On (Borel) Group Extensions

Linus Richter

Victoria University of Wellington

$(GT)^2$, 17 May 2022

Notation in this talk: $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ and $K_4 = \mathbb{Z}_2 \times \mathbb{Z}_2$.

Motivation I: Almost Homomorphisms

If an object "almost" satisfies a particular property, we sometimes ask "how much does it fail to do so?". For instance:

- cocycles that are "similar enough" are trivial (coboundaries);
- a map between structures is "almost" a homomorphism; with a metric, we can "measure" by how much it fails

Theorem

Let $f\colon (\mathbb{R},+) \to (\mathbb{R},+)$ be a group homomorphism that is Borel. Then $f(x) = rx$ for some $r \in \mathbb{R}$.

What if we only know that $f(x+y) - f(x) - f(y) \in G$ for some group G?

Question: is there a homomorphism $g\colon \mathbb{R} \to \mathbb{R}$ that approximates f? $\leftarrow$ Ulam's problem of stability of non-exact homomorphisms

Example

Consider the additive group $(\mathbb{R}, +)$. Suppose

- $f : \mathbb{R} \to \mathbb{R}$ is Borel;
- $f(x + y) - f(x) - f(y) \in G$ for some countable group $G \leq \mathbb{R}$.

Question: Is there a Borel (and hence continuous) homomorphism $g : \mathbb{R} \to \mathbb{R}$ that G-approximates f? (i.e. for which $f(x) - g(x) \in G$?)

Theorem (Kanovei, Reeken (2000))

If f is as above, then there is a continuous homomorphism $g : \mathbb{R} \to \mathbb{R}$ such that $f(x) - g(x) \in G$. (In fact, $g(x) = rx$ for some $r \in \mathbb{R}$.)

Proof uses **descriptive set theory**, especially **Polish groups**

What about other spaces? What about other groups G? What about structures other than groups?

Ulam's Stability Problem in general (Ulam, 1964)

- Take a theorem of your choice
- if we make a "small" change to the hypotheses, is the theorem still "almost" true?
- (Originally arose in mechanics: how much does a solution to a problem depend on initial values?)
- Example: consider a class of structures that admits homomorphisms
- can any "almost homomorphism" be "approximated" by a strict homomorphism?
  - both "almost", "approximate" depend on context

There is no universal solution – but partial solutions do exist!

Ulam Stability Framework

Ulam stability phenomena may be studied in any setting where one has:

1. *a notion of morphisms;*
2. *a notion of approximate morphisms;*
3. *a notion of closeness relating morphisms and approximate morphisms.*

Areas of interest (e.g.) C^*-algebras, Boolean algebras, groups (in particular Polish: tools from descriptive set theory are available)

We focus on groups.

Motivation II/Application: Group Extensions

- Classification of finite simple groups
- every finite group has a **composition series**: simple groups "build up" the finite groups.

So: if we

① understand finite simple groups, and

② how to construct finite groups from simple groups

then we can classify all finite groups!

But: ② is very hard. This is the **group extension problem**.

Definition (Composition Series)

Let G be a finite group. There exists a sequence of groups $(E_1, \ldots, E_n)$ such that

$$G = E_n \trianglerighteq E_{n-1} \trianglerighteq \ldots \trianglerighteq E_0 = 1$$

where each E_k/E_{k-1} is simple. These are the *composition factors*.

So a finite group can be decomposed into simple groups. And simple groups have a trivial composition series.

Example

- $\mathbb{Z}_4 \trianglerighteq \mathbb{Z}_2 \trianglerighteq 1$ (solvable)
- $S_4 \trianglerighteq A_4 \trianglerighteq K_4 \trianglerighteq \mathbb{Z}_2 \trianglerighteq 1$ (solvable)
- $S_5 \trianglerighteq A_5 \trianglerighteq 1$ (not solvable – think of Galois theory)

Finite groups from simple groups

$$S_4 \trianglerighteq A_4 \trianglerighteq K_4 \trianglerighteq \mathbb{Z}_2 \trianglerighteq 1$$

- *normal series*: each term is a normal subgroup of its predecessor
- *composition factors* are:
  - $\mathbb{Z}_2/1 \cong \mathbb{Z}_2$
  - $K_4/\mathbb{Z}_2 \cong \mathbb{Z}_2$
  - $A_4/K_4 \cong \mathbb{Z}_3$
  - $S_4/A_4 \cong \mathbb{Z}_2$

  which are *all simple*.

