Para cada $n \in \mathbb{N}$ está definido en $\mathbb{C}$ el conjunto

$$G_n = \{x \mid x^n = 1\}$$

Proposición

Para todo $n \in \mathbb{N}, G_n$, con el producto ordinarioen $\mathbb{C}$ es un grupo.

Demostración

Notemos que G_n es no vacío, pues $1^n = 1$ y por tanto $1 \in G_n$ Ahora sean $w, z \in G_n$. Entonces $w^n = z^n = 1$. Por lo tanto:

$$(wz)^n = w^n z^n = 1 \cdot 1 = 1$$

Es decir: $zw \in G_n$, de modo que el producto es un operación binaria sobre G_n, la cual es asociativa (por tratarse del producto ordinario sobre $\mathbb{C}$.

Ahora resta verificar que todo elemento de G_n es inversible. Sea $w \in G_n$. Como $w^n = 1$, entonces $w \neq 0$ y por lo tanto existe en $\mathbb{C}$ su inverso, u^{-1}. Para ver que $w^{-1} \in G_n$, notamos que:

$$1 = 1^n = (ww^{-1})^n = w^n(w^{-1})^n = (w^{-1})^n$$

Lo cual muestra que $w^{-1} \in G_n$.

Proposición

G_n es un grupo finito de orden n.

Como $w \in G_n \iff X^n - 1 = 0$, entonces hay a lo sumo n elementos en G_n. Para ver que son exactamente n se puede usar el criterio del *derivado*.

$$(X^n - 1)' = nX^{n-1}$$

Y está claro que la única raíz del derivado es 0, pero $0 \notin G_n$. Y el criterio afirma que si un polinomio tiene una raíz múltiple, entonces ésta es tanto raiz del polinomio como del derivado.

Sea

$$w_k = \cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n}$$

Entonces

(i) $w_k \in G_n$
(ii) $w_k = w_l \iff n|k-l$ (o sea si y sólo si $k \equiv l(n)$)

Proposición

$$G_n = \{w_0, w_1, \ldots, w_{n-1}\}$$

Proposición

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

Prueba. $G_n \cap G_m \subset G_{(n:m)}$. Sea $z \in G_n \cap G_m$. Luego $x^n = x^m = 1$. Además, existen s y t tales que $(n : m) = sn + tm$. Entonces:

$$z^{(n:m)} = z^{sn+tm} = z^{sn} z^{tm} = (z^n)^s (z^m)^t = 1^s 1^t = 1$$

Prueba $G_{(n:m)} \subset G_n \cap G_m$.

$(n : m)|n$. Entonces $z^n = z^{(n:m)k} = (z^{(n:m)})^k = 1^k = 1$ (Y análogamente para m).

Corolario

$$G_n \subset G_m \iff n|m$$

Demostración. $G_n \subset G_m \iff G_n \cap G_m = G_n \iff n = (n : m) \iff n|m$

Aplicación

$$X^n - 1 \mid X^m - 1 \iff n \mid m$$

Proposición

Sea G un grupo finito. Entonces, para todo $x \in G$ existe $j \in \mathbb{N}$ tal que $x^j = 1$.

Proposición

Definición (Orden de x)

Sea G un grupo finito. Sea $x \in G$. Se denomina *orden de* x al menor $j \in \mathbb{N}$ tal que $x^j = 1$. Notación escribiremos $ord(x)$ para denotar el orden de x.

Subgrupos

Sean G un grupo, $H \subset G$.

Definición (Subgrupo)

H es un *subgrupo* de G si: (i) $H \neq \emptyset$ (ii) $x, y \in H \rightarrow x \cdot y \in H$ (iii) $x \in H \rightarrow x^{-1} \in H$

Proposición

Sea G un grupo finito y sea $x \in G, ord(x) = n$ Entonces el subconjunto $H = \{1, x, \ldots, x^{n-1}\}$ de G es un subgrupo de G de orden n (?). Diremos además que H es el *grupo cíclico generado* por x en G, y lo notaremos $\langle x \rangle$

Definición.

Diremos que un grupo finito es *cíclico* si existe $x \in G : G = \langle x \rangle$.

Proposición

Sea $x \in G_n$. Entonces, si $ord(x) = k$, luego (i) $\langle x \rangle = G_k$ (ii) $k|n$.

Demostración (i). Toda potencia de x es raíz *k-ésima* de la unidad. Además, como $\langle x \rangle = k$, entonces es G_k.

Proposición

Sea p primo y $n \in \mathbb{N}$. Entonces G_{p^n} es cíclico.

Demostración En virtud de lo anterior teníamos que

$$G_p \subset G_{p^2} \subset \cdots \subset G_{p^{n-1}} \subset G_{p^n}$$

Sea $x \in G_{p^n}, x \notin G^{p^{n-1}}$. Sea $ord(x) = k$. Entonces x genera un subgrupo G_k. Como $G_k \subset G_{p^n}$, $k|p^n$. Es decir (como p es primo) $k = p^j, 0 \geq j \geq n$.