Integrals of groups

Francesco Matucci

(joint with J.Araújo, P.Cameron and C.Casolo)

Università di Milano - Bicocca and CEMAT Lisbon

June 12th, 2019

SandGAL 2019 - Semigroups and Groups, Automata, Logics

FCT
Fundação para a Ciência e a Tecnologia
MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E ENSINO SUPERIOR

UID/MULTI/04621/2019

Integrals of groups

Integrals of groups

Let G be a group. The **derived group** G' of G is the subgroup of G generated by all commutators $[g, h] = g^{-1}h^{-1}gh$ for $g, h \in G$.

Integrals of groups

Let G be a group. The **derived group** G' of G is the subgroup of G generated by all commutators $[g, h] = g^{-1}h^{-1}gh$ for $g, h \in G$.

By analogy with calculus, let us say that a group H is an **integral** of G if $H' = G$.

Integrals of groups

Let G be a group. The **derived group** G' of G is the subgroup of G generated by all commutators $[g, h] = g^{-1}h^{-1}gh$ for $g, h \in G$.

By analogy with calculus, let us say that a group H is an **integral** of G if $H' = G$.

By a similar analogy, we observe the following:

Lemma (Constant of integration)

1. *If* $G = G_1 \times G_2$, *then* $G' = G_1' \times G_2'$,
2. *Let* G *be a group, let* H *be an integral for* G *and let* A *be an abelian group. Then* $H \times A$ *is an integral for* G.

Integrals of groups

So integrals are not unique (if they exist) and we do not expect all groups to have integrals.

Problem

Which groups have integrals?

Integrals of groups

So integrals are not unique (if they exist) and we do not expect all groups to have integrals.

Problem

Which groups have integrals?

Example

We still do not know whether $D_8 \times D_8$ is integrable!

Integrable groups

Integrable groups

Remark

Not every group is integrable!

Integrable groups

Remark

Not every group is integrable!

Example

The smallest counterexample is the symmetric group $G = S_3$.

Integrable groups

Remark

Not every group is integrable!

Example

The smallest counterexample is the symmetric group $G = S_3$.

If there were H integral, then H acts on $C_3 = H''$ by conjugation.

Integrable groups

Remark

Not every group is integrable!

Example

The smallest counterexample is the symmetric group $G = S_3$.

If there were H integral, then H acts on $C_3 = H''$ by conjugation.

Since $\mathrm{Aut}(C_3)$ is abelian, then $H' = S_3$ acts trivially on $C_3 = H''$.

Contradiction!

Integrable groups

There are indeed classes of integrable groups, for example:

Integrable groups

There are indeed classes of integrable groups, for example:

Theorem (Guralnick, 1978)

Every (not necessarily finite) abelian group is integrable.

Integrable groups

There are indeed classes of integrable groups, for example:

Theorem (Guralnick, 1978)

Every (not necessarily finite) abelian group is integrable.

Proof. For every abelian group A we have

$$(A \wr C_2)' = \{(a, a^{-1}) \mid a \in A\} \cong A.$$

Integrable groups

Proposition

Let $G = G_1 \times G_2$.

Integrable groups

Proposition

Let $G = G_1 \times G_2$.

1. *If* G_1 *and* G_2 *are integrable, then so is* G.

Integrable groups

Proposition

Let $G = G_1 \times G_2$.

1. *If* G_1 *and* G_2 *are integrable, then so is* G.
2. *If* G *is integrable and* $\gcd(|G_1|, |G_2|) = 1$, *then* G_1 *and* G_2 *are integrable.*

Integrable groups

Proposition

Let $G = G_1 \times G_2$.

1. *If* G_1 *and* G_2 *are integrable, then so is* G.
2. *If* G *is integrable and* $\gcd(|G_1|, |G_2|) = 1$, *then* G_1 *and* G_2 *are integrable.*
3. *If* G_1 *is centerless and* G_2 *is abelian, then* G *is integrable if and only if* G_1 *is integrable.*

Integrable groups

Proposition

Let $G = G_1 \times G_2$.

