Astérisque

MARCEL HERZOG

New results on subset multiplication in groups

Astérisque, tome 258 (1999), p. 309-315

<http://www.numdam.org/item?id=AST_1999__258__309_0>

Astérisque **258**, 1999, p. 309–315

NEW RESULTS ON SUBSET MULTIPLICATION IN GROUPS

by

Marcel Herzog

Abstract. — This paper presents results and open problems related to the following topics: group with deficient multiplication sub-tables, product bases in finite groups.

In this paper, I would like to discuss several topics which deal with subset multiplication in groups. The topics are:

(1) Deficient squares groups;
(2) Squaring bounds in groups;
(3) Deficient products in groups;
(4) Product bases in finite groups.

The paper will be concluded by a list of some related open problems.

The letter G will always denote a group and the center of G will be denoted by $Z(G)$.

1. Deficient squares groups

Let m be an integer and let M be an *m-subset* of G, i.e. $M \subseteq G$ and $|M| = m$. We say that M has the *deficient square property* if

$$|M^2| := |\{xy | x, y \in M\}| < |M|^2 = m^2 \ . \tag{1}$$

A group G has the *deficient squares property for m* ($G \in DS(m)$ in short) if (1) holds for all m-subsets M of G. A group G has the *deficient squares property* ($G \in DS$ in short) if $G \in DS(m)$ for some integer m. If G is a finite group, then of course $G \in DS$.

The first mathematician to consider the $DS(m)$ property was Gregory Freiman, who classified in [8] the $DS(2)$-groups and who collaborated with others in the classification of the $DS(3)$-groups (see [2] and [19]). It was Peter Neumann who raised the problem of classifying the DS-groups. During his visit to Australia in 1989 Peter Neumann proved that DS-groups belong to the family of finite-by-abelian-by-finite

1991 ***Mathematics Subject Classification.*** — 20F99, 20E34.

Key words and phrases. — Deficient squares groups, squaring bounds in groups, deficient products in groups, product bases in finite groups.

groups [22]. In a recent paper, Patrizia Longobardi, Mercede Maj and myself completely characterized the DS-groups. We proved

***Theorem 1.1* (cf. [9]).** — *A group $G \in DS$ if and only if either G is nearly-dihedral or $|G^{(2)}|$ is finite.*

Here a group G is called *nearly-dihedral* if it contains an abelian normal subgroup H of finite index, such that each element of G acts on H by conjugation either as the identity automorphism or as the inverting automorphism. By $G^{(2)}$ we mean $\langle g^2 | g \in G \rangle$. Instead of requiring $|G^{(2)}|$ to be finite, we could have required the finiteness of $|\{g^2 | g \in G\}|$. Our proof relies on the above mentioned result of Peter Neumann, the proof of which was included in our paper by his permission.

A group G is called *central-by-finite* or an *FIZ-group* if the center of G is of finite index in G. Clearly $G \in FIZ$ implies that G is a nearly-dihedral group and it follows by Theorem 1.1 that DS-groups are a generalization of FIZ-groups. In 1976, B.H.Neumann proved the following beautiful theorem:

***Theorem 1.2* (cf. [21]).** — *The group $G \in FIZ$ if and only if G does not contain an infinite independent subset.*

A subset M of G is called *independent* if $xy = yx$ for $x, y \in M$ implies $x = y$. If $G \in FIZ$, say $|G : Z(G)| = n$, then clearly the size of an independent subset of G is bounded by n. The difficulty in Theorem 1.2 lies in proving the other direction of the theorem.

Recently, Carlo Scoppola and myself characterized the DS-groups in the spirit of the B.H.Neumann's result. Call a subset M of G *fully-independent* if $uv = yz$ for $u, v, y, z \in M$ implies $u = y$ and $v = z$. We proved

***Theorem 1.3* (cf. [11]).** — *The group $G \in DS$ if and only if G does not contain an infinite fully-independent subset.*

Again, one direction of the theorem is trivial, since the existence of an infinite fully-independent subset in G clearly implies that $G \notin DS$. In our proof of the opposite direction, the following result of Babai-Sós [1,Proposition 8.1] was very useful:

***Theorem 1.4* (cf. [1]).** — *If U is an infinite subset of the group G, then U contains an infinite subset V such that: if $u, v, y, z \in V$ and $|\{u, v, y, z\}| \geq 3$, then $uv \neq yz$.*

The only non-trivial relations allowed in V by Theorem 1.4 are $xy = yx$ and $x^2 = y^2$. Thus, if $G \notin DS$, in order to construct an infinite fully-independent subset of G it suffices to construct an infinite subset U of G satisfying: $xy \neq yx$ and $x^2 \neq y^2$ for $x, y \in U$, $x \neq y$. By Theorem 1.4 U contains an infinite fully-independent subset of G.

