# Notas das reuniões do PICME
# Segundo semestre de 2014

Leonardo Nagami Coregliano

3 de setembro de 2014

## Sumário

# 1 Transformada Rápida de Fourier e Multiplicação de Polinômios

## 1.1 Conceitos Básicos de Grupos e a Transformada de Fourier

26/08/2014 – Fernando Mário de Oliveira Filho

Iniciaremos relembrando alguns conceitos básicos de grupos.

**Definição 1.1.1.** Um *grupo* é uma tripla $(G, e, +)$, onde $G$ é um conjunto, $e \in G$ é um elemento de $G$ chamado *identidade* e $+\colon G \times G \to G$ é uma operação que satisfaz as seguintes propriedades.

i. (Associatividade) Para todos $x, y, z \in G$, temos $(x + y) + z = x + (y + z)$;

ii. (Elemento neutro) Para todo $x \in G$, temos $e + x = x$;

iii. (Elemento oposto) Para todo $x \in G$, existe $y \in G$ tal que $y + x = e$.

O elemento $y$ do Item iii é chamado de *oposto* de $x$ e é denotado por $-x$. Muitas vezes abusaremos da notação denotando por $x - y$ a fórmula $x + (-y)$. Também abusaremos da notação falando apenas que $G$ é um grupo, em vez de mencionar a tripla inteira e, salvo menção explícita ao contrário, a operação será sempre $+$ e a identidade será sempre $e$.

Um grupo $G$ que também satisfaz a propriedade abaixo é chamado de *grupo abeliano*.

v. (Comutatividade) Para todos $x, y \in G$, temos $x + y = y + x$.

Alguns exemplos clássicos de grupos abelianos são $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ com a operação de soma módulo $n$ e o toro $\mathbb{T} = \{z \in \mathbb{C} : |z| = 1\}$ com a operação de multiplicação (nesse último caso manteremos a notação multiplicativa para evitar confusões).

Exemplos simples de grupos não abelianos são o grupo $M_{n\times n}(\mathbb{R})$ das matrizes inversíveis de ordem $n \times n$ munidas da operação de multiplicação de matrizes e o grupo $\mathfrak{S}_n$ das permutações de tamanho $n$ (funções bijetoras de $[n]$ em $[n]$) munidas da composição de funções.

Deixamos algumas propriedades básicas de grupos como exercício.

**Exercício resolvido 1.1.2.** Suponha que $G$ é um grupo com identidade $e$. Valem as seguintes asserções.

1. (Caracterização do neutro) Para todo $x \in G$, temos $x + x = x$ se e só se $x = e$;

2. (Elemento oposto à direita) Para todo $x \in G$, temos $x + (-x) = e$;

3. (Elemento neutro à direita) Para todo $x \in G$, temos $x + e = x$;

4. (Unicidade do elemento neutro) Se $x, y \in G$ são tais que $x + y = y$, então $x = e$;

5. (Unicidade do elemento oposto) Se $x, y, z \in G$ são tais que $y + x = z + x = e$, então $y = z$;

6. (Bijeção através da operação) Para todo $y \in G$, a função $g_y\colon G \ni x \mapsto x + y \in G$ é bijetora.

Lembramos agora a definição de homomorfismos e isomorfismos de grupos.

**Definição 1.1.3.** Um *homomorfismo de grupos* do grupo $G$ no grupo $H$ é uma função $f\colon G \to H$ que preserva a operação, isto é, uma função tal que $f(x + y) = f(x) + f(y)$, para todos $x, y \in G$.

Um *isomorfismo de grupos* é um homomorfismo de grupos que é também bijetor.

Dizemos que um grupo $G$ é *isomorfo* a um grupo $H$ (e denotamos por $G \cong H$) se existe um isomorfismo de grupos de $G$ em $H$.

O exercício abaixo diz que homomorfismos também preservam identidade.

**Exercício resolvido 1.1.4.** Se $f$ é um homomorfismo de grupos do grupo $G$ no grupo $H$, então temos $f(e_G) = e_H$, onde $e_G$ e $e_H$ são as identidades de $G$ e $H$ respectivamente.

Um tipo particular de homomorfismos merece atenção especial.

**Definição 1.1.5.** Um *caracter* de um grupo $G$ é um homomorfismo de grupos de $G$ para o grupo $\mathbb{T} = \{z \in \mathbb{C} : |z| = 1\}$ (munido da multiplicação usual), isto é, um caracter é um homomorfismo $\chi\colon G \to \mathbb{T}$.

