Some algebraic properties of compact topological groups

Compact topological groups: examples

connected:

- S^1, circle group.
- $\mathrm{SO}(3, \mathbb{R})$, rotation group

not connected:

- Every finite group, with the discrete topology.
- $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$: inverse limit of finite Galois groups,
- $\mathbb{Z}_p$: inverse limit of finite cyclic groups

Such inverse limits inherit a topology from the discrete finite groups. It is

- *compact* (Tychonoff's Theorem) and
- *totally disconnected.*

Compact and tot. disconn. topological group = *profinite group* = inverse limit of finite groups

Familiar examples:

- infinite Galois groups
- matrix groups such as $\mathrm{GL}_n(\mathbb{Z}_p)$
- free profinite groups

Theorem 1 *Let G be a compact group with identity component G^0.*

(i) *G/G^0 is a profinite group*

(ii) *$G^0 = Z \cdot P$ where Z is the centre of G^0 and*

$$P \cong \frac{\prod S_i}{D}$$

is a Cartesian product of compact connected simple Lie groups S_i modulo a central subgroup D.

Part (ii) : Hilbert's 5th problem in compact case

Z is essentially a product of copies of S^1 : a 'protorus'

The compact connected simple Lie groups are well known – SO(n), SU(n) etc.

All results are joint work with **Nikolay Nikolov**.

G will denote a compact group

N is a normal subgroup of (the underlying *abstract group*) G.

Definition G is of *f.g. type* if *the maximal profinite quotient* G/G^0 is *topologically finitely generated*;

[equivalently: G/G^0 is an inverse limit of finite d-generator groups for some fixed number d.]

Theorem 2 ('Serre's question') *If G is of f.g. type and G/N is finite then N is open in G.*

Since the topology on a *profinite* group is defined by the family of all open subgroups (not true for connected groups!), an immediate consequence is

Corollary 1 ('rigidity') *If G is a finitely generated profinite group then every group homomorphism from G to any profinite group is continuous.*

In particular this shows that the **topology** on such a profinite group is uniquely determined by the **group-theoretic** structure.

Remarks. (i) In any compact group, open subgroups all have finite index (immediate from the definition).

(ii) A compact *connected* group has *no* proper subgroups of finite index: *not* obvious from the definition but follows from the structure theory, which implies that such a group is *divisible,* i.e. all elements have nth roots for all n. So the meat of Theorem 2 is in the *profinite* case.

(iii) The restriction to *f.g. type* is absolutely necessary: in infinitely generated profinite groups the topology is only loosely connected to the abstract group structure.

Examples: here C_q is a cyclic group of order q, and p is a prime.

- The profinite group $C_p^{\mathbb{Z}}$ has $2^{2^{\aleph_0}}$ subgroups of index p, but only countably many open subgroups.

This group therefore has many distinct topologies, but the resulting topological groups are all isomorphic.

- The profinite groups $A = \prod_{n \in \mathbb{N}} C_{p^n}$ and $A \times \mathbb{Z}_p$ are isomorphic as abstract groups, but not as topological groups.

However, every finite (abstract) image of A occurs also as a continuous image.

- There is a profinite group having no abelian continuous image, but having C_2 as an abstract image.

What about **countable images**?

A compact group can't be countably infinite.

Could there be a countably infinite *abstract* image? YES!

Let A be an infinite f.g. abelian profinite group. Then either A maps onto $\mathbb{Z}_p$ or A maps onto $B = \prod_{p\in P} C_p$ for some infinite set of primes P.

We have additive group homomorphisms

$$\mathbb{Z}_p \hookrightarrow \mathbb{Q}_p \to \mathbb{Q},$$

$$B \cong \prod_{p\in P} \mathbb{F}_p \twoheadrightarrow \prod_{p\in P} \mathbb{F}_p/\tilde{} = F \twoheadrightarrow \mathbb{Q},$$

where F is a non-principal ultraproduct, hence a field of characteristic 0.

In both cases these compose to give a group epimorphism from A onto $\mathbb{Q}$.

Main result:

Theorem 3 *If G is of f.g. type and G/N is countably infinite then G/N has an infinite virtually-abelian quotient.*

This implies for example that G cannot map onto a *countably infinite simple group*.

By Theorem 2, if G/N is residually finite then N is closed. As every finitely generated abelian group is residually finite, we get

Corollary 2 *If G/N is finitely generated (as abstract group) then G/N is finite (and so N is open in G).*

A generalisation

Let $\overline{N}$ denote the closure of N in G.

$$\begin{aligned} G/N \text{ countable} &\Longrightarrow G/\overline{N} \text{ a countable compact group} \\ &\Longrightarrow G/\overline{N} \text{ finite} \Longrightarrow \overline{N} \text{ open.} \end{aligned}$$

Definition N is *virtually dense* in G if $\overline{N}$ is open in G.

We have seen that these things can occur non-trivially in the abelian context. They also arise in a different way: if

$$G = \prod_{i \in I} H_i$$

is a product of non-trivial compact groups over an infinite index set I then the *restricted direct product*

$$N = \bigoplus_{i \in I} H_i$$

is dense in G, and has infinite index.

Definition G as above is *strictly infinite semisimple* if I is infinite and each of the H_i is either a *finite simple group* or a *connected simple Lie group.*

Theorem 4 *Let G be a compact group of f.g. type. Then G has a virtually-dense normal subgroup of infinite index if and only if G has a (continuous) quotient that is* either

- *infinite and virtually abelian* or
- *virtually (strictly infinite semisimple).*

Exercise. Deduce: if G is just-infinite and not virtually abelian then *every normal subgroup of G is closed.*

We can also characterize precisely those G that have a *proper dense* normal subgroup: the answer involves certain restrictions on the simple factors occurring in the strictly infinite semisimple quotient.