2. Squaring bounds in groups

Of course, we can require from G more than the DS-property, i.e. not only $|M^2| < |M|^2$ for all m-subsets, but some stronger inequality. Such questions were considered

by Leonid Brailovsky in his Ph.D. thesis, written under the supervision of G. Freiman and myself. L. Brailovsky proved, among other results, the following

***Theorem 2.1* (cf. [6]).** — *The group $G \in FIZ$ if and only if there exists a positive integer k, such that*

$$|K^2| \leq k^2 - k$$

for each k-subset K of G.

I want to prove one direction of Theorem 2.1. The other direction is easy too, but a bit more technical.

I'll prove: If k is an integer and $G \notin FIZ$ then $|K^2| > k^2 - k$ for some k-subset K of G.

By Theorem 1.2, there exists an infinite independent subset U of G and by Theorem 1.4, U contains an infinite subset V such that $uv \neq yz$ for $u, v, y, z \in V$ with $|\{u, v, y, z\}| \geq 3$. Thus, if K is a k-subset of V, then the only non-trivial equalities among the elements of K^2 are of the type $x^2 = y^2$, thus yielding

$$|K^2| \geq k^2 - (k-1) > k^2 - k \ .$$

The proof is complete.

Suppose now that G is an abelian group. Then clearly

$$|K^2| \leq \frac{1}{2}k(k+1) \quad \text{for } k\text{-subsets } K \text{ of } G. \tag{2}$$

Does this property characterize the abelian groups? Generally speaking, the answer is NO. For $k = 1$, the inequality (2) always holds and for $k = 2$, the groups $G = Q_8 \times E$ satisfy (2), where Q_8 is the quaternion group of order 8 and E denotes an elementary abelian 2-group, finite or infinite. Moreover, if G is finite and $\frac{1}{2}k(k+1) \geq |G|$, then again (2) is trivially satisfied. But for the majority of cases, the answer is YES. More precisely, Leonid Brailovsky proved in his thesis

***Theorem 2.2* (cf. [4]).** — *If $k > 2$ is an integer and G is an infinite group, then (2) implies that G is abelian. In the finite case the same is true provided that $k^3 - k < \frac{1}{2}|G|$.*

Theorem 2.2 also holds if the bound $\frac{1}{2}k(k+1)$ in (2) is increased to $\frac{1}{2}k(k+1) + \frac{1}{2}(k-3)$, but then in the finite case we must require that $(k^2-3)(k-1) < \frac{1}{15}|G|$ (see [5]).

In the infinite case much more can be proved. We define the integral valued function of an integral variable

$$f(n) = \left\lceil \frac{5n^2 - 3n - 2}{6} \right\rceil$$

where $\lceil x \rceil$ for a real x denotes the smallest integer m such that $x \leq m$. In his thesis, L.Brailovsky proved:

***Theorem 2.3* (cf. [6]).** — *Let $k \geq 2$ be an integer. Then:*

1 : *If $|K^2| \leq f(k)$ for all k-subsets K of an infinite group G, then G is abelian.*

2 : *There exists a non-abelian infinite group G such that $|K^2| \leq f(k) + 1$ for all k-subsets K of G.*

So $f(n)$ is the best possible squaring bound for infinite abelian groups. Moreover, there is a gap between $\frac{1}{2}k(k+1)$ and $\lceil \frac{5k^2-3k-2}{6} \rceil$. Each infinite abelian group satisfies $|K^2| \leq \frac{1}{2}k(k+1)$ for all k-subsets, whereas for infinite non-abelian groups the bound for $|K^2|$ on all k-subsets is larger than $\lceil \frac{5k^2-3k-2}{6} \rceil$.

3. Deficient products in groups

Let n be a positive integer. We say that G has the *deficient products property for n* ($G \in DP(n)$ in short) if for all couples of n-sets X and Y in G the following inequality holds:

$$|XY \cup YX| < 2n^2 \ . \tag{3}$$

More generally, if k is an integer with $k \geq 2$, we say that $G \in DP(n,k)$ if all k-tuples $X_1, X_2, \ldots, X_k$ of n-sets in G satisfy

$$UP(X_1, \ldots, X_k) =_{def} |\cup \{X_i X_j | 1 \leq i,j \leq k,\ i \neq j\}| < (k^2 - k)n^2 \ . \tag{4}$$

Thus $DP(n) = DP(n,2)$. Finally, we say that $G \in DP$ if $G \in DP(n,k)$ for some positive integers n, k, $k \geq 2$.

In a recent paper, Federico Menegazzo from Padova and myself proved the following results concerning groups satisfying the various conditions which were introduced above.

***Theorem 3.1* (cf. [10]).** — *Let G be an infinite group. Then $G \in DP(n)$ if and only if G is abelian.*

This theorem follows easily from the following characterization of infinite non-abelian groups. First a definition: two subsets A and B of G are *product-independent* if whenever $a, a' \in A$ and $b, b' \in B$, then $ab \neq b'a'$ and $ab = a'b'$ or $ba = b'a'$ only if $a = a'$ and $b = b'$.

