Álgebra 1

Práctica 6: Números Complejos, Raíces Primitivas

Patricia Jancsa

Viernes 11/6/2021

Suma de raíces primitivas

Ejemplo

i. Calcular G_6.

$G_6 = \{z \in \mathbb{C} : \omega^6 = 1\}$ entonces

- Módulo: $|\omega|^6 = |1| = 1 \rightarrow |\omega| = 1$
- Argumento: $6\ arg\ \omega = \ arg\ 1 + 2k\pi = 2k\pi : 0 \leq k \leq 5$

$$\Rightarrow arg\ \omega_k = \theta_k = \frac{2k\pi}{6} : 0 \leq k \leq 5$$

$$\Rightarrow \theta_k = 0;\ \frac{\pi}{3};\ \frac{2\pi}{3};\ \pi;\ \frac{4\pi}{3};\ \frac{5\pi}{3}$$

$$\Rightarrow \omega_k = (\cos\theta_k + i\ \mathrm{sen}\theta_k) = e^{\theta_k i} = e^{\frac{k\pi}{3} i} : 0 \leq k \leq 5$$

$$= \left[e^{\frac{\pi}{3} i}\right]^k : 0 \leq k \leq 5$$

Por lo tanto

$$\omega_0 = 1 \qquad \omega_1 = \frac{1}{2} + \frac{\sqrt{3}}{2}\, i$$

$$\omega_2 = -\frac{1}{2} + \frac{\sqrt{3}}{2}\, i \qquad \omega_3 = -1$$

$$\omega_4 = -\frac{1}{2} - \frac{\sqrt{3}}{2} i \qquad \omega_5 = \frac{1}{2} - \frac{\sqrt{3}}{2} i$$

son las 6 soluciones de $z^6 = 1$, que se ubican en el plano como los 6 vértices de un hexágono regular con primer vértice en $z_0 = 1 \in \mathbb{R}^2$.

Suma de raíces primitivas

Ejemplo

ii. Calcular la suma de las raíces primitivas de G_6.

$\Rightarrow$ Todo G_6 es: $\omega_0 = 1$ $\qquad$ $\omega_1 = e^{\frac{\pi}{3}i} = \frac{1}{2} + \frac{\sqrt{3}}{2}\, i \Longrightarrow$ *primitiva*

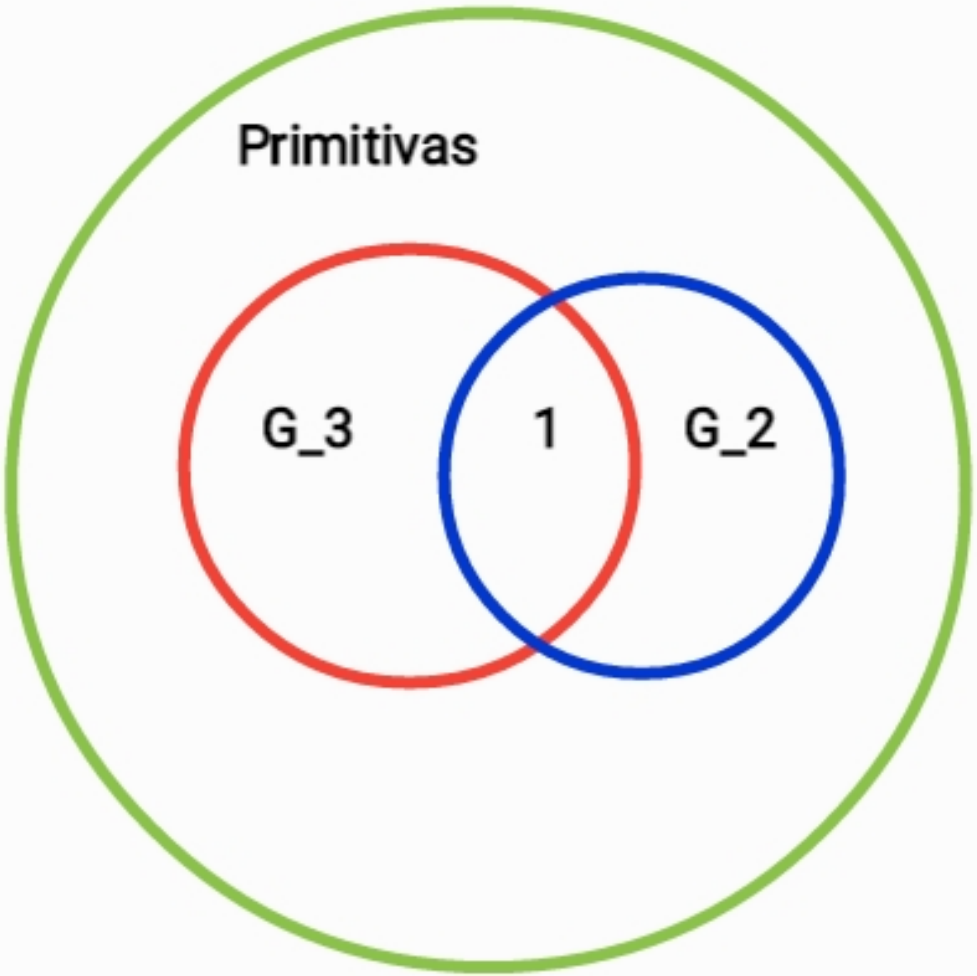
$\omega_2 = e^{\frac{2}{3}\pi i} = -\frac{1}{2} + \frac{\sqrt{3}}{2}\, i$ $\qquad$ $\omega_3 = e^{\pi i} = -1$

