DISCRETE FOURIER TRANSFORM

S. A.

ABSTRACT. Part of the course notes for this course. Sergey's notes for his lectures on the discrete Fourier transform.

1. THE GROUP OF CHARACTERS FOR A

Consider a finite Abelian group A. Recall that a group map $\chi: A \to \mathbb{C}^*$ is called a character of A. Notice that since for every $a \in A$ there exists $s: a^s = 1$, the absolute value $|\chi(a)| = 1$, i.e. the image of χ belongs to the circle subgroup $S = \{\alpha \in \mathbb{C} |\ |\alpha| = 1\}$.

We define the product of characters $\chi_1\chi_2$ pointwise. The trivial chracter is the unit function, the inverse character $\chi^{-1}(a) = \overline{\chi(a)}$.

Definition 1.1. The group of characters of A is called the Pontryagin dual group and is denoted by $\hat{A}$.

Denote the vector space of complex valued functions on A (resp. on $\hat{A}$) by $C(A)$ (resp. by $C(A)$).

Example 1.2.
(1) Any number $c \in \mathbb{C}$ defines a constant function, in particular 1 is the unit function in $C(A)$. Notice that pointwise multiplication makes $C(A)$ into an associative algebra with the unit.
(2) Any element $a \in A$ gives rise to a delta function δ_a whose value equals 1 at a and 0 at all other elements of A.
(3) Certainly any character $\chi \in \hat{A}$ provides an element in $C(A)$.

Remark 1.3. It is known from the algebra course that as elements of $C(A)$ all characters are linearly independent. In particular, the cardinality of $\hat{A}$ is no greater than the number of elements in A.

Example 1.4. Take the finite cyclic group $A = \mathbb{Z}/n = \{1, s, \ldots, s^{n-1}\}$. Then any $k \in \{0, \ldots, n-1\}$ provides a character $\chi_k: \mathbb{Z}/n \to \mathbb{C}^*, s^m \mapsto \xi^{mk}$. Here ξ denotes a chosen primitive root of unity of degree n. In particular, $\hat{A}$ is a cyclic group of the same order. It is isomorphic to A non-canonically.

Classification Theorem for finite Abelian groups implies that for any such A the group $\hat{A}$ is non-canonically isomorphic to A.

The vector space $C(A)$ (resp. $C(\hat{A})$) is equipped with a Hermitian form:

$$\langle f, g\rangle = \sum_{a \in A} f(a)\overline{g}(a).$$

Remark 1.5. Notice that the functions $\delta_a,\ a \in A$, form an orthonormal basis of $C(A)$.

Lemma 1.6. Let χ_1 and χ_2 be two different characters of A. Then as elements of $C(A)$ they are orthogonal to each other.

Proof. Let $b \in A$ be an element such that $\chi_1(b) \neq \chi_2(b)$. We have

$$\langle \chi_1, \chi_2 \rangle = \sum_{a\in A} \chi_1(a)\overline{\chi}_2(a) = \sum_{a\in A} \chi_1(ab)\overline{\chi}_2(ab) = (\sum_{a\in A} \chi_1(a)\overline{\chi}_2(a))\chi_1(b)\chi_2^{-1}(b).$$

By our choice of $b \in A$, the first factor in the last expression equals to 0. $\square$

Lemma 1.7. The map $A \to \hat{\hat{A}},\ a \to \hat{a},\ \hat{a}(\chi) = \chi(a)$, provides a canonical isomorphism between A and the double Pontryagin dual group of A.

Proof. We know that the source and the target of the canonical map have the same cardinality. It is clear that the map respects multiplication in the group. Moreover, for any non-unit a, the character $\hat{a}$ is non-trivial. It follows that the map is an injective. Thus it is an isoporphism. $\square$

2. Discrete Fourier transform

Definition 2.1. The vector space map

$$F:\ C(A) \to C(\hat{A}),\ F(f)(\chi) = \sum_{a\in A} f(a)\overline{\chi(a)},$$

is called the Fourier transform for the group A.

