Pontryagin Duality

Mitchell Riley

June 20, 2014

The Pontryagin duality theorem unifies a number of different aspects of Fourier analysis. For example, complex valued periodic functions on the real line have Fourier series, and the original function can be recovered from its series. This fact follows from the duality between the circle group $\mathbb{T}$ and the integers $\mathbb{Z}$.

The duailty theorem is analogous to the duality theorem for vector spaces; any vector space V is canonically isomorphic to its double dual $(V^*)^*$. Pontryagin duality states that any *locally compact abelian group* is canonically isomorphic to its double dual in a similar way.

This report first gives an overview of topological groups, then discusses the finite dimensional representations of $\mathbb{R}$ and $\mathbb{T}$. Then follows the precise statement of the Pontryagin duality theorem and an application of the theorem to abstract algebra in the proof of Kummer's theorem.

1 Topological Groups

First, some basic definitions and properties of topological groups.

Definition 1.1. A *topological group* is a group G together with a topology on G such that the group operation and inversion are continuous. In other words,

a) the map $p : G \times G \to G$ given by $p(g, h) = gh$ is continuous, where $G \times G$ has the product topology; and,

b) the map $inv : G \to G$ given by $inv(g) = g^{-1}$ is continuous.

Example 1.2. The following are all simple examples of topological groups:

1. Let G be any group with the discrete topology.
2. Let G be any group with the indiscrete topology.

3. $(\mathbb{R}, +)$ or $(\mathbb{R}^\times, \cdot)$ with the usual topology.
4. $(\mathbb{C}, +)$ or $(\mathbb{C}^\times, \cdot)$ with the usual topology.
5. $\mathbb{T} = \{z \in \mathbb{C} : |z| = 1\}$ with the subspace topology.
6. Every subgroup of a topological group, endowed with the subspace topology.

Given a normal subgroup of a topological group $N \lhd G$, we can put a topology on the quotient group G/N so G/N becomes a topological group.

First, recall that for any topological space X and equivalence relation $\sim$, there is a natural topology on the space of equivalence classes $X/\sim$. Let $q : X \to X/\sim$ be the quotient map. An open set $U \subseteq X/\sim$ is open if and only if $q^{-1}(U)$ is open in X.

Now, given a topological group G with subgroup H, we write G/H for $G/\sim$ where $\sim$ is the left coset equivalence relation.

Our theorem follows from the following two propositions.

Proposition 1.3. Let G be a topological group and H a subgroup. Then the quotient map $q : G \to G/H$ is open.

Proof. Let U be open in G. Then $q^{-1}(q(U)) = U \cdot H = \bigcup_{h \in H} Uh$. This is open as it is the union of open sets. By the definition of the quotient topology, $q(U)$ is also open. □

Proposition 1.4. Suppose $p_i : X_i \to Y_i$ is a collection of quotient maps which are open. Let $q : \prod_i X_i \to \prod_i Y_i$ be the projection map $x_i \mapsto (p_i(x_i))$. Then q is a quotient map.

Proof. $(\leftarrow)$ If $V \subseteq \prod_i Y_i$ is open, $q^{-1}(V)$ is open as q is continuous.

$(\to)$ Suppose $q^{-1}(V)$ is open; we have $q(q^{-1}(V)) = V$ since q is surjective. Since each p_i is open, so is q. Therefore, V is open. □

Theorem 1.5. Let G be a topological group and N a normal subgroup. Then G/N is a topological group.

Proof. We need to show that the product and inverse operations are continuous. Let $\widetilde{p} : G/N \times G/N \to G/N$ be the map given by $(gN, hN) \mapsto ghN$.

Applying the above proposition to $q : G \to G/N$, we have that $(q \times q) : G \times G \to G/N \times G/N$ is a quotient map. Showing $\widetilde{p}$ is continuous is equivalent to showing that $\widetilde{p}(q \times q)$ is continuous. But this last map is equal to composing $p : G \times G \to G$ with the quotient map q, both of which are continuous.