Dévissage: basic pieces will be *abelian groups*, *simple Lie groups*, and *finite simple groups*, or at least Cartesian products of such things.

Key question: how to get *topological* information from *algebraic* input?

Given: (i) definition of **topological group**: *group multiplication is continuous*,

(ii) the definition of **compact**, which implies that *a continuous image of a compact set is compact, hence closed.*

Lemma 1 *Let G be a compact group and H a closed subgroup of G. Then for each $g \in G$ the set*

$$[H, g] = \{[h, g] \mid h \in H\}$$

is closed in G.

Lemma 2 *Let X be a closed subset of a compact group G, with $1 \in X = X^{-1}$. Then the subgroup $\langle X \rangle$ generated* (algebraically) *by X is closed in G if and only if there exists n such that*

$$\begin{aligned} \langle X \rangle &= X^{*n} \\ &= \{x_1 \ldots x_n \mid x_i \in X\}. \end{aligned}$$

In this case, we say that X has *width* (at most) n in G, and write

$$m_X(G) \leq n.$$

If G is *profinite*,

$$m_X(G) = \sup m_{XK/K}(G/K)$$

where K ranges over all open normal subgroups of G. In this case the study of $m_X(G)$ can be reduced to the case where G is *finite*.

Results on finite groups

Definition. A finite group Q is *almost-simple* if

$$S \leq Q \leq \mathrm{Aut}(S)$$

for some simple (non-abelian) group S (identify S with its inner automorphism group)

Example: $Q = \mathrm{Sym}(n) > S = \mathrm{Alt}(n)$, $n \geq 5$.

Definition. For a finite group G,

$$G_0 = \bigcap \{K \lhd G \mid G/K \text{ is almost-simple}\}.$$

Theorem 5 *Let G be a finite d-generator group with a normal subgroup $H \leq G_0$. Let $\{y_1, \ldots, y_r\}$ be a symmetric subset of G such that*

$$H \langle y_1, \ldots, y_r \rangle = G' \langle y_1, \ldots, y_r \rangle = G.$$

Then the subgroup $[H, G] = \langle [h, g] \mid h \in H,\ g \in G \rangle$ satisfies

$$[H, G] = ([H, y_1] \ldots [H, y_r])^{*f}$$

where $f = f(d, r) = O(r^6 d^6)$.

(G' = derived group of G). Also true *without* assuming $H \leq G_0$ provided $\langle y_1, \ldots, y_r \rangle = G$.

Routine compactness arguments turn Theorem 5 into

Theorem 6 *Let G be a finitely generated profinite group with a closed normal subgroup H. Let Y be a finite symmetric subset of G such that*

$$H\overline{\langle Y \rangle} = G'\overline{\langle Y \rangle} = G.$$

If $H \leq G_0$ then

$$[H, G] = \left(\prod_{y \in Y} [H, y] \right)^{*f}$$

for some finite f.

(G_0 defined as in finite case, with K now ranging over all *open* normal subgroups of G such that G/K is almost-simple.)

Suppose that $Y \subseteq N \lhd G$. Then $[H, G] \leq N$. It is now easy to deduce the key '**reduction theorem**':

Corollary 3 *Let G be a finitely generated profinite group with a normal subgroup N. If*

$$NG' = NG_0 = G$$

then $N = G$.

Reduces problems about G to problems about

- G/G' : an **abelian** group,
- G/G_0 : an extension of a **semisimple** group by a **soluble** group. In fact there are closed normal subgroups

  $$A_0 \lhd A_1 \lhd A_2 \lhd A_3 = G/G_0$$

  with A_0 semisimple, A_i/A_{i-1} abelian ($i = 1, 2, 3$)

Application: quick proof of Theorem 2 ('Serre's question'). The abelian case is easy, and the semisimple case follows from

Theorem (Martinez/Zelmanov, Saxl/Wilson, 1996-97) *Let $q \in \mathbb{N}$. In any finite simple group S, the set $\{x^q \mid x \in S\}$ has width at most $f(q)$, a finite number depending only on q.*

For Theorem 3 we also need to study normal subgroups of infinite index in **semisimple groups**. This depends on some different ideas. Suppose

$$G = \prod_{i \in I} S_i$$

where I is an infinite index set and each S_i is a finite simple group; assume that G is of f.g. type. To each non-principal ultrafilter $\mathcal{U}$ on I we associate a certain normal subgroup $K_{\mathcal{U}}$ of G, and prove:

$$|G/K_{\mathcal{U}}| \geq 2^{\aleph_0}.$$

($G/K_{\mathcal{U}}$ is what is known as a 'metric ultraproduct'; it is a simple group.)

Proposition 1 *Let N be a proper normal subgroup of G. If N is dense in G then $N \leq K_{\mathcal{U}}$ for some non-principal ultrafilter $\mathcal{U}$.*

Together with a similar construction in the case where the S_i are simple compact Lie groups, it gives

Theorem 7 *Let G be a semisimple compact group of f.g. type and N a normal subgroup of G. If $|G/N|$ is infinite then $|G/N| \geq 2^{\aleph_0}$.*

N. Nikolov, D. Segal, 'Generators and commutators in finite groups; abstract quotients of compact groups', *Invent. Math.* (2012)