Self-duality of local fields

Bill Casselman
University of British Columbia
cass@math.ubc.ca

A unitary character of a locally compact Abelian group G is a continuous homomorphism from G to the group $\mathbb{S}$ of complex numbers of unit norm. The unitary dual $\widehat{G}$ of G is the group of all unitary characters, itself an Abelian topological group with group operation $[\varphi \cdot \psi](x) = \varphi(x)\psi(x)$. It has as basis of neighbourhoods of the identity the sets

$$W(\Omega, U) = \{\chi \,|\, \chi(\Omega) \subseteq U\}$$

for compact sets Ω in G and U open in $\mathbb{S}$. With this topology it becomes a locally compact group. Every element g of G determines the character of $\widehat{G}$ taking

$$\psi \longmapsto \psi(g)\,,$$

and we get in this way a canonical map from G to its double dual $\widehat{\widehat{G}}$. There is a general theory of duality due to Pontrjagin which asserts that this is an isomorphism. One standard reference for this is [Weil:1965].

Now suppose F to be the additive group of a local field and ψ a non-trivial unitary character of F. For every x in F define the unitary character

$$\psi_x\colon y \mapsto \psi(xy)\ .$$

The map taking x to ψ_x is a continuous homomorphism from F to its unitary dual. In this elementary note I shall prove the well known result that it is an isomorphism. This implies Pontrjagin's theorem in this case, and more.

Contents

1. A simple duality

I recall that the p-torsion in any Abelian group G is the subgroup of x in G such that $p^n x = 0$ for some $n \ge 0$. Let

$$\begin{aligned} \mu &= \mathbb{Q}/\mathbb{Z} \\ \mu(p^n) &= \{x \in \mu \,|\, p^n x = 0\} \\ \mu^{[p]} &= \textstyle\bigcup_n \mu(p^n)\,, \end{aligned}$$

Thus $\mu^{[p]}$ is the p-torsion in μ, equal to the union of the $(1/p^n)\mathbb{Z}$ modulo $\mathbb{Z}$. It may also be identified with $\mathbb{Q}/\mathbb{Z}_{(p)}$, or equivalently with $\mathbb{Q}_p/\mathbb{Z}_p$. Here $\mathbb{Z}_{(p)}$ is the **local ring** of all fractions $(m/n)p^k$ with $k \ge 0$, m and n relatively prime to p. The group $\mu^{[p]}$ may be considered a topological group, with the discrete topology.

If x lies in the ideal (p^n) and $p^n y$ lies in $\mathbb{Z}$, then xy lies in $\mathbb{Z}$. Therefore the map

$$(x, y) \longmapsto e^{2\pi i xy}$$

defines a pairing of $\mathbb{Z}/p^n$ with $\mu(p^n)$. In fact, it induces an isomorphism of .

Every z in $\mathbb{Z}_p$ determines a unique image z_n in each $\mathbb{Z}/p^n$, with

$$z_{n+1} \equiv z_n \pmod{p^n}.$$

Conversely, every sequence (z_n) satisfying this condition determines a unique z in $\mathbb{Z}_p$. In other words, $\mathbb{Z}_p$ is the **projective limit** of the finite rings $\mathbb{Z}/p^n$.

The isomorphism of $\mathbb{Z}/p^n$ with the dual of $\mu(p^n)$ therefore defines a map from $\mathbb{Z}_p$ to the dual of $\mu^{[p]}$.

1.1. Proposition. *This map from $\mathbb{Z}_p$ to the dual of $\mathbb{Q}_p/\mathbb{Z}_p$ is an isomorphism.*

More succinctly, to z in $\mathbb{Z}_p$ corresponds the character of $\mathbb{Q}_p/\mathbb{Z}_p$ taking

$$x \longmapsto e^{2\pi i x z}.$$

The torsion group $\mu^{[p]}$ has the discrete topology, and $\mathbb{Z}_p$ the projective limit topology, which makes it compact. In general, the dual of a discrete group is compact, and vice-versa. For example, the dual of $\mathbb{Z}$ is $\mathbb{S}$ itself.

