Inverse group theory

Peter J. Cameron
University of St Andrews
(with J. Araújo and F. Matucci)

CIRCA lunch
15 March 2018

Inverse group theory

Let F be a "functor" from groups to groups. (I don't intend any special sense here, just that $F(H)$ is a group constructed from the group H.)
Most investigation is about what properties $F(H)$ has.
The Inverse Problem asks: Given a group G, does there exist a group H with $F(H) = G$?
Some cases are trivial. For example:

> The centre $Z(H)$ of a group H must be abelian. But for every abelian group G, there is a group H with $Z(H) = G$: just take $H = G$.

Derived group

The only case I consider here is that of the derived group of a group.
The derived group H' of H is the subgroup of H generated by all commutators $[a, b] = a^{-1}b^{-1}ab$, for $a, b \in H$.
Following calculus, we will say that the group G is integrable if $G = H'$ for some group H.
I want to tell you two things about integrable groups.

Finiteness

Theorem

Let G be a finite group. If $G = H'$ for some group H, then there is a finite group H such that $G = H'$.

Proof.

First, we may suppose that H is finitely generated, since we can replace it by the subgroup generated by elements $a_1, b_1, \ldots$ whose commutators $[a_1, b_1], \ldots$ generate G.

Next, any conjugacy class in H is contained in a (finite) coset of $H' = G$, so H is a bfc-group. Now the centre of a finitely generated bfc-group is finitely generated, so is the direct product of a finite group and a torsion-free group; factoring out the torsion-free group gives the result. □

Orders of non-integrable groups

Theorem

Given a positive integer n, every group of order n is integrable if and only if n is cube-free and there do not exist prime divisors p, q of n with $q \mid p-1$.

This might remind you of another theorem:

Theorem

Given a positive integer n, every group of order n is abelian if and only if n is cube-free and there do not exist primes p and q such that either

- *p and q divide n, and $q \mid p-1$; or*
- *p^2 and q divide n, and $q \mid p+1$.*

There is indeed a connection …

Connection with abelian groups

Every finite abelian group is integrable. (This explains why the set in the second theorem is contained in the set in the first.) For, by the Fundamental Theorem of Abelian Groups, it is enough to prove that finite cyclic groups are integrable. Now, if n is odd, then $C_n = (D_{2n})'$, while if n is a power of 2, then $C_n = (D_{4n})'$.

To explain the difference, consider $n = 75$. There is a non-abelian group of this order, the group of maps $x \mapsto ax + b$ of the field F of order 25, where $b \in F$ and a is a cube root of unity in the field. But this is the derived group of the group of order 150 obtained by adjoining the Frobenius automorphism $x \mapsto x^5$.

Proof of the theorem

Here is a brief sketch. One can show that for any $m \geq 3$, and any prime p, there is a non-integrable group of order p^m. So, if every group of order n is integrable, then n must be cube-free. We may also assume that n is odd, since for every even $n > 4$ the dihedral group of order n is non-integrable.

Now show that a non-abelian group of order n must 'look like' our example of order 75 above, and hence must be integrable.