Denotamos o conjunto dos caracteres de $G$ por $\widehat{G}$.

É fácil ver que, dado um grupo $G$, o conjunto dos caracteres de $G$ munido do produto ponto-a-ponto de funções é um grupo abeliano e, dado um caractere $\chi$, seu elemento oposto (denotado $\chi^{-1}$ devido à notação multiplicativa) é exatamente seu conjugado complexo ponto-a-ponto (i.e., para todo $g \in G$, temos $\chi^{-1}(g) = \overline{\chi(g)}$).

Muitas vezes veremos caracteres como elementos do espaço vetorial $\mathbb{C}^G$ das funções de $G$ a $\mathbb{C}$. O teorema abaixo nos diz quanto é o produto interno entre dois caracteres.

**Teorema 1.1.6.** Se $\chi$ e $\psi$ são caracteres de um grupo abeliano finito $G$, então

$$\chi^*\psi = \langle \psi, \chi \rangle = \sum_{x \in G} \overline{\chi(x)}\psi(x) = \begin{cases} |G|, & \text{se } \chi = \psi; \\ 0, & \text{se } \chi \neq \psi. \end{cases}$$

*Demonstração.* Se $\chi = \psi$, então temos

$$\sum_{x \in G} \overline{\chi(x)}\psi(x) = \sum_{x \in G} |\chi(x)|^2 = \sum_{x \in G} 1 = |G|.$$

Suponha agora que $\chi \neq \psi$, então existe $y \in G$ tal que $\psi(y) \neq \chi(y)$, logo temos $\overline{\chi(y)}\psi(y) \neq 1$.

Por outro lado, temos

$$\overline{\chi(y)}\psi(y) \sum_{x \in G} \overline{\chi(x)}\psi(x) = \sum_{x \in G} \overline{\chi(x)\chi(y)}\psi(x)\psi(y) = \sum_{x \in G} \overline{\chi(x+y)}\psi(x+y) = \sum_{z \in G} \overline{\chi(z)}\psi(z),$$

donde segue que

$$(1 - \overline{\chi(y)}\psi(y))\chi^*\psi = 0,$$

e, portanto $\chi^*\psi = 0$. ∎

**Corolário 1.1.7.** Para o grupo $\mathbb{Z}_n$, cada $u \in \mathbb{Z}_n$ define um caracter

$$\begin{array}{rccc} \chi_u\colon & \mathbb{Z}_n & \longrightarrow & \mathbb{T} \\ & x & \longmapsto & e^{2\pi i u x/n}. \end{array}$$

Ademais a função $\mathbb{Z}_n \ni u \mapsto \chi_u \in \widehat{\mathbb{Z}_n}$ é um isomorfismo de grupos.

*Demonstração.* Sejam $u, x, y \in \mathbb{Z}_n$ arbitrários e observe que

$$\begin{aligned} \chi_u(x+y) &= \exp\left(\frac{2\pi i u((x+y) \bmod n)}{n}\right) = \exp\left(\frac{2\pi i u(x+y)}{n}\right) \\ &= \exp\left(\frac{2\pi i u x}{n}\right)\exp\left(\frac{2\pi i u y}{n}\right) = \chi_u(x)\chi_u(y), \end{aligned}$$

logo $\chi_u$ de fato é caracter de $\mathbb{Z}_n$ (também temos trivialmente que $|\chi_u(x)| = 1$ para todo $x \in \mathbb{Z}_n$).

Observe agora que

$$\chi_{x+y}(u) = \exp\left(\frac{2\pi i((x+y) \bmod n)u}{n}\right) = \chi_x(u)\chi_y(u),$$

logo a função $g\colon \mathbb{Z}_n \ni u \mapsto \chi_u \in \widehat{\mathbb{Z}_n}$ é um homomorfismo de grupos, resta provar apenas que essa função é bijetora.

Suponha que $x \neq y$ e observe que

$$\chi_x(1) = e^{2\pi i x/n} \neq e^{2\pi i y/n} = \chi_y(1),$$

logo a função $g$ é injetora.

Porém, o Teorema 1.1.6 nos diz que o conjunto $\widehat{\mathbb{Z}_n}$ é ortogonal no espaço vetorial $\mathbb{C}^G$, isso significa que

$$|\widehat{\mathbb{Z}_n}| \leqslant \dim \mathbb{C}^G = |G|,$$

e como $g$ é injetora temos que a imagem de $g$ possui cardinalidade maior ou igual a $|G|$. Portanto $g$ é bijetora (pois seu domínio é finito). ∎

Lembramos agora a definição de produto direto de grupos.

