Counting squares of two-subsets in finite groups

L.Brailovsky and M.Herzog
School of Mathematics and Statistics
The University of Sydney
Sydney, N.S.W., Australia
and
School of Mathematical Sciences
Raymond and Beverly Sackler Faculty of Exact Sciences
Tel-Aviv University, Tel-Aviv, Israel

Let G be a finite group of order g. If $K = (a, b)$ is a couple of elements of G - distinct or not - then the multiplication table

$$\begin{pmatrix} a^2 & ab \\ ba & b^2 \end{pmatrix}$$

of K is of one of the following types:

$$T_0 = \begin{pmatrix} A & A \\ A & A \end{pmatrix} \quad T_1 = \begin{pmatrix} A & B \\ B & A \end{pmatrix} \quad T_2 = \begin{pmatrix} A & B \\ B & C \end{pmatrix}$$
$$T_3 = \begin{pmatrix} A & B \\ C & A \end{pmatrix} \quad T_4 = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$$

where equal (distinct) letters denote the same (different) elements of K^2. Denote by $P_i(G) = P_i$ the number of couples K of elements of G of type T_i, $i = 0, 1, 2, 3, 4$. In this note we determine the values of the P_i in terms of $g = |G|$ and the number of certain conjugacy classes in G. It turns out that each P_i is a multiple of g. Moreover, we characterize groups satisfying $P_i = 0$ for all i except $i = 3$. Our final remark lists certain properties of groups satisfying $P_3 = 0$.

The results of this note are used in the forthcoming paper [3].

ARS COMBINATORIA 42(1996), pp. 207-210

Proposition 1. *Let G be a finite group. Then*

(1) $$P_0 = g$$

(2) $$P_1 = k_2 g$$

(3) $$P_2 = (k - 1 - k_2)g$$

(4) $$P_3 = (k_r - 1 - k_2)g$$

(5) $$P_4 = (g + 1 + k_2 - k - k_r)g$$

where k, k_2, k_r denote the number of conjugacy classes of G, the number of conjugacy classes of involutions in G and the number of real conjugacy classes of G (classes containing an element and its inverse), respectively.

Proof: It is clear that $P_0 = g$.

Suppose that $K = (a, b)$ is of type T_1; then $a^2 = b^2$ and $ab = ba$, but $a \neq b$. Let $b = ca$; then $c \in C_G(a)$ and $c^2 = 1$, so c is an involution. Conversely, if c is an involution and $a \in C_G(c)$, then (a, ca) is of type T_1. Thus

$$P_1 = \sum_{c^2=1, c\neq 1} |C_G(c)| = k_2 g .$$

In order to compute P_2, we shall compute $M = P_0 + P_1 + P_2$, which is the number of $K = (a, b)$ with $ab = ba$. Thus

$$M = \sum_{x \in G} |C_G(x)| = kg$$

and using the previous formulas we get (3).

In order to finish the proof, it clearly suffices to evaluate P_3. Consider $N = P_0 + P_1 + P_3$; then N is the number of $K = (a, b)$ with $a^2 = b^2$. For any $x \in G$ let

$$\theta_2(x) = |\{h \in G : h^2 = x\}| ;$$

then

$$N = \sum_{x \in G} \theta_2(x^2) .$$

Since θ_2 is a class function, we conclude that

$$\theta_2 = \sum_{\chi \in Irr(G)} \nu_2(\chi)\chi ,$$

where $Irr(G)$ is the set of irreducible characters of G and ν_2 is a complex function on $Irr(G)$. Hence

$$N = \sum_{x \in G} \sum_{\chi \in Irr(G)} \nu_2(\chi)\chi(x^2) = \sum_{\chi \in Irr(G)} \nu_2(\chi) \sum_{x \in G} \chi(x^2) .$$

It is known [2, 4.4] that

$$\nu_2(\chi) = \frac{1}{|G|} \sum_{x \in G} \chi(x^2) ,$$

so

$$N = |G| \sum_{\chi \in Irr(G)} (\nu_2(\chi))^2 .$$

Now $(\nu_2(\chi))^2 = 1$ if χ is real valued and $(\nu_2(\chi))^2 = 0$ otherwise [2, 4.5]. Moreover, the number of real valued irreducible characters of G is equal to the number of real conjugacy classes of G [2, Problem 6.13]. Thus

$$N = k_r g$$

and (4) follows by (1) and (2). □

Corollary 2. *Let G be a finite group and let Q_8 denote the quaternion group of order 8. Then*

(6) $P_1 = 0 \Longleftrightarrow$ *G is of odd order*

(7) $P_2 = 0 \Longleftrightarrow G \cong (Z_2)^n$

(8) $P_4 = 0 \Longleftrightarrow$ *either G is abelian or $G \cong Q_8 \times (Z_2)^n$*

Proof: Clearly (2) implies (6). It follows by (3) that $P_2 = 0$ if and only if the non-trivial conjugacy classes of G consist of involutions, which is clearly equivalent to G being isomorphic to $(Z_2)^n$. Finally, by (5), $P_4 = 0$ if and only if $g + 1 + k_2 - k - k_r = 0$. Since each real class with elements of order larger than two contains at least two elements, it is clear that in any group G we have

$$g \geq k + (k_r - 1 - k_2)$$

with equality if and only if two elements of G are conjugate only if they are the inverses of each other. Thus if $P_4 = 0$ then every subgroup of G is normal in G and hence $G = Q_8 \times (Z_2)^n \times A$, where A is an abelian group of odd order. Moreover, it follows from the above mentioned condition that $A = 1$. Conversely, in $Q_8 \times (Z_2)^n$ two elements are conjugate only if they are the inverses of each other. The proof of (8) is complete. □

Remarks:

(9) Another proof of (8) can be found in [1].

(10) The problem of characterizing groups satisfying $P_3 = 0$ remains open. The following remarks will contain some properties of such groups.

(11) Denote $G \in ES$ if $x^2 = y^2$ for $x, y \in G$ implies $xy = yx$, and denote $G \in CI$ if $x^{-1}yx = y^{-1}$ for $x, y \in G$ implies $y^2 = 1$. It follows from the definition of T_3 and from (4) that

$$P_3(G) = 0 \Longleftrightarrow G \in ES \Longleftrightarrow G \in CI .$$

(12) If $P_3(G) = 0$ and $H = \langle y \rangle$ is a cyclic subgroup of G of order 4, then $N_G(H) = C_G(H)$. Indeed, if $n \in N_G(H)$ then it follows from (11) that $G \in CI$ and hence if $n \in N_G(H)$ then $n^{-1}yn = y$. In particular if H is also normal in G then $H \leq Z(G)$.

(13) If $P_3(G) = 0$ then the involutions of G generate an abelian subgroup of G of exponent 2. Indeed, it follows from (11) that $G \in ES$ and hence if x, y are involution in G, then $xy = yx$.

References

[1] G.A.Freiman, On two- and three-element subsets of groups *Aequationes Mathematicae* **22** (1981), 140–152.

[2] I.M.Isaacs, Character Theory of Finite Groups, Academic Press, New York 1976.

[3] D.Slilaty and J.Vanderkam, Bounds on Squares of Two-Sets, To appear.