Example 2.2. Let us calculate some examples:

(1) $F(\delta_a)(\chi) = \overline{\chi(a)} = \hat{a}^{-1}(\chi)$.
(2) $F(1)(\chi) = \sum_{a\in A} \overline{\chi(a)}$. It is known that for a non-trivial character such sum equals to 0. The value at χ_0 equals to $\#(A)$. Thus we have $F(1) = \delta_{\chi_0}$.
(3) More generally, $F(\chi_1)(\chi_2) = \langle \chi_1, \chi_2 \rangle = 0$ for $\chi_1 \neq \chi_2$. We have $F(\chi)(\chi) = \langle \chi, \chi \rangle = \#(A)$. It follows that $F(\chi) = \#(A)\delta_\chi$.

Corrollary 2.3. It follows that the Fourier transform $F = F_A$ is an isomorphism of the vector spaces $C(A)$ and $C(\hat{A})$ with its inverse equal to $\#(A)F_{\hat{A}}$.

Remark 2.4. We have checked that an orthogonal basis in $C(A)$ is mapped to an orthogonal basis in $C(\hat{A})$. Thus up to a scalar multiple F is an isometry.

Definition 2.5. Given a map of finite sets $\alpha:\ X \to Y)$, consider the pull back morphism

$$\alpha^*:\ C(Y) \to C(X),\ \alpha^*(f)(x) = f(\alpha(x))$$

and the push forward morphism

$$\alpha_*:\ C(X) \to C(Y),\ \alpha_*(f)(y) = \sum_{\alpha(x)=y} f(x).$$

Remark 2.6. (1) The pull-back map respects the pointwise product of functions.
(2) For two maps $\alpha : X \to Y$ and $\beta : Y \to Z$ we have
$$(\beta \circ \alpha)^* = \alpha^* \circ \beta^*,\ (\beta \circ \alpha)_* = \beta_* \circ \alpha_*$$
. This is a direct calculation.

Let $\alpha : B \to A$ be a morphism of finite Abelian groups. Then any character of A defines a character of B. We obtain the Pontryagin dual map $\hat{\alpha} : \hat{A} \to \hat{B}$.

Lemma 2.7. We have $(\hat{\alpha})^* \circ F = F \circ \alpha_*$.

We introduce the second multiplication on $C(A)$. Denote the multiplication map $A \times A \to A$ by m.

Definition 2.8. For $f, g \in C(A)$ denote the function on $A \times A$ given by $(a, b) \mapsto f(a)g(b)$ by $f \times g$. The convolution $f \star g = m_*(f \times g)$.

Remark 2.9. (1) The element δ_1 is the unit for the operation.
(2) One checks directly that convolution is associative.
(3) Compare the definition of convolution with the following observation. Denote the diagonal embedding $A \to A \times A$ by Δ. The pointwise product of functions is given by $f \cdot g = \Delta^*(f \times g)$.

Lemma 2.10. We have $F(f \star g) = F(f) \cdot F(g)$.

Proof. Consider the map $\hat{m} : \hat{A} \to \hat{A} \times \hat{A}$. We have
$$\hat{m}(\chi)(a, b) = \chi(ab) = \chi(a)\chi(b) = (\chi \times \chi)(a, b).$$
Thus the Pontryagin dual for the product map is the diagonal embedding. The proof follows. □

Consider the argument shift operation $L_a : C(A) \to C(A), (L_a f)(b) = f(a + b)$.

Lemma 2.11. We have $(F \circ L_a)(f) = \hat{a} \cdot F(f)$.

Proof. The key observation in the proof is that $L_a(f) = \delta_a \star f$. Then use the previous Lemma. □

3. Generalized Poisson summation

Below we describe the setting for Poisson summation. Let A be a finite Abelian group with a subgroup B. Consider the embedding map $i : B \to A$ and the projection map $p : A \to A/B$. The map $\hat{i}$ is surjective, its kernel $B^\perp$ consists of characters χ whose restriction to B is trivial. We identify the kernel with $\widehat{(A/B)}$.

Theorem 3.1. For $f \in C(A)$, for any $a \in A$, we have
$$\sum_{b \in B} f(a + b) = \sum_{\chi \in B^\perp} F(f)(\chi)\overline{\chi}(a).$$

Proof. First notice that LHS in the formula in question equals $p_*(f)(aB)$. From Section 2 we know that the latter equals $F_{A/B}^{-1} \circ (\hat{p})^* \circ F_A$. Notice that

$$F_{A/B}^{-1} \circ (\hat{p})^* \circ F_A(f)(aB) = \sum_{\chi \in B^\perp} F(f)(\chi)\overline{\chi}(a).$$

$\square$