***módulo 2*:**

2.1.- SUBGRUPOS

Este capitulo entrega las herramientas necesarias para determinar cuándo estamos en presencia de un *Subgrupo*, a través del "*Criterio para subgrupo"*.

Estudiaremos también cuando un grupo o subgrupo es cíclico, lo que nos hace destacar que existen grupos que sin necesidad de ser cíclicos sus subgrupos si lo son o algunos de ellos. Aprenderemos también a determinar el orden de cualquier grupo y de sus elementos.

Definición 1: Dado $(G,*)$ un grupo y H un subconjunto no vacío de G, diremos que $(H,*)$ es un subgrupo de $(G,*)$, si y solo si, $*: H\times H \to H$ satisface las propiedades de grupo.

2.1.1.- Notamos del ejercicio sobre el grupo geométrico de las transformaciones de un polígono regular que lo dejan invariante como tal, es decir $(\tau_\Delta, \cdot)$ que sus ***subgrupos propios*** son los siguientes:

- $(H_1 = \{ R_0, R_1, R_2\}, \cdot)$
- $(H_2 = \{R_0, S_1\}, \cdot)$
- $(H_3 = \{ R_0, S_2\}, \cdot)$
- $(H_4 = \{ R_0, S_3\}, \cdot)$

Eduardo Cabrera de Arrizabalaga (profesor guía), Yesenia Briceño, Katherin Lara & Carolina Macaya (tesistas 2007)

2.1.2.- Los ***subgrupos triviales*** de un grupo son dos; el que contiene sólo al neutro del grupo y el grupo mismo. Del ejemplo del grupo $(\tau_\Delta, \cdot)$, podemos decir que los siguientes son sus subgrupos triviales:

- $H_5 = (\{R_0\}, \cdot)$
- $H_6 = (\tau_\Delta, \cdot)$

Cabe destacar que además los subgrupos propios de $(\tau_\Delta, \cdot)$ son abelianos en cambio $(\tau_\Delta, \cdot)$ no lo es.

2.2.- Grupos y Subgrupos Cíclicos

Definición 2: Un grupo $(G,*)$ se dice Cíclico si existe un elemento $g \in G$ tal que para cualquier elemento $x \in G$, existe un entero k tal que $x = g^k$. En tal caso $(G,*)$ es el grupo cíclico generado por g, y a su vez, g se llama generador del grupo $(G,*)$, y se denota por $G = \langle g \rangle$.

Los subgrupos propios de $(\tau_\Delta, \cdot)$ son grupos cíclicos y abelianos, de ellos podemos decir que:

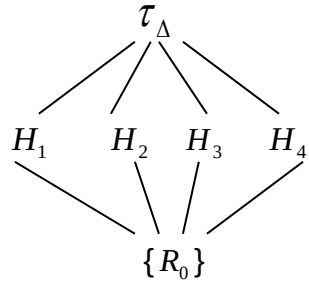
- $H_1 = \{R_0, R_1, R_2\}$ es cíclico generado por R_1, también generado por R_2, se denota por $H_1 = \langle R_1 \rangle = \langle R_2 \rangle$
- $H_2 = \{R_0, S_1\}$ es cíclico generado por S_1, que se denota por $H_2 = \langle S_1 \rangle$
- $H_3 = \{R_0, S_2\}$ es cíclico generado por S_2, que se denota por $H_3 = \langle S_2 \rangle$
- $H_4 = \{R_0, S_3\}$ es cíclico generado por S_3, que se denota por $H_4 = \langle S_3 \rangle$

Notemos que un elemento $g \in G$ es de orden k si $g^k = e_G$ (neutro), donde $k \in \mathbb{Z}$ es el menor entero positivo y se denota por $|g| = k$

¿Es $(\tau_\Delta, \cdot)$ cíclico?

No lo es, pues ninguno de sus elementos es de orden 6, lo que quiere decir que no existe para cada elemento de $(\tau_\Delta, \cdot)$ un menor entero positivo igual a 6 talque $x^6 = R_0$ donde $x \in \tau_\Delta$.

A continuación se presenta la red de subgrupos de $(\tau_\Delta, \cdot)$



Considerando el grupo $(\tau_\Delta, \cdot)$ podemos resolver la siguiente ecuación

$$\begin{aligned}
(R_1 \cdot R_2)^5 \cdot x^2 \cdot S_1 \cdot S_2 \cdot S_3 &= (S_2)^3 \\
(R_0)^5 \cdot x^2 \cdot (S_1 \cdot S_2) \cdot S_3 &= S_2 \\
R_0 \cdot x^2 \cdot R_1 \cdot S_3 &= S_2 \\
R_0 \cdot x^2 \cdot S_2 &= S_2 \\
x^2 \cdot S_2 &= S_2 \quad / \cdot S_2 \text{ derecha} \\
x^2 &= R_0
\end{aligned}$$

Solución $x \in \{R_0,\ S_1,\ S_2,\ S_3\}$

Este tipo de ejercicio es sencillo de responder al observar la tabla correspondiente.

