37. **Representations of compact topological groups**

37.1. **Existence of the Haar measure.** One can generalize integration theory to arbitrary compact and even to locally compact topological groups. For simplicity we will describe this generalization in the case of compact topological groups with a countable base.

Namely, let X be a compact Hausdorff topological space with a countable base. For compact Hausdorff spaces this is equivalent to being metrizable. Let $C(X,\mathbb{R})$ be the space of continuous real-valued functions on X. This is a real Banach space with norm

$$||f|| = \max_{x\in X} |f(x)|.$$

Recall that by the **Riesz-Markov-Kakutani representation theorem**, a finite Borel measure μ on X is the same thing as a positive continuous linear functional $I : C(X,\mathbb{R}) \to \mathbb{R}$ (i.e., such that $I(f) \geq 0$ for $f \geq 0$), namely,

$$I(f) = \int_X f d\mu.$$

Moreover, μ is a probability measure if and only if $I(1) = 1$, and any $\mu \neq 0$ has positive volume and so can be normalized to be a probability measure.

Now let G be a compact topological group with a countable base. It acts on $C(G,\mathbb{R})$ by left and right translations, so acts on nonnegative probability measures of G.

Theorem 37.1. *(Haar, von Neumann) G admits a unique left-invariant probability measure.*

This measure is also automatically right-invariant (since it is unique) and is called the **Haar measure** on G.

Remark 37.2. A unique up to scaling left-invariant regular Haar measure (albeit of infinite volume and not always right-invariant in the non-compact case) exists more generally for any locally compact group G (not necessarily having a countable base).[18] We will not prove this here, but we remark that Haar measures on Lie groups that we have constructed using top differential forms are a special case of this.

Proof. Let $g_i, i \geq 1$ be a dense sequence in G (it exists since G has a countable base, hence is separable, as you can pick a point in every open set of this base). Let p_i be a sequence of positive numbers

[18]Note that a finite Borel measure on a compact Hausdorff space with a countable base is necessarily regular.

such that $\sum_i p_i = 1$. To this data attach the **averaging operator** $A : C(G, \mathbb{R}) \to C(G, \mathbb{R})$ given by

$$(Af)(x) = \sum_i p_i f(xg_i).$$

This operator can be interpreted as follows: we have a Markov chain with states being points of G and the transition probability from x to xg_i equal to p_i, then $(Af)(x)$ is the expected value of f after one transition starting from x. It is clear that A is a left-invariant bounded operator (of norm 1). Moreover, A acts by the identity on the line $L \subset C(G, \mathbb{R})$ of constant functions.

For $f \in C(G, \mathbb{R})$ denote by $\nu(f)$ the distance from f to L, i.e.,

$$\nu(f) = \tfrac{1}{2}(\max f - \min f).$$

Then $\nu(Af) < \nu(f)$ unless $f \in L$. Indeed, if f is not constant and $x \in G$, pick j such that $f(xg_j) < \max f$ (exists since the sequence xg_i is dense in G), then

$$(Af)(x) = \sum_i p_i f(xg_i) \le (1 - p_j) \max f + p_j f(xg_j) < \max f.$$

So $\max(Af) < \max f$. Similarly, $\min(Af) > \min f$.

Now fix $f \in C(G, \mathbb{R})$ and consider the sequence $f_n := A^n f$, $n \ge 0$. This means that we let our Markov chain run for n steps. We know that for finite Markov chains there is an asymptotic distribution, and we'll show that this is also the case in the situation at hand, giving rise to a construction of the invariant integral.

Obviously, the sequence f_n is uniformly bounded by $\max |f|$. Also it is **equicontinuous**: for any $\varepsilon > 0$ there exists a neighborhood $1 \in U \subset G$ such that for any $x \in G$ and $u \in U$,

$$|f_n(x) - f_n(ux)| < \varepsilon.$$

Indeed, it suffices to show that f is uniformly continuous, i.e., for any ε find U such that for all $x \in G, u \in U$ we have $|f(x) - f(ux)| < \varepsilon$; this U will then work for all f_n. But this is guaranteed by Cantor's theorem. Namely, assume the contrary, that there is no such U. Then there are two sequences $x_i, u_i \in G$, $u_i \to 1$, with $|f(x_i) - f(u_i x_i)| \ge \varepsilon$. The sequence x_i has a convergent subsequence, so we may assume without loss of generality that $x_i \to x \in G$. Then taking the limit $i \to \infty$, we get that $\varepsilon \le 0$, a contradiction.

Therefore, by the **Ascoli-Arzela theorem** the sequence f_n has a convergent subsequence. Let us remind the proof of this theorem. We construct subsequences f_n^k of f_n inductively by picking f_n^k from f_n^{k-1} so that $f_n^k(g_k)$ converges (with $f_n^0 = f_n$), which can be done by the boundedness assumption, and then set $h_m := f_m^m = f_{n(m)}$. Then $h_m(g_i)$ converges, hence Cauchy, for all i, which by equicontinuity implies that $h_m(x)$ is a Cauchy sequence in $C(G,\mathbb{R})$, hence converges to some $h \in \mathbb{C}(G,\mathbb{R})$.

