Teoria Analítica dos Números

03/12/2025

TODO: Separar a prova do teorema principal desta aula em duas partes, uma relacionando caracteres com homomorfismo de (Z/qZ)* e outra com as raizes da unidade.

Na aula passada introduzimos os caracteres de Dirichlet. Um caractere de Dirichlet módulo q é uma função $\chi : \mathbb{Z} \to \mathbb{C}$ satisfazendo

- χ é periódica com período q: $\chi(n+q) = \chi(n)\ \forall n \in \mathbb{Z}$.
- χ é completamente multiplicativa.
- $\chi(n) \neq 0 \iff (n,q) = 1$ Então existe um caractere χ módulo q tal que $\chi(a) \neq 1$.

e mostramos os seguintes exemplos:

i) $\chi = \chi_0$ o caractere principal, onde

$$\chi_0(n) = \begin{cases} 1 \text{ se } (n,q) = 1, \\ 0 \text{ caso contrário.} \end{cases}$$

ii) $\chi = \left(\frac{\cdot}{q}\right)$ (Símbolo de Legendre (ou Jacobi)).

iii) $\chi = \left(\frac{-1}{\cdot}\right)$ (Símbolo de Jacobi "em baixo").

iv) Um exemplo diferente módulo 5:

$$\chi(n) = \begin{cases} 0 & \text{se } n \equiv 0 \pmod 5, \\ 1 & \text{se } n \equiv 1 \pmod 5, \\ i & \text{se } n \equiv 2 \pmod 5, \\ -i & \text{se } n \equiv 3 \pmod 5, \\ -1 & \text{se } n \equiv 4 \pmod 5. \end{cases}$$

Este foi o primeiro exemplo de um caractere cuja imagem não está contida em $\mathbb{R}$.

Proposição. *As seguintes afirmações sobre os caracteres de Dirichlet são válidas:*

i) Dado $n \in \mathbb{Z}$,$\chi(n)$ é igual a 0 ou a uma raiz da unidade. Mais precisamente, temos que se $\chi(n) \neq 0$, então $\chi(n) = e^{2\pi i \frac{k}{\phi(q)}}$.

ii) O conjunto $\mathfrak{X}_q : \{\chi \ \ caractere\ módulo q\}$ forma um grupo abeliano com respeito à multiplicação ponto-a-ponto e o inverso de um caractere é igual ao seu conjugado complexo $\overline{\chi}$, dado por $\overline{\chi}(n) = \overline{\chi(n)}$

Prova:

i) Basta mostrar que se $\chi(n) \neq 0$, então $\chi(n)^{\phi(q)} = 1$. Ora, se se $\chi(n) \neq 0$, pela propriedade 3 da de finição de Caracteres, $(n, q) = 1$. Então pelo Teorema de Euler,

$$n^{\phi(q)} \equiv 1 \pmod{q} \Longleftrightarrow n^{\phi(q)=1+tq}$$

para algum $t \in \mathbb{Z}$. Agora, pela propriedade 1,

$$1 = \chi(1) = \chi(1 + tq) = \chi(n^{\phi(q)}).$$

Finalmente, pela propriedade 2,

$$\chi(n)^{\phi(q)} = \chi(n^{\phi(q)}) = 1.$$

ii) A multiplicação é ponto-a-ponto:

$$(\chi_1 \cdot \chi_2)(n) := \chi_1(n) \cdot \chi_2(n)$$

- Associatividade $((\chi_1\chi_2)\chi_3 = \chi_1(\chi_2\chi_3))$

  Segue da associatividade de $\mathbb{C}$.

- Inverso $(\chi \cdot \chi^{-1} = e)$

  O elemento inverso é $\chi^{-1} = \overline{\chi}$. Temos que provar

$$\chi(n) \cdot \overline{\chi}(n) = \chi_0(n) \quad \forall n \in \mathbb{Z}. \tag{$*$}$$

  Se $(n, q) = 1$, pelo item *i*),

$$\chi(n) = e^{\frac{2\pi i k n}{\phi(q)}}.$$

  Logo,

$$\overline{\chi}(n) = e^{-\frac{2\pi i k n}{\phi(q)}}.$$

  De modo que $\chi(n) \cdot \overline{\chi}(n) = 1 = \chi_0(n)$.