2. p-adic fields

First let $F = \mathbb{Q}_p$. I start off by defining on F a character whose kernel is precisely the ring of p-adic integers $\mathbb{Z}_p$.

Every x in $\mathbb{Q}_p$ may be written as

$$x = x_{-n}p^{-n} + x_{-(n-1)}p^{-(n-1)} + \cdots x_0 + x_1 p + \cdots$$

with all x_i in $\mathbb{Z}$. Its **polar part** with respect to this expression is is the finite sum

$$\overline{x} = x_{-n}p^{-n} + x_{-(n-1)}p^{-(n-1)} + \cdots + x_{-1}p^{-1}.$$

The expression for x, however, is certainly not unique. But all possible choices are equivalent:

2.1. Lemma. *Any two polar parts for x in $\mathbb{Q}_p$ differ by an integer.*

As a consequence, the polar part gives us an embedding of $\mathbb{Q}_p/\mathbb{Z}_p$ into $\mathbb{Q}/\mathbb{Z}$, which identifies it with $\mu^{[p]}$.

We may now define an additive character Ψ of $\mathbb{Q}_p$, taking x to $e^{2\pi i\overline{x}}$. Its kernel is $\mathbb{Z}_p$.

I now claim that every character ψ of $\mathbb{Q}_p$ is of the form $x \mapsto \Psi_x(y) = \Psi(xy)$ for a unique x in $\mathbb{Q}_p$. Given ψ, its kernel must contain some (p^n), because of continuity, since $\mathbb{S}$ does not have small subgroups. Then $\psi(yp^n)$ is a character of $\mathbb{Q}_p/\mathbb{Z}_p$, which by Proposition 1.1 is of the form $\Psi(xy)$ for some x. But then $\psi(y) = \Psi(xyp^n)$.

The argument for an arbitrary finite extension of $\mathbb{Q}_p$ is similar. One gets a good character of F by combining Ψ with the trace from F to $\mathfrak{k} = \mathbb{Q}_p$. Then one has to be a bit careful, using the **relative different** defined by the condition

$$\vartheta^{-1}_{F/\mathfrak{k}} = \{x \in F \mid \mathrm{trace}(x\mathfrak{o}) \in \mathbb{Z}_p\}$$

where $\mathfrak{o}$ is the ring of integers in F. The analogue of Proposition 1.1 is that the pairing

$$(x, y) \longmapsto \Psi\big(\mathrm{trace}(xy)\big)$$

induces a well defined isomorphism of $\mathfrak{o}$ with F/ϑ^{-1}. The rest of the proof is almost identical.

3. The real and complex fields

For each x in $\mathbb{R}$, the map

$$\psi_y \colon x \longmapsto e^{2\pi i x y}$$

is a character of $\mathbb{R}$. It is to be shown that every character of $\mathbb{R}$ is of this form.

Suppose ψ to be a character of $\mathbb{R}$. Pick some small $\varepsilon > 0$ and let

$$c = \int_0^\varepsilon \psi(y)\, dy \neq 0\,.$$

Then

$$\begin{aligned} 1 &= \frac{1}{c}\int_0^\varepsilon \psi(t)\, dt \\ \psi(x) &= \psi(x)\, \frac{1}{c}\int_0^\varepsilon \psi(t)\, dy \\ &= \frac{1}{c}\int_0^\varepsilon \psi(x+t)\, dt \\ &= \frac{1}{c}\int_x^{x+\varepsilon} \psi(t)\, dt\,, \end{aligned}$$

The fundamental theorem of calculus now implies that φ is differentiable, and explicitly

$$\begin{aligned} \psi'(x) &= (1/c)(\psi(x+\varepsilon) - \psi(x)) \\ &= \psi(x)\frac{\psi(\varepsilon)-1}{c} \\ &= \psi'(0)\psi(x) \\ &= \text{(say) } 2\pi i C\, \psi(x)\,. \end{aligned}$$

This implies that ψ is smooth. Familiar results about differential equations imply that $\psi(x) = e^{2\pi i C x}$.

The case of $\mathbb{C}$ is an easy consequence.

4. References

1. André Weil, **L'intégration dans les groupes topologiques**, Hermann, 1965.