Integrals of groups

Peter J. Cameron
University of St Andrews

Group actions and transitive graphs
Shenzhen, October 2018

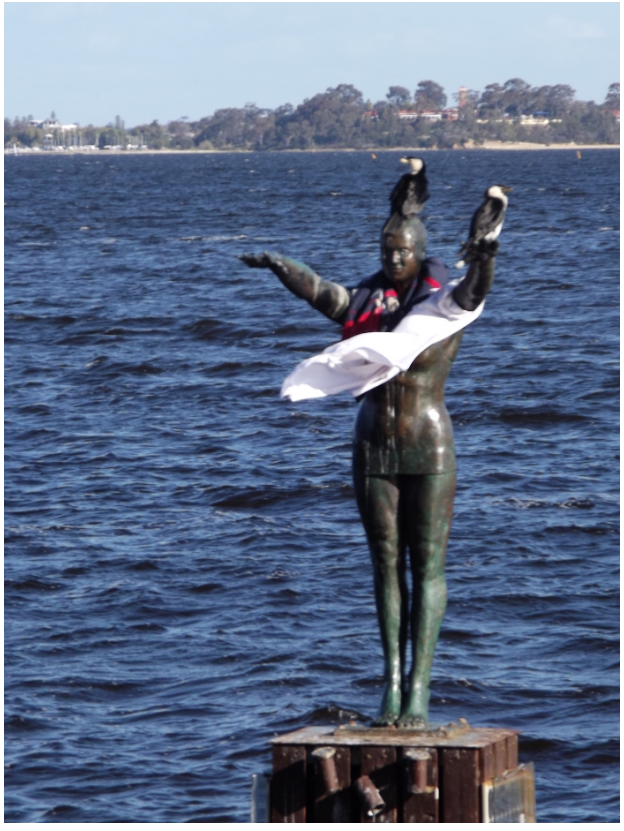
Happy Birthday, Cheryl!

Cheryl Praeger and I were both born in Toowoomba, an inland city in Queensland with many parks and gardens.

Cheryl and I both learned group theory at the University of Queensland.

We went to Oxford, where we were both supervised by Peter Neumann for our DPhil degrees.

Then Cheryl returned to Australia, while I stayed in Europe.



But we didn't lose touch. I have more papers with Cheryl than with any other except two of my coauthors (and there are papers in this list of which I am very proud):

- P. J. Cameron and C. E. Praeger, Graphs and permutation groups with projective subconstituents, *J. London Math. Soc.* (2) **25** (1982), 62–74.
- P. J. Cameron, C. E. Praeger, J. Saxl and G. M. Seitz, On the Sims conjecture and distance-transitive graphs, *Bull. London Math. Soc.* **15** (1983), 499–506.
- P. J. Cameron and C. E. Praeger, On 2-arc transitive graphs of girth 4, *J. Combinatorial Theory* (B) **35** (1983), 1–11.
- P. J. Cameron, L. G. Kovcs, M. F. Newman and C. E. Praeger, Fixed-point-free permutations in transitive permutation groups of prime power order, *Quart. J. Math. Oxford* (2) **36** (1985), 273–278.
- P. J. Cameron and C. E. Praeger, Partitioning into Steiner systems, pp. 61–71 in *Combinatorics '88* (ed. A. Barlotti et al.), Mediterranean Press, Roma, 1992.
- P. J. Cameron and C. E. Praeger, Block-transitive *t*-designs, I: point-imprimitive designs, *Discrete Math.* **118** (1993), 33–43.
- P. J. Cameron and C. E. Praeger, Block-transitive *t*-designs, II: large *t*, *Finite Geometry and Combinatorics* (ed. A. Beutelspacher et al.), Cambridge Univ. Press, 1993.
- P. J. Cameron, C. E. Praeger and N. C. Wormald, Highly arc-transitive digraphs and universal covering digraphs, *Combinatorica* **13** (1993), 1–21.
- P. J. Cameron and C. E. Praeger, Constructing flag-transitive, point-imprimitive designs, *J. Algebraic Combinatorics* **43** (2016), 755–769.

The photo on the first slide shows some members of our mathematical family. It was taken at my 60th birthday conference in Ambleside, UK.

Summary

This talk is joint work with João Araújo (Lisbon), Carlo Casolo (Firenze) and Francesco Matucci (Campinas).
I will start with integrals of groups, an elementary problem where some interesting things can be said but definitive results do not yet exist.
Then I will move to the more general topic in which this is located, which could be described as inverse group theory.
There are plenty of open problems here, and we invite you to join us in considering them.

