GROUPS WITH FEW ISOMORPHISM TYPES OF DERIVED SUBGROUPS

Derek J.S. Robinson

Department of Mathematics,

University of Illinois.

1. Introduction.

By a *derived subgroup* in a group G is meant the derived (or commutator) subgroup H' of a subgroup H of G. Define

$$\mathcal{D}(G)$$

to be the set of derived subgroups in the group G. A general question of interest is:

How important is the subset $\mathcal{D}(G)$ in $\mathcal{S}(G)$, the lattice of all subgroups of G?

One would expect consequences for the structure of G' if conditions are imposed on the set of derived subgroups.

A recent result in this direction is:

Theorem 1. *If G has finitely many derived subgroups and also G is locally graded, then G' is finite* ([2],[4]).

The classes $\mathfrak{D}_n$.

Let

$$\mathfrak{D}_n, \ (n \geq 1),$$

be the class of groups in which the number of isomorphism types of derived subgroup is at most n. Then

$$\mathfrak{D}_1 \subseteq \mathfrak{D}_2 \subseteq \cdots \mathfrak{D}_n \subseteq \cdots .$$

and $\mathfrak{D}_1$ is the class of abelian groups. Not much is known about $\mathfrak{D}_n$ for $n > 2$, apart from the following result.

Theorem 2.

(a) A finite $\mathfrak{D}_4$-group is soluble, but A_5 is a $\mathfrak{D}_5$-group.

(b) A finite soluble $\mathfrak{D}_n$-group has derived length at most n.

The class $\mathfrak{D}_2$.

We report on recent work on the structure of $\mathfrak{D}_2$-groups. (This is joint research with P. Longobardi, M. Maj and H. Smith [5]). First note that $G \in \mathfrak{D}_2$ *if and only if* $H' \simeq G'$ *for all non-abelian* $H \leq G$.

Examples of $\mathfrak{D}_2$-groups

(i) Abelian groups.

(ii) If G' is cyclic of order ∞ or a prime, then $G \in \mathfrak{D}_2$.

(iii) Free groups of countable rank.

(iv) Groups with all proper subgroups abelian, (and so all Tarski groups).

(v) $\mathbb{Q} * \mathbb{Z}$ (a locally free group).

(vi) Some examples of soluble $\mathfrak{D}_2$-groups are: S_3, A_4, $\mathrm{Dih}(2n)$ (n odd), $\mathrm{Dih}(\infty)$, $\mathbb{Z}\,\mathrm{wr}\,\mathbb{Z}$, $\mathbb{Z}_p\,\mathrm{wr}\,\mathbb{Z}$ ($p =$ a prime).

2. Some general results.

(i) *If $G \in \mathfrak{D}_2$, then G' is countable.*

For if G is non-abelian and $[g, h] \neq 1$ in G, let $H = \langle g, h\rangle$. Then $G' \simeq H'$, which is countable.

(ii) **Theorem 3.** *Let $G \in \mathfrak{D}_2$. If G has a non-trivial finite quotient, then $G \neq G'$*

Corollary. *Let $G \in \mathfrak{D}_2$. If G' has a proper subgroup of finite index, the derived series $\{G^{(\alpha)}\}$ of G reaches the identity subgroup transfinitely.*

Proof. Recall that $G^{(\alpha+1)} = \left(G^{(\alpha)}\right)'$ and, if λ is a limit ordinal, then $G^{(\lambda)} = \bigcap\limits_{\alpha<\lambda} G^{(\alpha))}$. There is an ordinal $\alpha \geq 1$ such that $G^{(\alpha)} = G^{(\alpha+1)}$, so that $G^{(\alpha)}$ is perfect. Suppose that $G^{(\alpha)} \neq 1$. Then $G^{(\alpha+1)} \neq 1$, so $G^{(\alpha)}$ is not abelian. Hence $G' \simeq \left(G^{(\alpha)}\right)' = G^{(\alpha+1)} = G^{(\alpha)}$, so that G' is perfect: but G' has a proper subgroup of finite index, contradicting Theorem 3.

A stronger result of a similar type is:

Theorem 4. *Let $G \in \mathfrak{D}_2$. If G'/G'' is non-trivial and has finite p-rank for $p \geq 0$, then G is soluble and G' is either finite elementary abelian-p or torsion-free abelian of finite rank.*

Corollary. *Let $G \in \mathfrak{D}_2$. If G is not soluble and G' is not perfect, then all elements of G with finite order belong to the centre $Z(G)$.*

Proof. Let $a, b \in G$ have a finite order and put $H = \langle a, b \rangle$. Suppose H is not abelian. Then $G' \simeq H'$ and $G'/G'' \simeq H'/H''$. Now H/H' is finite, so H' is finitely generated and not perfect. By Theorem 4 the subgroup H is soluble, whence G is too, a contradiction.

Hence H is abelian and the elements of finite order in G form an abelian normal subgroup F. If $F \not\leq Z(G)$, then $[F, g] \neq 1$ for some $g \in G$. Hence $\langle g, F \rangle' = [F, g] \neq 1$ and $G' \simeq [F, g] \leq F$, so G' is abelian, a contradiction. Therefore $F \leq Z(G)$.

