Characters and Fourier analysis on groups

Daniel EL-BAZ

November 8, 2012

The paragraphs between stars were not covered during the actual lecture (due to time constraints), but are nonetheless included for the interested reader.
Even if it is not explicitly written, $(G, +)$ is always assumed to be an abelian group in what follows.

1 Characters on a group

1.1 The discrete case

For now, we do not endow G with a topology (or, if you wish, endow it with the discrete topology, in which case every function from G to some other topological space is continuous).
Denote by S^1 the unit circle $\{z \in \mathbb{C} : |z| = 1\}$. Recall that $(S^1, \times)$ is a multiplicative abelian group which is isomorphic to the additive group $(\mathbb{T} = \mathbb{R}/\mathbb{Z}, +)$, the 1-dimensional torus.

Definition 1.1. *A* character *on G is a group homomorphism $\chi : (G, +) \to (S^1, \times)$. In formulas, $\chi : G \to S^1$ satisfies:*

$$\forall (t, u) \in G^2,\ \chi(t - u) = \chi(t)\chi(u)^{-1}.$$

The first two examples of discrete groups that come to mind are probably the integers and finite cyclic groups. Let us therefore compute the characters on these two groups to get a sense of what such objects look like.

- **The case of $G = \mathbb{Z}$**

As the additive group $(\mathbb{Z}, +)$ is generated by 1, values of a character χ on $\mathbb{Z}$

are completely determined by $\chi(1)$. Precisely, for $n \in \mathbb{Z}$, $\chi(n) = \chi(1)^n$.
Now $\chi(1) \in S^1$, so we may find an $\alpha \in \mathbb{R}$ with $\chi(1) = e^{2\pi i\alpha}$ meaning that every character χ on $\mathbb{Z}$ is of the form

$$\chi \colon n \in \mathbb{Z} \mapsto e^{2\pi i n\alpha} \in S^1.$$

Note that since the function $x \in \mathbb{R} \mapsto e^{2\pi i x} \in S^1$ is 1-periodic, α is determined up to an integer. Therefore, we have established the following bijective correspondence:

$$\{\text{characters on } \mathbb{Z}\} \longleftrightarrow \mathbb{R}/\mathbb{Z} = \mathbb{T}.$$

- **The case of $G = \mathbb{Z}/m\mathbb{Z}$**

Let $m \geq 1$ be a positive integer.
The characters on $\mathbb{Z}/m\mathbb{Z}$ are exactly the characters χ on $\mathbb{Z}$ satisfying the condition: $\forall n \in \mathbb{Z}$, $\chi(mn) = 1$. Hence we get $\chi(m) = 1$.
Since a character χ on $\mathbb{Z}$ is of the form $n \mapsto e^{2\pi i\alpha n}$ for some $\alpha \in \mathbb{R}$, the fact that $\chi(m) = 1$ reads $e^{2i\alpha m} = 1$, meaning that we may find $l \in \mathbb{Z}$ with $\alpha = \dfrac{l}{m}$.
Note that l is determined modulo m.
Therefore, we have established the following bijective correspondence:

$$\{\text{characters on } \mathbb{Z}/m\mathbb{Z}\} \longleftrightarrow \mathbb{Z}/m\mathbb{Z}\,(\longleftrightarrow \{m\text{-th roots of unity}\}).$$

*One important example of characters in number theory is given by the so-called Dirichlet characters, which are the characters on $(\mathbb{Z}/m\mathbb{Z})^\times$. A big advantage of these characters is their orthogonality relations, which yield the characteristic function $\mathbb{1}_{n \equiv l \pmod m}$ when $\gcd(l, m) = 1$.
More precisely,

$$\frac{1}{\varphi(m)} \sum_{\chi \mod m} \chi(n)\overline{\chi(l)} = \begin{cases} 1 & \text{if } n \equiv l \pmod m \\ 0 & \text{otherwise} \end{cases}.$$

(Here and in the rest of this text $z \mapsto \bar{z}$ simply denotes complex conjugation and φ is Euler's totient function.)
They were notably used by Dirichlet in the proof of his theorem on primes in arithmetic progressions.*

*Another example of a discrete group which might spring to mind is $(\mathbb{Q}, +)$. However, the description of the characters on $\mathbb{Q}$ is somewhat more involved than what we have seen so far. An excellent expository note is the one by Keith Conrad, available at `http://www.math.uconn.edu/~kconrad/`

`blurbs/gradnumthy/characterQ.pdf`.
For the reader in a rush, the result is that there is a bijective correspondence between characters on $\mathbb{Q}$ and $\mathbb{A}_{\mathbb{Q}}/\mathbb{Q}$, where $\mathbb{A}_{\mathbb{Q}}$ is the ring of (rational) adèles, which you can read about in Matt's lecture notes.*

1.2 The general case

In the case of $\mathbb{R}$, say, the purely algebraic definition of a character we gave above is not satisfactory. Considering it as a topological group, it is a good idea to impose the topological condition of continuity of the characters.