1. *If* G_1 *and* G_2 *are integrable, then so is* G.
2. *If* G *is integrable and* $\gcd(|G_1|, |G_2|) = 1$, *then* G_1 *and* G_2 *are integrable.*
3. *If* G_1 *is centerless and* G_2 *is abelian, then* G *is integrable if and only if* G_1 *is integrable.*

Remark

The "centerless" condition in the last part is essential since D_8 *is not integrable, but* $C_2 \times D_8$ *has an integral of order 128.*

Integrable groups

Proposition

Let $G = G_1 \times G_2$*.*

1. *If* G_1 *and* G_2 *are integrable, then so is* G*.*
2. *If* G *is integrable and* $\gcd(|G_1|, |G_2|) = 1$*, then* G_1 *and* G_2 *are integrable.*
3. *If* G_1 *is centerless and* G_2 *is abelian, then* G *is integrable if and only if* G_1 *is integrable.*

Remark

The "centerless" condition in the last part is essential since D_8 *is not integrable, but* $C_2 \times D_8$ *has an integral of order 128.*

Theorem

A finite group with an integral also has a finite integral.

Some folklore results on integrals

Some folklore results on integrals

Proposition

Let G be a group with a characteristic cyclic subgroup C which is not contained in $Z(G)$. Then G has no integral.

Some folklore results on integrals

Proposition

Let G be a group with a characteristic cyclic subgroup C which is not contained in $Z(G)$. Then G has no integral.

Corollary

1. *If n is even and $n > 4$, the dihedral group of order n is non-integrable.*

Some folklore results on integrals

Proposition

Let G be a group with a characteristic cyclic subgroup C which is not contained in $Z(G)$. Then G has no integral.

Corollary

1. *If n is even and $n > 4$, the dihedral group of order n is non-integrable.*
2. *Let p and q be primes and $q \mid p - 1$. Then the non-abelian group of order pq is centerless and non-integrable.*

Some folklore results on integrals

Proposition

Let G be a group with a characteristic cyclic subgroup C which is not contained in $Z(G)$. Then G has no integral.

Corollary

1. *If n is even and $n > 4$, the dihedral group of order n is non-integrable.*
2. *Let p and q be primes and $q \mid p - 1$. Then the non-abelian group of order pq is centerless and non-integrable.*

Proposition

For every $n \geq 5$, symmetric group S_n is non-integrable.

Smaller integrals?

Smaller integrals?

Proposition

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

Smaller integrals?

Proposition

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

Definition

A group G is **finitely integrable** if there exists a group H such that $H' \cong G$ and $|H : G|$ is finite.

Smaller integrals?

Proposition

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

Definition

A group G is **finitely integrable** if there exists a group H such that $H' \cong G$ and $|H : G|$ is finite.

Proposition

There exists torsion-free infinite abelian groups that are not finitely integrable.

Diverse behavior for the same order

Diverse behavior for the same order

Theorem

Of the two non-abelian groups of order p^3 (p odd prime), the group of exponent p has an integral, while that of exponent p^2 does not.

Diverse behavior for the same order

Theorem

Of the two non-abelian groups of order p^3 (p odd prime), the group of exponent p has an integral, while that of exponent p^2 does not.

Let $\mathcal{AB} = \{$positive integers n for which every group of order n is abelian$\}$, and $\mathcal{INT} = \{$positive integers for which every group of order n is integrable$\}$. By Guralnick's result, $\mathcal{AB} \subseteq \mathcal{INT}$.

Diverse behavior for the same order

Theorem

Of the two non-abelian groups of order p^3 (p odd prime), the group of exponent p has an integral, while that of exponent p^2 does not.

Let $\mathcal{AB} = \{$positive integers n for which every group of order n is abelian$\}$, and $\mathcal{INT} = \{$positive integers for which every group of order n is integrable$\}$. By Guralnick's result, $\mathcal{AB} \subseteq \mathcal{INT}$.

Theorem (Dickson, 1905)

An $n \in \mathbb{N}$ lies in $\mathcal{AB}$ if and only if n is cube-free and there do not exist primes p and q such that either

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

Diverse behavior for the same order

Theorem

Of the two non-abelian groups of order p^3 (p odd prime), the group of exponent p has an integral, while that of exponent p^2 does not.

Let $\mathcal{AB} = \{$positive integers n for which every group of order n is abelian$\}$, and $\mathcal{INT} = \{$positive integers for which every group of order n is integrable$\}$. By Guralnick's result, $\mathcal{AB} \subseteq \mathcal{INT}$.