But note that $\mathrm{Dih}(\infty)$ is generated by elements of order 2.

As an application one can prove that if A, B are non-trivial abelian groups, the free product $A * B$ belongs to $\mathfrak{D}_2$ if and only if either $|A| = 2 = |B|$ or A and B are countable and torsion-free.

3. Classifying $\mathfrak{D}_2$-groups.

A general classification of $\mathfrak{D}_2$-groups is not to be expected: there are too many different types. But it is possible for certain subclasses, for example nilpotent groups.

Theorem 5. *A nilpotent group G belongs to $\mathfrak{D}_2$ if and only if either it is abelian or G' is cyclic of prime or infinite order.*

Finite $\mathfrak{D}_2$-groups.

First we note that if *G is a finite $\mathfrak{D}_2$-group, then G' is abelian, so G is metabelian.* Indeed suppose G is not soluble. Then G' is not abelian. Hence G' has a minimal non-abelian subgroup H and $G' \simeq H'$. By a classical result of G.A. Miller and H.C. Moreno [6], H is soluble. Hence so is G', and thus G is soluble, a contradiction. It follows from Theorem 2 that G is metabelian.

Constructing finite $\mathfrak{D}_2$-groups.

Let p be a prime and $m > 1$ an integer prime to p. Let

$$n = |p|_m$$

be the *order of p modulo m*, i.e., the smallest $n > 0$ such that $p^n \equiv 1 \pmod{m}$. Let F be a finite field of order p^n. Then F^* has a (cyclic) subgroup $X = \langle x \rangle$ of order m.

We make $A = F^+$ into an X-module via the field multiplication and define

$$G(p, m) = X \ltimes A,$$

the semidirect product, which is a metabelian group of order mp^n.

Lemma 1. *$G(p, m) \in \mathfrak{D}_2$ if and only if $|p|_m = |p|_d$ for $1 < d|m$.*

(Call such a pair (p, m) an *allowable pair*)

Proof (sufficiency). Assume (p, m) allowable and let H be a non-abelian subgroup of $G = G(p, m)$. Then H has the form

$$\langle x^r a_0,\ H \cap A \rangle$$

where $1 \le r < m$, $a_0 \in A$ and $H \cap A \neq 1$. Now $H \cap A$ is an $\langle x^r \rangle$-submodule of A. Since $\gcd(p, m) = 1$, Maschke's Theorem shows that $H \cap A$ is a direct sum of faithful simple $\langle x^r \rangle$-modules, each of which has dimension $|p|_d$ where $d = |x^r| = \dfrac{m}{\gcd(m, r)} > 1$. By hypothesis $|p|_d = |p|_m = n$, so that $H \cap A = A$ and $A \le H$. Hence $H = \langle x^r, A \rangle$ and $H' = [A, x^r] = A$ since F is a field. Thus $G \in \mathfrak{D}_2$.

Arbitrary finite $\mathfrak{D}_2$-groups can be described in terms of these $G(p, m)$.

Theorem 6. *Let G be a non-nilpotent group with G' finite. Then $G \in \mathfrak{D}_2$ if and only if the following hold:*

(i) *$G = X \ltimes A$ where $A = G'$ is elementary abelian-p and $X/C_X(A)$ is cyclic of order m;*

(ii) *$C_X(A) = Z(G)$, $G/Z(G) \simeq G(p, m)$, and (p, m) is allowable.*

Some remarks on allowable pairs.

(i) (p, m) is allowable if and only if $|p|_m = |p|_q$ for all primes $q|m$.

(ii) Let $m = q_1^{e_1} \cdots q_k^{e_k}$ be the primary decomposition of m. Then (p, m) is allowable if and only if each $(p, q_i^{e_i})$ is allowable and $|p|_{q_1} = \cdots = |p|_{q_k}$.

This reduces the problem of finding allowable pairs (p, m) to the case $m = q^e$, with q a prime.

(iii) **Lemma 2.** *If $q \neq p$ is a prime, then (p, q^e) is allowable if and only if*

$$p^{q-1} \equiv 1 \pmod{q^e}.$$

The condition in Lemma 2 always holds if $e = 1$, but rarely if $e > 1$. Define $e(p, q) > 0$ to be maximum subject to

$$p^n \equiv 1 \pmod{q^{e(p,q)}}$$

where $n = |p|_q$. Then $1 \leq e(p, q) < p^n$. Clearly (p, q^e) is allowable if and only if $e \leq e(p, q)$.

Question: Given a prime p, does there exist a prime q such that $e(p, q) \geq 2$, or equivalently such that

$$p^{q-1} \equiv 1 \pmod{q^2}?$$

Group theoretically we are asking if $G(p, q^2) \in \mathfrak{D}_2$.

This is a hard number theoretic problem. A prime q such that $p^{q-1} \equiv 1 \pmod{q^2}$ is called a *base-p Wieferich prime* (after Arthur Wieferich 1884–1954). A computer search shows that for all $p < 100$, with the possible exception of $p = 47$, there is at least one base-p Wieferich prime.