  Se $(n, q) > 1$, os dois lados de $(*)$ se anulam.

- Elemento neutro: $(\chi \cdot e = e \cdot \chi = \chi)$

  O elemento neutro é $e = \chi_0$. Temos que mostrar que, para todo χ,

  $$\chi(n) \cdot \chi_0(n) = \chi(n), \quad \forall n \in \mathbb{Z}. \tag{$**$}$$

  Se $(n, q) = 1$, então $\chi_0(n) = 1$. Logo,

  $$\chi(n) \cdot \chi_0(n) = \chi(n) \cdot 1 = \chi(n)$$

  Se $(n, q) > 1$, os dois lados de $(**)$ devem ser 0.

- Comutatividade $(\chi\psi = \psi\chi)$

  Segue da associatividade de $\mathbb{C}$.

Vamos usar o seguinte teorema como **black box**:

Teorema (Caracterização dos grupos abelianos finitos)**.** *Seja G um grupo abeliano finito. Então existem $m_1, m_2, \ldots, m_k$ tais que:*

$$(G, \cdot) \simeq (\mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_k\mathbb{Z}, +).$$

Exemplo Se p é um primo ímpar e $k \geq 1$. Existe uma raiz primitiva módulo p^k. isto significa que existe uma bijeção entre $((\mathbb{Z}/p^k\mathbb{Z})^\times, \cdot)$ e $(\mathbb{Z}/p^{k-1}(p-1)\mathbb{Z}, +)$.

$$\begin{aligned} \mathbb{Z}/p^{k-1}(p-1)\mathbb{Z} &\longrightarrow \mathbb{Z}/p^k\mathbb{Z})^\times \\ k &\longmapsto \xi^k \end{aligned}$$

Para evitar trocar de notação (multiplicativa para aditiva), denote por $(G_m, \cdot)$ o (único) grupo cíclico com m elementos. Ou seja,

$$G_m = \langle \xi \mid \xi^m = 1 \rangle = \{1, \xi, \ldots, \xi^{m-1}\}.$$

Com esta notação, podemos substituir $(\mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_k\mathbb{Z}, +)$ por $(G_1 \times \cdots \times G_m, \cdot)$ no teorema acima.

A partir de agora todos os grupos vão ser multiplicativos então não vamos lembrar a operação.

Em particular, para todo q, existem $m_1, \ldots, m_k$ tais que:

$$(\mathbb{Z}/q\mathbb{Z})^* \cong G_{m_1} \times \cdots \times G_{m_k}$$

Exemplo:

$$(\mathbb{Z}/8\mathbb{Z})^* \cong G_2 \times G_2$$

$$(\mathbb{Z}/15\mathbb{Z})^* \cong (\mathbb{Z}/3\mathbb{Z})^* \times (\mathbb{Z}/5\mathbb{Z})^* \simeq G_2 \times G_4$$

Aplicação do teorema:

Chegamos ao teorema principal da aula de hoje.

Teorema. *Seja $\mathfrak{X}_q$ o conjunto dos caracteres módulo q. Então $\#\mathfrak{X}_q = \phi(q)$. Além disso, se $(a,q) = 1$ e $a \not\equiv 1 \pmod{q}$, existe algum $\chi \in \mathfrak{X}_q$ tal que $\chi(a) \neq 1$.*

A partir deste ponto é que precisar da uma mudada.

Prova: Para cada $n \in \mathbb{Z}$, denote por $n \pmod{q}$ a sua classe de congruência módulo q. Observe que $n \pmod{q} \in (\mathbb{Z}/q\mathbb{Z})^*$ se e somente se $(n,q) = 1$.