Integrals of groups

Let G be a group. The derived group of G is the subgroup of G generated by all commutators $[g,h] = g^{-1}h^{-1}gh$ for $g,h \in G$. It is the smallest normal subgroup N of G for which G/N is abelian. I don't have to persuade you of its importance in group theory! We denote the derived group of G by G'.
By analogy with calculus, let us say that a group H is an integral of G if H' is isomorphic to G. Thus we do not expect the integral to be unique, and we do not expect all groups to have integrals.
The main question is:

Problem

Which groups have integrals?

For example, we do not know whether $D_8 \times D_8$ is integrable.

A finiteness theorem

Theorem

Let G be a finite group. If G has an integral, then it has a finite integral.

I outline the proof. Suppose that G has an integral H. We may assume that H is finitely generated (since we only require elements of H whose commutators generate G).
Now since $H' = G$, each conjugacy class in H is contained in a coset of G, and so is of bounded finite size: H is a BFC-group. A finitely generated BFC-group has centre of finite index, and so has a torsion-free central subgroup A of finite index. Now H/A is finite and $(H/A)' = GA/A \cong G$.

Integrable groups

Not every group is integrable. The smallest counterexample is the symmetric group $G = S_3$. If H is finite and $H' = G$, then $H'' = C_3$ is normal in H. But the automorphism group of C_3 is abelian, so $H' = S_3$ centralises C_3, a contradiction.
However, there are some wide classes of integrable groups, for example:

Proposition

Every finite abelian group is integrable.

A simple proof was given by Bob Guralnick, who observed that the abelian group A is the derived group of $A \wr S_2$.

Smaller integrals?

If A is an abelian group of order n, then Guralnick's integral has order $2n^2$. Is there a smaller integral?
If $n = |A|$ is odd, then there is an integral of order $2n$, namely the generalised dihedral group

$$\langle A, t : t^2 = 1, t^{-1}at = a^{-1} \text{ for all } a \in A \rangle.$$

Many other *ad hoc* constructions can be found, but we have the following result:

Proposition

An abelian group of order n has an integral of order $n^{1+o(1)}$, but does not always have one of order $O(n)$.

We have some results on infinite abelian groups also. In particular, there are infinite abelian groups G such that, for any integral H, the index $|H : G|$ is infinite.

Orders

Let S_1 be the set of positive integers n for which every group of order n is abelian, and S_2 the set of positive integers for which every group of order n is integrable.
By Guralnick's result, $S_1 \subseteq S_2$.
The description of the set S_1 is a result of Dickson in 1905 (thanks to Roman Nedela for the reference), for which a proof by Robin Chapman on `MathOverflow` is recommended.

Theorem

The positive integer 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

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

The set S_2

The description of S_2 of orders for which every group is integrable is very similar, but easier to state:

Theorem

The positive integer 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 such that p and q divide n and $q \mid p-1$.

A brief word about the proof. If p and q are primes such that $q \mid p+1$, then there is a non-abelian group G of the form $\{x \mapsto ax+b\}$ of maps on $\mathrm{GF}(p^2)$, where $b \in \mathrm{GF}(p^2)$ and a is a q-th root of unity. But this group is integrable: an integral has the form $\{x \mapsto ax^\sigma + b\}$, where a, b are as above and σ is either the identity or the Frobenius automorphism $x \mapsto x^p$. So $p^2q \in S_2 \setminus S_1$.

We know quite a lot more about integrable groups (and their integrals). But some big open problems remain, among them these three:


Find a necessary and sufficient condition for a finite group to be integrable.


Find a good bound for the order of the smallest integral of an integrable group.


For a prime p, is it true that the proportion of groups of order p^n which are integrable tends to 0 as $n \to \infty$?

A solution to the second problem would help with the first. There obviously is a function f such that if G is an integrable group of order n then G has an integral of order at most $f(n)$. If we had a good estimate for $f(n)$, we could find all groups of order up to $f(n)$ and divisible by n and check whether their derived groups are isomorphic to G.

Integrating more than once

A perfect group (one satisfying $G = G'$) is its own integral, and so trivially can be integrated n times for every n.
An abelian group can also be integrated arbitrarily often.
(Suppose that R is a ring with additive group A. Then the group of upper unitriangular matrices of order $2^n + 1$ over R has the property that its nth derived group has elements of A in the top right corner, 1 on the diagonal and 0 elsewhere, and so is isomorphic to A.) Note that this group is nilpotent.
This is essentially all:

Theorem

A finite group G can be integrated n times for every natural number n if and only if it is the central product of an abelian group and a perfect group.

