Possible Honours Project Topic (2015):

The Class Equation in Group Theory and its Applications

In a group G, we say that b is a *conjugate* of a if $b = cac^{-1}$ for some c. This is an equivalence relation on G, so G is partitioned by its *conjugacy classes*. The conjugacy class $\{cac^{-1} \colon c \in G\}$ containing a is denoted by (a). It consists of nothing but a iff a commutes with all elements of G, i.e., a belongs to the *centre* Z_G of G. For finite groups G, it follows that $|G| = |Z_G| + \sum_{i=1}^{n} |C_i|$, where $C_1, \ldots, C_n$ are the distinct conjugacy classes having more than one element. This is called the *class equation* of G. Despite its simplicity, it is a useful tool in arguments and has many interesting applications. A related result says that $|G| = |Z_a| \, . \, |(a)|$ for all $a \in G$, where Z_a is the set of all elements of G that commute with a.

One of the first uses of these equations comes when we address the converse of Lagrange's Theorem. In a finite group G, this theorem says that if H is a subgroup of G, then $|H|$ is a divisor of $|G|$. The converse, if it were true, would say that if k is any positive divisor of $|G|$, then G should have a subgroup of size k. This is already false in the 12-element alternating group A_4, which can be shown to have no subgroup of size 6. In what groups (and for which values of k) does the converse of Lagrange's Theorem hold?

It is a corollary of the Fundamental Theorem of Abelian Groups that the converse of Lagrange's Theorem holds in all *abelian* (finite) groups. After we see this, the question remains of interest for non-abelian groups. A theorem of Sylow establishes that, in an arbitrary finite group G, if a prime power p^r divides $|G|$, then G has a subgroup of size p^r. There is more than one way to prove this. One approach uses conjugacy classes and the class equation. These tools can also be applied to show that, for any prime number p, every group of order p^2 is abelian.

Among many further applications of the class equation, there is a famous result of Wedderburn. Recall that a *division ring* is a ring with unity, in which every nonzero element is invertible. Thus, a *field* is just a commutative division ring. The quaternions provide an example of a division ring $\mathbb{H}$ that is not a field. This ring $\mathbb{H}$ is infinite. Wedderburn's Theorem says that every *finite* division ring R is a field (i.e., its multiplication is commutative). Again, one way of proving Wedderburn's Theorem uses the class equation of the underlying group of nonzero elements of R.

A theorem of Landau says that, for any positive integer k, there are only finitely many (non-isomorphic) finite groups with exactly k conjugacy classes. In general, finding a lower bound for the number $k(G)$ of conjugacy classes of a finite group G (in terms of $|G|$) is an important topic in contemporary group theory. There are a number of open problems here. For example, it has been conjectured that there is a constant $C > 0$ for which every finite group G satisfies $k(G) > C \log_2 |G|$. A stronger conjecture due Bertram says that $k(G) \geq \log_3 |G|$.

The intended project would work through the theory of conjugates, centralizers and the class equation for finite groups, and would then explore a number of applications of the theory, including some of those mentioned above. The candidate would need a solid background in abstract algebra and should therefore have mastered WTW 381. Exposure to WTW 731 is not essential, but might be advantageous.

JG RAFTERY and HP TONG-VIET