Now go backwards: from the composition factors $(\mathbb{Z}_2, \mathbb{Z}_2, \mathbb{Z}_3, \mathbb{Z}_2)$, can we *recover* S_4? **Yes! But it's hard.**

Example

$$G = E_2 \trianglerighteq E_1 \trianglerighteq E_0 = 1 \text{ with composition factors } (\mathbb{Z}_3, \mathbb{Z}_2)$$

Work from right-to-left:

1. Need: $E_1/1 \cong \mathbb{Z}_3$; hence $E_1 \cong \mathbb{Z}_3$.
2. Need: $E_2/E_1 \cong \mathbb{Z}_2$. So: $|E_2/E_1| = |E_2|/|E_1| = 2$, so $|E_2| = 2|\mathbb{Z}_3| = 6$. How many groups of order 6 exist? Two:
   - $\mathbb{Z}_6 = \mathbb{Z}_3 \times \mathbb{Z}_2$
   - S_3

   Both contain a normal subgroup of order 3. Hence both work.

Observe that $S_3 \ncong \mathbb{Z}_3 \times \mathbb{Z}_2$!

Definition

We say that E_2 is *an extension of E_2/E_1 by E_1*. Possibly unfortunate notation – and NOT universally agreed

So: $\mathbb{Z}_6, S_3$ extend $\mathbb{Z}_2$ by $\mathbb{Z}_3$. And $\mathbb{Z}_6$ extends $\mathbb{Z}_3$ by $\mathbb{Z}_2$, but S_3 does not.

Group Extensions

Definition (Group Extensions)

Let A, H be abelian groups. We call E an *extension of A by H* if:

1. there exists $N \trianglelefteq E$ such that $N \cong H$; and
2. $E/N \cong A$.

A more useful (for our purposes) characterisation from *category theory*:

Definition

E extends A by H if and only if

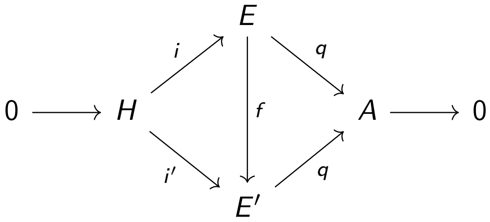
$$1 \longrightarrow H \xrightarrow{\;i\;} E \xrightarrow{\;q\;} A \longrightarrow 1$$

is a *short exact sequence*: so i is an injection, q is a surjection, and $\mathrm{im}(i) = \ker(q)$.

Finding all such extensions is the **group extension problem**.

Some facts about group extensions

- If E extends A by H and A, H are abelian, is E abelian, too?
  - No. $E = S_3$ contains a subgroup of order 3, so $S_3/\mathbb{Z}_3 \cong \mathbb{Z}_2$.
- If E, E' extend A by H, are E, E' necessarily isomorphic?
  - No. Above, $S_3 \ncong \mathbb{Z}_3 \times \mathbb{Z}_2$.
- Extensions E, E' are equivalent if commutes (then f is an isomorphism):



- If E, E' are isomorphic and extend A by H, are they equivalent?
  - No. Take $E = \mathbb{Z}_9, A = H = \mathbb{Z}_3$. Put $i(1) = 3, i'(1) = 6$. Then $f(1) \in \{2, 5, 8\}$, but $q(1) \neq q(f(1)) = q(2) = q(5) = q(8)$.

...and in general?

That's a hard question to answer...

- ...it's exactly the *group extension problem*
- O. Hölder (1893), via factor sets $\leftarrow$ these give group cohomology...
- O. Schreier (1924), non-abelian extensions
- semi-direct products to classify all *split extensions*

...but there is no unified theory that captures and classifies *all* extensions.

> But: if all groups are abelian, then we can identify the group extensions with *abelian 2-cocycles*!

Using Group Cohomology

We restrict our attention to abelian extensions!

Let A, H be abelian groups.

Definition

$C\colon A^2 \to H$ is an *abelian (2-)cocycle* if

1. $C(x, y) = C(y, x)$ ← abelian
2. $C(x, y) + C(x + y, z) = C(x, z) + C(x + z, y)$. ← cocycle property

If there is a map $\eta\colon A \to H$ such that

$$C(x, y) = \eta(x) + \eta(y) - \eta(x + y)$$

then C is a *(2)-coboundary*. ↑ the cocycle "measures" how much η fails to be a homomorphism...

2-cocycle gives rise to group extension – and vice versa!