$\omega_4 = e^{\frac{4}{3}\pi i} = -\frac{1}{2} - \frac{\sqrt{3}}{2} i$ $\qquad$ $\omega_5 = e^{\frac{5}{3}\pi i} = \frac{1}{2} - \frac{\sqrt{3}}{2} i \Longrightarrow$ *primitiva*

$$\textit{pues } \omega_2^3 = 1 = \omega_4^3, \quad \omega_3^2 = 1$$

$$\Longrightarrow \sum_{\omega \text{ primitivas}} \omega = \frac{1}{2} + \frac{\sqrt{3}}{2} i + \frac{1}{2} - \frac{\sqrt{3}}{2} i = 1 \checkmark$$

G_6



Suma de raíces primitivas

Sin saber explícitamente cuánto vale ω en forma binómica:

$$\Longrightarrow \text{suma de todas } 0 = \sum_{k=0}^{k=5} \omega_k = \sum_{\omega \text{ primitivas}} \omega + \sum_{\omega \text{ no primitivas}} \omega$$

$$= \underbrace{\omega_1 + \omega_5}_{\text{primitivas}} + \underbrace{1 + \omega_2 + \omega_4}_{=0 \in G_3} + \underbrace{\omega_3}_{\in G_2}$$

$$= \underbrace{\omega_1 + \omega_5}_{\text{primitivas}} + \underbrace{1 + \omega_2 + \omega_4}_{=0 \in G_3} + \underbrace{1 + \omega_3}_{=0 \in G_2} - 1$$

$$\Longrightarrow \sum_{\omega \text{ primitivas}} \omega = +1 \checkmark$$

Propiedades de G_n

$$G_n = \left\{ \omega_k = (\cos\theta_k + i\,\mathrm{sen}\theta_k) = e^{\theta_k i} = e^{\frac{2k\pi}{n} i} : 0 \leq k \leq n-1 \right\}$$

- G_n es grupo abeliano con el producto:

$$z, w \in G_n \Rightarrow z \cdot w \in G_n;\ \textit{elemento neutro es } z_0 = 1 \in G_n$$

- Todo $\omega \in G_n$ tiene inverso en G_n dado por $\omega^{-1} = \overline{\omega} = \omega^{n-1}$

$$\textit{Si } \omega = \omega_k = e^{\frac{2k\pi}{n} i} \Rightarrow \omega^{-1} = \omega_{n-k} = e^{\frac{2(n-k)\pi}{n} i}$$

- Si $d = (k : n)$ y $n = \ell \cdot d \Rightarrow (\omega_k)^{\ell} = 1$ pues
$d|k \Rightarrow k = d' \cdot d \Rightarrow k \cdot \ell = d' d \cdot \ell = d' n \equiv 0 \ mod\ n$
- $n|m \Leftrightarrow G_n \subset G_m$
- $m \equiv m' \ mod\ n \Leftrightarrow \omega^m = \omega^{m'}$.
- $\omega = -1 \in G_n \Longleftrightarrow n$ es par

Propiedades de G_6

$$G_6 = \left\{ \omega_k = (\cos\theta_k + i\,\mathrm{sen}\theta_k) = e^{\theta_k i} = e^{\frac{2k\pi}{n} i} : 0 \leq k \leq 5 \right\}$$

- G_6 es grupo abeliano con el producto:

  $z, w \in G_6 \Rightarrow z \cdot w \in G_6$; *elemento neutro es* $z_0 = 1 \in G_6$

- Todo $\omega \in G_6$ tiene inverso en G_6 dado por

$$\omega_k = e^{\frac{2k\pi}{n} i} \Rightarrow \text{ su inverso es } \omega_{6-k} = e^{\frac{(6-k)\pi}{3} i}$$

- $m \equiv m' \ mod\ 6 \Rightarrow \omega^m = \omega^{m'}$.
- $(2:6) = 2 = (4:6) \Rightarrow (\omega_2)^3 = 1 = (\omega_4)^3$:

$$\omega_2 = e^{\frac{2\pi}{3} i} \Rightarrow (\omega_2)^3 = \left(e^{\frac{2\pi}{3} i}\right)^3 = e^{2\pi i} = 1 = e^{4\pi i} = (\omega_4)^3$$

- $\omega_3 = -1 \in G_6$ pues $n = 6$ es par $\Rightarrow (\omega_3)^6 = (-1)^2 = 1$.