The case $p = 2$.

Only two base-2 Wieferich primes q are known, i.e., such that $2^{q-1} \equiv 1 \pmod{q^2}$, namely

$$1093 \text{ and } 3511.$$

There are no others $< 6 \cdot 10^9$.

There is a connection with Fermat's Last Theorem. In 1909 Wieferich proved that if there is a non-trivial solution of $x^q + y^q = z^q$ with q a prime and $q \nmid xyz$, (which is referred to as FLT1), then q is a base-2 Wieferich prime. This was subsequently extended to base-p Wieferich primes for primes $p \leq 89$ by Granville and Monagan [3].

4. Soluble $\mathfrak{D}_2$-groups.

Theorem 7. *Let G be a non-nilpotent soluble $\mathfrak{D}_2$-group. Then*

(i) *$A = G'$ is abelian, so G is metabelian.*

(ii) *A is elementary$-p$ or free abelian or torsion-free of finite rank.*

(iii) *If A is torsion-free of finite rank, then $G/C_G(A)$ is finitely generated and each $x \in G \backslash C_G(A)$ acts fixed-point-freely on A.*

(iv) *If $1 < [B, \langle x \rangle] \leq B \leq A$ where $x \in G$, then $B \simeq A$.*

(v) *Nilpotent subgroups of G are abelian.*

Note that (iv) is a weak form of $\langle x \rangle$-simplicity

The case of finite rank.

When $A = G'$ is torsion-free of finite rank, a soluble $\mathfrak{D}_2$-group G is constructible up to finite index from an algebraic number field.

Construction.

Let F be an algebraic number field and let $1 < X \leq F^*$ with X finitely generated. Put $A_0 = F^+$; then A_0 is an X-module via the field multiplication. Set $C = \mathrm{Rg}\,\langle X \rangle$, which is a submodule of A_0, and define

$$G(F, X) = X \ltimes C.$$

Then $G(F, X)$ is finitely generated and metabelian, since $G(F, X) = \langle X, 1_F \rangle$. Note that if X is a group of algebraic units in F, then $G(F, X)$ is polycyclic.

Lemma 3. *With the above notation, $G(F, X)$ is in $\mathfrak{D}_2$ if and only if $B \simeq A$ whenever $0 \neq B = Bx \leq A$, $x \neq 1$ in X. (*This is a strong form of rational irreducibility*).*

Call (F, X) *allowable* in analogy with the finite case.

Theorem 8. *Let $G \in \mathfrak{D}_2$ be an infinite soluble group with G' of finite rank. Then there is a normal subgroup G_0 with finite index in G such that $G_0/Z(G_0) \simeq G(F, X)$ where (F, X) is allowable.*

Example

Let $F = \mathbb{Q}(\sqrt{3})$, $c = 1 + \sqrt{3}$ and $X = \langle c \rangle$. Then $c^2 - 2c - 2 = 0$, so $C = \mathrm{Rg}\,\langle c \rangle$ satisfies $C = 2C$. Hence C is a free $\mathbb{Q}_2$-module of rank 2 where $\mathbb{Q}_2 = \left\{ \frac{m}{2^n} | m, n \in \mathbb{Z} \right\}$. Let $k > 0$; then c^k has irreducible polynomial of the form $t^2 + 2rt + 2s$, $(r, s \in \mathbb{Z})$. If $0 \neq B = Bc^k \leq A$, then $B = 2B$, so B is a free $\mathbb{Q}_2$-submodule of rank 2, since $\mathbb{Q}_2$ is a PID. Hence $B \simeq A$, so (G, X) is allowable and $G(F, X) \in \mathfrak{D}_2$.

Finally, a result on insoluble $\mathfrak{D}_2$-groups.

Theorem 9. *Let G be a group with a non-cyclic free subgroup. Then $G \in \mathfrak{D}_2$ if and only if G' is free of countable rank and L' is not finitely generated whenever L is a non-abelian subgroup of G.*

Corollary. *A locally free group G belongs to $\mathfrak{D}_2$ if and only if G' is is a free group of countable rank.*

References

[1] F. de Giovanni and F. de Mari. Groups with finitely many derived subgroups of non-normal subgroups. Arch. Math. (Basel) **86** (2006), 310–316.

[2] F. de Giovanni and D.J.S. Robinson. Groups with finitely many derived subgroups. J. London Math. Soc. (2) **71** (2005), 658–668.

[3] A. Granville and M.B. Monagan. The first case of Fermat's Last Theorem is true for all prime exponents up to 714, 591, 416, 091, 389. Trans. Amer. Math. Soc. **306** (1988), 329-359.

[4] M. Herzog, P. Longobardi and M. Maj. On the number of commutators in groups. Ischia Group Theory 2004, 181-192, Contemp. Math., **402**, Amer. Math. Soc., Providence, RI, 2006.

[5] P. Longobardi, M. Maj, D.J.S Robinson and H. Smith. preprint.

[6] G.A. Miller and H.C. Moreno. Non-abelian groups in which every subgroup is abelian. Trans. Amer. Math. Soc. **4** (1903), 398–404.