***Theorem 3.2* (cf. [10]).** — *Let G be an infinite group. Then G is non-abelian if and only if it contains two infinite product-independent subsets.*

Theorem 3.1 generalizes Theorem B of [17]. We proved also the following characterization of FIZ-groups.

***Theorem 3.3* (cf. [10]).** — *Let G be an infinite group. Then G contains $\aleph_0$ mutually product-independent infinite subsets if and only if $G \notin FIZ$.*

The characterization of infinite DP-groups is an easy consequence of Theorem 3.3.

***Theorem 3.4* (cf. [10]).** — *Let G be an infinite group. Then $G \in DP$ if and only if $G \in FIZ$.*

Consider now related but different conditions. Let $(n) = (n_1, n_2, \dots)$ be an infinite sequence of positive integers. We say that $G \in P^*_{(n)}$ ($G \in P^{**}_{(n)}$) if every infinite sequence $X_1, X_2, \dots$ of distinct subsets of G of sizes $|X_i| = n_i$ for all i contains a pair X, Y of distinct members satisfying $XY = YX$ ($|XY \cup YX| < 2|X||Y|$). If $n_i = n$ for all i write P^*_n for $P^*_{(n)}$. Theorem 1.2 states that $G \in P^*_1$ if and only if $G \in FIZ$. In [20] F. Menegazzo proved that an infinite group G satisfies P^*_n for $n \geq 2$ if and only if G is abelian. In [10] we proved:

Theorem 3.5. — *Let G be an infinite group. Then $G \in P^*_{(n)}$ with $n_i \geq 2$ for all i if and only if G is abelian.*

It is easy to see that Theorem 3.3 implies:

Theorem 3.6. — *Let G be an infinite group. Then $G \in P^{**}_{(n)}$ if and only if $G \in FIZ$.*

4. Product bases in finite groups

A subset A of a finite group G is called a *basis (2-basis)* of G if $A^2 =_{def} \{ab | a, b \in A\} = G$. The problem of finding bases for G of size $c|G|^{\frac{1}{2}}$ for families of finite groups, where c denotes a fixed real number, was first posed by H. Rohrbach in 1937 in [23]. Such bases were found for certain families by Rohrbach himself [23], by Bertram and Herzog [3] and by Jia [12,13]. Recently, two graduate students in the Tel-Aviv University Gadi Kozma and Arie Lev proved that such bases exist for the family of all finite groups. They proved:

Theorem 4.1 **(cf. [15])**. — *If G is a finite group then there exists $A \subset G$ such that $A^2 = G$ and $|A| \leq \frac{4}{\sqrt{3}}|G|^{\frac{1}{2}} \approx 2.3094|G|^{\frac{1}{2}}$.*

The proof of Theorem 4.1 was based on the following strengthening of the Brauer-Fowler theorem:

Theorem 4.2 **(cf. [18])**. — *If G is a finite group of a non-prime order then there exists a proper subgroup H of G with $|H| \geq |G|^{\frac{1}{2}}$.*

Brauer and Fowler proved only that $|H| \geq |G|^{\frac{1}{3}}$ for groups G of even order. However, the proof of Theorem 4.2 uses the classification of the finite simple groups. We were recently informed that results similar to Theorems 4.1 and 4.2 appeared in the computer-science oriented papers [14] and [7].

Finally, if h is a positive integer, a subset A of a finite group is called an *h-basis* if $A^h = G$. Kozma and Lev proved the following theorem about h-bases in finite solvable groups:

Theorem 4.3 **(cf. [16])**. — *Let G be a finite solvable group. Then G contains an h-basis A such that $|A| \leq (2h-1)|G|^{\frac{1}{h}}$.*

A similar theorem is probably true for all finite groups.

5. Some open problems

I am going to list now some open problems, which are related to the results mentioned in this lecture.

1. Let $G \in DS(m)$. Prove that there exists an integer $N = f(m)$ such that either $|G^{(2)}| \leq N$ or G is nearly-dihedral with $|G : H| \leq N$ (see Theorem 1.1).

2. Does there exist a purely graph-theoretical proof of Theorem 1.3? In other words, can one prove directly that the existence of fully-independent subsets of G of size m for all integers m implies the existence of an infinite fully-independent subset of G?

