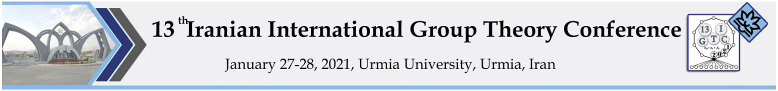
Integrals of groups

Peter J. Cameron, University of St Andrews

Joint work with João Araújo and Francesco Matucci

In memory of Carlo Casolo



Integrals of groups

The derived group G' of a goup G is the group generated by all the commutators $[x, y] = x^{-1}y^{-1}xy$ for $x, y \in G$.
Alireza Abdollahi suggested that, by analogy with the Fundamental Theorem of Calculus, a group H such that $H' \cong G$ should be called an integral of G.
Though the name is quite new, the concept is much older; many famous group theorists have considered integrals of groups. The oldest reference I know is a paper of Burnside in 1913, which I will mention later.
More generally, we can consider inverse group theory: if F is any group-theoretic construction, we can ask whether, for a given group G, there is a group H such that $F(H) = G$. I will mention some instances later.

I began working on this project with João Araújo and Francesco Matucci some years ago.
When the first paper was nearly ready, we sent a copy to Francesco's teacher Carlo Casolo, who made some significant contributions, some of which were incorporated, and he was included as a co-author.
Subsequently we started preparing a second paper on the topic. Carlo arranged for Francesco and me to visit the beautiful city of Florence to work on it.

At that time (February 2020), COVID had reached north Italy but Florence was not yet locked down, so I was able to make the trip, despite the fact that my flight was delayed a day by a severe storm.
It was a very successul trip, and we began preparing the paper. Then came the news that Carlo had died in March, of a heart problem. So we interpreted his research notes as well as we could and wrote the paper, which we dedicated to his memory. Some things we were not able to reproduce; I will mention these as open problems later.

Examples

Proposition

Every abelian group is integrable.

This was observed by Bob Guralnick. If G is abelian then it is the derived group of $G \wr C_2$. If every element of G is a square, there is a much smaller integral, the generalised dihedral group

$$\langle G, t : t^2 = 1, t^{-1}gt = g^{-1} \text{ for all } g \in G \rangle,$$

since $[g, t] = g^{-2}$.
At the other end of the scale, every perfect group is integrable, since it is its own integral.

p-integrable groups

Thus, of the five groups of order 8, three of them are abelian and so are integrable. The quaternion group Q_8 is integrable (the group $\mathrm{SL}(2,3)$ of order 24 is an integral), but it has no 2-group as an integral; the dihedral group D_8 is not integrable. Some of this follows from the result of Burnside (1913) I mentioned. If G is a p-group, where p is prime, say H is a p-integral of G if H is a p-group and $H' = G$.

Theorem (Burnside)

Let G be a p-group such that either $Z(G)$ is cyclic, or $|G : G'| = p^2$. Then G has no p-integral.

Finite groups

The following theorem gives us a good start:

Theorem

- *A finitely generated integrable group has a finitely generated integral.*
- *A finite integrable group has a finite integral.*

Here is a sketch. The first part is easy. If $G = \langle g_1, \ldots, g_r \rangle$ and $G = H'$, express each of $g_1, \ldots, g_r$ as products of commutators in H; then $G = K'$, where K is generated by the elements of H included in these commutators.
If G is finite, every conjugacy class in H is contained in a coset of G and so is finite. So H is a finitely generated BFC-group, and so its centre has finite index and is finitely generated; factoring out the torsion-free part of the centre gives a finite integral of G.

Two questions

To our embarrassment, here are two questions we can't answer.

Problem

- *Is there a computational test for integrability?*
- *Is there a good bound for the order of some integral of an integrable group of order n?*

These questions are related. We can program a computer to list all groups whose order is divisible by n and test whether their derived groups are isomorphic to a given group G; if G is integrable we will find an integral, but if not, the program will not terminate.
But, if we had a recursive bound $f(n)$ for the second question, we would only need to test groups with orders up to $f(n)$.

We can show that it would suffice to find a bound for the exponent of the centre of some integral of an integrable group. Then we hit an obstacle.
For $n \geq 3$, the group

$$\langle a, b : a^{2^{n-1}} = b^2 = 1, b^{-1}ab = a^{2^{n-2}+1} \rangle$$

is an integral of C_2 whose centre has exponent 2^{n-2}; all its proper subgroups and quotients are abelian, so it is not clear how we could "reduce" to a smaller integral.

For which n is every group of order n integrable?

A folklore result asserts that the natural number n has the property that 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

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

The result with "integrable" in place of "abelian" is similar:

Theorem

The natural number n has the property that every group of order n is integrable if and only if n is cube-free and there do not exist primes p and q dividing n such that $q \mid p-1$.

This small change in the conditions doesn't change the asymptotic density of the set of such n: there are about

$$e^{-\gamma}x/\log\log\log x$$

such n with $n \leq x$, where γ is Euler's constant.