We claim that $h \in L$. Indeed, we have

$$\nu(f_{n(m)}) \geq \nu(f_{n(m)+1}) = \nu(Af_{n(m)}) \geq \nu(f_{n(m+1)}),$$

so taking the limit when $m \to \infty$, we get

$$\nu(h) \geq \nu(Ah) \geq \nu(h),$$

i.e., $\nu(Ah) = \nu(h)$. The assignment $f \mapsto h$ is therefore a continuous left-invariant positive linear functional $I : C(G,\mathbb{R}) \to L = \mathbb{R}$, and $I(1) = 1$, as claimed.

Similarly, we may construct a right-invariant integral

$$I_* : C(G,\mathbb{R}) \to L = \mathbb{R}$$

with $I_*(1) = 1$, and by construction for any left invariant integral J we have $J(f) = J(I_*(f))$. Thus for every left invariant integral J with $J(1) = 1$ we have $J(f) = I_*(f)$; in particular $I(f) = I_*(f)$. This shows that I is unique, invariant on both sides and independent on the choice of g_i, p_i, and hence that $A^n f \to I(f)$ as $n \to \infty$. □

Example 37.3. A basic example of a compact topological group with countable base which is, in general, not a Lie group, is a **profinite group**. Namely, let $G_1, G_2, ...$ be finite groups and $\phi_i : G_{i+1} \to G_i$ be surjective homomorphisms. Then the **inverse limit** $G := \varprojlim G_n$ is the group consisting of sequences $g_1 \in G_1, g_2 \in G_2, ...$ where $\phi_i(g_{i+1}) = g_i$. This group G has projections $p_n : G \to G_n$ and a natural topology, for which a base of neighborhoods of 1 consists of $\mathrm{Ker}(p_n)$. (This topology can be defined by a bi-invariant mertic: $d(\mathbf{a},\mathbf{b}) = C^{n(\mathbf{a},\mathbf{b})}$, where $n(\mathbf{a},\mathbf{b})$ is the first position at which $\mathbf{a},\mathbf{b}$ differ, and $0 < C < 1$). A sequence $\mathbf{a}^n$ converges to $\mathbf{a}$ in this topology if for each k, a_k^n eventually stabilizes to a_k. It is easy to show that G is compact.

Profinite groups are ubiquitous in mathematics. For example, the p-**adic integers** $\mathbb{Z}_p$ for a prime p form a profinite group, namely the inverse limit of $\mathbb{Z}/p^n\mathbb{Z}$; in fact, it is a profinite ring. The multiplicative group of this ring $\mathbb{Z}_p^\times$ is also a profinite group. One may also consider non-abelian profinite groups $GL_n(\mathbb{Z}_p)$, $O_n(\mathbb{Z}_p)$, $Sp_{2n}(\mathbb{Z}_p)$, etc. Finally, absolute Galois groups, such as $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, are (very complicated) profinite groups.

Note that infinite profinite groups are uncountable and **totally disconnected**, i.e., $G^\circ = 1$.

More generally, the inverse limit makes sense if G_i are compact Lie groups. In this case G is equipped with the product topology, so also compact (by Tychonoff's theorem). For example, consider the sequence of Lie groups $G_n = \mathbb{R}/\mathbb{Z}$ and maps $\phi_i : G_{i+1} \to G_i$ given by $\phi_i(x) = px$ for a prime p. We can realize G_n as $\mathbb{R}/p^n\mathbb{Z}$, then $\phi_i(y) = y \bmod p^i$. Let $G := \varprojlim G_n$. We have projections $p_n : G \to G_n$, and an element $a \in \mathrm{Ker}(p_1)$ is a sequence of elements $a_n \in \mathbb{Z}/p^n$ such that a_{n+1} projects to a_n, i.e., $\mathrm{Ker}(p_1) = \mathbb{Z}_p$. Thus we have a short exact sequence of compact topological groups

$$0 \to \mathbb{Z}_p \to G \to \mathbb{R}/\mathbb{Z} \to 0$$

(non-split, as G is connected). In fact, we can obtain G as a quotient $(\mathbb{R} \times \mathbb{Z}_p)/\mathbb{Z}$ where $\mathbb{Z}$ is embedded diagonally.

Corollary 37.4. *Finite dimensional (continuous) representations of a compact topological group G with a countable base are unitary and completely reducible.*

The proof is the same as for Lie groups, once we have the integration theory, which we now do.

37.2. **The Peter-Weyl theorem for compact topological groups.**

Theorem 37.5. *(i) (Peter-Weyl theorem) Let G be a compact topological group with a countable base. Then the set* $\mathrm{Irrep}G$ *is countable, and*

$$L^2(G) = \widehat{\bigoplus}_{V \in \mathrm{Irrep}(G)} V \otimes V^*$$

as a $G \times G$-module.

