HOJA N°

FECHA

Raíz de la unidad

$$G_n = \{ \omega \in \mathbb{C} : \omega^n = 1 \}$$

Prop) $\omega \in G_n \Rightarrow |\omega| = 1$

$\Rightarrow \omega^{-1} = \bar{\omega} = \omega^{n-1}$

$G_n \cap G_m = G_{(n:m)}$

$G_n \subseteq G_m$ sii $n \mid m$

$(G_n, \cdot)$ grupo abeliano, cíclico.

Def: $\omega \in G_n$ es un generador s. $\{\omega_0, \cdots, \omega_{n-1}\} = G_n$

$\omega_1 = e^{\frac{2\pi i}{n}}$ es generador

$\omega_k = (\omega_1)^k = e^{\frac{2\pi i}{n} \cdot k}$

Obs: hay más generadores

$1 \in G_n$ no es generador

a) $\omega \in G_n$ es Primitiva sii $n = \min\{r \in \mathbb{N} : \omega^r = 1\}$

Teorema: a) $\omega \in G_n$ es Primitiva sii $\omega^m = 1 \quad n \mid m$

b) s. $\omega \in G_n$ primitiva y $j \in \mathbb{N}$

$\Rightarrow \omega^j$ es Primitiva sii $(j : n) = 1$

c) Hay exactamente $\varphi(n)$ raíces n-ésimas Primitivas

Def: $\omega \in G_n$ es una raíz m-ésima Primitiva

si ω es generador de G_n

Dem: $\Leftarrow$) si $n = \min\{r \in \mathbb{N},\ \omega^r = 1\}$ entonces hay que ver que

$G_n \supset \{\omega^0, \dots, \omega^{n-1}\}$ tiene n elementos (todos diferentes) $\forall 0 \le r < s \le n-1$ $\omega^r \neq \omega^s$

Esto ocurre porque si $\omega^r = \omega^s \Rightarrow 1 = \omega^{s-r}$ con $0 < s-r \le n-1$ ABSURDO

$\Rightarrow$) si $\omega \in G_n$ es raíz n-ésima primitiva $\{\omega_0, \dots, \omega^{n-1}\}$

son todos distintos

si $\omega^r = 1$ con $r \in \mathbb{N}$ entonces $r > n-1$ $\Rightarrow$

$\Rightarrow \min\{r \in \mathbb{N},\ \omega^r = 1\} > n-1$

Como $\omega^n = 1 \Rightarrow n = \min\{r \in \mathbb{N},\ \omega^r = 1\}$

$\Rightarrow$) si $\omega \in G_n$ primitiva, sea $n \in \mathbb{Z} / \omega^n = 1 \Rightarrow$

$\Rightarrow m = n \cdot q + r$, $0 \le r < n$ (algoritmo div)

pvq $r = 0$

$1 = \omega^m = \omega^{nq+r} = \omega^{nq} \cdot \omega^r = (\omega^n)^q \cdot \omega^r = 1^q \cdot \omega^r = \omega^r$

$\Leftarrow$) $\omega \in G_n$ / si $\omega^m = 1 \Rightarrow n \mid m$, mejor que ω es primitiva

pvq $\min\{r \in \mathbb{N} : \omega^r = 1\} = n$

si $\omega^r = 1$, $r \in \mathbb{N}$ entonces por hipótesis $n \mid r \Rightarrow$

$\Rightarrow n \le r \Rightarrow$ ningún número $r, (1 < r < n-1) \in \{r \in \mathbb{N} : \omega^r = 1\}$

Como n pertenece entonces $n = \min\{r \in \mathbb{N} : \omega^r = 1\}$

$\Rightarrow$)

2) Sea $\omega \in G_n$ Primitiva y sea $j \in \mathbb{N}$ / ω^j es Primitiva $\Rightarrow$

$\Rightarrow (j : n) = 1$

[illegible]

Supongamos que $(j:n) = d > 1 \Rightarrow \omega^j = \omega^{d \cdot f}$

además $d \mid n \Rightarrow n = d \cdot t \quad (t < n)$

entonces $(\omega^j)^t = \omega^{d \cdot f \cdot t} = \omega^{n \cdot f} = 1^f = 1$

entonces ω^j no es raíz Primitiva $\forall f \; t \in \{r \in \mathbb{N} : (\omega^j)^r = 1\}$ y $t < n$

ABSURDO

$\Leftarrow$) Si $(j:n) = 1 \Rightarrow \omega^j$ es Primitiva

$(j:n) = 1 \Rightarrow 1 = j \cdot k + n \cdot f \Rightarrow \omega = \omega^{jk + n \cdot f} = \omega^{jk}$