A corollary

Corollary

For a natural number n, the following are equivalent:

1. *every group of order n is abelian;*
2. *every group of order n can be integrated twice;*
3. *every group of order n can be integrated k times, for every natural number k;*
4. *n is cubefree and has no prime divisors p and q such that either $q \mid p-1$, or $q \mid p+1$ and $p^2 \mid n$.*

Infinitely integrable groups

Aside from perfect groups, there is no infinitely integrable finite group G, in the sense that there exists an infinite chain of finite groups of the form

$$G = G_1' \leq G_1 = G_2' \leq G_2 = G_3' \leq \dots$$

Indeed, Bernhard Neumann showed that there is no strictly increasing such sequence if G_2 is finitely generated.
However, if we relax the assumptions, we can succeed: there are sequences as above with G finite but G_i infinite for $i > 1$, and also sequences of finite groups such that

- $G_n' \geq G_{n-1}$ for $n > 0$,
- $G_n^{(n)} = G_0$.

A few open questions

Does the set of numbers n for which every group of order n is integrable have a density? If so, what is it?

Which infinite integrable groups G have an integral H such that $|H : G|$ is finite?

If $\mathfrak{V}$ is a variety of groups, then the set $\mathfrak{W}$ of all integrals of groups in $\mathfrak{V}$ is a variety. If we have a basis for the identities of $\mathfrak{V}$, can we find such a basis for $\mathfrak{W}$?

Is it true that, given a presentation for a group G, the problem of deciding whether G is integrable is undecidable? Are there classes of groups (maybe one-relator groups) for which this problem is decidable?

Does there exist a finite non-integrable group G for which $G \times G$ is integrable?

Inverse group theory

The material just discussed can be regarded as part of inverse group theory. Given a construction F on groups, decide for which groups G there exists a group H such that $F(H) = G$. There are many group-theoretic constructions other than derived group: centre, central quotient, derived quotient, Frattini subgroup, Fitting subgroup, Schur multiplier, other cohomology groups, and various constructions from permutation groups.

As we will see, many of these problems are trivial, and others have been "solved" (though open questions remain), but a number of interesting and challenging questions are still unsolved.

Trivial cases

We shall regard the inverse problem arising from a construction F as being trivial if

$$G = F(H) \Rightarrow G = F(G).$$

For example:

- The centre of any group is abelian; but an abelian group is its own centre.
- The Fitting subgroup of any group is nilpotent; but a nilpotent group is its own Fitting subgroup.
- The derived quotient of any group is abelian; but an abelian group is its own derived quotient.

So these (and several other) inverse problems are trivial.

Frattini subgroup

The Frattini subgroup $\Phi(G)$ of a finite group G can be defined in several ways. For example,

- it is the intersection of the maximal subgroups of G;
- it is the set of non-generators of G, elements which can be dropped from any generating set.

It is known that the Frattini subgroup is nilpotent. So the inverse problem is:

> *Which nilpotent groups are Frattini subgroups of finite groups?*

Bettina Eick's Theorem

After preliminary work by Bernhard Neumann, Gaschütz, Allenby, and Wright, a definitive result was proved by Bettina Eick:

Theorem

The finite group G is the Frattini subgroup of a finite group H if and only if $\mathrm{Inn}(G)$ *is contained in the Frattini subgroup of* $\mathrm{Aut}(G)$*, where* $\mathrm{Aut}(G)$ *and* $\mathrm{Inn}(G)$ *are the automorphism group and inner automorphism group of G.*

However, this is not the end of the story. Eick herself remarks that the classes of Frattini subgroups of finite groups, Frattini subgroups of finite soluble groups, and Frattini subgroups of finite nilpotent groups are all distinct.

Questions on inverse Frattini

Find characterisations of Frattini subgroups of p-groups, nilpotent groups, and soluble groups.

Is it true that the proportion groups of order p^n which are Frattini subgroups tends to 0 as $n \to \infty$? Find estimates for this proportion.

Schur multiplier

The Schur multiplier of a finite group G is the largest group Z for which there exists $\bar{G}$ with $Z \subseteq \bar{G}' \cap Z(\bar{G})$; alternatively it is the first cohomology group of G with coefficients in $\mathbb{C}^\times$.
We know that every abelian group is the Schur multiplier of a group. But not every abelian p-group is the Schur multiplier of a p-group. (For example, $C_p \times C_p$ is not.) Which groups can occur?

Permutation groups: Derangements

This question was raised by Rosemary Bailey, Michael Giudici, Gordon Royle, and me in an unpublished preprint.
Let G be a transitive finite permutation group of degree $n > 1$. By a theorem of Jordan, G contains a derangement. Let $D(G)$ be the normal subgroup generated by the derangements in G. Then $D(G)$ is transitive and contains all elements of G whose number of fixed points is different from 1. Moreover, $G/D(G)$ permutes the $D(G)_\alpha$-orbits semiregularly, so $|G/D(G)| \leq n-1$.
Clearly any Frobenius complement can occur as $G/D(G)$, since if G is a Frobenius group then $D(G)$ is the Frobenius kernel.
By examining lists of transitive groups, we observed that both the Klein group V_4 and the symmetric group S_3 can also occur. Could it be true that every finite group occurs?


THANK YOU