

Vol. 945: Measure Theory. Oberwolfach 1981, Proceedings. Edited by D. Kölzow and D. Maharam-Stone. XV, 431 pages. 1982.

Vol. 946: N. Spaltenstein, Classes Unipotentes et Sous-groupes de Borel. IX, 259 pages. 1982.

Vol. 947: Algebraic Threefolds. Proceedings, 1981. Edited by A. Conte. VII, 315 pages. 1982.

Vol. 948: Functional Analysis. Proceedings, 1981. Edited by D. Butković, H. Kraljević, and S. Kurepa. X, 239 pages. 1982.

Vol. 949: Harmonic Maps. Proceedings, 1980. Edited by R.J. Knill, M. Kalka and H.C.J. Sealey. V, 158 pages. 1982.

Vol. 950: Complex Analysis. Proceedings, 1980. Edited by J. Eells. IV, 428 pages. 1982.

Vol. 951: Advances in Non-Commutative Ring Theory. Proceedings, 1981. Edited by P.J. Fleury. V, 142 pages. 1982.

continued on page 249

Dedicated to the memory of

DR. RITA HERZOG

the late wife of the second editor

Products of Conjugacy Classes in Groups

CONTENTS

Introduction.

This book presents recent progress on covering theorems for simple groups. These results, as well as the methods, have applications in diverse areas of group theory.

Let G be a group, C any nontrivial conjugacy class of G. We define a regular covering theorem to be a theorem which guarantees, under certain conditions, that for a positive integer m and every conjugacy class $C \neq 1$, $C^m = G$. An extended covering theorem guarantees, under appropriate conditions, that for a positive integer r, $\prod_{i=1}^{r} C_i = G$ for every sequence $C_1, C_2, \ldots, C_r$ of (not necessarily distinct) nontrivial conjugacy classes of G.

The basic theorems establish the existence of such m and r for finite nonabelian simple groups and for certain types of infinite simple groups. While the general problem of determining minimal values for m and r is as yet unsolved, we have obtained a number of interesting results. We denote by $cn(G)$ (covering number of G) and $ecn(G)$ (extended covering number of G) the minimal values for m and r, respectively. Clearly $cn(G) \leq ecn(G)$.

Covering theorems for finite simple groups were first studied by J. Brenner and his associates [2-10]. Focusing especially on An, $n \geq 5$, they determined conjugacy classes C satisfying $C^m = G$, where $m = 2$, 3, or 4. In [2] the following conjecture appears: for $n \geq 6$, $cn(An) = [\frac{n}{2}]$. In [16] J. Stavi proved this conjecture. In Chapter 3 Y. Dvir showed that $ecn(An) = [\frac{n}{2}] + 1$, $n \geq 6$, and that this result implies $cn(An) = [\frac{n}{2}]$, $n \geq 6$. It is easy to check that $cn(A_5) = 3$, $ecn(A_5) = 4$.

In order to establish these extended covering numbers, Dvir developed a theory of the products of conjugacy classes in An and Sn, $n \geq 5$. This theory provided answers to a number of questions raised by Brenner. For example, in Chapter 3, Section 10, Dvir presents a characterization of conjugacy classes C of An which satisfy $C^3 = An$ (See [9]). In addition, a criterion is given which determines whether or not a permutation is a product of two cycles (see [7]).

Dvir's theory gives a new proof of a well-known theorem of Ree [15,11]. It also generalizes results of Brenner [10] and Bertram [1] and improves results of Herzog and Reid [12,13].

Let S denote the set of finite simple groups G for which we have computed cn(G) and ecn(G). This set consists of

1) An, $n \geq 6$ (Chapter 3)

2) $Sz(2^{2n+1})$, $n \geq 1$, cn(G) = 3, ecn(G) = 4 (Chapter 4)

3) PSL(2,q), $q = p^n > 2$, p a prime, cn(G) =3, ecn (G) = 4 (Chapter 4)

4) Nonabelian simple groups of order less than one million (Chapter 2)

5) M11, M12, M22, M23, M24, J_1, J_2, J_3, HS, SUZ, MCL, RU, HE, ON, C3 (Chapter 2).

