Commuting elements in conjugacy classes: An application of Hall’s Marriage Theorem

John R. Britnell and Mark Wildon

December 9, 2008

Let $G$ be a finite group and let $H$ be a normal subgroup of prime index. Since the quotient group $G/H$ is abelian, each $G$-conjugacy class lies entirely within a coset of $H$. We say that the $G$-conjugacy class $g^G$ is non-split if $g^G = g^H$; this is the case if and only if $g$ commutes with an element of $G \setminus H$, or equivalently, if Cent$_G(g)$ meets every coset of $H$. The object of this paper is to prove the following theorem.

**Theorem 1.** Let $G$ be a finite group with a normal subgroup $H$ of prime index $p$. Let $Hx$ be any non-identity coset in the quotient group $G/H$. The collection of non-split conjugacy classes of $G$ may be partitioned into sets of the form

$$\{g_0^G, g_1^G, \ldots, g_{p-1}^G\}$$

where $g_m^G \subseteq Hx^m$ and $g_0, g_1, \ldots, g_{p-1}$ commute with one another.

Part of Theorem 1 is the purely numerical result that the number of non-split conjugacy classes lying in $H$ is equal to the number of conjugacy classes lying in any other coset of $H$. This is a special case of a far more general result of the authors [1], which describes the conjugacy classes and centralisers in any finite group $G$ which has a normal subgroup $H$ such that $G/H$ is cyclic. We remark here that if $H$ has arbitrary index $n$ in $G$, then the proof below will show that this numerical result still holds, provided we look only at the cosets of $H$ which generate $G/H$.

The proof of Theorem 1 has two steps. We first use a simple counting argument to give a direct proof of the numerical result just mentioned. We then use the famous Marriage Theorem of Philip Hall [2] to produce the required partition of the conjugacy classes of $G$.

**Theorem 2** (Hall’s Marriage Theorem). Suppose that $X$ and $Y$ are finite sets each with $k$ elements, and that a relation $\sim$ is defined on $X \times Y$. It is possible to order the elements of $X$ and $Y$ so that $X = \{x_1, x_2, \ldots, x_k\}$, $Y = \{y_1, y_2, \ldots, y_k\}$ and $x_i \sim y_i$ for $1 \leq i \leq k$, if and only if for every set of $r$ distinct elements of $X$, the total number of elements of $Y$ which relate to one of these elements is at least $r$. 
Many readers of this journal will already be familiar with Philip Hall’s result. For those who are not, we explain its name by mentioning that in one interpretation, $X$ is a set of men, $Y$ is a set of women, and two people are related by $\sim$ if they are willing to marry one another. Hall’s Marriage Theorem then gives a necessary and sufficient condition for $k$ marriages to take place. Halmos and Vaughan use this interpretation to give an elegant proof in [3].

Proof of Theorem 1

Since every class contained in $Hx$ is non-split, we may establish the purely numerical part of Theorem 1 by proving the following lemma.

Lemma 3. The number of conjugacy classes contained in $Hx$ is equal to the number of non-split classes contained in $H$.

Proof. Let $S$ be the set of elements of $H$ which belong to a non-split conjugacy class. The number of non-split conjugacy classes lying in $H$ is given by

$$\sum_{h \in S} \frac{1}{|h^G|} = \frac{1}{|G|} \sum_{h \in S} |\text{Cent}_G(h)|.$$

If $h \in S$ then its centraliser $\text{Cent}_G(h)$ meets every coset of $H$, and so $|\text{Cent}_G(h)| = p |\text{Cent}_{Hx}(h)|$. We use this to rewrite the second sum above as follows:

$$\frac{1}{|G|} \sum_{h \in S} |\text{Cent}_G(h)| = \frac{1}{|H|} \sum_{h \in S} |\text{Cent}_{Hx}(h)| = \frac{1}{|H|} \sum_{g \in Hx} |\text{Cent}_S(g)|.$$

Now, if $g \in Hx$ commutes with an element $h \in H$, then $h$ must belong to a non-split class. It follows that we may replace $\text{Cent}_S(g)$ with $\text{Cent}_H(g)$ in the last sum above. This shows that the number of non-split conjugacy classes lying in $H$ is

$$\frac{1}{|H|} \sum_{g \in Hx} |\text{Cent}_H(g)| = \frac{1}{|G|} \sum_{g \in Hx} |\text{Cent}_G(g)| = \sum_{g \in Hx} \frac{1}{|g^G|},$$

which is the number of conjugacy classes contained in $Hx$. $\square$

We now refine this lemma using Hall’s Marriage Theorem. Given two conjugacy classes $C$ and $D$ of $G$ we shall say that $C$ is linked to $D$, if there exist elements $s \in C$ and $t \in D$ such that $s$ and $t$ commute.
Lemma 4. Let $C_1, \ldots, C_k$ be the non-split conjugacy classes contained in $H$. The conjugacy classes contained in $H \times G$ may be ordered $D_1, \ldots, D_k$ so that $C_i$ is linked to $D_i$ for $1 \leq i \leq k$.