Finally, the inverse operation is continuous as it is the composition of the continuous maps $inv : G \to G$ and $q : G \to G/N$. □

Given two topological groups G and K, the appropriate type of map between them is one that respects both the group and topological structures, i.e., *continuous homomorphisms.* Two groups are *topologically isomorphic* if there exists a map $\pi : G \to K$ that is both a group isomorphism and a topological homeomorphism.

There exists an analogue of the first isomorphism theorem for topological groups.

Theorem 1.6. Let $\pi : G \to K$ be a continuous, onto homomorphism with kernel $H = \ker(\pi)$. If π is an open map, then $\widetilde{\pi} : G/H \to K$ is a topological isomorphism.

Proof. From the ordinary first isomorphism theorem for groups, we know that $\widetilde{\pi}$ is an isomorphism. All that remains is to show that $\widetilde{\pi}$ and $\widetilde{\pi}^{-1}$ are continuous.

Let q be the quotient map $q : G \to G/H$. First we have $\widetilde{\pi}q = \pi$, because $\widetilde{\pi}(q(g)) = \widetilde{\pi}(gH) = \pi(g)$. Because π is continuous and q is a quotient map, it follows that $\widetilde{\pi}$ is continuous.

Similarly, $\widetilde{\pi}^{-1}\pi = q$. Because π is continuous, open and onto, it is a quotient map. It follows that $\widetilde{\pi}^{-1}$ is continuous. □

Example 1.7. Consider the map $\pi : (\mathbb{R}, +) \to \mathbb{T}$ given by $\pi(t) = e^{2\pi it}$. This is a continuous, onto homomorphism with kernel $\mathbb{Z}$. π is also open, as it takes open intervals to open arcs. Therefore, $\widetilde{\pi} : \mathbb{R}/\mathbb{Z} \to \mathbb{T}$ is a topological isomorphism.

2 Representations of Topological Groups

To discuss representation theory of topological groups, we need a sensible topology on $GL(n, \mathbb{R})$ and $GL(n, \mathbb{C})$. Let $GL(n, \mathbb{R})$ be endowed with the Euclidean topology by identifying each matrix with a vector in $\mathbb{R}^{n^2}$. Similarly, give $GL(n, \mathbb{C})$ a topology by identifying matrices with vectors in $\mathbb{R}^{2n^2}$.

Theorem 2.1. $GL(n, \mathbb{R})$ and $GL(n, \mathbb{C})$ are topological groups.

Proof. Let $M(n, \mathbb{R})$ denote the set of all $n \times n$ matrices with entries in $\mathbb{R}$. Then, the map $M(n, \mathbb{R}) \times M(n, \mathbb{R}) \to M(n, \mathbb{R})$ given by matrix multiplication is continuous. To see this, recall that a map to $\mathbb{R}^{n^2}$ is continuous if and only if each component map is continuous. Given $A, B \in M(n, \mathbb{R})$, each matrix entry of AB is a polynomial and therefore continuous function of the matrix entries of A and B. Restricting to $GL(n, \mathbb{R})$, we have that multiplication in $GL(n, \mathbb{R})$ is continuous.

The determinant map $\det : GL(n, \mathbb{R}) \to \mathbb{R}$ is continuous, as it is a polynomial function of the entries of a matrix. Cramer's rule gives an expression for the entries of the inverse of a matrix A in terms of $\det A$ and $\det A'$, where A' is a matrix obtained by deleting a row and column from A. For each entry this expression is continuous, so the inverse map is continuous.

The complex case is identical. □

If we are given any real, finite dimensional vector space V, by choosing a basis we have a group isomorphism $\pi : GL(V) \to GL(n, \mathbb{R})$. Endowing $GL(V)$ with the topology of $GL(n, \mathbb{R})$ makes $GL(V)$ into a topological group.