Theorem (Dickson, 1905)

An $n \in \mathbb{N}$ lies in $\mathcal{AB}$ if and only if n is cube-free and there do not exist primes p and q such that either

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

Theorem

An $n \in \mathbb{N}$ lies in $\mathcal{INT}$ 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 $q \mid p-1$.

Can we integrate infinitely many times?

Can we integrate infinitely many times?

A **perfect group** (one satisfying $G = G'$) is its own integral, and so trivially can be integrated n times for every n.

Can we integrate infinitely many times?

A **perfect group** (one satisfying $G = G'$) is its own integral, and so trivially can be integrated n times for every n.

Theorem

A finite group G can be integrated n times for every $n \in \mathbb{N}$ if and only if it is the central product of an abelian group and a perfect group.

Can we integrate infinitely many times?

A **perfect group** (one satisfying $G = G'$) is its own integral, and so trivially can be integrated n times for every n.

Theorem

A finite group G can be integrated n times for every $n \in \mathbb{N}$ if and only if it is the central product of an abelian group and a perfect group.

Question

Is there an infinitely integrable finite group G, in the sense that there exists an infinite chain of finite groups of the form

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

Can we integrate infinitely many times?

Remark

Bernhard Neumann showed in 1956 that there is no strictly increasing such sequence if G_2 is finitely generated.

Can we integrate infinitely many times?

Remark

Bernhard Neumann showed in 1956 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

Can we integrate infinitely many times?

Remark

Bernhard Neumann showed in 1956 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 $n > 0$,
- $G_n^{(n)} = G_0$.

Some things we do not know

Some things we do not know

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

Some things we do not know

1. Find a necessary and sufficient condition for a finite group to be integrable.
2. Find a good bound for the order of the smallest integral of an integrable group.

Some things we do not know

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

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

A solution to the second problem would help with the first.

Some things we do not know

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

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

A solution to the second problem would help with the first.

Theorem

Let G be a group of order n with $Z(G) = 1$. Then, if G is integrable, it has an integral of order at most $n^{\log_2 n}$.

Some things we do not know

1. Find a necessary and sufficient condition for a finite group to be integrable.
2. Find a good bound for the order of the smallest integral of an integrable group.

A solution to the second problem would help with the first.

Theorem

Let G be a group of order n with $Z(G) = 1$. Then, if G is integrable, it has an integral of order at most $n^{\log_2 n}$.

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 $f(n)$.

Some things we do not know

1. Find a necessary and sufficient condition for a finite group to be integrable.
2. Find a good bound for the order of the smallest integral of an integrable group.

A solution to the second problem would help with the first.

Theorem

Let G be a group of order n with $Z(G) = 1$. Then, if G is integrable, it has an integral of order at most $n^{\log_2 n}$.

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.

Some more things we do not know

Some more things we do not know

1. For which finite non-abelian groups G is it true that, for all finite groups H with $G' = H'$, it holds that H is integrable if and only if G is? (All finite abelian groups have this property, but it fails for D_8 and Q_8.)

Some more things we do not know

1. For which finite non-abelian groups G is it true that, for all finite groups H with $G' = H'$, it holds that H is integrable if and only if G is? (All finite abelian groups have this property, but it fails for D_8 and Q_8.)

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

Some more things we do not know

1. For which finite non-abelian groups G is it true that, for all finite groups H with $G' = H'$, it holds that H is integrable if and only if G is? (All finite abelian groups have this property, but it fails for D_8 and Q_8.)

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

3. 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?

Some more things we do not know

1. For which finite non-abelian groups G is it true that, for all finite groups H with $G' = H'$, it holds that H is integrable if and only if G is? (All finite abelian groups have this property, but it fails for D_8 and Q_8.)

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

3. 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?

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

Infinite groups

Infinite groups

Proposition

Let G be finitely generated. If G has an integral, then it has a finitely generated integral.

Infinite groups

Proposition

Let G be finitely generated. If G has an integral, then it has a finitely generated integral.

Theorem

Any free group is integrable.

Infinite groups

Proposition

Let G be finitely generated. If G has an integral, then it has a finitely generated integral.

Theorem

Any free group is integrable.

Remark

The free product of integrable groups may or may not be integrable. For example,

- $C_2 * C_2$ *is the infinite dihedral group, which is not integrable (by the same argument as for finite dihedral groups).*
- $C_3 * C_3$ *is the derived group of* $\mathrm{PGL}(2, \mathbb{Z})$.