Definición 3: Dado G un grupo cíclico finito generado por el elemento $g \in G$, diremos que el orden de cualquier elemento $x \in G$ es el menor entero positivo m talque $x^m = e$, donde e es el neutro del grupo G.

Observación: Como $x \in G = \langle g \rangle$, entonces $x = g^k$, $k \in \mathbb{Z}^+$, luego $|x| = ord(x) = m \Rightarrow (g^k)^m = e$.

Nota: g^k se refiere a notación multiplicativa.

Ejemplo 1: Determine el orden de los elementos de:

a) $(\tau_\Delta \cdot)$

Sabemos que el neutro en $(\tau_\Delta, \cdot)$ es R_0, entonces:

$$(R_0)^1 = R_0 \qquad (R_1)^1 = R_1 \qquad (R_2)^1 = R_2$$
$$(R_1)^2 = R_2 \qquad (R_2)^2 = R_1$$
$$(R_1)^3 = R_0 \qquad (R_2)^3 = R_0$$
$$\therefore |R_0| = 1 \qquad \therefore |R_1| = 3 \qquad \therefore |R_2| = 3$$

$$(S_1)^1 = S_1 \qquad (S_2)^1 = S_2 \qquad (S_3)^1 = S_3$$
$$(S_1)^2 = R_0 \qquad (S_2)^2 = R_0 \qquad (S_3)^2 = R_0$$
$$\therefore |S_1| = 2 \qquad \therefore |S_2| = 2 \qquad \therefore |S_3| = 2$$

Eduardo Cabrera de Arrizabalaga (profesor guía), Yesenia Briceño, Katherin Lara & Carolina Macaya (tesistas 2007)

b) $\mathbb{Z}_2 \times \mathbb{Z}_4$

$\mathbb{Z}_2 \times \mathbb{Z}_4 = \{ (\bar{0}, \bar{0}) , (\bar{0},\bar{1}) , (\bar{0},\bar{2}) , (\bar{0},\bar{3}) , (\bar{1},\bar{0}) , (\bar{1},\bar{1}) , (\bar{1},\bar{2}) , (\bar{1},\bar{3}) \}$

Sabemos que el neutro en $\mathbb{Z}_2 \times \mathbb{Z}_4$ es $(\bar{0},\bar{0})$, entonces:

$$
\begin{array}{lll}
(\bar{0},\bar{1})^1 = (\bar{0},\bar{1}) & & (\bar{1},\bar{0})^1 = (\bar{1},\bar{0}) \\
(\bar{0},\bar{1})^2 = (\bar{0},\bar{2}) & & (\bar{1},\bar{0})^2 = (\bar{0},\bar{0}) \\
(\bar{0},\bar{1})^3 = (\bar{0},\bar{3}) & & (\bar{1},\bar{1})^1 = (\bar{1},\bar{1}) \\
(\bar{0},\bar{1})^4 = (\bar{0},\bar{0}) & & (\bar{1},\bar{1})^2 = (\bar{0},\bar{2}) \\
(\bar{0},\bar{2})^1 = (\bar{0},\bar{2}) & & (\bar{1},\bar{1})^3 = (\bar{1},\bar{3}) \\
(\bar{0},\bar{2})^2 = (\bar{0},\bar{0}) & & (\bar{1},\bar{1})^4 = (\bar{0},\bar{0}) \\
(\bar{0},\bar{3})^1 = (\bar{0},\bar{3}) & & (\bar{1},\bar{2})^1 = (\bar{1},\bar{2}) \\
(\bar{0},\bar{3})^2 = (\bar{0},\bar{2}) & & (\bar{1},\bar{2})^2 = (\bar{0},\bar{0}) \\
(\bar{0},\bar{3})^3 = (\bar{0},\bar{1}) & & (\bar{1},\bar{3})^1 = (\bar{1},\bar{3}) \\
(\bar{0},\bar{3})^4 = (\bar{0},\bar{0}) & & (\bar{1},\bar{3})^2 = (\bar{0},\bar{2}) \\
 & & (\bar{1},\bar{3})^3 = (\bar{1},\bar{1}) \\
 & & (\bar{1},\bar{3})^4 = (\bar{0},\bar{0})
\end{array}
$$

Luego el orden de los elementos es:

$$
\left| (\bar{0},\bar{1}) \right| = 4 \qquad \left| (\bar{0},\bar{2}) \right| = 2 \qquad \left| (\bar{0},\bar{3}) \right| = 4 \qquad \left| (\bar{1},\bar{0}) \right| = 2 \qquad \left| (\bar{1},\bar{1}) \right| = 4
$$

Teorema: Sea G un grupo cíclico finito, generado por g y $|G| = n$, entonces $g^n = e$ y los elementos de G son exactamente $g^1, g^2, ..., g^{n-1}, g^n = e$.