If we choose a different basis for V, we have a different map $\rho : GL(V) \to GL(n, \mathbb{R})$, but the topology we obtain for $GL(V)$ will be the same. This is because π and ρ differ only by conjugation by an element of $GL(n, \mathbb{R})$, and this operation is a topological isomorphism.

Definition 2.2. Let G be a topological group and V a finite dimensional vector space. A *continuous representation of* G is a continuous homomorphism $\pi : G \to GL(V)$.

If we choose a basis for V, then a map $\pi : G \to GL(V)$ is continuous if and only if in the matrix form $\pi(g) = (f_{i,j}(g))$ each of the $f_{i,j}$ is continuous.

The character of a representation $\pi : G \to GL(V)$ is defined in the same way as for finite groups. The character of π is the continuous function $\chi_\pi(g) = \mathrm{Tr}(\pi(g))$.

2.1 One Dimensional Representations of $\mathbb{R}$ and $\mathbb{T}$

Now let us look at the simplest examples of continuous representations, the one dimensional representations of $\mathbb{R}$ and $\mathbb{T}$. Here I will skip some of the proofs, as they are not very illuminating!

Lemma 2.3. Any continuous homomorphism $\pi : (\mathbb{R}, +) \to (\mathbb{R}^\times, \cdot)$ is of the form $\pi(t) = e^{at}$ for some $a \in \mathbb{R}$

Proof. There is a unique number a such that $\pi(1) = e^a$. Then $\pi(n) = e^{an}$. Let $g(x) = \pi(x)e^{-ax}$, then $g(0) = 1$, $g(x + y) = g(x)g(y)$, $g(n) = 1$. But $g(n/m)^m = g(n) = 1$ for all m, n. Therefore $g(q) = 1$ for all rationals and by continuity for all of $\mathbb{R}$.

Therefore $\pi(t) = e^{at}$. □

Lemma 2.4. Any continuous homomorphism $\rho : (\mathbb{R}, +) \to \mathbb{T}$ is of the form $\rho(t) = e^{ibt}$ for some $b \in \mathbb{R}$.

Proof. Omitted. □

Theorem 2.5. Let $\pi : (\mathbb{R}, +) \to \mathbb{C}^\times$ be a one dimensional representation. Then $\pi(t) = e^{\lambda t}$ for some $\lambda \in \mathbb{C}$.

Proof. Let $\pi_1 : (\mathbb{R}, +) \to \mathbb{R}^\times$ be defined by $\pi_1(t) = |\pi(t)|$. Then π_1 is a continuous homomorphism and therefore has the form $\pi_1(t) = e^{at}$ for some $a \in \mathbb{R}$.

Now let $\rho(t) = \pi(t)e^{-at}$. This is a continuous homomorphism from $(\mathbb{R}, +)$ to $\mathbb{T}$ and therefore has the form $\rho(t) = e^{ibt}$.

Hence $\pi(t) = \pi_1(t)\rho(t) = e^{(a+ib)t}$. □

Corollary 2.6. Let $\pi : (\mathbb{R}, +) \to \mathbb{C}^\times$ be a bounded continuous homomorphism. Then $\pi(\mathbb{R}) \subseteq \mathbb{T}$ and π is of the form $\pi(t) = e^{ibt}$

Proof. For π to be bounded, we must have $a = 0$ in the above theorem. □

Theorem 2.7. Let $\gamma : \mathbb{T} \to \mathbb{C}^\times$ be a one dimensional representation. Then $\gamma(z) = z^n$ for some $n \in \mathbb{Z}$.

Proof. Let $\rho(t) = \gamma(e^{2\pi it})$, then ρ is a one dimensional representation of $(\mathbb{R}, +)$. Because $\mathbb{T}$ is compact, $\gamma(\mathbb{T})$ is compact in $\mathbb{C}$ and hence bounded. Therefore $\rho(t) = e^{ibt}$ for some $b \in \mathbb{R}$. But $\gamma(1) = \rho(1) = e^{ib} = 1$, so $b = 2\pi n$ for some integer n.

