Some algebraic properties of compact topological groups

I've directed this talk to a general audience, but I hope some of it will be new to some of the group theory specialists. To keep these awake I'll include a couple of *exercises* to do in your head.

Compact topological groups arise in many areas of mathematics. Probably the first example one thinks of is S^1, the circle group. When the theory of Lie groups was being developed a century ago it was recognized that every simple Lie group has a compact real form, typified by groups like $\mathrm{SO}(3,\mathbb{R})$, higher-dimensional versions of S^1 considered as the one-dimensional rotation group.

Of course every finite group can be thought of as a compact group, with the discrete topology. This seems a quixotic remark but it leads to a whole different universe of compact groups, developed in the last century by number theorists: the absolute Galois group of $\mathbb{Q}$ is an inverse limit of finite Galois groups, and the group $\mathbb{Z}_p$ of p-adic integers is the inverse limit of finite cyclic groups. Such inverse limits inherit a topology from the discrete finite groups; this topology is still *compact* (Tychonoff's Theorem), but it is far from discrete – instead it is *totally disconnected*. A topological group that is compact and totally disconnected is called *profinite*. Familiar examples of profinite groups are infinite Galois groups and matrix groups such as $\mathrm{GL}_n(\mathbb{Z}_p)$. We also have the *free profinite groups*: the d-generator free profinite group maps onto every d-generator finite group, and is useful as a compact object that encapsulates everything there is to know about *all* those infinitely many finite groups.

Now the structure of an arbitrary compact group G (always assumed to be Hausdorff) breaks into pieces in a nice way:

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) is the compact version of the solution of Hilbert's 5th problem (it is less deep than the general case). The abelian group Z is essentially a product of copies of S^1. The compact connected simple Lie groups are well known; and the study of the general compact group G tends to break up into two parts, one involving these Lie groups and the other delving into finite group theory. These investigations don't exactly overlap, but in some parts they run along parallel lines: the classification of finite simple groups shows that 'most' of the finite simple groups are groups of Lie type, analogues of the simple Lie groups.

Given a topological group G, we may hope (or assume) that the *closed* normal subgroups are more or less understood – they correspond to continuous morphisms (if G is a Galois group, the closed subgroups correspond exactly to the intermediate fields). Now algebraists are interested in group-theoretic structure, so we may wonder: what can be said about normal subgroups and homomorphisms of the underlying abstract group?

I will discuss some recent results obtained in joint work with Nikolay Nikolov.

Throughout G will denote a compact group, and N a normal subgroup of (the underlying abstract group) G.

I'll say that G is of *f.g. type* if *the maximal profinite quotient* G/G^0 is *topologically finitely generated*; this means that G/G^0 contains a finite subset X such that the subgroup generated by X is dense in G/G^0, or equivalently that G/G^0 is an inverse limit of finite d-generator groups for some fixed number d.

The key result is

Theorem 2 *If G is of f.g. type and G/N is finite then N is open in G.*

This answers a question posed long ago by J.-P. Serre, who proved it for the special case where G is a pro-p group. 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). So the point of the theorem is that the *converse* holds in the f.g. case.

(ii) A compact *connected* group has *no* proper subgroups of inite index: this is 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.

(a) 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.

(b) 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.

(c) We can construct a profinite group having no abelian continuous image, but having C_2 as an abstract image. (By 'continuous image' I always mean one that is a Hausdorff topological group – every image can be given the indiscrete topology, making every map continuous in a trivial way.)

What about *countable* images? *A compact group can't be countably infinite*: this is kind of obvious for Lie groups, and it is a basic fact about profinite groups. Could there be a countable *abstract* image? It may seem implausible, but actually these are easy to find! Suppose A is 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 $\mathbb{Q}$.

The additive group of $\mathbb{Q}$ has no (nontrivial) finite images: this is no accident. A group is *residually finite* if its normal subgroups of finite index intersect in $\{1\}$; and an immediate consequence of Theorem 2 is

Corollary 2 *If G is of f.g. type and G/N is residually finite and countable then G/N is finite.*

The next result needs a lot more work:

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

(*Virtually-abelian* means it has an abelian normal subgroup of finite index.)

Thus for example G can't have a countably infinite *simple* image. Can there be an uncountably infinite simple image? YES: easy if G is connected, but *also true* and less obvious if G is *profinite* – this will appear later.