**Definição 1.1.8.** O *produto direto* dos grupos $G$ e $H$ é o grupo $G \times H$ munido da operação definida por

$$(g_1, h_1) + (g_2, h_2) = (g_1 + g_2, h_1 + h_2),$$

para todos $g_1, g_2 \in G$ e $h_1, h_2 \in H$.

A identidade de $G \times H$ é o elemento $(e_G, e_H)$, onde $e_G$ é a identidade de $G$ e $e_H$ é a identidade de $H$.

O exercício abaixo caracteriza os caracteres de um produto direto.

**Exercício resolvido 1.1.9.** Se $\chi$ é caracter de $G$ e $\psi$ é caracter de $H$, então

$$\begin{array}{rccc} \chi \otimes \psi\colon & G \times H & \longrightarrow & \mathbb{T} \\ & (g, h) & \longmapsto & \chi(g)\psi(h) \end{array}$$

é caracter de $G \times H$.

Ademais, se $\varphi$ é caracter de $G \times H$, então existem $\chi$ caracter de $G$ e $\psi$ caracter de $H$ tais que $\varphi = \chi \otimes \psi$.

Lembramos do seguinte fato de álgebra.

**Fato 1.1.10.** Se $G$ é um grupo abeliano finito, então existem $k_1, k_2, \ldots, k_n \in \mathbb{N}^*$ tais que

$$G \cong \mathbb{Z}_{k_1} \times \mathbb{Z}_{k_2} \times \cdots \times \mathbb{Z}_{k_n}.$$

Finalmente definimos a Transformada de Fourier.

**Definição 1.1.11.** Seja $G$ um grupo abeliano finito e considere o espaço vetorial $\mathbb{C}^G$ munido do produto interno

$$\langle f, g \rangle = \sum_{x \in G} f(x)\overline{g(x)},$$

para todos $f, g \in \mathbb{C}^G$.

Considere também fixada uma decomposição de $G$ como produto direto de $\mathbb{Z}_k$'s como no Fato 1.1.10.

A *Base Canônica* de $\mathbb{C}^G$ é a base $(e_u)_{u \in G}$, onde

$$e_u(x) = \begin{cases} 1, & \text{se } x = u; \\ 0, & \text{se } x \neq u; \end{cases}$$

para todos $u, x \in G$.

A *Base de Fourier* de $\mathbb{C}^G$ é a base $(\chi_u)_{u \in G}$, onde $\chi_u$ é o caractere associado a $u$ conforme o Corolário 1.1.7 e o Exercício 1.1.9.

A *Transformada de Fourier* (ou *Transformada Direta de Fourier*) de um elemento $f \in \mathbb{C}^G$ é a função

$$\begin{array}{lll} \widehat{f}\colon G & \longrightarrow \mathbb{C} \\ u & \longmapsto \langle f, \chi_u \rangle . \end{array}$$

Da definição da Transformada de Fouriere do Teorema 1.1.6, segue que

$$f = \frac{1}{|G|} \sum_{u \in G} \widehat{f}(u)\chi_u,$$

que é comumente dita *Transformada Inversa de Fourier* do elemento $\widehat{f}$.

Para o caso em que $G = \mathbb{Z}_n$, temos

$$\widehat{f}(u) = \sum_{x \in \mathbb{Z}_n} f(x)e^{-2\pi iux/n} \quad \text{para todo } u \in \mathbb{Z}_n;$$

$$f(x) = \frac{1}{n} \sum_{u \in \mathbb{Z}_n} \widehat{f}(u)e^{2\pi iux/n} \quad \text{para todo } x \in \mathbb{Z}_n.$$

Como $G$ é abeliano, segue também que $\chi_u(x) = \chi_x(u)$, para todos $u, x \in G$.

A proposição abaixo mostra a relação entre a Transformada Direta e a Transformada Inversa de Fourier.

**Proposição 1.1.12.** Se $f \in \mathbb{C}^G$ e $g = \overline{\widehat{f}}$, então temos

$$\overline{\widehat{g}(x)} = |G| f(x),$$

para todo $x \in G$.