Now, if $z \in \mathbb{T}$, i.e., $z = e^{2\pi i\theta}$, $\gamma(z) = \rho(\theta) = e^{2\pi in\theta} = z^n$. □

2.2 Finite Dimensional Representations of $\mathbb{R}$ and $\mathbb{T}$

Recall that, given a matrix $A \in M(n, \mathbb{C})$, the matrix exponential e^A is given by

$$e^A = I + A + \frac{A^2}{2!} + \cdots = \sum_{n=0}^{\infty} \frac{A^n}{n!}$$

Proposition 2.8. Let $A \in M(n, \mathbb{C})$, then $\pi(t) = e^{At}$ is a representation $\pi : (\mathbb{R}, +) \to GL(n, \mathbb{C})$.

Proof. We can show π is a homomorphism as follows.

$$\begin{aligned}\pi(t)\pi(s) = e^{tA}e^{sA} &= \sum_{n=0}^{\infty} \sum_{k+j=n} \frac{(tA)^k}{k!} \frac{(sA)^j}{j!} \\ &= \sum_{n=0}^{\infty} \left(\sum_{k+j=n} \frac{t^k s^j}{k! j!} \right) A^n \\ &= \sum_{n=0}^{\infty} \left(\sum_{k=0}^{n} \frac{t^k s^{n-k}}{k!(n-k)!} \right) A^n \\ &= \sum_{n=0}^{\infty} \left(\sum_{k=0}^{n} \frac{n!}{k!(n-k)!} t^k s^{n-k} \right) \frac{A^n}{n!} \\ &= \sum_{n=0}^{\infty} \frac{(t+s)^n A^n}{n!} \\ &= e^{(t+s)A} = \pi(t+s)\end{aligned}$$

Also, because $\pi(t)\pi(-t) = I$, we have that $\pi(t)$ is invertible for all t, so the range of π lies inside $GL(n, \mathbb{C})$. □

Stone's theorem, specialised to complex matrices, states that these representations are all the representations of $\mathbb{R}$.

Theorem 2.9 (Stone)**.** Let $\pi : (\mathbb{R}, +) \to GL(n, \mathbb{C})$ be a representation. Then $A = \lim_{t\to 0} \frac{\pi(t)-I}{t}$ exists, and $\pi(t) = e^{tA}$.

Proof. Omitted. [1] □

The finite dimensional representations of $\mathbb{T}$ are also easy to describe.

Proposition 2.10. Let $A \in M(n, \mathbb{C})$. Then $\{e^{tA} : t \in \mathbb{C}\}$ is bounded if and only if A is similar to a diagonal matrix with purely imaginary entries.

Proof. Consider the Jordan form of A. If any of the blocks in this form are larger than 1×1, then e^{tA} will contain an entry of the form $te^{t\lambda}$, which is unbounded for all λ.

Hence, every Jordan block has size 1×1, and A is similar to a diagonal matrix. The exponential of a diagonal matrix $A = \operatorname{diag}(\lambda_1, \ldots, \lambda_n)$ is $e^A = \operatorname{diag}(e^{\lambda_1}, \ldots, e^{\lambda_n})$, so to remain bounded, the λ_i must all be purely imaginary. □

Theorem 2.11. Let $\pi : \mathbb{T} \to GL(n, \mathbb{C})$ be a representation. Then π is of the form $\pi(z) = S^{-1} \operatorname{diag}(z^{k_1}, \ldots, z^{k_n})S$ for an invertible matrix S and integers k_i.

Proof. Consider the representation $\rho : \mathbb{R} \to GL(n, \mathbb{C})$ defined by $\rho(t) = \pi(e^{it})$. Since $\mathbb{T}$ is compact, the image of π is bounded hence ρ is also bounded.