Proof. In order to apply Hall’s Marriage Theorem we only need to show that for any given indices $1 \leq i_1 \leq \cdots \leq i_r \leq k$, the number of conjugacy classes contained in $H \times G$ that are linked to one of $C_{i_1}, \ldots, C_{i_r}$ is at least $r$. Set $S = C_{i_1} \cup \cdots \cup C_{i_r}$. A conjugacy class is linked to one of $C_{i_1}, \ldots, C_{i_r}$ if and only if it contains an element commuting with at least one element from $S$. The number of linked conjugacy classes contained in $H \times G$ is therefore

$$\sum_{g \in H \times G} \frac{1}{|g^G|}.$$

Following closely the calculation used to prove Lemma 3, we have

$$\sum_{g \in H \times G} \frac{1}{|g^G|} = \frac{1}{|G|} \sum_{g \in H \times G} |\text{Cent}_G(g)|$$

$$= \frac{1}{|H|} \sum_{g \in H \times G} |\text{Cent}_H(g)|$$

$$\geq \frac{1}{|H|} \sum_{g \in H \times G} |\text{Cent}_S(g)|$$

$$= \frac{1}{|H|} \sum_{h \in S} |\text{Cent}_H(h)|$$

$$= \frac{1}{|G|} \sum_{h \in S} |\text{Cent}_G(h)|$$

$$= \sum_{h \in S} \frac{1}{|h^G|} = r,$$

which is the inequality we require. \[\square\]

To establish the existence of a partition of the collection of non-split $G$-conjugacy classes with the properties stated in Theorem 1, we shall need to invoke the following lemma.

Lemma 5. Let $c$ be an integer coprime with $|G|$. The function on $G$ given by $g \mapsto g^c$ induces a bijection between the conjugacy classes in $H \times G$ and the conjugacy classes in $H \times G^c$.

Proof. Suppose that $y$ and $z$ lie in $H \times G$ and that $y^c$ and $z^c$ are conjugate. Since $c$ is coprime with $|G|$, there exists an integer $d$ such that
\(cd \equiv 1 \mod |G|\). Now \(y^{cd} = y\) and \(z^{cd} = z\), and it follows that \(y\) and \(z\) are conjugate. Hence the function induced on the conjugacy classes is injective. By Lemma 3, the number of classes in \(Hx\) is the number of non-split classes in \(H\). But \(Hx\) is also a generator of the quotient group \(G/H\) (since \(p\) does not divide \(c\)), and so it contains the same number of classes as \(Hx\). Thus the function induces a bijection, as required.

Now suppose that in the pairing given by Lemma 4, the non-split conjugacy class \(hG \subseteq H\) is paired with \(gG \subseteq Hx\) where \(h\) and \(g\) commute. For \(i = 2, \ldots, p - 1\), let \(c_i\) be an integer coprime with \(|G|\) such that \(c_i \equiv i \mod p\). (If \(p, q_1, \ldots, q_r\) are all the primes dividing \(|G|\) then suitable \(c_i\) may be found by solving the simultaneous congruences \(c_i \equiv 1 \mod q_1, \ldots, c_i \equiv 1 \mod q_r\).)

Consider the set of conjugacy classes
\[
\{h^G, g^G, (g^{c_2})^G, \ldots, (g^{c_{p-1}})^G\}.
\]

It is clear that the elements of the set lie in distinct cosets of \(H\), since the integers \(c_i\) together with \(0\) and \(1\) form a complete set of residues modulo \(p\). Moreover, the elements \(\{h, g, g^{c_i} : i = 2 \ldots p - 1\}\) certainly commute with one another. Consider the collection of sets which are obtained in this way. Lemma 5 ensures that distinct sets are disjoint, and it follows easily that they partition the set of non-split classes of \(G\). This completes the proof of Theorem 1.

References

[1] J. R. Britnell and M. Wildon, On the distribution of conjugacy classes between the cosets of a finite group in a cyclic extension, Preprint (2007).

[2] P. Hall, On representatives of subsets, J. London Math. Soc., 10 (1935) 26–30.

[3] P. R. Halmos and H. E. Vaughan, The marriage problem, Amer. J. Math., 72 (1950) 214–215.