Minimal Fitting Classes

Brendan McCann

This short survey provides an introduction to a developing area of finite soluble group theory. In it all groups considered will be taken to be finite and soluble, though some of the ideas discussed will have a more general validity. Background to the group theory involved can be found in [8]. We begin with the definition of a Fitting Class:

Definition 1 A Fitting Class $\mathcal{F}$ is a set of groups such that

(a) if $G$ belongs to $\mathcal{F}$ then so does every isomorphic copy of $G$ — this is the "class" property of $\mathcal{F}$;

(b) if $N \triangleleft G \in \mathcal{F}$ then $N \in \mathcal{F}$ i.e., $\mathcal{F}$ is closed with respect to normal subgroups;

(c) if $G = N_1N_2$, where $N_1$ and $N_2$ are normal subgroups of $G$ and belong to $\mathcal{F}$, then $G \in \mathcal{F}$ i.e., $\mathcal{F}$ is closed with respect to "normal products";

(d) $\mathcal{F}$ is non-empty — so all groups of order one are in $\mathcal{F}$.

Some examples of Fitting Classes are: $S_p$, the class of all $p$-groups for a fixed prime $p$; $S_\pi$, the class of all (soluble) $\pi$-groups, where $\pi$ is a collection of primes; $N_\pi$, the class of all nilpotent $\pi$-groups.

In order to provide a group-theoretic motivation for the study of Fitting Classes we mention briefly a result of Fischer, Gaschütz and Hartley [8]:

Theorem If $G$ is a finite soluble group and $\mathcal{F}$ is a Fitting Class, then there exists a unique conjugacy class of $\mathcal{F}$-injectors in $G$.

An $\mathcal{F}$-injector is a subgroup, $I$, of $G$ such that if $N$ is subnormal in $G$ (i.e., if there exists a finite chain $N \triangleleft N_1 \triangleleft \cdots \triangleleft N_k = G$) then $I \cap N$ is $\mathcal{F}$-maximal in $N$, that is $I \cap N \in \mathcal{F}$ and $I \cap N$ is contained in no other subgroup of $G$ which is in $\mathcal{F}$.

For example, the $S_p$-injectors of $G$ are the Sylow $p$-subgroups of $G$, and the Hall $\pi$-subgroups are the $S_\pi$-injectors.

Rather than pursue this structure-theoretic aspect of soluble group theory, we turn to the more mundane question of determining the smallest (i.e., minimal) Fitting Class containing some given group $G$. In most cases this is complicated and requires extensive knowledge about automorphism groups and normal products.

Definition 2 The Fitting class $\text{Fit}(G)$ is defined by

$\text{Fit}(G) = \bigcap \{\mathcal{F} : \mathcal{F}$ a Fitting Class containing $G\}$

$\text{Fit}(G)$ can be considered as the Fitting Class generated by $G$, since it is a Fitting Class which contains $G$ and is contained in every Fitting Class of which $G$ is an element. If $G$ is non-trivial $\text{Fit}(G)$ will contain all finite direct products of copies of $G$ and its normal subgroups. However, there are also normal products which are not direct products - and this fact makes the construction of Fitting Classes in general very difficult: For example the group $S_3 \times C_2$ (the normal group on three symbols, $C_2$ a cyclic group of order 2) is the normal (but not direct) product of two subgroups isomorphic to $S_3$. Thus by 1(c) $S_3 \times C_2 \in \text{Fit}(S_3)$ and then by 1(b) we also have $C_2 \in \text{Fit}(S_3)$. So there are 2-groups in $\text{Fit}(S_3)$, even though $S_3$ itself has no (sub)normal 2-subgroups.

There is one case where minimal Fitting Classes have been determined, namely: if $P$ is a non-trivial $p$-group then $\text{Fit}(P) = S_p$ (see [8] for a sketch of the proof); and, more generally, if $H$ is nilpotent and $|H| = P_1^{\alpha_1} \cdots P_k^{\alpha_k}$ where $P_i$ is a prime and $\alpha_i \neq 0, \ i = 1, \ldots, k$, then

$\text{Fit}(H) = N_\pi$

where

$\pi = \{p_1, \ldots, p_k\}$.

By considering non-nilpotent soluble groups, we come to the idea of Fitting length:

Definition 3 The Fitting length (also known as nilpotent length) of the soluble group $G$ is the smallest number $k$ such that there exists a series:

\[G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_k = 1\]
Minimal Fitting Classes

If $G_1$ and $G_2$ are both groups of Fitting length $k$, do either of the relations:

$$G_1 \in \text{Fit}(G_2) \text{ or } G_2 \in \text{Fit}(G_1)$$

hold?

In the case of Fitting length three, this question can be resolved in certain cases by using constructions due to Dark [4] and McCann [7,8]. These constructions take a single group $G$, which satisfies suitable restrictions about normal structure and its automorphism group, and derive a Fitting Class from it which is, like those of Hawkes, "near to being" $\text{Fit}(G)$. The fact that $G$ has Fitting length three is exploited in the proof in each case.

In order to state one of the nicer results we recall the definition of the Frattini subgroup:

The Frattini subgroup, $\Phi(G)$, of $G$ is the intersection of all maximal subgroups of $G$. $\Phi(G)$ can also be characterised in the following way:

$\Phi(G)$ consists of those elements which can be discarded from any set of generators so that the reduced set still generates $G$. Now let $G$ be a group such that

$$G/\Phi(O_2(G)) \cong S_4$$

where $O_2(G)$ is the product of all normal 2-subgroups of $G$. Then either $G \cong S_4$ or $G \notin \text{Fit}(S_4)$ and $S_4 \notin \text{Fit}(G)$. (The constructions used are essentially those of [8]).

Apart from direct applications of results about Fitting classes of Fitting length three or less, little is known about minimal Fitting classes of groups of Fitting length four or greater. It is possible that, due to their more complicated nilpotency structure, different problems will arise in the determination of such classes, but at present one can only speculate (no doubt vainly) as to what future research will reveal.

References


Asymmetric Cryptography

Patrick Fitzpatrick

1 Introduction

In recent years a great deal of attention has been focussed internationally on the twin problems of security and authentication in the use of electronic communication systems for a wide variety of transactions including information storage and retrieval, banking and financial transactions and the transfer of legal documents (contracts, invoices etc.). These problems may be summarised as follows:

(a) security – the message must not be capable of interpretation or alteration in any way by an unauthorised person;

(b) authentication — the identities of the parties involved in the communication must be reliably established in such a way that neither can later repudiate any part of the transaction.

The need for cryptographic systems is thus placed firmly in the public domain and is no longer the sole preserve of government, diplomatic and military establishments.

The classical solution to problem (a) is the encryption of messages using a secret key known only to the transmitter and receiver. The key itself must be exchanged by some reliable method — a trusted courier, for instance. However, as the number of participants grows (consider, for example, the national and international branch network of a large banking corporation) the problem of distribution and secure storage of keys becomes exceedingly difficult. Moreover, the classical method provides no solution whatever to problem (b).

Since the publication of Diffie and Hellman’s fundamental paper [8], it has widely been recognised that asymmetric (or two-key or public-key) cryptosystems represent in theory the best approach towards a solution of these problems. In practice there are few realistic working models — proposed implementatins have either been shown to be insecure or too costly for application in general. As a consequence, a good deal of research has also been devoted to other methods (such as Siegenthaler’s work on stream ciphers [40, 41]) and, in addition, attempts have been made to apply asymmetric tech-