Therefore, by the above, $p(t) = S^{-1} \operatorname{diag}(e^{ib_1 t}, \dots, e^{ib_n t})S$. As in the one dimensional case, we have $b_i = 2\pi k_i$ for some integer k_i. If we have $z \in \mathbb{T}$, so $z = e^{i\theta}$, then $\pi(z) = \rho(\theta) = S^{-1} \operatorname{diag}(e^{2\pi i k_1 t}, \dots, e^{2\pi i k_n t})S = S^{-1} \operatorname{diag}(z^{k_1}, \dots, z^{k_n})S$. □

3 Pontryagin Duality

A Hausdorff topological space X is called *locally compact* if for every $x \in X$, there is a neighbourhood U of x such that the closure of U is compact.

Example 3.1.

- $\mathbb{R}$ is not compact but it is locally compact.
- $\mathbb{T}$ is compact and therefore locally compact.
- Any discrete group is locally compact.

Given any abelian locally compact group, we define the dual group as follows.

Definition 3.2. Let G be a locally compact abelian group. A *character* of G is a continuous homomorphism $\chi : G \to \mathbb{T}$. The *dual group* of G, written $\widehat{G}$ is the set of characters of G, with group operation pointwise multiplication.

In other words we define $\widehat{G} = \operatorname{Hom}(G, \mathbb{T})$.

We give $\widehat{G}$ the 'compact-open' topology as follows. Let $K \subset G$ be a compact subset, and $U \subset \mathbb{T}$ an open subset. Let $V(K, U)$ denote the set of all characters $f \in \widehat{G}$, such that $f(K) \subset U$. Then the collection of all $V(K, U)$ forms a subbase for the topology on $\widehat{G}$.

Example 3.3.

- The dual of $\mathbb{Z}$ is $\mathbb{T}$, and the dual of $\mathbb{T}$ is $\mathbb{Z}$.
- Every finite abelian group is isomorphic its own dual.
- $\mathbb{R}^n$ is isomorphic its own dual for every n.

Theorem 3.4 (Pontryagin)**.** For every locally compact abelian group G, G and its double dual $\widehat{\widehat{G}}$ are topologically isomorphic, and this isomorphism is canonical.

The canonical isomorphism has the same form as the isomorphism between a vector space and its double dual. To each $x \in G$ we associate the map $\chi \mapsto \chi(x)$, an element of $\widehat{\widehat{G}}$. This map is clearly a homomorphism; the content of the theorem is that this map is surjective.

In the language of category theory, $G \mapsto \widehat{G}$ is a functor **LCA** $\to$ **LCA**, writing **LCA** for the category of locally compact abelian groups. The duality theorem states that this functor is a contravariant equivalence of categories.

In fact, we can say more:

Theorem 3.5 (Pontryagin)**.** The equivalence $G \mapsto \widehat{G}$ restricts to equivalences:

$$\begin{aligned} \{\textit{compact groups}\} &\longleftrightarrow \{\textit{discrete groups}\} \\ \{\textit{finite groups}\} &\longleftrightarrow \{\textit{finite groups}\} \\ \{\textit{finite cyclic groups}\} &\longleftrightarrow \{\textit{finite cyclic groups}\} \end{aligned}$$

Further, if G and H are dual there is a bijection:

$$\begin{array}{rcl} \{\textit{closed subgroups of } G\} & \longleftrightarrow & \{\textit{closed subgroups of } H\} \\ U & \longmapsto & U^{\perp} = \{h \in H : \forall g \in U, h(g) = 1\} \\ V^{\perp} = \{g \in G : \forall h \in V, h(g) = 1\} & \longleftarrow\!\shortmid & V \end{array}$$

4 Kummer Theory

Kummer theory provides a characterisation for certain kinds of field extensions. If a field K contains a primitive nth root of unity, the theorem states that cyclic extensions of K can understood in terms of extracting roots.

The central theorem of Kummer theory can be proved using Pontryagin duality. [4]

Definition 4.1. A group G is of *exponent* m if $g^m = e$ for every $g \in G$. A field extension L/K is of *exponent* m if it is Galois, and the Galois group is of exponent m.