Demostración:

Supongamos por el contrario que existe $m \in \mathbb{Z}^+$, talque $g^m = e$, $\forall\ m < n$.

Sea $x \in G$, entonces $x = g^k$, $k \in \mathbb{Z}^+$, aplicando Algoritmo de la división a los enteros k y m (con $m < k$), entonces existen enteros q y r talque $k = m\,q + r$, donde $0 \leq r < m$.

Luego con $0 < r < m$ se tiene:

$$g^k = g^{mq+r} = g^{mq}\, g^r = (g^m)^q\, g^r = g^r, \text{ donde } g^m = e.$$

Esto nos dice que $x = g^r \in G$, es decir que el grupo G posee a lo menos m elementos, lo que es una contradicción con el orden de G, que posee n elementos.

Luego no existe $m < n$, talque g^m=e. En consecuencia, si $|G| = n$, $g^n = e$ donde $G = \langle g \rangle$.

Sólo falta verificar que todos los elementos de G son distintos, para ello supondremos que g^i, $g^j \in G$, con $g^i = g^j$, donde $i < j < n$.

Luego tenemos $g^i = g^j \,/\, g^{-i}$

$$\Rightarrow \quad e = g^{j-i}, \text{ donde } 0 < j - i < n.$$

¡Es una contradicción!, por lo demostrado previamente. Luego todos los elementos de G son distintos.

Observación: Si G es un grupo cíclico finito de orden n, entonces n es el menor entero positivo talque $g^n = e$

2.3.- Criterio para Subgrupo

Hasta aquí hemos definido $(G, *)$ como un grupo, y un subgrupo de el como una dupla $(H, *)$, tal que $\varnothing \neq H \subseteq G$, donde $(H, *)$ es un grupo. H es subgrupo de G, recordando que se denota por $H \leq G$.

Proposición: "Criterio para Subgrupo"

Dado $(G, *)$ un grupo, y $\varnothing \neq H \subseteq G$, entonces, $H \leq G$ ssi:

(i) Dados $x, y \in H \Rightarrow x * y \in H$

(ii) Dado $x \in H \Rightarrow x^{-1} \in H$, ($x^{-1}$ es el inverso de x en el grupo H).

Demostración:

$\Rightarrow$] *Hipótesis:* $H \leq G$

Tesis: (i) Dados $x, y \in H \Rightarrow x * y \in H$

(ii) Dado $x \in H \Rightarrow x^{-1} \in H$, ($x^{-1}$ es el inverso de x en el grupo H).

Por hipótesis se tiene que $H \leq G$, esto quiere decir que H es un grupo, luego las condiciones (i) y (ii) se cumplen.

$\Leftarrow$] *Hipótesis:* (i) Dados $x, y \in H \Rightarrow x * y \in H$

(ii) Dado $x \in H \Rightarrow x^{-1} \in H$, ($x^{-1}$ es el inverso de x en H)

Tesis: $H \leq G$.

Aquí debemos demostrar que H es grupo con la operación del grupo G, como se satisfacen las condiciones (i) y (ii) por hipótesis sólo basta probar que "$*$" es asociativa en H y que $\exists!\ e_G \in G$.

Como $H \subseteq G$, se cumple asociatividad pues se hereda del grupo G.

Por ver que $e_G \in H$:

Tenemos por (ii) que si $x \in H \Rightarrow x^{-1} \in H$, ($x^{-1}$ es el inverso de x) y por (i) que dados x, $x^{-1} \in H \Rightarrow x * x^{-1} \in H$

$$\therefore\ e_G \in H.$$

De esta manera queda demostrado el criterio para subgrupo.

Corolario: (del criterio de subgrupo)

Dado $(G,*)$ un grupo y H un subconjunto no vacío de G, entonces, $(H,*)$ es un subgrupo de $(G,*)$ si y sólo si:

(i) $\forall\ x, y \in H : x * y^{-1} \in H$, ($y^{-1}$ es el inverso de y en el grupo H).