As mentioned above, cn(G) ≤ ecn(G). We found, for all the groups in S, but one, that ecn(G) = cn(G) + 1, and in particular, a product of cn(G) nontrivial conjugacy classes covers at least $G - \{1\}$. The exception is C3 with cn(C3) = 3 and ecn(C3) = 5.

In addition we computed in Chapter 4, cn(G) for several families of infinite simple groups. We found an infinite simple group for which cn(G) = 2, but ecn(G) ≥ 4. M. Droste [18] state the following as a corollary of results of Chapter 4: Every infinite group G can be embedded into a simple group H of the same cardinality which satisfies cn(H) = 2.

The calculations drew upon the theories of permutations and group characters. A large digital computer was used extensively.

We conjecture that if G is a nonabelian simple group with k conjugacy classes, then cn(G) ≤ k-1 if G is finite, and cn(G) ≤ 2(k-1) if G is infinite. In Chapter 1 we show that for G

finite,

$cn(G) \le \min\{k(k-1)/2, 4k^2/9\}$ (Theorem 8.11),

$ecn(G) \le k(k+1)/2$ (Theorem 9.6),

$ecn(G) \le |G|$ (Theorem 9.8).

We obtained a sharper bound than $ecn(G) \le |G|$ by using the theory of group characters:

$ecn(G) \le 4|G|^{\frac{1}{2}} \ln|G|$ (Theorem 10.10).

J. Thompson conjectured that if G is a finite simple group, then there exists a conjugacy class C such that $C^2 = G$. We verified Thompson's conjecture for all the groups in S. This conjecture would imply the well-known conjecture of Ore [14] that every element of a finite nonabelian simple group is a commutator. We prove that if G is a finite simple group in which every element is a commutator, then $cn(G) \le 2(k-1)$. In view of the classification of the finite simple groups and our results, in order to establish these conjectures, it would suffice to compute cn(G) and ecn(G) for the remaining sporadic and Chevalley groups. For many of the Chevalley groups, this appears to be a difficult task.

For the following six groups in S we found that $C \nsubseteq C^2$ for a nonidentity conjugacy class C: U(3,3), U(4,2), U(3,4), L(3,5), HS and C3 (Chapter 2)

In every one of the groups in S we found a set of three distinct nontrivial conjugacy classes, whose product is G, and we conjecture that this holds for all nonabelian finite simple groups.

In Chapter 4 we show that if $cn(G) = 2$, and G is finite, then G is isomorphic to J1. For infinite groups, on the other hand, we present numerous examples of groups for which $cn(G) = 2$.

We conjecture that the product of two nontrivial conjugacy classes of a nonabelian finite simple group is not a conjugacy class. This holds for all groups in S. Proving this conjecture would provide an affirmative answer to a famous conjecture of Szep [17] that a factorizable group $G = AB$, where A and B are proper subgroups of G with nontrivial centers, is not simple. Special cases, which have been proved, include Burnside's $p^{\alpha}q^{\beta}$ Theorem and the Kegel-Wielandt Theorem on the solvability of groups which are a product of two nilpotent subgroups.

In Section 3 of Chapter 1 we generalize covering theory to perfect groups. We also study properties of products of subsets of G which are not necessarily conjugacy classes (Chapter 1, Section 3-6).

These investigations received their initial impetus from answering a question arising in Universal Algebra and Model Theory (Chapter 1, Section 2). The answer is an application of the basic covering theorem.

Each chapter of the book has been written as an independent article, with its own bibliography. Together they give a comprehensive picture of recent results on coverings of groups.

References

[1] E.A. Bertram, Even permutations as product of two conjugate cycles, J. Combinatorial Theory (A) 12 (1972), 368-380.

[2] J.L. Brenner, Covering theorems for finite nonabelian simple groups, l, Colloq. Math. 32 (1974), 39-48.

[3] J.L. Brenner, Covering theorems for nonabelian simple groups, ll, J. Combinatorial Theory, (A) 14 (1973), 264-269.

[4] J.L. Brenner and L. Carlitz, Covering theorems for finite nonabelian simple groups, lll Solution of the equation $x^2+y^2+y^{-2}=a$ in a finite field, Rend. Seminario Mat. di Padova 55 (1976), 81-90.

[5] J.L. Brenner, Covering theorems for finite nonabelian simple groups, lV, Jñānabha, Sec. A, 3 (1975), 77-84.