Theorem

Let $C\colon A^2 \to H$ be a cocycle. Then P_C defined on $A \times H$ by

$$(a, h) + (a', h') = (a + a', h + h' + C(a, a'))$$

is an abelian group extension of A by H.

$$0 \longrightarrow H \xrightarrow{\ i\ } P_C \xrightarrow{\ q\ } A \longrightarrow 0$$

If $P \geq H$ is abelian and $A \cong P/H$ then there is a cocycle C such that $P \cong P_C$. Then P and P_C are also congruent group extensions!

group extensions $\leftrightarrow$ abelian 2-cocycles

A few facts about cocycles

- Cocycles C, C' are *cohomologous* if

$$C(x,y) - C'(x,y) = \alpha(x) + \alpha(y) - \alpha(x+y)$$

  for some $\alpha\colon A \to H$ (iff their difference is a coboundary)
- Cohomologous cocycles generate equivalent group extensions
- The trivial extension

$$0 \longrightarrow H \xrightarrow{\ i\ } A \times H \xrightarrow{\ q\ } A \longrightarrow 0$$

  is generated by the trivial cocycle $C(x,y) = 0$.

Coboundaries generate the trivial extension!

The Borel Case

Definition

A top. space is called *Polish* if it separable and completely metrisable. A group A is a *Borel group* if it is a Polish space whose group operation and inverse map are Borel.

Borel functions (and sets) are "definable"

Definition

A cocycle is *Borel* if it is a Borel map between Borel groups. If C is Borel then P_C is a *Borel group extension*.

The group of *Borel group extensions* is denoted by $H^2_{\mathrm{Bor}}(A, H)$. It's the quotient of Borel cocycles by Borel coboundaries.

Borel group extensions of $\mathbb{R}(^n)$

Let G be abelian and countable. Consider the additive group $(\mathbb{R}, +)$.

Theorem (Kanovei, Reeken (2000))

The group $H^2_{\mathrm{Bor}}(\mathbb{R}, G)$ of abelian Borel group extensions of $\mathbb{R}$ by G is trivial.

Corollary

For countable $G \leq \mathbb{R}$ and $f : \mathbb{R} \to \mathbb{R}$ Borel s.t. $f(x + y) - f(x) - f(y) \in G$ there exists a Borel (and hence necessarily continuous) homomorphism $g : \mathbb{R} \to \mathbb{R}$ for which $f(x) - g(x) \in G$. (It's $x \mapsto rx$ for some $r \in \mathbb{R}$.)

Theorem (Lupini, R.)

The group $H^2_{\mathrm{Bor}}(\mathbb{R}^n, G)$ of abelian Borel group extensions of $\mathbb{R}^n$ by G is trivial for all $n > 1$.

The proof uses **descriptive set theory**, and **forcing**.

A snapshot of forcing

- Paul Cohen (1963): showed ZF is independent of CH
- similar arguments already in use in computability theory (Kleene, Post 1954), later adapted

The main idea

- Build an object by approximation
- Conditions are partially ordered in $\mathbb{P}$
- A filter G on $\mathbb{P}$ is *generic* if it meets "enough" dense open sets of $\mathbb{P}$

Cohen Forcing: Construct real number by initial segments; approximations are *open intervals with rational endpoints*.

Generics are *not special* – they don't satisfy "rare" properties!

Sketch of the proof for $n = 1$ (Kanovei, Reeken, 2000)

Let $C\colon \mathbb{R}^2 \to G$ be a Borel cocycle (we show it's a Borel coboundary).

- C is Borel, and G is countable, so there's an open interval I on whose *generic pairs* C is constant (follows straight from Baire Category)
- C behaves nicely on generics in I: generics are not special, so (a simple shift of) C is "robust": invariant under sums of generics in I
- If $x \in \mathbb{R}$ is not generic in I, express as a sum of generics from I (so *cover* $\mathbb{R}$ with multiples of I) and use that C is nice on generics of I: so C is nice on x
- Otherwise, *mirror* into a multiple nI of I using cocycle property

$$C(x, y) = C(x, z) + C(x + z, y) - C(x + y, z)$$

  via some z, then express the mirror image as sum of generics of I.
- Since C is nice on generics of I, we just need to ensure that the cover-and-mirror maps are Borel, which they are.

The case $n > 1$

- Open interval on which C is constant is now an open n-dimensional box $\mathbf{I}$
- what is "generic" e.g. in $\mathbb{R}^2$? A pair of points is generic if *both points are generic w.r.t. each other*
- *mirroring* in $\mathbb{R}^2$ requires more care: open intervals are open boxes, which must be shifted and extended to allow for covering-and-mirroring argument

. . . but the argument relies on the connectedness of $\mathbb{R}^n$, and, after accounting for technicalities, the same strategy works.

Outlook

What about other Polish spaces? In other words, how much does the result depend on the topological properties (connectedness, for instance) of $\mathbb{R}$?

What about Ulam Stability questions? They might yield more tools for homological algebra (extension questions etc).