Astérisque

YAKOV BERKOVICH

Questions on set squaring in groups

Astérisque, tome 258 (1999), p. 249-253

<http://www.numdam.org/item?id=AST_1999__258__249_0>

Astérisque **258**, 1999, p. 249–253

QUESTIONS ON SET SQUARING IN GROUPS

by

Yakov Berkovich

Abstract. — Some questions on small subsets in groups are posed and discussed.

Let M be a subset of a group G. Define

$$M^2 = \{x \mid x = ab, a, b \in M\},$$

the square of M. M is a set with a large square if $a, b, c, d \in M$ and $ab = cd$ implies $a = c, b =$ d. If M is a finite set note that $\mid M^2 \mid = \mid M \mid^2$. In the opposite case M is said to be a set with small square.

It is natural to consider two group subsets M, N as equivalent if they have equal multiplication tables. To be more precise, we give the following

Definition. — *Let $M \subseteq G, N \subseteq H$ where G, H are groups. A bijection φ from M onto N is said to be an S -isomorphism if for $a, b, c, d \in M$ the equality $ab = cd$ implies $\varphi(a)\varphi(b) = \varphi(c)\varphi(d)$, and conversely.*

The group isomorphism is an S-isomorphism, but the converse assertion is not true. Moreover, if G is a group with non-trivial centre then there exists an S-isomorphism from G onto G which is not a group isomorphism. The automorphism group AUT(M) of a group subset M is defined as usual. If M is a finite group set with great squaring then AUT(M) $\cong S_n$ where $n = \mid M \mid$.

Question 1. — *Find all group n-sets M with* AUT$(M) \cong \{1\}$.

Question 2. — *Is there for any group H a group set M such that* AUT(M) $\cong H$ *?*

Question 3. — *Find all group n-sets M such that* AUT(M) $\cong S_n$.

Question 4. — *Find all group n-sets M such that* AUT(M) $\cong A_n$ *(may be the set of all such M for $n > 3$ is empty).*

1991 ***Mathematics Subject Classification.*** — 20E34.
Key words and phrases. — Deficient squares groups, Squaring bounds in groups.

The classification of all group n-sets is a very difficult problem. Let Set(n) be the number of all pairwise non-isomorphic group n-sets. Then Set(2) = 4, Set(3) = 54 (G. Freiman); see[4,6].

Question 5. — *Find Set(4).*

Consider the easiest case $n = 2$. As we saw there are four distinct group 2-sets with the following squares (i.e., their multiplication tables):

$$\begin{array}{cccc} AB & AB & AB & AB \\ BA & BC & CA & CD \end{array}$$

We note that the number $Gr(n)$ of pairwise non-isomorphic groups of order n is not a monotone function. In the same time Set(n) is a monotone function.

Let us continue to consider the case $n = 2$. Suppose that G is finite. Denote by $P_G(i)$ the number of 2-sets of type i in G. The following result is due to Freiman: If $P_G(4) = 0$ then G is abelian or a dedekindian 2-group, and conversely [6]. Now $P_G(1) = 0$ if and only if G is of odd order, and $P_G(2) = 0$ if and only if G is an elementary abelian 2-group. Lastly $P_G(3) = 0$ if and only if a Sylow 2-subgroup S is normal in G and $P_S(3) = 0$ [4]. As A. Mann showed, a 2-group S has no squares of third type if and only if $x^2 = y^2 \Leftrightarrow (xy^{-1})^2 = 1$ for $x, y \in$ S. Next
$P_G(1) + P_G(2) =\mid G \mid k(G)$ where $k(G)$ is the class number of G(A.Mann);
$P_G(1) + P_G(3) =\mid G \mid r(G)$ where $r(G)$ is the number of real G-classes (a class K is real if $x \in K \Leftrightarrow x^{-1} \in K$);
$P_G(1) =\mid G \mid k_i(G)$ where $k_i(G)$ is the number of G-classes containing involutions. Note that $P_G(1) + P_G(3) =\mid \{(x, y) \in G \times G \mid x^2 = y^2\} \mid$.

In particular $P_G(i) \equiv 0 (\mathrm{mod} \mid G \mid)$.

Now we see that a fraction of commutative 2×2-squares in G is equal to

$$mc(G) =\mid G \mid k(G)/ \mid G \mid^2 = k(G)/ \mid G \mid,$$

the measure of commutativity of G. Note that $k(G) =$|Irr(G)|, the number of ordinary irreducible characters of G. Therefore we may study $mc(G)$ by means of representation theory. This function has a number of nice properties. For example, if $H \leq G$ then $mc(H) \geq mc(G)$; if H is normal in G then $mc(G) \leq mc(H)mc(G/H)$; see [1], §§7.8,7.11,11.3.

Question 6. — *Is it true that the number of n-subsets of given type in G is divisible by* $\mid G \mid$ *for small values n (for example, for* $n = 3$*) and large* $\mid G \mid$ *?*

A number of authors have classified all groups without 3×3-squares with 9 distinct elements; see [2].

Question 7. — *Classify all groups without* 4×4*-squares with 16 distinct elements.*

P. Neumann showed that if all n-subsets of G have small squares, then G contains a finite normal subgroup H such that G/H is an extension of an abelian group by a finite group. Herzog, Longobardi and Maj classified all such groups; see [7].

B. Neumann showed that $| G : Z(G) |$ is finite if and only if any infinite subset of G contains a pair of commuting elements.