Inversos en G_6

- Todo $\omega \in G_6$ tiene inverso en G_6 dado por

$$\omega_k = e^{\frac{2k\pi}{6} i} \Rightarrow \text{ su inverso es } \omega_{6-k} = e^{\frac{(6-k)\pi}{3} i}$$

$$\omega_k \cdot \omega_{6-k} = e^{\frac{k\pi}{3} i} \cdot e^{\frac{(6-k)\pi}{3} i} = 1$$

Es decir
- $\omega_0 \cdot \omega_0 = 1$
- $\omega_1 \cdot \omega_5 = e^{\frac{\pi}{3} i} \cdot e^{\frac{5\pi}{3} i} = e^{\frac{(1+5)\pi}{3} i} = 1$
- $\omega_2 \cdot \omega_4 = e^{\frac{2\pi}{3} i} \cdot e^{\frac{4\pi}{3} i} = e^{\frac{(2+4)\pi}{3} i} = 1$
- $\omega_3 \cdot \omega_3 = (-1)(-1) = 1$

Ej. 1.

Calcular la suma de las raíces primitivas de G_{16}

$$G_{16} = \left\{ \omega_k = (\cos\theta_k + i\,\mathrm{sen}\theta_k) = e^{\frac{2k\pi}{16} i} \right\} = \left\{ \omega_k = e^{\frac{k\pi}{8} i} : 0 \leq k \leq 15 \right\}$$

No primitivas :

$$\omega_0 = 1$$
$$\omega_2 = e^{\frac{2}{8}\pi i}$$
$$\omega_4 = e^{\frac{4}{8}\pi i}$$
$$\omega_6 = e^{\frac{6}{8}\pi i}$$
$$\omega_8 = e^{\frac{8}{8}\pi i} = -1$$
$$\omega_{10} = e^{\frac{10}{8}\pi i}$$
$$\omega_{12} = e^{\frac{12}{8}\pi i}$$
$$\omega_{14} = e^{\frac{14}{8}\pi i}$$

Primitivas

$$\omega_1 = e^{\frac{\pi}{8} i}$$
$$\omega_3 = e^{\frac{3}{8}\pi i}$$
$$\omega_5 = e^{\frac{5}{8}\pi i}$$
$$\omega_7 = e^{\frac{7}{8}\pi i}$$
$$\omega_9 = e^{\frac{9}{8}\pi i}$$
$$\omega_{11} = e^{\frac{11}{8}\pi i}$$
$$\omega_{13} = e^{\frac{13}{8}\pi i}$$
$$\omega_{15} = e^{\frac{15}{8}\pi i}$$

- *Si k par*, $k = 2d \Longrightarrow (\omega_{2d})^8 = \left[e^{\frac{2d}{8}\pi i}\right]^8 = e^{2d\pi i} = 1$

$\Longrightarrow$ *Toda* ω_{2d} *es de orden* $\leq 8 < 16 \Longrightarrow$ *Toda* $\omega_{2d} \in G_8$

$\Longrightarrow$ no es primitiva

- Sea *k impar*, $k = 2d + 1 \in \mathbb{N}$ y supongamos $1 = \left[e^{\frac{2d+1}{8}\pi i}\right]^m$, comparemos los argumentos:

$$\frac{(2d+1)m}{8}\pi = 2\ell\pi \Longrightarrow (2d+1)m = 16\ell \Longrightarrow \underbrace{(2d+1)}_{\textit{impar}} m \equiv 0\,(16)$$

$\Longrightarrow m \equiv 0\ mod 16$ *pues* $(2d + 1 : 16) = 1$

$\Longrightarrow 16|m \Longrightarrow$ es primitiva

$$\Longrightarrow \text{suma de todas } 0 = \sum_{k=0}^{k=15} \omega_k = \sum_{\omega \text{ primitivas}} \omega + \sum_{\omega \text{ no primitivas}} \omega$$

$$= \underbrace{\omega_1 + \omega_3 + \omega_5 + \omega_7 + \omega_9 + \omega_{11} + \omega_{13} + \omega_{15}}_{\text{primitivas}}$$

$$+ \underbrace{1 + \omega_2 + \omega_4 + \omega_6 + \omega_8 + \omega_{10} + \omega_{12} + \omega_{14}}_{=0 \in G_8}$$

$$\Longrightarrow \sum_{\omega \text{ primitivas}} \omega = 0 \checkmark$$

Ej 2.

i. Calcular las raíces primitivas de G_{42}.
ii. ¿Es cierto que $G_6 \subset G_{42}$? Describirlo.
iii. Calcular la suma de las raíces primitivas de G_{42}.
iv. Considerar en G_{42} la relación dada por

$$a \sim b \iff \textit{existe } z \in G_6 : a = z \cdot b$$

a) Probar que la relación es de equivalencia.
b) Calcular la cantidad de clases de equivalencia y describirlas.