3. Let n and m denote positive integers. A group G has the *deficient n-powers property for m* ($G \in DNP(m)$ in short) if $|M^n| < |M|^n$ for all m-subsets M of G. A group $G \in DNP$ if $G \in DNP(m)$ for some integer m. A subset M of G is *n-fully-independent* if $x_1x_2 \dots x_n = y_1y_2 \dots y_n$ for $x_i, y_j \in M$ implies $x_i = y_i$ for $i = 1, 2, \dots, n$. Is it true that: $G \in DNP$ if and only if G does not contain an infinite n-fully-independent subset? (see Theorem 1.3)

4. Does there exist a constant c such that if $k > 2$ is an integer and G is a finite group satisfying condition (2), then G is abelian, provided that $k^2 < c|G|$? (see Theorem 2.2)

5. Does there exist a constant c such that if G is a finite group and $|G| \neq p, p^2, pq$, where p and q are arbitrary distinct primes, then there exists a proper subgroup H of G satisfying $|H| \geq c|G|^{\frac{2}{3}}$? (see Theorem 4.2)

6. Prove: Let h be a positive integer. Then there exists a function $f(x)$ such that if G is a finite group, then G has an h-basis A satisfying $|A| \leq f(h)|G|^{\frac{1}{h}}$? (see Theorem 4.3)

References

[1] Babai L. and Sós V.T., *Sidon sets in groups and induced subgraphs of Cayley graphs*, Europ. J. Combinatorics, **6**, 1985, 101-114

[2] Berkovich Ja.G., Freiman G.A. and Praeger C.E., *Small squaring and cubing properties for finite groups*, Bull. Austral. Math. Soc., **44**, 1991, 429-450

[3] Bertram E.A. and Herzog M., *On medium-size subgroups and bases of finite groups*, J. of Combin. Theory, Series A, **57**, 1991, 1-14

[4] Brailovsky L., *A characterization of abelian groups*, Proc. Amer. Math. Soc., **117**, 1993, no. 3, 627–629.

[5] Brailovsky L., *On the small squaring and commutativity*, Bull. London Math. Soc., **25**, 1993, 330–336.

[6] Brailovsky L., *Combinatorial conditions forcing commutativity of an infinite group*, J. of Algebra, **165**, 1994, no. 2, 394–400.

[7] Finkelstein L., Kleitman D. and Leighton T., *Applying the classification theorem for finite simple groups to minimize pin count in uniform permutation architectures*, VLSI algorithms and architectures, J.H. Reif(ed), Springer, 1989, 247-256

[8] Freiman G.A., *On two and three-element subsets of groups* Aeq. Math.,**22**, 1981, 140-152

[9] Herzog M., Longobardi P. and Maj M., *On a combinatorial problem in group theory*, Israel J. Math., **82**, 1993, no. 1-3, 329–340.

[10] Herzog M. and Menegazzo F., *On deficient products in infinite groups*, Rend. Sem. Mat. Univ. Padova, **93**, 1995, 1–6.

[11] Herzog M. and Scoppola C.M., *On deficient squares groups and fully-independent subsets* Bull. London Math. Soc., **27**, 1995, no. 1, 65–70.

[12] Jia X-D., *Thin bases for abelian groups*, J. Number Theory, **36**, 1990, 254-256

[13] Jia X-D., *Thin bases for finite nilpotent groups*, J. Number Theory, **41**, 1992, 303-313

[14] Kilian J., Kipnis S. and Leierson Ch.E., *The organization of permutation architectures with bussed interconnections*, Proc. 1987 IEEE Conf. On The Foundation Of Comp. Science, IEEE, 1987, 305-315

[15] Kozma G. and Lev A., *Bases and decomposition numbers of finite groups*, Arch. Math., **58**, 1992, 417-424

[16] Kozma G. and Lev A., *On h-bases and h-decompositions of the finite solvable and alternating groups*, J. Number Theory, **49**, 1994, no. 3, 385–391

[17] Lennox J.C., Hassanabadi A.M. and Wiegold J., *Some commutativity criteria*, Rend. Sem. Mat. Univ. Padova, **84**, 1990, 135-141

[18] Lev A., *On large subgroups of finite groups*, J. of Algebra, **152**, 1992, 434-438

[19] Longobardi P. and Maj M., *The classification of groups with the small-squaring property on 3-sets*, Bull. Austral Math. Soc., **46**, 1992, 263-269

[20] Menegazzo F., *A property equivalent to commutativity for infinite groups* Rend. Sem. Mat. Univ. Padova, **87**, 1992, 299-301

[21] Neumann B.H., *A problem of Paul Erdős on groups*, J. Austral. Math. Soc., **21**, 1976, 467-472, *Selected works of B.H.Neumann and Hanna Neumann*, **5**, 1003-1008

[22] Neumann P.M., *A combinatorial problem in group theory*, Private communication.

[23] Rohrbach H., *Anwendung eines Satzes der additiven Zahlentheorie auf eine gruppentheoretishe Frage*, Math. Z., **42**, 1937, 538-542

M. Herzog, School of Mathematical Sciences, Faculty of Exact Sciences, Tel-Aviv University, Tel-Aviv, Israel