Now we stick with countable images. From Theorem 3 it is not hard to deduce

Corollary 3 *Suppose G is of f.g. type. Then G has a countably infinite abstract image if and only if G has an infinite virtually-abelian continuous quotient.*

Corollary 4 *If G/N is finitely generated (as abstract group) then G/N is finite (and so N is open in G).*

A while ago, in a paper on Arxiv, Nikolay asked 'how strange can an abstract group image of a compact group be?'. As we've seen, such an image can be countably infinite, which is a bit strange; the last result perhaps restores one's faith in the balance of things by showing that such an image can't be so strange as to be a finitely generated infinite group. This is reminiscent of the Burnside Problem, and in fact some parts of the proof move into that kind of territory.

Suppose now that G is a compact group and N is a normal subgroup (of the underlying abstract group) such that G/N is countable. Let $\overline{N}$ denote the closure of N. Then $G/\overline{N}$ is a countable compact group, so it is *finite*. in this case, we say that N is *virtually-dense* 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.

The final theorem shows that these examples account for all possibilities. We say that G 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*. (proved by A. Jaikin for pro-p groups.)

(*Just-infinite* means: infinite but every proper continuous quotient is finite.)

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.

What kind of mathematics lies behind these results? The standard working method in group theory is *dévissage*: you deconstruct your group as far as possible and then examine the pieces. Theorem 1 suggests that the basic pieces will be abelian groups, simple Lie groups, and finite simple groups, or at least Cartesian products of such things. The hardest part of the work – taking as given the classifications of finite simple groups and simple Lie groups, which were also quite hard! – is a rather technical 'reduction theorem'.

Before stating this, let's recall what we are looking for.

The key question is: how to get *topological* information from *algebraic* input? All we have to work with is (i) the definition of topological group: *group multiplication is continuous*, and (ii) the definition of compact, which implies that *a continuous image of a compact set is compact, hence closed*. These combine to give the fundamental

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.

Here

$$[h, g] = h^{-1}g^{-1}hg$$

is the *commutator*.

If we want to obtain a closed *subgroup* we have to combine this with

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

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

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

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

Now if G is a *profinite* group, one has

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

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

To state our main theorem on finite groups we need another definition. A finite group Q is *almost-simple* if

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

for some simple (non-abelian) group S. Example: the symmetric group S_n, $n \geq 5$. For a finite group G,

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

The same definition applies for a profinite group G, with N now ranging over all open normal subgroups of G

The derived group of G is denoted G' (this is the smallest normal subgroup N such that G/N is abelian).

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

I should also mention the more elegant, but less powerful, theorem that gives the same conclusion for an *arbitrary* $H \lhd G$ under the stronger hypothesis $\langle y_1, \ldots, y_r \rangle = G$.

Now Theorem 5 translates immediately 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.

It follows that if $Y \subseteq N$ for some normal subgroup N of G then $[H, G] \leq N$. It is now easy to deduce the key '**reduction theorem**':

Corollary 5 *Let G be a finitely generated profinite group with a normal subgroup N. If*

$$NG' = NG_0 = G$$

then $N = G$.

This is used to reduce problems about G to problems about the *abelian* group G/G' and the group G/G_0; the point is that G/G_0 is also very nice: it is an extension of a semisimple group by a soluble group.

For example, Theorem 2, the case where N has finite index in G ('Serre's problem'), now quickly drops out. The abelian case is easy, and the semisimple case follows from the 15-year old

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.

Another easy application is the proof of Theorem 4 (virtually dense normal subgroups) in the *profinite* case **(Exercise)**. (The general case is a lot harder).

The study of normal subgroups of infinite index in semisimple groups needs some different ideas. Suppose now that

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

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 that

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

In fact we have recently found these in the literature, where the quotient $G/K_{\mathcal{U}}$ is called a 'metric ultraproduct'.

[**On board?** Define

$$h_{\mathcal{U}} : G \to [0,1]$$

by

$$h_{\mathcal{U}}(\mathbf{g}) = \lim_{\mathcal{U}} \lambda_{S_i}(g_i)$$

where

$$\lambda_S(x) = \frac{\log \left|x^S\right|}{\log |S|}.$$

Then

$$K_{\mathcal{U}} = h_{\mathcal{U}}^{-1}(0).$$

We show that $h_{\mathcal{U}}$ induces a map from $G/K_{\mathcal{U}}$ *onto* $[0,1]$.]

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

The proof depends on properties of the finite simple groups, to do with the *width of conjugacy classes* in these groups.

A similar procedure is applied in the case where each S_i is a compact connected simple Lie group. We don't get such an elegant construction for the subgroups $K_{\mathcal{U}}$, but it is good enough to give

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

This is the final step needed for the proof of Theorem 3.

For details see: N. Nikolov and D. Segal, `arXiv: 1102.3037`