[6] J.L. Brenner, R.M. Cranwell and J. Riddell, Covering theorems for nonabelian simple groups, V, Pacific J. Math. 58 (1974), 55-60.

[7] J.L. Brenner and J. Riddell, Noncanonical factorization of a permutation (≡Covering theorems Vl), Amer. Math. Monthly, 84 (1977), 39-40.

[8] J.L. Brenner and J. Riddell, Covering theorems for nonabelian simple groups, Vll, Asymptotics in the alternating groups, Ars Combinatoria 1 (1976), 77-108.

[9] J.L. Brenner, Covering theorems for Finasigs Vlll - Almost all conjugacy classes in An have exponent ≤ 4, J. Austral. Math. Soc. 25 (1978), 210-214.

[10] J.L. Brenner, Covering theorems for finite nonabelian simple groups, lX, ARS Combinatoria 4 (1977), 151-176.

[11] W. Feit, R. Lyndon and L. Scott, A remark about permutations, J. Combinatorial Theory 18 (1975), 234-238.

[12] M. Herzog and K.B. Reid, Number of factors in k-cycle decompositions of permutations, Proc-4th Australian Conference Combinatorial Math (Springer Lecture Notes in Math. 560 (1976), 123-131.

[13] M. Herzog and K.B. Reid, Representation of permutations as products of cycles of fixed length, J. Austral. Math. Soc. 22 (1977), 321-331.

[14] O. Ore, Some remarks on commutators, Proc. Amer. Math. Soc. 2 (1951), 307-314.

[15] R. Ree, A theorem on permutations, J. Combinatorial Theory 10 (1971), 174-175.

[16] J. Stavi, Covering numbers of the alternating groups (manuscript).

[17] J. Szep, Sui gruppi factorizabili non semplici, Rend. Mat. e Appl. 22 (1963), 245-252.

[18] M. Droste, Products of conjugacy classes of the infinite symmetric groups, Discrete Math. 47 (1983), 35-48.

Chapter 1

Powers and Products of Conjugacy Classes in Groups

Z. Arad and J. Stavi

Bar-Ilan University
Ramat Gan, Israel

M. Herzog

Tel-Aviv University
Tel-Aviv, Israel

Contents

§1. Introduction

Let A be a subset of a group G. We say that A *covers* a subgroup H of G if there exists an integer n such that $A^n = H$. One of the major problems considered in this research is whether or not A covers G, and if so, what is the minimal integer satisfying $A^n = G$. In particular, we consider the case when A is a conjugacy class of G. The smallest integer n satisfying $C^n = G$ for each non-trivial conjugacy class of G is called the *covering number* of G and is denoted by $cn(G)$. The *extended covering number* of G, denoted by $ecn(G)$, is the smallest integer m such that $C_1 \cdot \ldots \cdot C_m = G$ for every choice of m non-trivial conjugacy classes $C_1, \ldots, C_m$ of G. If G is finite, then $cn(G)$ and $ecn(G)$ exist if and only if G is non-abelian simple. Upper bounds for $cn(G)$ and $ecn(G)$ are given in Sections 8, 9 and 10 of this research. The values of $cn(G)$ and $ecn(G)$ for some families of simple groups will be studied in other chapters of this book.

Covering problems for special families of groups, in particular the A_n, were studied by J. Brenner et al. in a series of paper [B1]-[B9], with an emphasis on classes C such that $C^2 = G$. Our interest in this subject arose from the direction of model theory and Boolean algebras. If G is a finite group and $\mathcal{B}$ is a Boolean algebra, then the existence of $cn(G)$ implies that the Boolean power $G(\mathcal{B})$ determines $\mathcal{B}$ uniquely up to isomorphism. Section 2 of this research is devoted to this problem; see also [St] and [BM].

Properties of powers of a subset A of a finite group G are investigated in Sections 3 and 4. In particular, it is shown that there always exists n such that A^n is a subgroup of G. In Section 5 some of these results are generalized to infinite groups.

In Section 6 some technical lemmas are proved, which are useful in Sections 8 and 9 for obtaining upper bounds for $cn(G)$.

Section 7 is devoted to derivation of bounds for various exponents of conjugacy classes of G, such as $e_3 = \min\{n \mid C^n$ is a subgroup of $G\}$, where C is a fixed conjugacy class of G. It is shown, for example, that $e_3 \leq \frac{1}{2}k^2$, where k denotes the number of conjugacy classes of G.