(ii) The subspace $L^2_{\mathrm{alg}}(G) = \oplus_{V \in \mathrm{Irrep}(G)} V \otimes V^*$ is dense in $C(G)$ in the supremum norm.

Again, the proof is analogous to Lie groups, using a delta-like sequence of continuous hat functions. Namely, we may take

$$h_N(x) = c_N \max\left(\tfrac{1}{N} - d(x, 1), 0\right),$$

where d is some metric defining the topology of G, and $c_N > 0$ are normalization constants such that $\int_G h_N(x)dx = 1$.

Remark 37.6. If G is profinite then finite dimensional representations of G are just representations of G_n for various n:

$$\mathrm{Irrep}G = \cup_{n \geq 1} \mathrm{Irrep}G_n$$

(nested union).

Corollary 37.7. *Any compact topological group with countable base is an inverse limit of a sequence of compact Lie groups* $... \to G_1 \to G_0$*, where the maps* $G_{i+1} \to G_i$ *are surjective.*

Proof. Let $V_1, V_2, ...$ be the irreducible representations of G. Let $K_m = \mathrm{Ker}(\rho_{V_1} \oplus ... \oplus \rho_{V_m}) \subset G$, a closed normal subgroup. Then $G/K_m \subset U(V_1 \oplus ... \oplus V_n)$ is a compact Lie group, and $\cap_m K_m = 1$, so G is the inverse limit of G/K_m. □

Exercise 37.8. (i) Let $\mathbb{Q}_p = \mathbb{Z}_p[1/p]$ be the field of p-adic numbers, i.e., the field of fractions of $\mathbb{Z}_p$. Construct the Haar measure $|dx|$ on the additive group of $\mathbb{Q}_p$ in which the volume of $\mathbb{Z}_p$ is 1 using the Haar measure on $\mathbb{Z}_p$.

(ii) Show that $\mathbb{Q} \subset \mathbb{Q}_p$ and $\mathbb{Q}_p = \mathbb{Q} + \mathbb{Z}_p$, and use this to define an embedding $\mathbb{Q}_p/\mathbb{Z}_p \to \mathbb{Q}/\mathbb{Z}$. Show that $\mathbb{Q}/\mathbb{Z} = \oplus_{p \text{ prime}} \mathbb{Q}_p/\mathbb{Z}_p$.

(iii) Define the additive character $\psi : \mathbb{Q}_p \to U(1) \subset \mathbb{C}^\times$ by $\psi(x) := \exp(2\pi i \overline{x})$, where $\overline{x}$ is the image of x in $\mathbb{Q}/\mathbb{Z}$. Use ψ to label the characters (=irreducible representations) of $\mathbb{Z}_p$ by $\mathbb{Q}_p/\mathbb{Z}_p$.

(iv) Let $|x|$ be the p-adic norm of $x \in \mathbb{Q}_p$ ($|x| = p^{-n}$ if $x \in p^n\mathbb{Z}_p$ but $x \notin p^{n+1}\mathbb{Z}_p$, and $|0| = 0$). For which $s \in \mathbb{C}$ is the function $|x|^s$ in $L^2(\mathbb{Z}_p)$?

(v) The Peter-Weyl theorem in particular implies that any L^2 function f on a compact abelian group G with a countable base can be expanded in a Fourier series

$$f(x) = \sum_j c_j \psi_j(x),$$

where ψ_j are the characters of G. Write the Fourier expansion of $|x|^s$ when it is in $L^2(\mathbb{Z}_p)$.

(vi) Show that $\frac{|dx|}{|x|}$ is a Haar measure on the multiplicative group $\mathbb{Q}_p^\times = GL_1(\mathbb{Q}_p)$. More generally, show that $|dX| := \frac{\prod_{1 \le i,j \le n} |dx_{ij}|}{|\det(X)|^n}$ is a Haar measure on $GL_n(\mathbb{Q}_p)$ (where $X = (x_{ij})$).

(vii) Classify characters of $\mathbb{Z}_p^\times$.

(viii) Let S be the the space of locally constant functions on $\mathbb{Q}_p$ with compact support (i.e., linear combinations of indicator functions of sets of the form $a + p^n\mathbb{Z}_p$, $a \in \mathbb{Q}_p$). Show that the Fourier transform operator

$$\mathcal{F}(f) = \int_{\mathbb{Q}_p} \psi(xy) f(y) |dy|$$

maps S to itself, and $(\mathcal{F}^2 f)(x) = f(-x)$. Show that $\mathcal{F}$ preserves the integration pairing on S, $(f, g) = \int_{\mathbb{Q}_p} f(x)\overline{g(x)}|dx|$, and therefore extends to a unitary operator $L^2(\mathbb{Q}_p) \to L^2(\mathbb{Q}_p)$.

18.755 Lie Groups and Lie Algebras II
Spring 2024