Ejemplo 1: Sea $(G,\cdot)$ un grupo y $a \in G$ fijo, entonces:

$H_a := \{\ x \in G : x \cdot a = a \cdot x\ \} \leq G$.

Demostración:

(i) Es claro que $H_a \subseteq G$, además $H_a \neq \varnothing$, pues $e_G \in H_a$, luego podemos asegurar que $e_G \cdot a = a \cdot e_G$.

Eduardo Cabrera de Arrizabalaga (profesor guía), Yesenia Briceño, Katherin Lara & Carolina Macaya (tesistas 2007)

(ii) Dados $x, y \in H_a$, por demostrar que $x \cdot y \in H_a$, es decir se debe verificar $(x \cdot y) \cdot a = a \cdot (x \cdot y)$.

Se tiene por asociatividad en G que:

$$\begin{aligned} (x \cdot y) \cdot a &= x \cdot (y \cdot a) && ; \ y \in H_a \\ &= x \cdot (a \cdot y) && ; \text{asociatividad de } G \\ &= (x \cdot a) \cdot y && ; \ x \in H_a \\ &= (a \cdot x) \cdot y \\ &= a \cdot (x \cdot y) \end{aligned}$$

$$\therefore (x \cdot y) \in H_a$$

(iii) Dado $x \in H_a$, por demostrar que $x^{-1} \in H_a$, es decir se debe verificar $x^{-1} \cdot a = a \cdot x^{-1}$.

Sabemos que $x \in H_a$, esto es:

$$\begin{aligned} x \cdot a &= a \cdot x && ; \ x^{-1} \text{ por izquierda} \\ x^{-1} \cdot (x \cdot a) &= x^{-1} \cdot (a \cdot x) && ; \text{por asociatividad} \\ a &= x^{-1} \cdot a \cdot x && ; \ x^{-1} \text{ por derecha} \\ a \cdot x^{-1} &= x^{-1} \cdot a \end{aligned}$$

$$\therefore x^{-1} \in H_a$$

En consecuencia de (i), (ii), (iii) tenemos que $H_a \leq G$

Ejemplo 2: Pruebe que $6\mathbb{Z} \leq 2\mathbb{Z} \leq \mathbb{Z}$ ($n\mathbb{Z}$ grupo aditivo)

Demostración:

(i) Claramente $6\mathbb{Z} \subseteq 2\mathbb{Z}$, ya que si $x \in 6\mathbb{Z}$

Entonces tenemos:

$$x = 6 \cdot k \quad ; k \in \mathbb{Z}$$
$$= 2 \cdot (3 \cdot k) \quad ; 3 \cdot k \in \mathbb{Z}$$
$$\therefore x \in \mathbb{Z}$$

Además $6\mathbb{Z} \neq \varnothing$, pues $0_{\mathbb{Z}} \in 6\mathbb{Z}$.

(ii) Dados $x, y \in 6\mathbb{Z}$ por demostrar que $x + y \in 6\mathbb{Z}$, luego:

Si $x, y \in 6\mathbb{Z}$, tenemos $x = 6 \cdot k$, $y = 6 \cdot t$ con $k, t \in \mathbb{Z}$

Luego; $x + y = 6 \cdot (k + t)$; $(k + t) \in \mathbb{Z}$

$$\therefore x + y \in 6\mathbb{Z}$$

(iii) Si $x \in 6\mathbb{Z}$ por demostrar que $-x \in 6\mathbb{Z}$, entonces:

Como $x \in 6$ se tiene:

$$x = 6 \cdot k \quad ; k \in \mathbb{Z}$$
$$-x = -6 \cdot k$$
$$= 6 \cdot (-k) \quad ; -k \in \mathbb{Z}$$
$$\therefore -x \in 6\mathbb{Z}$$

En consecuencia de (i), (ii), (iii) tenemos que $6\mathbb{Z} \leq 2\mathbb{Z}$

Nota: En general $n\mathbb{Z} \leq \mathbb{Z}$

Ejemplo 3: Sea G un grupo abeliano, entonces $H := \{ x \in G : x^2 = e \} \leq G$.

Demostración:

(i) Claramente $H \neq \varnothing$, $H \subseteq G$, pues $e_G \in H$ esto es: $e^2 = e$.

(ii) Si $x, y \in H$, por demostrar que $(x \cdot y) \in H$, se verifica que $(x \cdot y)^2 \in H$.