Question 8. — *What we may say about a structure of G if any of its infinite subset contains a small square?*

If for some $k > 1$ there is a connection between $| M^2 |$ and k for all k-subsets M of G then in some cases we may make strong assertions on G. We note the following characterization of abelian groups:

Theorem **(L. Brailovsky)**. — *Let $k > 2$ be a positive integer such that $(k^2-3)(k-2) <| G | /15$ if G is finite. If*

$$| M^2 | \leq (k^2 + 2k - 3)/2$$

is true for any $M \subset G$ with $| M | = k$ then G is abelian.

We note that if G is abelian then $| M^2 | \leq k(k+1)/2$ for all such M.

It is interesting to consider a group generated by a set with small square or cube. Some results in this direction are contained in the following theorem

Theorem **(S. Brodsky)**

(a) If $| \{a,b\}^3 | < 7$ then the subgroup $\langle a,b\rangle$ is solvable.
(b) If $| \{a,b\}^4 | < 11$ then the subgroup $\langle a,b\rangle$ is solvable.
(c) The author completely described groups $G = \langle a,b\rangle$ for which

$$| \{a,b\}^3 | > 6 \text{ and } | \{a,b\}^4 | < 14.$$

This theorem was proved by means of a computer; see [5].

The set Q of $n \times n$-squares is said to be minimal, corresponding to a $n \times n$-square q, if it satisfies the following conditions:

(a) $q \in$ Q.
(b) Let $q_1 \in Q - \{q\}$ and T be the set of all groups containing $Q - \{q_1\}$. Then there exists a square $q_0 \notin Q - \{q_1\}$ which is contained in all groups of the set T.

Question 9. — *Find all one element minimal sets of $n \times n$-squares.*

Question 10. — *For $n = 3$ find for any square q all minimal sets containing q.*

We consider in the remaining part of the lecture "large subsets".

Theorem **(G. Freiman)**. — *Let M be a finite subset of a group G such that $\langle M\rangle = G$. Suppose that $| M^2 | < 1.5 | M |$. Then one of the following assertions is true;*
(a) M^2 is a subgroup of G.
(b) $M^2 = xH$ where H is a normal subgroup of G.

Question 11. — *Change in this theorem 1.5 to 2, i.e., consider the case when $| M^2 | \leq 2 | M | -1$.*

L. Brailovsky and G. Freiman described for torsion free groups the case when $| K^2 | = 2 | K | -1$. If K, M are finite subsets of a torsion free group then $| KM | \geq | K | + | M | -1 (Kemperman)$. L. Brailovsky and G. Freiman showed that if $| KM | = | K | + | M | -1$ then K and M are geometric progressions with the same factor.

Question 12. — *Let $M \subset G$ and for any $c \in G$ one has*

$$| (M \cup c)^2 - M^2 | \leq 1. \qquad (*)$$

Describe the position of M in G.

It is easy to show that if in Question 12 $| M | > 1$ then $G = \langle M \rangle$. Now if $| M | = 2$ then G is solvable of derived length 2. But in the case $| M | = 3$ this question is very complicated.

Many results on squares of large subsets are contained in the lecture of M. Herzog.

Question 12 is, in some sense, a development of the idea of special elements, which was studied by Brailovsky, Freiman, and Herzog. An element $a \in G$ is said to be (m, n)-special if for any $b \in G$ one has $| \{a, b\}^m | \leq$ n.

Let $S_{m,n}(G)$ be the set of all (m, n)-special elements of a group G. The same three authors proved that $S_{2,3}(G)$ and $S_{3,5}(G)$ are characteristic subgroups of G. We may consider the sets $S_{m,n}(G)$ as natural generalizations of the centre $Z(G)$ of G(we note that $Z(G) \subset S_{2,3}(G)$). However Brailovsky showed that, in general, $S_{3,6}(G)$ is not a subgroup of G(he found that among 2,328 groups of order 2^7 only two cases for which this subset is not a subgroup).

A group G is said to be a $P(m, n)$-group if for any subset $\{a_1, \ldots, a_m\}$ of G one has

$$| \{a_{\sigma(1)} \ldots a_{\sigma(m)} \mid \sigma \in S_m\} | \leq \text{ n.}$$

G. Freiman and B. Schein showed that G is a $P(3, 2)$-group if and only if $| G' | \leq 2$. They also proved the analogous result for $P(3, 3)$-groups. They obtained many important results on $P(3, 4)$-groups.

I hope that the approach inspired by Freiman's number theoretical investigations on finite subsets with small doubling will considerably increase the subjects of group theory and will lead to new interesting results. For further information and references, see Freiman's survey.

References

[1] Berkovich Y. G., Zhmud' E. M., *Characters of finite groups*, Part 1,2, Amer. Math. Soc., Providence, Rhode Island, 1998.

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

[3] Brailovsky L., Freiman G. A. and Herzog M., *Special elements in groups* , Suppl. Rend. Circ. Mat. Palermo, **2 (23)**, 1990, 33–42.

[4] Brailovsky L., Freiman G. A., *On two-elements subsets in groups*, Ann. N.Y. Acad. Sci., **373**, 1981, 183–190.

[5] Brodsky S., this volume.

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

[7] Herzog M., Longobardi P. and Maj M., *On a combinatorial problem in group theory*, Israel J. Math., **82**, 1993, 329–340.

Y. Berkovich, Department of Mathematics and Computer Science, University of Haifa, 31905 Haifa, Israel • *E-mail :* berkov@mathcs2.haifa.ac.il