Sejam $m_1, \ldots, m_k$ tais que

$$(\mathbb{Z}/q\mathbb{Z})^* \cong G_{m_1} \times \cdots \times G_{m_k}. \qquad (\bigstar)$$

Sejam $g_1, \ldots, g_k$ geradores de $G_{m_1}, \ldots, G_{m_k}$ respectivamente. Seja

$$Z = \mu_{m_1} \times \mu_{m_2} \times \cdots \times \mu_{m_k},$$

onde

$$\begin{aligned} \mu_m &= \{\text{raízes } m\text{-ésimas da unidade}\} \\ &= \{\omega \in \mathbb{C};\ \omega^m = 1\} \\ &= \{e^{\frac{2\pi i k}{m}} \mid k = 0, 1, \ldots, m-1\}. \end{aligned}$$

Em particular, $\#\mu_m = m$ e, consequentemente,

$$\begin{aligned} \#Z &= m_1 m_2 \cdots m_k \\ &= \#\left(G_{m_1} \times \cdots \times G_{m_k}\right) \\ &= \#\left(\mathbb{Z}/q\mathbb{Z}\right)^\times = \phi(q). \end{aligned}$$

Nosso objetivo é encontrar um bijeção entre $\mathfrak{X}_q$ e Z.

Para cada $i = 1, \ldots, k$, seja $x_i \in (\mathbb{Z}/q\mathbb{Z})^*$ correspondendo ao elemento

$$(1, 1, \ldots, 1, \underbrace{g_i}_{i\text{-ésima posição}}, 1, \ldots, 1).$$

Construa a seguinte função

$$\begin{aligned} \varphi : \mathfrak{X}_q &\longrightarrow Z \\ \chi &\longmapsto (\chi(n_1), \chi(n_2), \ldots, \chi(n_k)), \end{aligned}$$

onde $n_i \in \mathbb{Z}$ é tal que $n_i \pmod{q} = x_i$. Para verificar que φ está bem definida. é necessário mostrar que $\chi(n_i)^{m_i} = 1$. Como x_i corrsponde a $(1, 1, \ldots, 1, g_i, 1, \ldots, 1)$ pelo homomorfismo $(\bigstar)$, como $g_i^{m_i} = 1$, segue que $x_i^{m_i} = 1$ em $(\mathbb{Z}/q\mathbb{Z})^\times$. Ou seja,

$$n_i^{m_i} \equiv 1 \pmod{q}.$$

Em particular,

$$\chi(n_i)^{m_i} = \chi(n_i^{m_i}) = \chi(1) = 1,$$

o que mostra que φ está de fato bem-definida.

Injetividade de φ:

Para mostrar que φ é injetiva, vamos mostrar que $\varphi(\chi)$ determina todos os valores de χ. Em outras palavras, vamos mostrar como determinar o valor de $\chi(n)$ para qualquer $n \in \mathbb{Z}$ a partir dos valores de $\chi(n_1), \ldots, \chi(n_k)$.

Seja $\chi \in \mathfrak{X}_q$ e seja $(\omega_1, \ldots, \omega_k) = \varphi(\chi)$. Dado $n \in \mathbb{Z}/\{0\}$, se $(n, q) > 1$, então $\chi(n) = 0$. Se $(n, q) = 1$, seja

$$x = n \pmod{q} \in (\mathbb{Z}/q\mathbb{Z})^\times.$$

Pelo homomorfismo ($\bigstar$), $n \pmod{q}$ corresponde a um elemento de $G_1 \times \cdots \times G_k$ da forma

$$(\xi_1^{t_1}, \ldots, \xi_k^{t_k}) = \underbrace{(\xi_1, 1, \ldots, 1)^{t_1}}_{\text{correspondendo a } x_1} \quad \cdots \quad \underbrace{(1, \ldots, 1, \xi_k)^{t_k}}_{\text{correspondendo a } x_k}.$$

Como ($\bigstar$) é homomorfismo, segue que $(\xi_1^{t_1}, \ldots, \xi_k^{t_k})$ corresponde a $x_1^{t_1} \cdots x_k^{t_k}$. Ou seja, $x = x_1^{t_1} \cdots x_k^{t_k}$. Como

$$x = n \pmod{q}, \quad x_i = n_i \pmod{q},$$

segue que

$$n \equiv n_1^{t_1} \cdots n_k^{t_k} \pmod{q}.$$

Portanto,

$$\begin{aligned} \chi(n) &= \chi(n_1)^{t_1} \cdots \chi(n_k)^{t_k} \\ &= \omega_1^{t_1} \cdots \omega_k^{t_k}, \end{aligned}$$

mostrando que n só depende de $\varphi(\chi) = (\omega_1, \ldots, \omega_k)$.

