UNFUSED INVOLUTIONS IN FINITE GROUPS - AN ADDENDUM

Martin R. Pettet
Department of Mathematics
The University of Toledo
Toledo, Ohio, U.S.A. 43606
E-mail: mpettet@math.utoledo.edu

Abstract

If p is a prime, r is an integer and $p^r > 2$, there exist infinitely many finite simple non-abelian groups containing an element x of order p^r such that if P is a Sylow p-subgroup of G containing x, $x^G \cap P = x^P$.

Let p be a prime. In [1], a p-element x of a finite group G was said to be *unfused* if for some (and hence, for any) Sylow p-subgroup P of G containing x, all G-conjugates of x in P are P-conjugate to it (i.e. $x^G \cap P = x^P$). The main result was that no non-abelian finite simple group can contain an unfused involution and in fact, if x is an unfused involution in an arbitrary finite group G, then $x \notin [G, x]$ (a result which bears some formal similarity to Glauberman's Z^*-theorem). Mentioned in the introduction was the fact that while this conclusion fails in general for elements of order 4, it holds for elements of arbitary p-power order if G is p-solvable. In this addendum, we record a simple demonstration that no such generalization of the unfused involution theorem can apply to arbitrary finite groups. In fact, *for any prime power $p^r \neq 2$, there exist infinitely many finite, simple, non-abelian groups containing unfused elements of order p^r.*

To facilitate a relatively uniform treatment of the cases $p = 2$ and $p > 2$, we let $p^* = 4$ if $p = 2$ and $p^* = p$ if $p > 2$. For any positive integer i, let i_p denote the largest power of p dividing i. Note that if k, i are integers with $1 \leq i \leq k$ and $d = \gcd(k, i)$ then the binomial coefficient $\binom{k}{i}$ is divisible by $\frac{k}{d}$. For $\frac{k}{d}\binom{k-1}{i-1}/\frac{i}{d} = \binom{k}{i} \in \mathbf{Z}$ and so, since $\gcd(\frac{i}{d}, \frac{k}{d}) = 1$, $\frac{i}{d}$ divides $\binom{k-1}{i-1}$, whence, $\binom{k}{i}/\frac{k}{d} = \binom{k-1}{i-1}/\frac{i}{d} \in \mathbf{Z}$.

An elementary number theoretic observation is needed to identify Sylow p-subgroups in our examples; namely, if q is an integer such that $q \equiv 1 \pmod{p^*}$ then $(q^k - 1)_p = k_p(q-1)_p$ for any positive integer k. Let $(q-1)_p = p^* p^t$ so $q = ap^*p^t + 1$ with $\gcd(a, p) = 1$ and $t \geq 0$. For any positive integer k,

$$q^k - 1 = (ap^*p^t + 1)^k - 1 = \sum_{i=0}^{k-2} a^{k-i} \binom{k}{i} (p^*p^t)^{k-i} + akp^*p^t.$$

Let $k_p = p^r$. We claim that for each i, $0 \leq i \leq k-2$, the corresponding term in the summation above is divisible by p^*p^{r+t+1}. Let $i_p = p^u$ and $j = \min(r, u)$. By the remark above, $\binom{k}{i}_p \geq p^{r-j}$ and so it suffices to show that p^{j+1} divides $(p^*)^{k-i-1}p^{t(k-i-1)}$. Because $k-i-1 \geq 1$, we may assume that $j \geq 1$. Also $p^j \leq k-i$ (since, in fact, p^j divides $k-i$) and so it is enough to show that p^{j+1} divides $(p^*)^{p^j-1}$. But for any $j \geq 1$, $j+1 \leq 2(2^j-1)$ and if $p > 2$ then $j+1 \leq p^j - 1$, so the claim is proved.

If $s = k/k_p$, it follows that $q^k - 1 = cp^*p^{r+t+1} + asp^*p^{r+t} = p^*p^{r+t}(cp+as)$ for some $c \in \mathbf{Z}$. Since $\gcd(as,p) = 1$, $(q^k-1)_p = p^*p^{r+t} = k_p(q-1)_p$ as required.

