Answer to a 1962 question of Zappa on cosets of Sylow subgroups

Marston Conder

University of Auckland

Groups St Andrews, Birmingham, August 2017

Questions about cosets of Sylow subgroups

In 1962, Guido Zappa asked the following questions:

(1) Can a non-trivial coset Pg contain only elements whose orders are powers of p?

(2) If 'yes', can at least one element of Pg have order p?

Zappa derived some elementary properties of groups for which the answer to one or both of these questions is 'Yes', but was not able to answer the questions.

A similar question was raised by L.J. Paige:

(3) Does a non-trivial coset Pg of a Sylow 2-subgroup always contain an element of odd order?

Paige's question was answered by John Thompson, who showed in 1967 that that for certain primes q, such as 53, the group $\mathrm{SL}(2, q)$ is a counter-example; or in other words, a non-trivial coset of a Sylow 2-subgroup can sometimes contain only elements of even order.

This was taken further in 2014 by Daniel Goldstein and Robert Guralnick, who showed that for every odd prime p, there exist infinitely many finite simple groups in which some non-trivial coset Pg of a Sylow p-subgroup P contains only elements whose orders are divisible by p. Also Goldstein and Robert Guralnick repeated the first question of Zappa.

Until recently, however, both of the two questions by Zappa remained open.

A few observations (made by Zappa)

Suppose P is a Sylow p-subgroup of the finite group G, and every element of the non-trivial coset Pg is a p-element. WLOG we can assume G is generated by P and g. Then:

(a) If $p = 2$ then P cannot have exponent 2

Why? If $x \in P$ and $x^2 = g^2 = (xg)^2 = 1$ then g commutes with x, so $G = \langle P, g \rangle \cong P \times C_2$ but then P is not Sylow ...

(b) If $p = 3$ then P cannot have exponent 3

Why? A similar argument, showing that otherwise the subgroup C generated by conjugates of g by elements of P is an abelian 3-group, normalised by P, so PC is a 3-subgroup of G, and then $g \in C \subseteq P$, contradiction.

(c) The group G is insoluble

Why? If G were soluble, then by a 1928 theorem of Philip Hall (on Hall subgroups), P would have a p'-complement H in G, and then H would be a transversal for P in G, so every non-trivial coset of P would contain a p'-element.

(d) If G is the smallest finite group with the given property for the prime p, then G is a non-abelian simple group

Why? If G has a non-trivial normal subgroup N, then $N \neq P$, for otherwise g normalises P and $\langle P, g \rangle$ is a larger p-subgroup. Also $\overline{P} = PN/N \cong P/(P \cap N)$ is a Sylow p-subgroup of $\overline{G} = G/N$, and every element of $\overline{Pg} = NPg/N$ is a p-element, making $\overline{G} = G/N$ a smaller group with the given property. So G is simple, and as its order is not p, it is also non-abelian.

Some other consequences [MC]

(e) If $p = 2$, then P is non-cyclic and has order at least 8

Why? We know from (a) that P cannot have exponent 2, so $|P| \geq 4$ and $P \ncong C_2 \times C_2$. But also no finite non-abelian simple group has a cyclic Sylow 2-subgroup, and so P is not cyclic. In particular, $P \ncong C_4$, and thus $|P| \geq 8$.

(f) If $p = 3$, then $|P| \geq 9$, and if $|P| = 9$ then $P \cong C_9$

Easy, since C_3 and $C_3 \times C_3$ have exponent 3.

(g) $|P| \geq 5$

This follows immediately from (e) and (f).

Bigger theorem [MC]

The group G cannot be PSL$(2,q)$ for any prime-power q.

Proof: Assume the contrary, and that $G = \mathrm{PSL}(2,q)$.

Case 1) Suppose p divides q.

If $p = 2$ then P has exponent 2, which is impossible, so p is odd. Also P can be taken as the projective image of the subgroup of SL$(2,q)$ consisting of 2×2 matrices of the form $\begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}$, and every p-element of G is the projective image of a matrix with trace ± 2.

So now let g be the projective image of $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, with

$ad - bc = 1$ and $a + d = 2$ in GF(q). Then for every non-zero $\alpha \in$ GF(q) we have

$$\begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a + \alpha c & b + \alpha d \\ c & d \end{pmatrix},$$

with trace $a + \alpha c + d = 2 + \alpha c$.

If $c \neq 0$ then we can choose $\alpha \in$ GF(q) so that $\alpha c \notin \{0, -4\}$ and then this trace is not ± 2, so the corresponding element of Pg cannot have order p.

On the other hand, if $c = 0$ then both P and g lie in the projective image of the subgroup of upper triangular matrices, so $\langle P, g \rangle \neq G$. Hence this case is impossible.

Case 2) Suppose p does not divide q, and that p is odd.

Then P is cyclic, say of order $n = p^r$, and this divides one of $q+1$ or $q-1$ but not both.

By conjugating within $\mathrm{GL}(2,q)$ or $\mathrm{GL}(2,q^2)$ if necessary, we may suppose that P is generated by the projective image of

$$X = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}$$

for some primitive nth root λ of 1 in $\mathrm{GF}(q^2)$, and also that g is the projective image of $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ where $ad - bc = 1$ and $a + d = \mathrm{Tr}(A) = \lambda^t + \lambda^{-t}$ for some $t \in \mathbb{Z}_n \setminus \{0\}$.

Then $X^i A = \begin{pmatrix} \lambda^i a & \lambda^i b \\ \lambda^{-i} c & \lambda^{-i} d \end{pmatrix}$ and $\mathrm{Tr}(X^i A) = \lambda^i a + \lambda^{-i} d$.