Integrability within a class

Let $\mathcal{C}$ be a class of groups. Given a integrable group G in $\mathcal{C}$, does it have an integral in the class $\mathcal{C}$? We already considered this for finite and finitely generated groups (the answer is "yes") and for finite p-groups (the answer is "no").
I mention here one easy result.

Theorem

Let $\mathfrak{V}$ be a variety of groups. Then the class of all integrals of groups in $\mathfrak{V}$ is a variety; in fact it is the product variety $\mathfrak{V}\mathfrak{A}$, where $\mathfrak{A}$ is the variety of abelian groups.

The product variety $\mathfrak{V}\mathfrak{A}$ consists of all extensions of groups in $\mathfrak{V}$ by groups in $\mathfrak{A}$.

Profinite groups

What happens for profinite groups? We distinguish between an abstract integral and a profinite integral (whose topological derived group is G).

Theorem

- *Let G be a profinite group which has an abstract integral H such that G has finite index in H. Then G has a profinite integral.*
- *Let G be a finitely generated profinite group which has an abstract integral. Then G has a profinite integral.*
- *There is a profinite group which has an abstract integral but has no profinite integral.*

An example for the third part is the Cartesian product of countably many copies of the dihedral group of order 8.

Small integrals of abelian groups

We saw that an abelian group G with every element a square has an integral H with $|H : G| = 2$. Is there a constant upper bound on $|H : G|$, where G is a finite abelian group?
No: the obstruction is the product of cyclic 2-groups of different orders.

Theorem

An abelian group of order n has an integral of order $n^{1+o(1)}$; but there is no constant c such that every abelian group has an integral of order at most cn.

There are estimates for the upper bound, but they are a bit messy …

Infinite abelian groups

We say that a group G is finitely integrable if it has an integral H with $|H : G|$ finite.

Problem

Which infinite abelian groups are finitely integrable?

The direct product of cyclic groups of order 2^n for $n \in \mathbb{N}$ is an example of a group which is not finitely integrable. However, an abelian torsion group A with no elements of order 2 has index 2 in the integral $\langle A, t : (\forall a \in A) a^t = a^{-1} \rangle$. The question for torsion groups can be reduced to the case of 2-groups; there should be a condition in terms of the Ulm–Kaplansky invariants, but we have not succeeded in finding one.

Torsion-free abelian groups of finite rank are finitely integrable, but we know little about the general case!

Inverse group theory

Now it is time to widen our question.
Given any group-theoretic construction (I don't say "functor", since I don't restrict to functorial constructions) $\mathcal{F}$, which groups G have inverse $\mathcal{F}$-groups? That is, for which G does there exist a group H such that $\mathcal{F}(H) = G$?
You may think of various examples: centre, central quotient, derived group (this is what we have been looking at), derived quotient, Frattini or Fitting subgroup, automorphism group or outer automorphism group, Schur multiplier, etc.

Trivial and non-trivial inverse problems

Examples of trivial inverse problems are:

- The centre of a group is abelian. But every abelian group is its own centre. (So the answer to the inverse centre problem is: all abelian groups.)
- The Fitting subgroup of a group is nilpotent. But every nilpotent group is its own Fitting subgroup.
- The derived quotient H/H' is abelian. But every abelian group is its own derived quotient.

Even after discarding these, we are left with some interesting problems.

The inverse Frattini problem

The Frattini subgroup $\Phi(G)$ of a finite group G is the intersection of the maximal subgroups of G. Equivalently, it is the set of non-generators of G, the elements which can be dropped from every generating set.

Problem

For which finite groups G does there exist a group H such that the Frattini subgroup $\Phi(H)$ is isomorphic to G?

The Frattini subgroup of a finite group is nilpotent (a simple application of the Frattini argument), so we only have to look among finite nilpotent groups.

This problem goes back to Bernhard Neumann, and has been studied by many group theorists. After preliminary results by several people including Allenby and Wright, a beautiful solution was given by Bettina Eick:

Theorem

Let G be a finite group. There exists a finite group H with $\Phi(H) \cong G$ if and only if $\mathrm{Inn}(G) \leq \Phi(\mathrm{Aut}(G))$, where $\mathrm{Aut}(G)$ and $\mathrm{Inn}(G)$ are the automorphism group and inner automorphism group of G.

Thus, unlike the case for the derived group, we can tell whether G has an inverse Frattini group just from the structure of G. Note that the condition of the theorem implies that the inner automorphism group of G is nilpotent; so G is centre-by-nilpotent, and hence is nilpotent.

A surprising result

We saw the characterisation of natural numbers n such that every group of order n is integrable; it is slightly larger than the class of n for which every group of order n is abelian.
The next result came as a surprise to us, but with the help of Reg Allenby we now have two different proofs.