$$G_{42} = \{z \in \mathbb{C} : z^{42} = 1\} = \{1,\ e^{\frac{2k}{42}\pi i} :\ 1 \leq k \leq 41\}$$

$$= \{e^{\frac{k}{21}\pi i} :\ 0 \leq k \leq 41\}$$

$$= \{\omega^k :\ 0 \leq k \leq 41,\ \omega \textit{ una primitiva fija}\}$$

Primitivas de G_{42}

$\omega = e^{\frac{k}{21}\pi i}$ es primitiva $\Leftrightarrow (k : 42) = 1$:

$$Si\ 1 = \omega^n = \left[e^{\frac{k}{21}\pi i}\right]^n = e^{\frac{kn}{21}\pi i} \Rightarrow \frac{kn}{21}\pi = 2\ell\pi \Rightarrow kn = 42 \cdot \ell$$

$$Si\ (k : 42) = 1 \Rightarrow 42|n \Rightarrow \omega = e^{\frac{k}{21}\pi i}\ es\ primitiva$$

Recíprocamente, si $\omega = e^{\frac{k}{21}\pi i}$ es primitiva y fuera

$$1 < d = (n : k) \Rightarrow \begin{cases} n = dd' \\ k = dk' \end{cases} \Rightarrow 1 \leq d' < n$$

$$\Rightarrow (\omega_k)^{d'} = (\omega_k)^{\frac{n}{d}} = (\omega_1)^{\frac{nk}{d}} = (\omega_1)^{nk'} = 1,\ absurdo \Rightarrow (42 : k) = 1$$

$\Rightarrow$ *Todas las primitivas son* $G_{42}^* = \{\omega^k : \ (k:42) = 1, \ \omega \ \textit{primitiva}\}$

Cantidad de primitivas $=$ cantidad de coprimos
$= 1 \cdot 2 \cdot 6 = \phi(2)\phi(3)\phi(7) = 12$:

$$12 \ \textit{coprimos} = \{1, 5, 11, 13, 17, 19, 23, 25, 29, 31, 37, 41\}$$

$$30 \ \textit{no comprimos} = \{2, 3, 4, 6, 7, 8, 9, 10, 12, 14, 15, 16, 18, 20, 21,$$
$$22, 24, 26, 27, 28, 30, 32, 33, 34, 35, 36, 38, 39, 40, 42\}$$

$$\Longrightarrow \mathcal{P}(G_{42}) = G_{42}^* = \left\{ e^{\frac{1}{21}\pi i}, \ e^{\frac{5}{21}\pi i}, \ e^{\frac{11}{21}\pi i}, \ e^{\frac{13}{21}\pi i}, \ e^{\frac{17}{21}\pi i}, \ e^{\frac{19}{21}\pi i}, \ e^{\frac{23}{21}\pi i}, \right.$$
$$\left. e^{\frac{25}{21}\pi i}, \ e^{\frac{29}{21}\pi i}, \ e^{\frac{31}{21}\pi i}, \ e^{\frac{37}{21}\pi i}, \ e^{\frac{41}{21}\pi i} \right\} \checkmark$$

ii. Las no primitivas son: $\{\omega^k : (k:42) > 1,\ \omega \textit{ primitiva}\}$

Dentro de G_{42} se tiene en particular: $e^{\frac{7d}{21}\pi i} \Leftarrow$ no primitivas

$$\Rightarrow \left[e^{\frac{7d}{21}\pi i}\right]^6 = e^{\frac{7\cdot 6\cdot d}{21}\pi i} = e^{2\cdot\pi i} = 1 \Rightarrow e^{\frac{7d}{21}\pi i} \in G_6$$

$$\Rightarrow G_6 = \{1,\ e^{\frac{7}{21}\pi i},\ e^{\frac{14}{21}\pi i},\ e^{\frac{21}{21}\pi i},\ e^{\frac{28}{21}\pi i},\ e^{\frac{35}{21}\pi i}\}$$

$$= \{1,\ e^{\frac{1}{3}\pi i},\ e^{\frac{2}{3}\pi i},\ e^{\pi i} = -1,\ e^{\frac{4}{3}\pi i},\ e^{\frac{5}{3}\pi i}\} \subset G_{42} \checkmark$$

Más aún, para cada $\ell \in \mathbb{N}$:

$$\ell | 42 \Leftrightarrow G_\ell \subset G_{42}$$

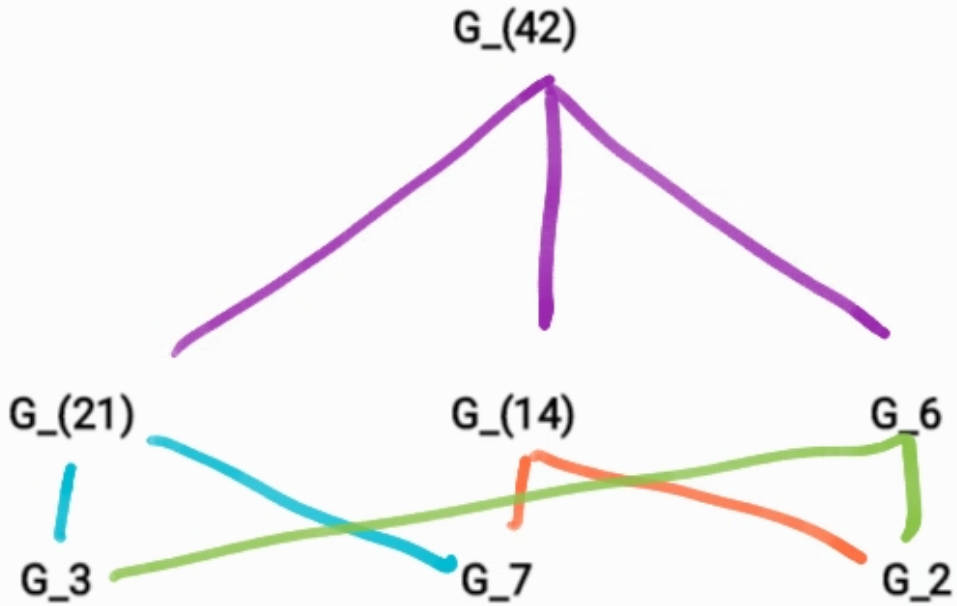
Hay $2 \cdot 2 \cdot 2 = 8$ divisores de 42 $\Rightarrow$ sólo 6 son propios

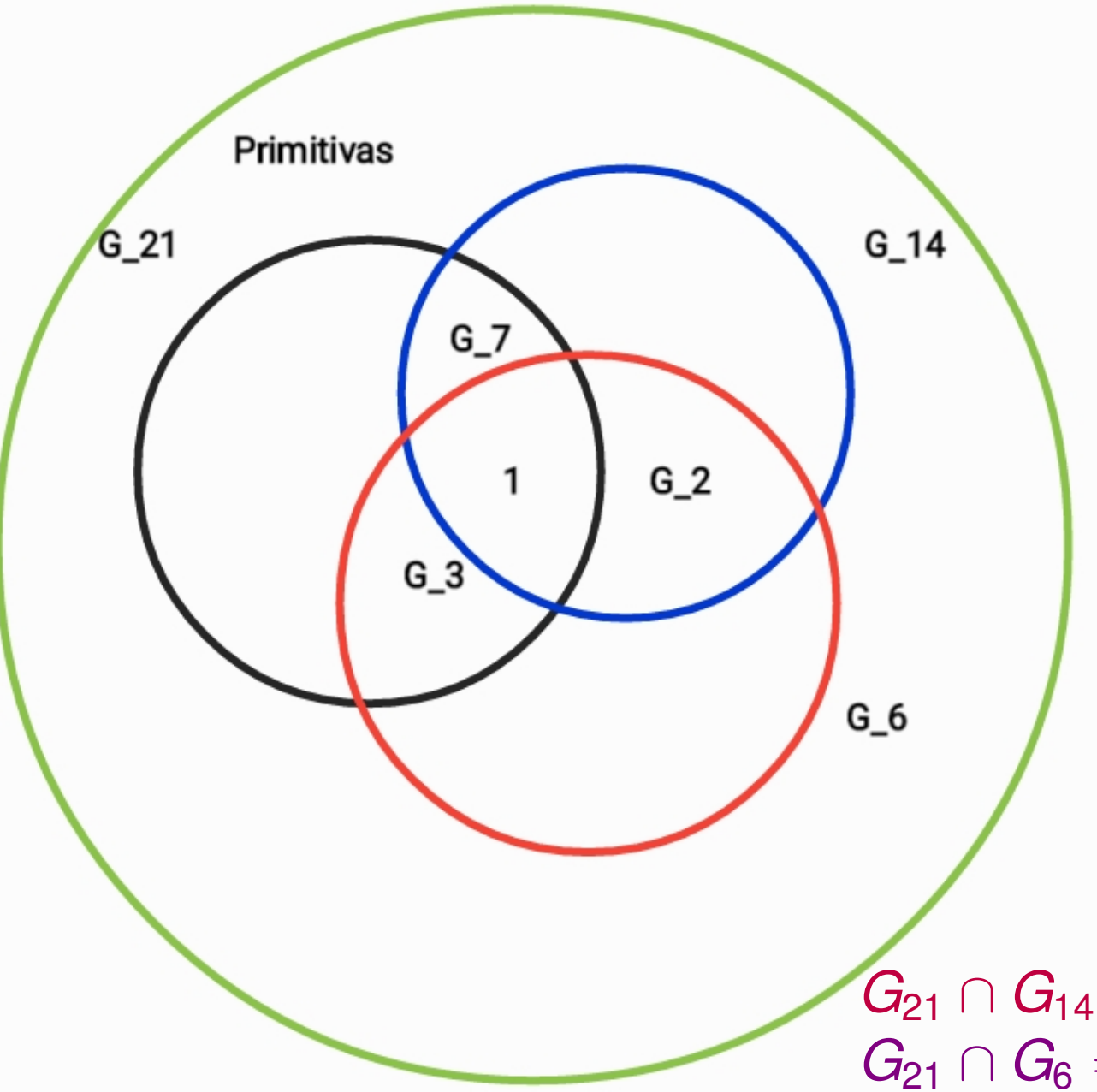
$$\Rightarrow \quad G_2, \quad G_3, \quad G_6, \quad G_7, \quad G_{14}, \quad G_{21} \subset G_{42}$$