Definition 1.2. *A* character *on a topological abelian group is a continuous group homomorphism $\chi : (G, +) \to (S^1, \times)$.*

- **The case of $G = \mathbb{R}$**

Claim 1.1. *For every character χ on $\mathbb{R}$, there exists a unique $s \in \mathbb{R}$ such that $\chi \colon t \in \mathbb{R} \mapsto e^{2\pi ist} \in S^1$.*

Proof. Let χ be a character on $\mathbb{R}$. By definition, we get:

$$\forall (t,u) \in \mathbb{R}^2,\ \chi(t+u) = \chi(t)\chi(u) \qquad (\clubsuit)$$

Now since χ is continuous we may write, for an arbitrary $t_0 > 0$,

$$\chi(t)\int_0^{t_0} \chi(u)du = \int_0^{t_0} \chi(t+u)du = \int_t^{t+t_0} \chi(u)du.$$

Noting that $\chi(0) = 1$ and thanks to the continuity of χ, it is easily seen that for t_0 small enough, the integral on the left-hand side is non-zero and of the order of t_0. (To be precise and give the details: we may find $\delta > 0$ such that, if $|u|$ is less than δ, then $|\chi(u) - 1|$ is less than $\frac{1}{2}$, say.
Then write $\chi(u)$ as $1 + (\chi(u) - 1)$ and use the triangle inequality to get

$$\left|\int_0^{t_0} \chi(u)du\right| \geq t_0 - \left|\int_0^{t_0} (\chi(u) - 1)du\right| \geq \frac{1}{2}t_0 > 0.)$$

We thus get

$$\forall t \in \mathbb{R},\ \chi(t) = \frac{\int_t^{t+t_0} \chi(u)du}{\int_0^{t_0} \chi(u)du}.$$

In particular, χ is continuously differentiable on $\mathbb{R}$, which allows to differentiate (♣) with respect to u, say. We get $\forall (t,u) \in \mathbb{R}^2$, $\chi'(t+u) = \chi(t)\chi'(u)$. Let us plug in $u = 0$ to get $\forall t \in \mathbb{R}$, $\chi'(t) = \chi'(0)\chi(t)$, which readily implies that we may find $z \in \mathbb{C}$ such that $\forall t \in \mathbb{R}$, $\chi(t) = e^{zt}$.
Finally, since χ has absolute value 1, we may find a unique $s \in \mathbb{R}$ such that $z = 2\pi i s$, hence the conclusion. □

This result allows to find the characters on another group in a straightforward way, namely the (one-dimensional) torus $\mathbb{T}$.

- **The case of $G = \mathbb{T}$**

To get the characters on $\mathbb{T}$ from those on $\mathbb{R}$, we proceed as we did to get the characters on $\mathbb{Z}/m\mathbb{Z}$, $m \geq 1$ from the characters on $\mathbb{Z}$.
In general (exercise!), if H is a closed subgroup of a topological group G, the characters on the quotient G/H are given by those characters on G with $\forall h \in H$, $\chi(h) = 1$.
In our case, this yields:

Claim 1.2. *For every character χ on $\mathbb{T}$, there exists a unique integer $n \in \mathbb{Z}$ such that $\chi \colon t \in \mathbb{T} \mapsto e^{2\pi i n t} \in S^1$.*

Proof. Let χ be a character on $\mathbb{T}$. It may be identified with a character on $\mathbb{R}$ which, by Claim 1.1, is of the form $\chi(t) = e^{2\pi i s t}$ where $s \in \mathbb{R}$ is uniquely determined. For χ to be a character on $\mathbb{T}$, we need $\forall k \in \mathbb{Z}$, $e^{2\pi i s k} = 1$, which implies $e^{2\pi i s} = 1$, that is $s \in \mathbb{Z}$. □

Martin's lecture provides us with another interesting example of a (locally compact abelian) topological group, namely the p-adic numbers $\mathbb{Q}_p$. As in the case of (the locally compact abelian group) $\mathbb{R}$ above, the characters on $\mathbb{Q}_p$ are in bijective correspondence with $\mathbb{Q}_p$ itself. To see a proof of this fact, read the aforementioned note by Keith Conrad (`http://www.math.uconn.edu/~kconrad/blurbs/gradnumthy/characterQ.pdf`, Appendix A).