*Demonstração.* Segue direto de

$$\begin{aligned}\overline{\widehat{g}(x)} = \overline{\langle g, \chi_x \rangle} &= \overline{\sum_{u \in G} g(u)\overline{\chi_x(u)}} \\ &= \sum_{u \in G} \overline{g(u)}\chi_x(u) = \sum_{u \in G} \widehat{f}(u)\chi_u(x) \\ &= |G| f(x).\end{aligned}$$

■

# A Soluções dos exercícios resolvidos

**Exercício resolvido.** (1.1.2) Suponha que $G$ é um grupo com identidade $e$. Valem as seguintes asserções.

1. (Caracterização do neutro) Para todo $x \in G$, temos $x + x = x$ se e só se $x = e$;

2. (Elemento oposto à direita) Para todo $x \in G$, temos $x + (-x) = e$;

3. (Elemento neutro à direita) Para todo $x \in G$, temos $x + e = x$;

4. (Unicidade do elemento neutro) Se $x, y \in G$ são tais que $x + y = y$, então $x = e$;

5. (Unicidade do elemento oposto) Se $x, y, z \in G$ são tais que $y + x = z + x = e$, então $y = z$;

6. (Bijeção através da operação) Para todo $y \in G$, a função $g_y \colon G \ni x \mapsto x + y \in G$ é bijetora.

*Demonstração.* Para a asserção da caracterização do elemento neutro, temos

$$x + x = x \Longrightarrow (-x) + (x + x) = (-x) + x \Longrightarrow e + x = e \Longrightarrow x = e.$$

Por outro lado, se $x = e$, então trivialmente $x + x = e + e = e$.

Para a asserção do elemento oposto à direita, observe que se $x \in G$, temos que

$$(x + (-x)) + (x + (-x)) = x + e + (-x) = x + (-x),$$

logo, da caracterização do elemento neutro, segue que $x + (-x) = e$.

Para a asserção do elemento neutro à direita, observe que se $x \in G$, temos que

$$x + e = x + ((-x) + x) = e + x = x.$$

Para a asserção da unicidade do elemento neutro, basta observar que $x + y = y$ implica que $x + y + (-y) = y + (-y)$, logo temos $x = e$.

Para a asserção da unicidade do elemento oposto, basta observar que $y + x = z + x$ implica que $y + x + (-x) = z + x + (-x)$ e pelas asserções do elemento oposto à direita e elemento neutro à direita, segue que $y = z$.

Finalmente, para a asserção da bijeção através da operação, observe que se $g_y(x) = g_y(z)$, então $y + x = y + z$, logo $x = z$. Por outro lado, para todo $x \in G$, temos que $g_y((-y) + x) = y + (-y) + x = x$. ■

**Exercício resolvido.** (1.1.4) Se $f$ é um homomorfismo de grupos do grupo $G$ no grupo $H$, então temos $f(e_G) = e_H$, onde $e_G$ e $e_H$ são as identidades de $G$ e $H$ respectivamente.

*Demonstração.* Basta observar que

$$f(e_G) = f(e_G + e_G) = f(e_G) + f(e_G),$$

logo, da caracterização da identidade (Exercício 1.1.2), segue que $f(e_G) = e_H$. ■

**Exercício resolvido.** (1.1.9) Se $\chi$ é caracter de $G$ e $\psi$ é caracter de $H$, então

$$\begin{array}{rccc} \chi \otimes \psi \colon & G \times H & \longrightarrow & \mathbb{T} \\ & (g, h) & \longmapsto & \chi(g)\psi(h) \end{array}$$

é caracter de $G \times H$.

Ademais, se $\varphi$ é caracter de $G \times H$, então existem $\chi$ caracter de $G$ e $\psi$ caracter de $H$ tais que $\varphi = \chi \otimes \psi$.

*Demonstração.* Observe primeiramente que se $(g_1, h_1), (g_2, h_2) \in G \times H$, então temos

$$\begin{aligned}\chi \otimes \psi((g_1, h_1) + (g_2, h_2)) &= \chi \otimes \psi((g_1 + g_2, h_1 + h_2)) = \chi(g_1 + g_2)\psi(h_1 + h_2) \\ &= \chi(g_1)\chi(g_2)\psi(h_1)\psi(h_2) = \chi(g_1)\psi(h_1)\chi(g_2)\psi(h_2) \\ &= \chi \otimes \psi((g_1, h_1))\chi \otimes \psi((g_2, h_2)).\end{aligned}$$

Portanto $\chi \otimes \psi$ é caracter de $G \times H$.