The methods of Sections 1-9 are elementary, while in Section 10 we use the character theory in order to improve some results of the earlier sections.

Notation and the basic covering theorem.

We shall use the standard notation of group theory. The identity element of every group G will be denoted by 1. The set $\{1\}$ will also be denoted by 1 and called the trivial subgroup (or conjugacy class) of G. If H is a nonempty subset of the group G, then $H \leq G$, $H \trianglelefteq G$, $H < G$, $H \triangleleft G$, denote, respectively: H is a subgroup of G, H is a normal subgroup of G, H is a proper subgroup of G and H is a proper normal subgroup of G. We shall often use the fact that if A is a nonempty *finite* subset of G and products of every two element of A belong to A, then $A \leq G$. The subgroup of G generated by a nonempty subset A (or $\{a, b, c, \ldots\}$) will be denoted by $<A>$ (or $<a, b, c, \ldots>$). To each $\phi \neq A \subseteq G$ there corresponds the normalizer subgroup of A in G, which is defined by $N_G(A) = \{x \in G \mid xA = Ax\}$. The subset A will be called normal in G if $N_G(A) = G$. If $\phi \neq A, B \subseteq G$ and at least one of the subsets is normal in G, then $AB = BA$, where $AB = \{ab \mid a \in A, b \in B\}$. The conjugacy class of $a \in G$ will be denoted by $Cl_G(a)$ or $Cl(a)$, where $Cl(a) = \{xax^{-1} \mid x \in G\}$. The conjugacy classes of G are normal subsets and therefore their multiplication is commutative. If $\phi \neq A_1, \ldots, A_n \subseteq G$, we define

$$\Pi\{A_i \mid i=1,\ldots,n\} = \{a_1 \cdot a_2 \cdot \ldots \cdot a_n \mid a_1 \in A_1, a_2 \in A_2, \ldots, a_n \in A_n\} .$$

Clearly $\{a^n \mid a \in A\} \subseteq A^n$; however, in general, these sets are not equal. The product of zero nonempty subsets of G is defined to be 1. In particular, $A^0 = 1$. If

$<A>$ is finite, then $<A> = \cup\{A^n \mid n = 0,1,...\}$. We also define $A^{-1} = \{a^{-1} \mid a \in A\}$ and for $n > 0$, $A^{-n} = (A^{-1})^n = (A^n)^{-1}$

Following Brenner [B1] the abbreviation FINASIG will be used for: finite non-abelian simple group

The following basic theorem is not new (see [B1] or [Fe, §6, Theorem 6]). However, the method of its proof reveals the basic technique which will be used in this paper in order to prove many of its generalizations.

Theorem 1.1. *(The basic covering theorem). Let G be a FINASIG and let $C \neq 1$ be a conjugacy class in G. Then there exists a positive integer m such that $C^m = G$.*

Proof. Choose $r > 0$ such that $1 \in C^r$. For example, choose r to be the order of a, where $C = Cl(a)$. For each $k \geq 0$ clearly:

$$C^{r(k+1)} = C^{rk} C^r \supseteq C^{rk} \cdot 1 = C^{rk}$$

and consequently:

$$1 \subseteq C^r \subseteq C^{2r} \subseteq \dots \ .$$

Since G is finite, there exists $k > 0$ such that $C^{kr} = C^{(k+1)r}$ and hence $C^{kr} = C^{(k+j)r}$ for each $j \geq 0$. In particular, $C^{kr} = C^{2kr} = (C^{kr})^2$ and since G is finite, $C^{kr} \leq G$. But C is a conjugacy class, hence a normal subset of G, and consequently $C^{kr} \trianglelefteq G$. Now G is a FINASIG, so it has a trivial center and thus $|C| > 1$. Let a,b be distinct elements of C. Then a^{kr} and $a^{(kr-1)}b$ are distinct elements of C^{kr} and therefore $C^{kr} \neq 1$. The simplicity of G now implies that $C^{kr} = G$, completing the proof of Theorem 1.1. □

If m is an integer satisfying Theorem 1.1, then clearly $C^{m+1} = GC = G$ and in general $C^n = G$ for $n \geq m$. As G has only a finite number of conjugacy classes, we obtain

Corollary 1.2. *If G is a FINASIG, then there exists a positive integer m such that $C^m = G$ for every nontrivial conjugacy class C in G.*

The minimal m with the property of Corollary 1.2 will be called *the covering number* of G. One of the basic goals of this paper, as well as of some papers to follow, will be to supply estimates for the covering number.