We now proceed with the construction of the promised examples. Let p be a prime and assume that $p^r \neq 2$. Let F_q be a finite field of order q where $(q-1)_p \geq p^*p^r$ and let $n \geq 3$ be a divisor of $(q-1)_p/p^r$. Let $V = (F_q)^n$ be the natural $GL_n(F_q)$-module with standard basis $\{v_1, v_2, \ldots, v_n\}$ and let $V_i = \langle v_i \rangle$ for $1 \leq i \leq n$.

Let $G = SL_n(F_q)$ and let x be the $n \times n$ diagonal matrix $diag(\lambda, \mu, \ldots, \mu)$, where μ is a primitive np^r-th root of unity in F_q and $\lambda = \mu^{1-n}$ (so $x \in G$). Note that $\lambda^{p^r} = \mu^{p^r}$ but $\lambda^{p^{r-1}} = \mu^{p^{r-1}}\mu^{-np^{r-1}} \neq \mu^{p^{r-1}}$ so $\bar{x} = xZ(G)$ has order p^r in $\bar{G} = G/Z(G) \cong PSL_n(F_q)$. We prove that $\bar{x}$ is unfused in $\bar{G}$.

Let M denote the subgroup of monomial matrices in $GL_n(F_q)$ (i.e. those which permute the V_i's) so $M = [D]X \cong (F_q^\times) \wr Sym(n)$, where $D \cong (F_q^\times)^n$ and $X \cong Sym(n)$ are the groups of $n \times n$ diagonal and permutation matrices, respectively. If $R \in Syl_p(X)$ then $S = [O_p(D)]R \in Syl_p(M)$. In fact, application of the number theoretic observation above to the formula $|GL_n(F_q)| = q^{n(n-1)/2}\prod_{i=1}^n (q^i - 1)$ yields that $|GL_n(F_q)|_p = |M|_p$ and so $S \in Syl_p(GL_n(F_q))$. Therefore, if $P = S \cap G$, then $x \in P \in Syl_p(G)$ and P consists entirely of monomial matrices. Note that $X \cap G \cong Alt(n)$ and $R \cap G \in Syl_p(X \cap G)$, whence, because n is a power of p and $n \geq 3$, $R \cap G$ is transitive on $\{V_1, V_2, \ldots, V_n\}$.

Assume now that $g \in G$ such that $x^g \in P$ (so x^g permutes the V_i's). The minimal polynomial of x^g is the quadratic $m(t) = (t-\lambda)(t-\mu)$ and so for any $v \in V$, the set $\{v, v^{x^g}, v^{(x^g)^2}\}$ is linearly dependent. In particular, every orbit of $\langle x^g \rangle$ in $\{V_1, V_2, \ldots, V_n\}$ has length at most 2. Therefore, $(x^g)^2$ leaves each V_i invariant and so each $V_i^{g^{-1}}$ is invariant under $x^2 = diag(\lambda^2, \mu^2, \ldots, \mu^2)$. Since $\lambda^2 \neq \mu^2$, this implies that each $V_i^{g^{-1}}$ is contained either in V_1 or in $V_2 \oplus V_3 \oplus \ldots \oplus V_n$. But then $(V_i^{g^{-1}})^x = V_i^{g^{-1}}$ for all i and so, in fact, each V_i is invariant under x^g (i.e. x^g is a diagonal matrix). The eigenvalues of x^g being the same as those of x, there is an integer $k \in \{1, 2, \ldots, n\}$ such that x^g has eigenvalue λ on V_k and μ on V_j for all $j \neq k$. But if $h \in R \cap G$ such that $V_1^h = V_k$, then this is true also of x^h. Hence, $x^g = x^h \in x^P$ and so $\bar{x}^{\bar{g}} \in \bar{x}^{\bar{P}}$. This proves that $\bar{x}^{\bar{G}} \cap \bar{P} = \bar{x}^{\bar{P}}$ and so $\bar{x}$ is unfused in the simple group $\bar{G}$.

Acknowledgements. The author is indebted to the Department of Mathematics and Statistics at McGill University for its kind hospitality during the preparation of this note.

References

[1] Martin R. Pettet, Unfused involutions in finite groups, *Comm. Algebra* (to appear).