Seja agora $\varphi$ um caracter qualquer de $G \times H$. Sejam $e_G$ e $e_H$ as identidades de $G$ e $H$ respectivamente e defina $\chi(g) = \varphi(g, e_H)$ para todo $g \in G$ e $\psi(h) = \varphi(e_G, h)$ para todo $h \in H$.

Observe que, para todos $g_1, g_2 \in G$, temos

$$\chi(g_1 + g_2) = \varphi((g_1 + g_2, e_H)) = \varphi((g_1, e_H) + (g_2, e_H)) = \varphi((g_1, e_H))\varphi((g_2, e_H)) = \chi(g_1)\chi(g_2).$$

Analogamente, para todos $h_1, h_2 \in H$, temos

$$\psi(h_1 + h_2) = \varphi((e_G, h_1 + h_2)) = \varphi((e_G, h_1) + (e_G, h_2)) = \varphi((e_G, h_1))\varphi((e_G, h_2)) = \psi(h_1)\psi(h_2).$$

Portanto $\chi$ é caracter de $G$ e $\psi$ é caracter de $H$.

Observe agora que para todo $(g, h) \in G \times H$, temos

$$\chi \otimes \psi((g, h)) = \chi(g)\psi(h) = \varphi((g, e_H))\varphi((e_G, h)) = \varphi((g + e_G, e_H + h)) = \varphi((g, h)).$$

Portanto $\varphi = \chi \otimes \psi$. ■

# B Notação

$$\mathbb{N} = \{0, 1, 2, 3, \ldots\}$$
$$\mathbb{N}^* = \mathbb{N} \setminus \{0\}$$
$$\mathbb{R}_+ = \{x \in \mathbb{R} : x \geqslant 0\}$$
$$[n] = \{1, 2, \ldots, n\}, \text{ para } n \in \mathbb{N}^*$$
$$\mathbb{J}_n \text{ denota a matriz } n \times n \text{ com todas as entradas 1}$$
$$f(n) \sim g(n) \text{ significa } \lim_{n \to +\infty} \frac{f(n)}{g(n)} = 1$$
$$f(n) = O(g(n)) \text{ significa } \limsup_{n \to +\infty} \left| \frac{f(n)}{g(n)} \right| < +\infty$$
$$f(n) = \Omega(g(n)) \text{ significa } g(n) = O(f(n))$$
$$f(n) = \Theta(g(n)) \text{ significa } f(n) = O(g(n)) \text{ e } f(n) = \Omega(g(n))$$
$$f(n) \asymp g(n) \text{ significa } f(n) = \Theta(g(n))$$
$$f(n) = o(g(n)) \text{ significa } \limsup_{n \to +\infty} \left| \frac{f(n)}{g(n)} \right| = 0$$
$$f(n) = \omega(g(n)) \text{ significa } g(n) = o(f(n))$$
$$\pi(n) = |\{a \in [n] : a \text{ é primo}\}|, \text{ para } n \in \mathbb{N}$$
$$\lfloor x \rfloor \text{ denota o maior inteiro menor ou igual a } x, \text{ para } x \in \mathbb{R}$$
$$\lceil x \rceil = - \lfloor -x \rfloor$$
$$\binom{A}{k} = \{B \subset A : |B| = k\}, \text{ para } A \text{ um conjunto}$$
$$\binom{A}{\leqslant k} = \{B \subset A : |B| \leqslant k\}, \text{ para } A \text{ um conjunto}$$
$$n \mid m \text{ significa } n \text{ divide } m, \text{ para } n, m \in \mathbb{Z}, m \neq 0$$
$$N_G(v) = \{w \in V(G) : vw \in E(G)\}, \text{ para } G \text{ um grafo e } v \in V(G)$$
$$d_G(v) = |N_G(v)|, \text{ para } G \text{ um grafo e } v \in V(G)$$
$$N_G(X) = \bigcup_{x \in X} N_G(x), \text{ para } G \text{ um grafo e } X \subset V(G)$$
$$\delta_G(X) = \{xy \in E(G) : x \in X\}, \text{ para } G \text{ um grafo e } X, Y \subset V(G)$$
$$\delta_G(X, Y) = \{xy \in E(G) : x \in X \text{ e } y \in Y\}, \text{ para } G \text{ um grafo e } X, Y \subset V(G)$$
$$\delta(G) = \min\{d_G(v) : v \in V(G)\}, \text{ para } G \text{ um grafo}$$
$$\Delta(G) = \sup\{d_G(v) : v \in V(G)\}, \text{ para } G \text{ um grafo}$$

# Índice de palestrantes

# Índice de nomes

## Referências