ARTICLES

Minimal Fitting Classes

Brendan McCann

This short survey provides an introduction to a developing area of fini soluble group theory. In it all groups considered will be taken to be finite a soluble, though some of the ideas discussed will have a more general validit Background to the group theory involved can be found in [8]. We begin wi 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 t "class" property of $\mathcal{F}$;

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

(c) If $G = N_1N_2$, where N_1 and N_2 are normal subgroups of G and belong $\mathcal{F}$, 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: $\mathcal{S}_p$ the class of all p-groups for t prime p; $\mathcal{S}_\pi$ the class of all (soluble) π-groups, where π is a collection of prim $\mathcal{N}_\pi$, the class of all nilpotent π-groups.

In order to provide a group-theoretic motivation for the study of Fitti Classes we mention briefly a result of Fischer, Gaschütz and Hartley [5]:

Theorem *If G is a finite soluble group and $\mathcal{F}$ is a Fitting Class, then the 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 if there exists a finite chain $N \lhd N_1 \lhd \cdots \lhd N_k = G$) then $I \cap N$ is $\mathcal{F}$-maxim in N, that is $I \cap N \in \mathcal{F}$ and $I \cap N$ is contained in no other subgroup of which is in $\mathcal{F}$.

For example, the $\mathcal{S}_p$-injectors of G are the Sylow p–subgroups of G, and the Hall π-subgroups are the $\mathcal{S}_\pi$-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 $\mathbf{Fit}(G)$ is defined by

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

$\mathbf{Fit}(G)$ 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 $\mathbf{Fit}(G)$ 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 $S_3 \times C_2$ (S_3 is the symmetric 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) $S_3 \times C_2 \in \mathbf{Fit}(S_3)$ and then by 1(b) we also have $C_2 \in \mathbf{Fit}(S_3)$. So there are 2-groups in $\mathbf{Fit}(S_3)$, 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 $\mathbf{Fit}(P) = \mathcal{S}_p$ (see [8] for a sketch of the proof); and, more generally, if H is nilpotent and $|H| = P_1^{\alpha_1} \dots P_k^{\alpha_k}$ where P_i is a prime and $\alpha_i \neq 0, \quad i = 1, \dots, k$, then

$$\mathbf{Fit}(H) = \mathcal{N}_\pi$$

where

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

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:

$$1 = N_0 \lhd N_1 \lhd N_2 \lhd \cdots \lhd N_k = G\,,$$

with N_i/N_{i-1} nilpotent (for $i \geq 1$) and $N_i \lhd G$ (for each i).

Thus nilpotent groups are of Fitting length one, – the terms "metanilpotent" and "nilpotent by nilpotent" are used for fitting length two. The task of determining minimal metanilpotent Fitting Classes has turned out to be very complicated indeed. We return to the group S_3, which is the "smallest" metanilpotent group. We already have $C_2 \in \mathbf{Fit}(S_3)$ and so:

$$\mathbf{Fit}(C_2) = S_2 \subseteq \mathbf{Fit}(S_3)$$

Furthermore, from Hawkes [6], we have that if $G = PQ$, $P \lhd G$, P an elementary abelian 3-group, Q a 2-group, then $G \in \mathbf{Fit}(S_4)$.

However $\mathbf{Fit}(S_3)$ is *not* the class of all "3 by 2" groups (that is $\{2,3\}$-groups with normal Sylow 3-groups), since Camina [2] has shown: $D_{18} \notin \mathbf{Fit}(S_3)$ – where D_{18}, the dihedral group of order 18, is "the" non-trivial extension of C_9 by C_2.

In fact we do not know at present what groups $\mathbf{Fit}(S_3)$ consists of, and the same applies to the Fitting classes generated by most other "well-known" small soluble groups, such as e.g. A_4, the alternating group on four symbols, or D_{14}.

Some progress has been made with metanilpotent groups whose structures are more complicated than those of S_3 or A_4. By specifying a suitable group, H, say, of the form $H = AB$, $A \lhd H$, A a p-group of nilpotent class 2 or greater, B a q-group $p \neq q$, and by placing suitable restrictions on the q-automorphisms of H, constructions of Hawkes [6] and Cossey [3] will define a Fitting Class containing H, thus narrowing the range of groups which might possibly be in $\mathbf{Fit}(H)$. Indeed, Brison, using the Hawkes construction, has in [1] been able to give an example of a minimal Fitting class for a metanilpotent group. It must be noted, however, that these are rather isolated examples and that much awaits discovery in the area of minimal metanilpotent Fitting Classes.

Given that Fitting Classes of Fitting length three or more must contain metanilpotent groups, the determination of minimal Fitting classes for groups of Fitting length three or more will have to wait until the metanilpotent question has been resolved. However, some progress has been made on the following less general question:

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

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

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" $\mathbf{Fit}(G)$. 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 characterized 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 $G \notin \mathbf{Fit}(S_4)$ and $S_4 \notin \mathbf{Fit}(G)$. (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

[1] O. Brison, *Relevant Groups for Fitting Classes*, J. Algebra 68, 1981, 31-54.

[2] A.R. Camina, *A note on Fitting Classes*, Math. Zeitschrift 136, 1974, 351-352.

[3] J. Cossey, *On metanilpotent Fitting Classes*, Research Report No. 18, 1986, Australian National University, Canberra.

[4] R.S. Dark, *Some examples in the theory of injectors of finite soluble groups*, Math. Zeitschrift 127, 1972, 145-156.

[5] B. Fischer, W. Gaschütz and B. Hartley, *Injektoren endlicher auflösbare Gruppen*, Math. Zeitschrift 102, 1963, 300-305.

[6] T.O. Hawkes, *On metanilpotent Fitting Classes*, J. Algebra 63, 1980, 495-483.

[7] B. McCann, *On Fitting Classes of Groups of Nilpotent Length Three*, Dissertation, Universität Würzburg, 1985.

[8] B.McCann, *Examples of minimal Fitting Classes of Finite Groups*, Archiv der Mathematik,49(3), 1987, 179–186

Department of Mathematics
University College Galway

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)* cryptosymtems 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-