Diagrama de Hasse

iii. $42 = 2 \cdot 3 \cdot 7$

$$\mathcal{D}_+(42) = \{1, 2, 3, 6, 7, 14, 21, 42\}$$





$$G_{21} \cap G_{14} = G_{mcd(21:14)} = G_7,$$
$$G_{21} \cap G_6 = G_{mcd(21:6)} = G_3,$$
$$G_{14} \cap G_6 = G_{mcd(14:6)} = G_2$$

Suma de raíces primitivas

Atención: $G_{21} \cap G_{14} = G_{mcd(21:14)} = G_7$,
$G_{21} \cap G_6 = G_{mcd(21:6)} = G_3$,
$G_{14} \cap G_6 = G_{mcd(14:6)} = G_2$

$$\Longrightarrow \text{suma de todas } = 0 \; = \sum_{k=0}^{k=41} \omega_k = \sum_{\omega \text{ primitivas}} \omega + \sum_{\omega \text{ no primitivas}} \omega$$

$$= \sum_{\omega \text{ primitivas}} \omega + \sum_{\omega \in G_{21}} \omega + \sum_{\omega \in G_{14}} \omega + \sum_{\omega \in G_6} \omega$$

$$- \sum_{\omega \in G_7} \omega - \sum_{\omega \in G_3} \omega - \sum_{\omega \in G_2} \omega + \sum_{\omega = 1 \in G_2 \cap G_3 \cap G_7} \omega = 1$$

$$\Longrightarrow \sum_{\omega \text{ primitivas}} \omega = -1 \; \checkmark$$

La relación es de equivalencia

iv. Sea en G_{42} la relación:

$$a \sim b \iff \text{existe } z \in G_6 : a = z \cdot b$$

- Reflexividad: $a \sim a$ pues

$$a = 1a : 1 \in G_6$$

- Simetría: sean $a, b \in G_{42} : a \sim b$ entonces existe $z \in G_6 : a = z \cdot b$, luego

$$b = z^{-1}a \text{ con } z^{-1} \in G_6 \text{ pues } G_6 \text{ es grupo}$$

G_6 es grupo abeliano con el producto
$\Longrightarrow$ todo elemento tiene inverso multiplicativo dentro de G_6.

Transitividad

- Transitividad: Sup. $a \sim b$ y $b \sim c$ entonces existen $\omega, z \in G_6$: $a = \omega \cdot b$ y $b = z \cdot c$, luego

$$a = \omega \cdot b = \omega \cdot z \cdot c = (\omega \cdot z) \cdot c \text{ con } \omega \cdot z \in G_6 \text{ grupo} \Rightarrow a \sim c$$

Por lo tanto,

la relacion es de equivalencia ✓

Clases de equivalencia: $\omega,\ z \in G_6 \Rightarrow \omega \sim z$ pues

$$\omega = \omega(z^{-1}z) = (\omega z^{-1})z \text{ donde } \omega z^{-1} \in G_6$$

¿Qué otros se relacionan entre sí?

Cantidad de clases de equivalencia

$$G_{42} = \{z \in \mathbb{C} : z^{42} = 1\}$$
$$= \{1,\ \omega^k :\ 1 \leq k \leq 41,\ \omega \textit{ una primitiva fija}\}$$

Notar que

$$\omega \sim \omega^8 \sim \omega^{15} \sim \omega^{22} \sim \omega^{29} \sim \omega^{36}$$

pues

$$\omega^8 = \omega^7 \cdot \omega \quad \textit{con} \quad (\omega^7)^6 = \omega^{42} = 1 \Rightarrow \omega^7 \in G_6$$
$$\Rightarrow \omega \sim \omega^8$$

Afirmación:

$$\ell \equiv k \textit{ mod } 7 \iff \omega^\ell \sim \omega^k \textit{ en } G_{42}$$