Sobrejetividade de φ:

Para cada $(\omega_1, \ldots, \omega_k) \in Z$, precisamos construir $\chi \in \mathfrak{X}_q$ tal que $\chi(n_i) = \omega_i$, $i = 1, 2, \ldots, k$.

Defina χ da seguinte maneira:

- Se $(n, q) > 1$, $\chi(n) = 0$.
- Se $(n, q) = 1$, pelo argumento acima, existem $t_1, \ldots, t_k$ tais que

$$n \equiv n_1^{t_1} \cdots n_k^{t_k} \pmod{q}.$$

  Então defina

$$\chi(n) = \omega_1^{t_1} \cdots \omega_k^{t_k}$$

OBS: Os números $t_1, \dots t_k$ não são únicos mas, como veremos, isto não será um problema.

Para ver que χ está bem definida, suponha que $t'_1, \dots, t'_k$ també são tais que

$$n \equiv n_1^{t'_1} \cdots n_k^{t'_k} \pmod{q},$$

Então temos

$$n_1^{t'_1} \cdots n_k^{t'_k} \equiv n_1^{t_1} \cdots n_k^{t_k} \pmod{q}$$

Ou seja,

$$x_1^{t'_1} \cdots x_k^{t'_k} = x_1^{t_1} \cdots x_k^{t_k} \iff x_1^{t_1 - t'_1} \cdots x_k^{t_k - t'_k} = 1.$$

Pela correspondência ($\bigstar$), isto significa que

$$(\xi_1^{t'_1 - t_1}, \xi_2^{t'_2 - t_2}, \dots, \xi_k^{t'_k - t_k}) = (1, \dots, 1)$$

Isto quer dizer que

$$\xi_i^{t'_i - t_i} = 1, \quad i = 1, \dots, k.$$

Como a ordem de ξ_i é m_i, segue que

$$t'_i - t_i = m_i \cdot s_i$$

para algum $s_i \in \mathbb{Z}$. Agora, como ω_i é uma raiz m_i-ésima da unidade,

$$\omega_i^{t'_i - t_i} = 1 \Longrightarrow \omega_i^{t'_i} = \omega_i^{t_i}.$$

De modo que

$$\omega_1^{t'_1} \cdots \omega_k^{t'_k} = \omega_1^{t_1} \cdots \omega_k^{t_k},$$

concluindo a prova de que χ está bem definida.

A construção acima só depende da classe de congruência de $n \pmod{q}$, e por construção $\chi(n) \neq 0 \iff (n, q) = 1$. De modo que as propriedades 1 e 3 da definição de caractere são satisfeitas. Resta mostrar que a definição acima de χ fornece uma função completamente multiplicativa. Para ver que isto, dividimos em dois casos:

- Se $(m, q) > 1$ ou $(n, q) > 1$, segue que $(mn, q) > 1$ e, portanto, $\chi(mn) = 0 = \chi(m)\chi(n)$.
- Se $(m, q) = (n, q) = 1$, basta notar que se

  $$m \equiv n_1^{t_1} \cdots n_k^{t_k} \pmod{q}$$
  $$n \equiv n_1^{l_1} \cdots n_k^{l_k} \pmod{q}$$

  então

  $$mn \equiv n_1^{t_1 + l_1} \cdots n_k^{t_k + l_k} \pmod{q},$$

d modo que

$$\begin{aligned}\omega_1^{t_1+l_1}\cdots\omega_k^{t_k+l_k} &= (\omega_1^{t_1}\cdots\omega_k^{t_k})(\omega_1^{l_1}\cdots\omega_k^{l_k})\\ \Leftrightarrow \chi(mn) &= \chi(m)\chi(n)\end{aligned}$$

Ou seja χ é um caractere e, por construção, $\varphi(\chi) = (\omega_1, \ldots, \omega_k)$. Como as raízes da uniade ω_i podem ser escolhidos arbitrariamente, provamos que φ é sobrejetivo.

Exercício: Mostrar a última parte do teorema: Para todo $a \not\equiv 1 \pmod{q}$, existe $\chi \in \mathfrak{X}_q$ tal que $\chi(a) \neq 1$.