Definition 4.2. A Kummer extension is an abelian extension of some exponent m.

For example, let $a \in K$, and m an integer not divisible by the characteristic of K. Then the extension $K(\sqrt[m]{a})/K$ is a Kummer extension of exponent m.

Lemma 4.3. Any subextension of a Kummer extension is a Kummer extension.

This follows from the fact that the Galois group of a subextension must be a quotient of the total Galois group. The quotient of a group of exponent m is another group of exponent m.

Lemma 4.4. Let $\{L_i\}$ be a family of Kummer subextensions of any field extension. Then the composite L is a Kummer extension.

It follows from the above two lemmas that:

Proposition 4.5. Let $\overline{K}$ denote the algebraic closure of K. There is a unique Kummer subextension K_m/K of $\overline{K}/K$, which contains all other Kummer subextensions of $\overline{K}/K$. All subextensions of K_m/K are Kummer extensions.

We can now state the central theorem. Let $K^\times$ denote the multiplicative group of K, and $K^{\times m}$ the subgroup of all mth powers of elements of $K^\times$.

Theorem 4.6 (Kummer)**.** Let K be a field and m a positive integer which is not divisible by the characteristic of K. Assume that K contains a primitive mth root of unity. Then there is a bijection:

$$\{\textit{subgroups of } K^\times/K^{\times m}\} \quad \longleftrightarrow \quad \{\textit{abelian extensions of } K \textit{ of exponent } m\}$$

Proof. (Sketch) Let K_m be the maximal Kummer extension from earlier, and set $G = Gal(K_m/K)$ and $H = K^\times/K^{\times m}$. Fix an embedding of the mth roots of unity into $\mathbb{T}$, and define a bilinear map ψ as follows:

$$\begin{aligned} \psi : G \times H &\to \mathbb{T} \\ (g, a) &\mapsto \frac{g(\alpha)}{\alpha} \end{aligned}$$

where $\alpha^m = a$.

To get a feel for this map, let $a \in K^\times$ be any element. An mth root of a, α, is an element of K_m as $K(\sqrt[m]{a})$ is a Kummer extension. Given $g \in G$, $g(\alpha)$ is another mth root of a, so must be of the form $\omega\alpha$ for some root of unity ω. We therefore have that $\psi(g, a) = \omega\alpha/\alpha = \omega \in \mathbb{T}$.

ψ induces a group isomorphism: (proof omitted)

$$\begin{aligned} H &\to \widehat{G} \\ a &\mapsto \psi(-, a) \end{aligned}$$

Galois groups are always compact. It follows from Pontryagin duality that $\widehat{G}$ is discrete, so we give H the discrete topology to turn the above map into a topological isomorphism.

Hence, we get the following chain of bijections:

$$\begin{aligned} & \{\textit{Kummer subextensions of } \overline{K}\} \\ = \quad & \{\textit{subextensions of } K_m\} \\ \longleftrightarrow \quad & \{\textit{closed subgroups of } \mathrm{Gal}(K_m/K)\} \\ \longleftrightarrow \quad & \{\textit{subgroups of } K^\times/K^{\times m}\} \end{aligned}$$

where the first bijection follows from Galois theory and the second bijection from Pontryagin duality. □

References

[1] Sven Möller. “Stone’s Theorem and Applications”. In: (2010). URL: `http://www3.mathematik.tu-darmstadt.de/fileadmin/home/users/340/bachelor_mathe.pdf`.

[2] nLab. *Pontrjagin dual.* 2013. URL: `http://ncatlab.org/nlab/show/Pontrjagin+dual`.

[3] Vern Paulsen. “An Introduction to the Theory of Topological Groups and Their Representations”. In: (2011). URL: `http://math.uh.edu/~vern/grouprepn.pdf`.

[4] Marco Streng. *Pontryagin Duality and Kummer Theory.* 2005. URL: `http://pub.math.leidenuniv.nl/~strengtc/kummer.ps`.