Similarly, yet another example of a (locally compact abelian) topological group is given by the rational adèles $\mathbb{A}_{\mathbb{Q}}$ introduced in Matt's lecture, and the characters are yet again in bijective correspondence with $\mathbb{A}_{\mathbb{Q}}$ itself.

1.3 The dual group of a topological group

Let G be a topological abelian group. If χ and $\tilde{\chi}$ are two characters on G, we get a third character by taking their product. Indeed, the map $t \mapsto \chi(t)\tilde{\chi}(t)$ from G to S^1 is a character, which we denote by $\chi \cdot \tilde{\chi}$.

In the case of $\mathbb{Z}$, taking the product of two characters corresponds to addition modulo 1, and we thus get the structure of a group on the set of characters of $\mathbb{Z}$: it is the dual group of $\mathbb{Z}$, which is isomorphic (as a group) to $\mathbb{T}$. In the case of $\mathbb{Z}/m\mathbb{Z}$, taking the product of two characters corresponds to addition modulo m, and we thus get the structure of a group on the set of characters of $\mathbb{Z}/m\mathbb{Z}$: it is the dual group of $\mathbb{Z}/m\mathbb{Z}$, which is isomorphic (as a group) to itself.

This motivates the following definition.

Definition 1.3. *The* dual group *(sometimes called the* Pontryagin dual*) of a group G is the topological group $\widehat{G}$ given by the set of characters on G endowed with the product law $(\chi, \tilde{\chi}) \mapsto \chi \cdot \tilde{\chi}$.*

To get the structure of a *topological* group on $\widehat{G}$, we had better define a topology on $\widehat{G}$. This is done in Sam's lecture notes and it might then be a good idea to go through our four cases and check (elementarily) that things match up. Of course, those cases are instances of and hint at the general theory developed in Sam's notes, namely that of the Pontryagin duality (for example, we saw that the dual group of the *compact* abelian group $\mathbb{T}$ is the *discrete* group $\mathbb{Z}$).

2 Fourier analysis on groups

2.1 Integration on groups

Thanks to the general theory of Lebesgue integration, the Haar measure on a locally compact abelian group G (see Efthymios's lecture notes) allows us to construct the space $L^1(G)$ of integrable functions on such a group G.

2.2 Fourier transform and Fourier inversion

For a function $f \in L^1(G)$ where G is a locally compact abelian group, we can define its Fourier transform as the function $\widehat{f}$ on $\widehat{G}$ given by:

$$\forall \chi \in \widehat{G},\ \widehat{f}(\chi) = \int_G f(g)\overline{\chi(g)}.$$

A particularly useful result is the ability to recover most functions given their Fourier transform:

Theorem 2.1 (Fourier inversion formula). *If G is a locally compact abelian group and μ is the Haar measure on G, then there exists a unique Haar measure $\hat{\mu}$ on $\widehat{G}$ such that for every function $f \in L^1(G)$ satisfying $\hat{f} \in L^1(\widehat{G})$ we have, for $\hat{\mu}$-almost every $g \in G$,*

$$f(g) = \int_{\widehat{G}} \hat{f}(\chi)\chi(g)d\hat{\mu}(\chi).$$

For a detailed account and a proof of this result, see section 3.3 of the book by Ramakrishnan and Valenza [2].

2.3 Familiar examples

If we apply our definition to the examples we discussed in the first section, we get back to familiar ground.
Indeed:
in the case of $\mathbb{Z}$, what we get are the familiar *Fourier series*;
in the case of $\mathbb{Z}/m\mathbb{Z}$, what we get is the familiar *discrete Fourier transform*, for which the inversion formula is elementary;
in the case of $\mathbb{R}$, what we get is the familiar *Fourier transform*;
in the case of $\mathbb{T}$, what we get are the familiar *Fourier coefficients*.

3 Some applications

3.1 Uncertainty principle in finite abelian groups

Let G be a finite abelian group. If $f\colon G \to \mathbb{C}$ is a function on G, our definition of its Fourier transform $\hat{f}\colon \widehat{G} \to \mathbb{C}$ becomes, after normalizing:

$$\forall \chi \in \widehat{G},\ \hat{f}(\chi) = \frac{1}{|G|}\sum_{g \in G} f(g)\overline{\chi(g)}.$$

Recall the definition of the support of f (respectively of $\hat{f}$):
$\mathrm{supp}(f) = \{x \in G \mid f(x) \neq 0\}$ (respectively $\mathrm{supp}(\hat{f}) = \{\chi \in \widehat{G} \mid \hat{f}(\chi) \neq 0\}$).
The following theorem was first proved in the case of a finite cyclic group by Donoho and Stark in 1989 [1], then in full generality by Smith in 1990 [3].