But also the projective image of each X^iA lies in the non-trivial coset Pg, and hence is a non-trivial p-element, so $\mathrm{Tr}(X^iA)$ must be $\pm(\lambda^s + \lambda^{-s})$ for some $s \in \{1, 2, \ldots, \frac{n-1}{2}\}$.

By the pigeonhole principle, the traces of 3 such elements must coincide (up to multiplication by ± 1), and we find that $\mathrm{Tr}(X^iA) = \mathrm{Tr}(X^jA) = \pm\mathrm{Tr}(X^kA)$, which then implies that

$$\lambda^i a + \lambda^{-i} d = \lambda^j a + \lambda^{-j} d = \pm(\lambda^k a + \lambda^{-k} d).$$

Rearranging these gives $\lambda^{i+j} a = d = \pm\lambda^{j+k} a$, and therefore $0 = \lambda^{i+j} a \mp \lambda^{j+k} a = \lambda^j(\lambda^i \mp \lambda^k)a$.

But this gives $a = 0$ and then also $d = 0$, which contradicts the fact that $a + d = \mathrm{Tr}(A) = \lambda^t + \lambda^{-t} \neq 0$. Hence this case is impossible too.

Case 3) Suppose $p = 2$ and does not divide q.

This case is similar to case 2), and can be eliminated too.

Thus G cannot be $\mathrm{PSL}(2, q)$.

Corollary If $p = 2$ then $|P| \geq 16$.

Proof: Assume the contrary, and let G be a counter-example of minimum order. Then $|P| = 8$, since we know $|P| \geq 5$. Also we may assume that G is a non-abelian simple group,

Now up to isomorphism there there are just five groups of order 8, namely C_8, $C_4 \times C_2$, $C_2 \times C_2 \times C_2$, D_4 and Q_8, but:

- $P \ncong C_8$ since a Sylow 2-subgroup of G cannot be cyclic
- $P \ncong C_2 \times C_2 \times C_2$ since that has exponent 2
- $P \ncong C_4 \times C_2$ by a theorem of Walter (1969)
- $P \ncong Q_8$ by the Brauer-Suzuki theorem (1959).

Thus P is dihedral (of order 8). But now by the Gorenstein-Walter theorem (1962), G is isomorphic to A_7 or PSL$(2, q)$ for some odd prime-power q, and A_7 is easy to eliminate, and we just proved that PSL$(2, q)$ is impossible too. $\square$

So what are the answers to Zappa's two questions?

Is there an example where the non-trivial coset Pg contains only p-elements? or are there NONE?

Answers to both questions of Zappa

Quick answer: In the simple group PSL(3, 4) of order 20160, many non-trivial cosets of a Sylow 5-subgroup P contain only elements of order 5.

Proof: Let x and g be the projective images of the matrices

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & \lambda \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ \lambda^2 & 1 & \lambda \end{pmatrix}$$

where λ is an element of GF(4) such that $1 + \lambda + \lambda^2 = 0$, and let P be the cyclic subgroup generated by x. Then P is a Sylow 5-subgroup of PSL(3, 4), of order 5, and every element $x^i g$ of the coset Pg has order 5.

Alternative answer:

Consider the group generated by two elements x and g such that $x^5 = g^5 = (xg)^5 = (x^{-1}g)^5 = (x^2g)^5 = (x^{-2}g)^5 = 1$.

Adding the two relations

$$(xg^2)^4 = xgxgx^{-1}gx^{-1}g^{-1}xg^{-1}x^{-1}g^{-1}xg^{-1} = 1$$

gives a quotient G of order 20160 isomorphic to PSL(3, 4), and then in this group, the image of the coset Pg of the subgroup $P = \langle x \rangle$ has the required properties.

Other examples

Some other examples can be obtained simply by considering groups that contain a subgroup isomorphic to PSL(3, 4) with index coprime to 5, such as the direct product $\mathsf{PSL}(3,4) \times C_k$ for any $k \not\equiv 0 \bmod 5$, as well as PGL(3, 4), PSU(4, 3) and the Mathieu groups M_{22}, M_{23} and M_{24}.

Also there are other cases where P and g generate a larger group G, such as PSU(5, 2) and the Janko group J_3, as well as PSU(4, 3) again.

These can be found/verified with the help of MAGMA.

Some computations

Using MAGMA, it's possible to search through the database of all non-abelian simple groups of order up to 10^9 to find all small examples. We can ignore the groups PSL$(2, q)$, and some other cases – e.g. those where $p = 2$ and $|P| \leq 8$, or $p = 3$ and P has exponent 3.

The only examples that arise are those described earlier, viz. where G is one of PSL$(3, 4)$, M_{22}, PSU$(4, 3)$, M_{23}, PSU$(5, 2)$, J_3 or M_{24} (of orders 20160, 443520, 3265920, 10200960, 13685760, 50232960 and 244823040.

In all of these cases, $P \cong C_5$.

Summary

For a positive answer to Zappa's first question, we now know that $|P| \geq 5$ but $|P| \neq 8$ and $P \ncong C_3 \times C_3$.

We have many examples with $|P| = 5$, but none with $|P| \neq 5$.

Details published in *Adv. Math.* 313 (2017).

It is an open question as to whether P can be C_7 or C_9, or $|P| = 11$, or 13, or 16, etc.

Conjecture (somewhat flimsy) : $|P|$ can only be 5.

THANK YOU