Clases de equivalencia

$$\ell \equiv k \ mod\ 7 \iff \omega^{\ell} \sim \omega^{k} \ en\ G_{42}$$

Dem: $\Longrightarrow$ Sup $\ell - k = 7q$ entonces $\omega^{\ell} = \omega^{\ell-k}\omega^{k}$ *con* $\omega^{\ell-k} \in G_6$

$$es\ decir,\ \omega^{\ell-k} = \omega^{7q} =: z \in G_6 \Rightarrow \omega^{\ell} = z \cdot \omega^{k}$$

$$\Rightarrow \omega^{\ell} \sim \omega^{k}$$

$\Longleftarrow$ Sup $\omega^{\ell} \sim \omega^{k}$ entonces existe $z \in G_6 : \omega^{\ell} = z\omega^{k}$

$$\omega^{\ell-k} = \omega^{\ell}\omega^{-k} = z\omega^{k}\omega^{-k} = z \Rightarrow \omega^{\ell-k} = z \in G_6$$

$$\Rightarrow 1 = (\omega^{\ell-k})^6 = \omega^{(\ell-k)6}$$

$$Pero\ \omega\ es\ primitiva\ en\ G_{42} \Rightarrow 42|(\ell-k)6 \Rightarrow (\ell-k)6 = 42q$$

$$\Rightarrow \ell - k = 7q: \quad q \in \mathbb{Z} \Rightarrow \ell - k \equiv 0\ mod\ 7$$

Por lo tanto, hay una biyección:

Cantidad de clases de equivalencia $\leftrightarrow$ restos módulo 7

$\Rightarrow$ hay 7 clases de equivalencia y cada clase tiene 6 elementos

Clases de equivalencia

$$C_{\overline{0}} : 1 \sim \omega^7 \sim \omega^{14} \sim \omega^{21} \sim \omega^{28} \sim \omega^{35}$$

$$C_{\overline{1}} : \omega \sim \omega^8 \sim \omega^{15} \sim \omega^{22} \sim \omega^{29} \sim \omega^{36}$$

$$C_{\overline{2}} : \omega^2 \sim \omega^9 \sim \omega^{16} \sim \omega^{23} \sim \omega^{30} \sim \omega^{37}$$

$$C_{\overline{3}} : \omega^3 \sim \omega^{10} \sim \omega^{17} \sim \omega^{24} \sim \omega^{31} \sim \omega^{38}$$

$$C_{\overline{4}} : \omega^4 \sim \omega^{11} \sim \omega^{18} \sim \omega^{25} \sim \omega^{32} \sim \omega^{39}$$

$$C_{\overline{5}} : \omega^5 \sim \omega^{12} \sim \omega^{19} \sim \omega^{26} \sim \omega^{33} \sim \omega^{40}$$

Ej. 3.

Sea $\omega \in G_{70}^*$. Hallar los $n \in \mathbb{N} : \bar{\omega}^{16765-217n} = 1$.

Solución: Sabemos que $\omega \in G_{70}$ primitiva:

- $1 = |\omega|^2 = \bar{\omega}\omega \Rightarrow \bar{\omega} = \omega^{-1}$
- $\omega^{70} = 1, \quad \omega^k \neq 1 \; \forall 1 \leq k \leq 69$
- $\omega^k = 1 \Leftrightarrow k \equiv 0 \; mod \; 70$
- $\omega^{35} = -1$

pues $1 = \omega^{70} = (\underbrace{\omega^{35}}_{:=z})^2 =: z^2 \Longrightarrow z = \pm 1$ pero no puede ser 1

$$\Longrightarrow \omega^{35} = -1$$

Estudiemos el exponente módulo $70 = 2 \cdot 5 \cdot 7$:

$$16765 = 14000 + 2765 = 14000 + 2800 - 35 \equiv -35 \ mod\ 70$$

$$\Rightarrow 1 = \bar{\omega}^{16765-217n} = \omega^{-16765+217n} = \omega^{-16765} \cdot \omega^{\overbrace{217n}^{\equiv 7n}} = \omega^{35+7n}$$

$$\Leftrightarrow 7n + 35 \equiv 0 \ mod\ 70$$

$$\Leftrightarrow 7n \equiv 35 \ mod\ 70 \Leftrightarrow 70 \cdot \ell = 7n - 35 \Leftrightarrow 10 \cdot \ell = n - 5$$

$$\Leftrightarrow n - 5 \equiv 0 \ mod\ 10$$

$$\Longrightarrow \text{Solución} := \{n = 10\ell + 5 : \ell \geq 0,\ n \in \mathbb{Z}\} \checkmark$$

Ej. 4.

Sea $\omega \in G_{26}*$. Hallar los $n \in \mathbb{N} : \omega^{5^n+8} = -\sum_{k=0}^{1820} \bar{\omega}^{15k}$

Solución: • $1820 = 26 \cdot 70$

• $\omega \in G_{26}* \Rightarrow u := \bar{\omega}^{15} = \omega^{26-15} = \omega^{11} \neq 1$

$$\Rightarrow \sum_{k=0}^{1820} \bar{\omega}^{15k} = \sum_{k=0}^{1820} u^k = \frac{1-u^{1821}}{1-u} = \frac{1-u^{1820}\cdot u}{1-u} = \frac{1-u}{1-u} = 1$$