Theorem

Let n be a natural number. Then the following three conditions are equivalent:

(a) *every group of order n is abelian;*
(b) *every group of order n has an inverse Frattini group;*
(c) *n is not divisible by the cube of a prime, or by pq where p and q are primes with $q \mid p-1$, or by p^2q where p and q are primes with $q \mid p+1$.*

The equivalence of (a) and (c) is well-known, but we didn't expect that (b) would give exactly the same set!

Schur multiplier

The Schur multiplier $M(G)$ of a finite group G is the largest abelian group Z such that there exists H with $Z \leq Z(H) \cap H'$ and $H/Z \cong G$. It can be variously described: for example, it is $H_2(G, \mathbb{Z})$ or $H^2(G, \mathbb{C}^\times)$, or $(F' \cap R)/[F, R]$ where $G = F/R$ is a presentation of G.

Theorem

Every finite abelian group is the Schur multiplier of a finite group.

However, not every finite abelian group is the Schur multiplier of a finite abelian group. It is possible to describe those that are. The question reduces to considering abelian p-groups, for p prime. In particular, we find that $C_p \times C_p$ is not the Schur multiplier of any finite abelian p-group.
Incidentally, $C_2 \times C_2$ is the Schur multiplier of $\mathrm{Sz}(8)$.

Automorphism groups

The general inverse problem would ask: Which groups G are isomorphic to the automorphism group of some group? I willl briefly look at a different question.

Problem

Which groups are outer automorphism groups of simple groups?

We know from the Classification of Finite Simple Groups that Schreier's Conjecture is true: the outer automorphism group of a finite simple group is solvable. Indeed it has a very restricted structure: an extension of a metacyclic group by a symmetric group of degree at most 3. But this is false in the infinite case: the outer automorphism group of the alternating group of countable degree is an extension of C_2 by an uncountably infinite simple group.

So let's specialise further:

Problem

Which infinite simple groups have finite outer automorphism groups?

Theorem

For every n, there is an infinite simple group X whose outer automorphism group is S_n.

The group X is the automorphism group of the "random n-coloured complete graph on a countable set".

Derangement quotients

In a recent paper with R. A. Bailey, Michael Giudici and Gordon Royle, we considered, for a transitive permutation group G, the normal subgroup $D(G)$ generated by the derangements (fixed-point-free elements) in G. This is a large subgroup: $G/D(G)$ has order at most $n-1$, if n is the degree of G. We call $G/D(G)$ the derangement quotient of G.
Most transitive groups G satisfy $D(G) = G$. In a Frobenius group, $D(G)$ is the Frobenius kernel, so $G/D(G)$ is the Frobenius complement.

Problem

Which finite groups can arise as the derangement quotient of a transitive permutation group?

Thus every Frobenius complement can arise. It is quite difficult to find others. All those we were able to find are quotients of Frobenius complements. Is every derangement quotient a quotient of a Frobenius complement?

Widening the scope

Stepping beyond groups, we can ask questions such as the following:

- Which rings (or near-rings) are endomorphism rings (near-rings) of abelian groups (groups)?
- Which lattices are subgroup lattices of groups?

Of course, for any such question we can restrict the class of groups, or the class of rings/near-rings-/lattices …

Systems of inverse problems

I will illustrate this with just a single example.

Theorem

Let A and B be finite abelian groups. Then there is a group G such that $Z(G) \cong A$ and $G/G' \cong B$.

Proof.

Take the direct product of a perfect group with centre A and a centreless group with derived quotient B. □

That was simple enough, but we feel sure that there are more interesting questions of this sort which have not been considered …

An inverse inverse problem

Are there any general results about classes of inverse problems? Recall Eick's theorem: G is the Frattini subgroup of some group if and only if $\mathrm{Inn}(G) \leq \Phi(\mathrm{Aut}(G))$. We cannot hope for such strong results in general, but we could ask:

Problem

For which constructions $\mathcal{F}$ is $\mathrm{Inn}(G) \leq \mathcal{F}(\mathrm{Aut}(G))$ a necessary condition for the $\mathcal{F}$-inverse problem for G to have a solution?

Theorem

A sufficient condition for the above is that the following both hold:

- *$\mathcal{F}$ is monotonic ($A \leq B$ implies $\mathcal{F}(A) \leq \mathcal{F}(B)$);*
- *if B is normal in A then $\mathcal{F}(A/B) = \mathcal{F}(A)B/B$.*

Taking $\mathcal{F}$ to be a verbal subgroup of G, these conditions are satisfied. But that is not all: Frattini subgroup does not satisfy the conditions of the theorem.

- A. Abdollahi, Integral of a group, in Proceedings of the 29th Iranian International Conference on Mathematics, Amirkabir University of Technology, Tehran, 1998.
- J. Araújo, P. J. Cameron, C. Casolo and F. Matucci, Integrals of groups, *Israel J. Math.* **234** (2019), 149–178.
- J. Araújo, P. J. Cameron, C. Casolo and F. Matucci, Integrals of groups II, arXiv `2008.13675`

for your attention. Stay well!