Inverse group theory

Inverse group theory

The material just discussed can be regarded as part of inverse group theory. Given a construction $\mathcal{F}$ on groups, decide for which groups G there exists a group H such that $\mathcal{F}(H) = G$.

Inverse group theory

The material just discussed can be regarded as part of inverse group theory. Given a construction $\mathcal{F}$ on groups, decide for which groups G there exists a group H such that $\mathcal{F}(H) = G$.

There are many group-theoretic constructions other than derived group: center, central quotient, derived quotient, Frattini subgroup, Fitting subgroup, Schur multiplier, other cohomology groups, and various constructions from permutation groups.

Inverse group theory

The material just discussed can be regarded as part of inverse group theory. Given a construction $\mathcal{F}$ on groups, decide for which groups G there exists a group H such that $\mathcal{F}(H) = G$.

There are many group-theoretic constructions other than derived group: center, central quotient, derived quotient, Frattini subgroup, Fitting subgroup, Schur multiplier, other cohomology groups, and various constructions from permutation groups.

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.

Inverse group theory

We consider an inverse problem arising from a construction $\mathcal{F}$ to be **trivial** if

$$G = \mathcal{F}(H) \implies G = \mathcal{F}(G).$$

Inverse group theory

We consider an inverse problem arising from a construction $\mathcal{F}$ to be **trivial** if

$$G = \mathcal{F}(H) \implies G = \mathcal{F}(G).$$

Example

1. The center of any group is abelian; but an abelian group is its own center.

Inverse group theory

We consider an inverse problem arising from a construction $\mathcal{F}$ to be **trivial** if

$$G = \mathcal{F}(H) \implies G = \mathcal{F}(G).$$

Example

1. The center of any group is abelian; but an abelian group is its own center.

2. The Fitting subgroup of any group is nilpotent; but a nilpotent group is its own Fitting subgroup.

Inverse group theory

We consider an inverse problem arising from a construction $\mathcal{F}$ to be **trivial** if

$$G = \mathcal{F}(H) \implies G = \mathcal{F}(G).$$

Example

1. The center of any group is abelian; but an abelian group is its own center.

2. The Fitting subgroup of any group is nilpotent; but a nilpotent group is its own Fitting subgroup.

3. The derived quotient of any group is abelian; but an abelian group is its own derived quotient.

Frattini subgroup

Frattini subgroup

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

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

Frattini subgroup

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

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

Problem

Which nilpotent groups are Frattini subgroups of finite groups?

Frattini subgroup

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

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

Problem

Which nilpotent groups are Frattini subgroups of finite groups?

Theorem (Eick, 1997)

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 $\mathrm{Aut}(G)$.

Schur multipliers

Schur multipliers

The **Schur multiplier** $M(G)$ of a finite group G is

1. isomorphic to $(R \cap F')/[F, R]$ if $G \cong F/R$ is a presentation for G, for some free group F and a normal subgroup R
2. the second cohomology group $H^2(G, \mathbb{C}^*)$.

Schur multipliers

The **Schur multiplier** $M(G)$ of a finite group G is

1. isomorphic to $(R \cap F')/[F, R]$ if $G \cong F/R$ is a presentation for G, for some free group F and a normal subgroup R
2. the second cohomology group $H^2(G, \mathbb{C}^*)$.

Theorem

Every abelian group is the Schur multiplier of a group.

Schur multipliers

The **Schur multiplier** $M(G)$ of a finite group G is

1. isomorphic to $(R \cap F')/[F, R]$ if $G \cong F/R$ is a presentation for G, for some free group F and a normal subgroup R
2. the second cohomology group $H^2(G, \mathbb{C}^*)$.

Theorem

Every abelian group is the Schur multiplier of a group.

Remark

$C_p \times C_p$ *is not the Schur multiplier of a p-group.*

Schur multipliers

The **Schur multiplier** $M(G)$ of a finite group G is

1. isomorphic to $(R \cap F')/[F, R]$ if $G \cong F/R$ is a presentation for G, for some free group F and a normal subgroup R
2. the second cohomology group $H^2(G, \mathbb{C}^*)$.

Theorem

Every abelian group is the Schur multiplier of a group.

Remark

$C_p \times C_p$ *is not the Schur multiplier of a p-group.*

Question

Which abelian p-groups occur as Schur multipliers of p-groups?