$\omega \in \{(\omega^j)^0 ; (\omega^j)^1 ; \dots ; (\omega^j)^{n-1}\}$

entonces $\underbrace{\{\omega^0 ; \dots ; \omega^{n-1}\}}_{\text{"}G_n} \subseteq \underbrace{\{(\omega^j)^0 ; \dots ; (\omega^j)^{n-1}\}}_{G_n}$

$\Downarrow$

$\{(\omega^j)^0 ; \dots ; (\omega^j)^{n-1}\} = G_n$

$\Downarrow$

ω^j es raíz Primitiva

3) Sabemos que $\omega_1 = e^{\frac{2\pi i}{n}}$ es una raíz n-ésima Primitiva

Sabemos que ω_1^j es Primitiva si $(j:n) = 1$ si: $j \in \{\ell \in \mathbb{N} : (\ell:n) = 1\}$

además como $\omega_j^0 = \omega_1^j$ debe ocurrir que $0 \leq j < n$

Entonces $j \in \{\ell \in \mathbb{N} : 1 \leq \ell < n \quad (\ell:n) = 1\}$

Por definición hay $\phi(n)$ elementos en este conjunto

* $\phi(n)$: cantidad de números entre 1 y n coprimos con n

eg) Si P es Primo entonces todo elemento de G_p distinto de 1 es raíz Primitiva

Dem: ya que $G_p = \{\omega_0; \ldots; \omega_{p-1}\}$ con $\omega_\ell = e^{\frac{2\pi i \ell}{p}} = \omega_1^\ell$ y

$(\ell:p) = 1 \Rightarrow \omega_\ell$ es Primitiva

ej) G_{12} las raíces 12-ésimas Primitivas son

$$G_{12} = \{\omega_0; \ldots; \omega_{11}\} = \{(\omega_1)^k \;/\; 0 \leq k < 12\}$$

y $\omega_1 = e^{\frac{2\pi i \ell}{12}}$

Entonces las raíces 12-ésimas Primitivas son $\{(\omega_1)^\ell, (\ell:12)=1, 1 \leq \ell < 12\}$

$\ell = 1, 5, 7, 11$

$$\{\omega_1; \omega_5; \omega_7; \omega_{11}\} = \{\omega_1, \omega_5, \overline{\omega_5}, \overline{\omega_1}\}$$

q) Si ω es raíz n-ésima Primitiva entonces $\overline{\omega} = \omega^{-1}$ tmb es raíz Primitiva

Teorema: 1) $\sum_{\omega \in G_n} \omega = \begin{cases} 0 & n \neq 1 \\ 1 & n = 1 \end{cases}$

2) Si $\omega \in G_n$, ω raiz n-ésima entonces

$$\sum_{k=0}^{n-1} \omega^k = \begin{cases} 0 & \text{si } \omega \neq 1 \\ n & \text{si } \omega = 1 \end{cases}$$

3) $$\prod_{\omega \in G_n} \omega = \begin{cases} -1 & \text{si } n \text{ es Par} \\ +1 & \text{si } n \text{ es impar} \end{cases}$$

Dem: 2) $$\sum_{k=0}^{n-1} \omega^k = \begin{cases} \dfrac{\omega^n - 1}{\omega - 1} & \text{si } \omega \neq 1 \\ n & \text{si } \omega = 1 \end{cases} = \begin{cases} 0 \\ 1 \end{cases}$$

(suma serie geométrica)

1) Sea ω_1 una raíz primitiva de 1

entonces $\sum_{\omega \in G_n} \omega = \sum_{k=0}^{n-1} \omega_1^k = 0$ $n \neq 1$

si $n = 1 \Rightarrow \sum_{G_1} 1 = 1$

3) Si $\omega \in G_n \Rightarrow \bar{\omega} \in G_n$ (las raíces vienen de a pares)

$$\Rightarrow \prod_{\omega \in G_n} \omega = \prod_{\substack{\omega \in G_n \\ \omega \notin \mathbb{R}}} \omega \cdot \prod_{\substack{\omega \in G_n \\ \omega \in \mathbb{R}}} \omega$$

$$= \begin{cases} 1 \cdot -1 = -1 & \text{si } n \text{ es Par} \\ 1 & \text{si } n \text{ es impar} \end{cases}$$

$\omega \neq \bar{\omega}$ si $\mathrm{Im}(\omega) \neq 0$

$\omega \cdot \bar{\omega} = |\omega|^2 = 1$ (en este caso)