Finally we shall state Corollary 1.2 in a different way, which will be useful in the following section. We shall call a finite group $G \neq 1$ m- *good* if given any two elements a and b of G, $a \neq 1$, the following property holds: b is a product of m conjugates of a. In other words: $b \in (Cl(a))^m$ holds for every $a, b \in G$ such that $a \neq 1$. Clearly that is equivalent to the condition $C^m = G$ for every nontrivial conjugacy class C of G. Thus Corollary 1.2 states that a FINASIG G is m-good for some positive integer m. However, the converse is also true.

Corollary 1.3. *Let G be a nontrivial finite group. Then G is a FINASIG if and only if there exists m such that G is m-good.*

Proof. Suppose that G is m-good. In view of Corollary 1.2, we have only to prove that G is a FINASIG. If H is a normal subgroup of G containing $a \neq 1$, then $G = (Cl(a))^m \leq H$ and hence G is simple. Moreover, G is nonabelian, since otherwise $\{a\} = Cl(a)$ for each $a \in G$ and $G = \{a^m\}$ for every $a \neq 1$, a contradiction as $G \neq 1$. □

§2. Applications to Boolean powers

If G is a finite group, viewed as a discrete topological space, and if X is any topological space, define $C(X, G)$ as the group of all continuous functions from X to G with multiplication defined by $(fg)(x) = f(x)g(x)$ for every $f, g \in C(X, G)$ and $x \in X$. Notice that if $f \in C(X, G)$, then f obtains a finite number of values (since G is finite) and each value is obtained on an open and closed subset of X.

Denote by $Clop(x)$ the collection of open and closed subsets of X and view it as a Boolean algebra with the set-theoretical operations of union, intersection and complement. One can view $Clop(X)$ also as a partially ordered set with respect to the inclusion $\subseteq$ relation. It is well known that a partial ordering of a Boolean algebra determines its operations.

Theorem 2.1. *Let G be a nontrivial finite group and suppose that G is m-good for some positive integer m (by Corollary 1.3 this is equivalent to the condition: G is a FINASIG). Let X, Y be any topological spaces. If the groups $C(X,G)$ and $C(Y,G)$ are isomorphic, then the Boolean algebras $Clop(X)$ and $Clop(Y)$ are isomorphic.*

Proof. It suffices to show how the structure of $Clop(X)$ as a partially ordered set is determined by the structure of the group $C(X,G)$. In order to do so, we define for each $f \in C(X,G)$ its support by: $s(f) = \{x \in X \mid f(x) \neq 1\}$. For each $f \in C(X,G)$, $s(f)$ is an open and closed subset of X. Since G is nontrivial, for each set A in $Clop(X)$ there exists $f \in C(X,G)$ such that $A = s(f)$. Therefore, each set in $Clop(X)$ can be represented as an equivalence class of elements of $C(X,G)$ with respect to the relation $s(f) = s(g)$, and the partial ordering of $Clop(X)$ is induced on the equivalence classes by the relation $s(f) \subseteq s(g)$. Thus it suffices to show that it is possible to define the relations $s(f) = s(g)$, $s(f) \subseteq s(g)$ between elements f and g of $C(X,G)$ in an algebraic way from the group structure of $C(X,G)$. Now we shall apply the assumption that G is m-good in order to prove:

Lemma 2.2. *Let $g, f \in C(X,G)$. Then $s(f) \subseteq s(g)$ if and only if f is a product of m conjugates of g in the group $C(X,G)$.*

Proof of Lemma 2.2. Suppose, first, that $f = \Pi\{h_i g h_i^{-1} \mid i=1, \ldots, m\}$, where $h_1, \ldots, h_m \in C(X,G)$. Then whenever $g(x) = 1$, also $f(x) = 1$ and consequently, $s(f) \subseteq s(g)$. Suppose, on the other hand, that $s(f) \subseteq s(g)$. Let $(X_1, \ldots, X_n)$ be