Theorem 3.1 (Smith, 1990). *If $f \neq 0$ is not identically zero, then*

$$|\mathrm{supp}(f)| \cdot |\mathrm{supp}(\hat{f})| \geq |G|.$$

3.2 Interlude: Parseval's identity

While it is possible to prove the above theorem using the Fourier inversion formula (exercise!), it provides us with a good opportunity to introduce Parseval's identity and p-norms in the context of this section.

In this instance, Parseval's identity takes the form:

$$\frac{1}{|G|}\sum_{g\in G}|f(g)|^2 = \sum_{\chi\in\widehat{G}}\left|\hat{f}(\chi)\right|^2.$$

Thanks to the triangle inequality, we also get:

$$\forall\chi\in\widehat{G},\ \left|\hat{f}(\chi)\right| \leq \frac{1}{|G|}\sum_{g\in G}|f(g)|.$$

Define, for functions on G, $\|f\|_p = \left(\frac{1}{|G|}\sum_{g\in G}|f(g)|^p\right)^{1/p}$. Using the notation $\left\|\widehat{f}\right\|_\infty$ on $\widehat{G}$ as well, the two results above can be written as:

$$\|f\|_2^2 = \sum_{\chi\in\widehat{G}}\left|\hat{f}(\chi)\right|^2 \tag{1}$$

and

$$\left\|\widehat{f}\right\|_\infty \leq \|f\|_1. \tag{2}$$

We are now ready for a proof of the theorem.
We may assume (why?) that $\|f\|_2 = 1$. Thanks to the Cauchy–Schwarz inequality, we get the estimate:

$$\|f\|_1^2 = \frac{1}{|G|}^2\left(\sum_{g\in\operatorname{supp}(f)}|f(g)|\right)^2 \leq \frac{1}{|G|^2}\cdot|\operatorname{supp}(f)|\cdot\sum_{g\in\operatorname{supp}(f)}|f(g)|^2.$$

Note that $\frac{1}{|G|}\sum_{g\in\operatorname{supp}(f)}|f(g)|^2 = \|f\|_2^2 = 1$, so the above inequality is

$$\|f\|_1^2 \leq \frac{|\operatorname{supp}(f)|}{|G|}. \tag{3}$$

On the other hand, thanks to (1) and (2), we get:

$$\begin{aligned} 1 = \sum_{\chi \in \widehat{G}} \left|\hat{f}(\chi)\right|^2 &= \sum_{\chi \in \operatorname{supp}(\hat{f})} \left|\hat{f}(\chi)\right|^2 \\ &\leq |\operatorname{supp}(\hat{f})| \cdot \|\hat{f}\|_\infty^2 \\ &\leq |\operatorname{supp}(\hat{f})| \cdot \|f\|_1^2 \leq \frac{|\operatorname{supp}(\hat{f})| \cdot |\operatorname{supp}(f)|}{|G|}, \end{aligned}$$

where the last inequality follows from (3). Equivalently,

$$|\operatorname{supp}(\hat{f})| \cdot |\operatorname{supp}(f)| \geq |G|.$$

3.3 Improvement for cyclic groups of prime order

Theorem 3.1 was substantially improved by Tao in 2004 [4] in the special case when $G = \mathbb{Z}/p\mathbb{Z}$ is a cyclic group of prime order p :

Theorem 3.2 (Tao, 2004)**.** *If $p \in \mathbb{P}$ and $f \colon \mathbb{Z}/p\mathbb{Z} \to \mathbb{C}$ is not identically zero, then*

$$|\operatorname{supp}(f)| + |\operatorname{supp}(\hat{f})| \geq p + 1.$$

(How is it an improvement?)

Perhaps amazingly, the celebrated Cauchy–Davenport inequality is a fairly straightforward corollary of this result:

Problem. Deduce the Cauchy–Davenport inequality

$$\forall (A, B) \subset (\mathbb{Z}/p\mathbb{Z})^2,\, p \in \mathbb{P},\, |A + B| \geq \min\{p, |A| + |B| - 1\}$$

from Tao's theorem.

For more applications of character theory and Fourier analysis on groups, see Chris's lecture notes.

References

[1] D. L. Donoho and P. B. Stark, *Uncertainty principles and signal recovery*, SIAM J. Appl. Math. **49** (1989), 906-931.

[2] D. Ramakrishnan and R. J. Valenza, *Fourier analysis on number fields*, Springer, New York, 1999.

[3] K. T. Smith, *The uncertainty principle on groups*, SIAM J. Appl. Math. **50**, 876-882.

[4] T. Tao, *An uncertainty principle for cyclic groups of prime order*, Math. Res. Lett., vol. 12, no. 1, 121-127, 2005.