Luego, la condición es $\omega^{5^n+8} = -1 = \omega^{13} \Leftrightarrow \omega^{5^n+8-13} = 1$

$$\Leftrightarrow \omega^{5^n-5} = 1$$

$$\Leftrightarrow 5^n - 5 \equiv 0 \ mod\ 26$$

Por lo tanto, $\omega^{5^n+8} = -1 = \omega^{13} \Leftrightarrow \omega^{5^n+8-13} = 1$

$$\Leftrightarrow 5^n - 5 \equiv 0 \ mod\ 26$$

$$\Leftrightarrow 5^n \equiv 5 \ mod\ 26 \Leftrightarrow -5^{n+1} \equiv -5^2 \equiv 1 \Leftrightarrow 5^{n+3} \equiv 1 \ mod\ 26$$

$$\Leftrightarrow \begin{cases} 5^{n+3} & \equiv 1 \ mod\ 13 \\ 5^{n+3} & \equiv 1 \ mod\ 2 \Longrightarrow vale\ \forall\ n \checkmark \end{cases}$$

Teorema y colorarios de Fermat: $(a : p) = 1$

- $a^{p-1} \equiv 1 \ mod\ p$
- $r \equiv 0 \ mod\ p-1 \Rightarrow a^r \equiv 1 \ mod\ p \ \ \forall (a : p) = 1,\ a \in \mathbb{Z}$

$$\Rightarrow n + 3 \equiv 0 \ \Rightarrow n \equiv 9 \ mod\ 12 \ sirve$$

pero puede haber más soluciones

$5^{n+3} \equiv 1 \mod 13$

En efecto, vimos que

$$5^2 = 25 \equiv -1 \ mod\ 13 \Rightarrow 5^4 \equiv (-1)^2 \equiv 1 \ mod\ 13$$

Por lo tanto, como no hay otra potencia menor que sea solución, la ecuación tiene única solución módulo 4:

$$5^{n+3} \equiv 1 \mod 13 \Leftrightarrow n+3 \equiv 0 \mod 4 \Leftrightarrow n \equiv 1 \ mod\ 4$$

$$Soluciones = \{n = 4q + 1 : q \in \mathbb{Z}\} \checkmark$$

Práctica 7: Polinomios

Introducción

$$\mathbb{K} \textit{ cuerpo} \Rightarrow \mathbb{K} = \mathbb{C},\ \mathbb{R},\ \mathbb{Q},\ \mathbb{Z}_p : p \textit{ primo}$$

$$\Rightarrow \mathbb{K}[x] \text{ anillo conmutativo íntegro:}$$

$$f \cdot g = 0 \Rightarrow f = 0 \text{ ó bien } g = 0 \textit{ en } \mathbb{K}[x]$$

Ejemplo: $f = 2x^5 + 1 \in \mathbb{R}[x]$, $f \in \mathbb{Q}[x]$ ó en $\mathbb{C}[x]$.
grado de f es $gr(f) = 5$, el coeficiente principal es $a_5 = 2$

Si $a_n = 1 \Rightarrow f$ se dice mónico.

Ej. 5.

Determinar el grado, el coeficiente principal y el coeficiente de x^{20}, si $f = (2x^5 + 1)^9 - (2^{\frac{3}{5}}x^3 - 1)^{15} \in \mathbb{R}[x]$

Solución:

$$f = (2x^5 + 1)^9 - (2^{\frac{3}{5}}x^3 - 1)^{15}$$

$$= \sum_{k=0}^{9} \binom{9}{k} (2x^5)^k - \sum_{\ell=0}^{15} \binom{15}{\ell} (2^{\frac{3}{5}}x^3)^{\ell} (-1)^{15-\ell}$$

$$= (2x^5)^9 + \sum_{k=0}^{8} \binom{9}{k} 2^k x^{5k} - (2^{\frac{3}{5}}x^3)^{15} - \sum_{\ell=0}^{14} \binom{15}{\ell} 2^{\frac{3}{5}\ell} x^{3\ell} (-1)^{15-\ell}$$

$$= 2^9 x^{45} + \sum_{k=0}^{8} \binom{9}{k} 2^k x^{5k} - 2^9 x^{45} - \sum_{\ell=0}^{14} \binom{15}{\ell} 2^{\frac{3}{5}\ell} x^{3\ell} (-1)^{15-\ell}$$

$$= \cancel{2^9 x^{45}} + \sum_{k=0}^{8} \binom{9}{k} 2^k x^{5k} - \cancel{2^9 x^{45}} - \sum_{\ell=0}^{14} \binom{15}{\ell} 2^{\frac{3}{5}\ell} x^{3\ell} (-1)^{15-\ell}$$

$$= 9 \cdot 2^8 x^{40} + \sum_{k=0}^{7} \binom{9}{k} 2^k x^{5k} + 15 \cdot 2^{\frac{3}{5}14} x^{42} - \sum_{\ell=0}^{13} \binom{15}{\ell} 2^{\frac{3}{5}\ell} x^{3\ell} (-1)^{15-\ell}$$

$\Longrightarrow$ grado $(f) = 42$ y el coeficiente principal es

$$a_{42} = +15 \cdot 2^{\frac{42}{5}}$$

Notar que el grado de la suma verifica:

$$gr(g - h) \leq \ Max\{gr(g),\ gr(h)\}$$