Se tiene:

$$\begin{aligned} (x \cdot y)^2 &= (x \cdot y)\cdot(\quad ; G \text{ es abeliano.} \\ & \quad x \cdot y) \\ &= (x \cdot y)\cdot(y \cdot x) \\ &= x \cdot (y \cdot y)\cdot x \quad ; y \in H \\ &= x \cdot e \cdot x \\ &= x \cdot x \quad ; x \in H \\ &= e \end{aligned}$$

$$\therefore (x \cdot y) \in H .$$

(iii) Si $x \in H$ entonces por demostrar que $x^{-1} = e$, esto es: $(x^{-1})^2 = e$

Se tiene:

$$\begin{aligned} (x^{-1})^2 &= x^{-1} \cdot x^{-1} \quad \text{;inverso del binomio} \\ &= (x \cdot x)^{-1} \quad ; x \in H \\ &= e^{-1} \\ &= e \end{aligned}$$

$$\therefore x^{-1} \in H .$$

En consecuencia de (i), (ii), (iii), tenemos que $H \leq G$.

Ejemplo 4: Sea G un grupo, si $H, T \leq G$ entonces demostrar que $H \cap T \leq G$.

Demostración:

(i) Es claro que $H \cap T \subseteq G$, pues $H \subseteq G \wedge T \subseteq G$, además $H \cap T \neq \varnothing$, ya que $e_G \in H$ y además $e_G \in T$, entonces $e_G \in H \cap T$.

$$\therefore \; H \cap T \subseteq G$$

(ii) Si $x, y \in H \cap T$ por demostrar que $(x \cdot y) \in H \cap T$.

Por hipótesis se tiene:

$$x, y \in H \quad \wedge \quad x, y \in T$$

$$\Rightarrow (x \cdot y) \in H \text{ , pues } H \leq G \quad \wedge \quad \Rightarrow (x \cdot y) \in T \text{ , pues } T \leq G$$

$$\therefore (x \cdot y) \in H \cap T.$$

(iii) Dado $x \in H \cap T$, por demostrar que $x^{-1} \in H \cap T$:

Si $x \in H \cap T$, se tiene;

$$x \in H \quad \wedge \quad x \in T$$

$$\text{pero} \quad H \leq G \quad \wedge \quad T \leq G$$

luego $x^{-1} \in H \quad \wedge \quad x^{-1} \in T$

$$\therefore \quad x^{-1} \in H \cap T .$$

En consecuencia de (i), (ii), (iii), se tiene que $H \cap T \leq G$.

Nota: *Generalizando; Sea* G *un grupo y* $\{ H_i : i \in I \}$ *una familia de subgrupos de* G. *Entonces:* $\bigcap_{i \in I} H_i \leq G$

Definición 4: $Z(G) := \{ x \in G : x \cdot y = y \cdot x , \forall y \in G \}$ es el centro del grupo G, o bien el centralizador del grupo en el grupo, se anota $C(G, G)$.

Ejercicio: Sea G un grupo, entonces $Z(G) \leq G$.

Demostración:

(i) $Z(G) \subseteq G$ por definición de centralizador, además $Z(G) \neq \varnothing$, pues se tiene que $e_G \in Z(G)$, esto es; $e \cdot y = y \cdot e \quad ; \forall y \in G$.

$$\therefore Z(G) \subseteq G .$$

(ii) Dados $x , y \in Z(G)$ por demostrar que: $x \cdot y \in Z(G)$, es decir se debe verificar $(x \cdot y) \cdot z = z \cdot (x \cdot y) ; \forall z \in G$.

Se tiene:

$$\begin{aligned} (x \cdot y) \cdot z &= x \cdot (y \cdot z) && ; y \in Z(G) , \forall z \\ &= x \cdot (z \cdot y) && ;\text{asociatividad en } G \\ &= (x \cdot z) \cdot y && ; x \in Z(G) , \forall z \end{aligned}$$

$= (z \cdot x) \cdot y$; asociatividad en G

$= z \cdot (x \cdot y)$; $\forall\ z$

$\therefore\ x \cdot y \in Z(G)$.

(iii) Dado $x \in Z(G)$, por demostrar que $x^{-1} \in Z(G)$, es decir:

$$x^{-1} \cdot z = z \cdot x^{-1} \quad ; \forall\ z \in G$$

Sabemos que $x \cdot z = z \cdot x$, $\forall\ z \in G$ pues $x \in Z(G)$, entonces tenemos;

$x \cdot z = z \cdot x$ / x^{-1} por izquierda

$x^{-1} \cdot x \cdot z = x^{-1} \cdot z \cdot x$

$e \cdot z = x^{-1} \cdot z \cdot x$ / x^{-1} por derecha

$e \cdot z \cdot x^{-1} = x^{-1} \cdot z \cdot x \cdot x^{-1}$

$z \cdot x^{-1} = x^{-1} \cdot z$ / $\forall\ z \in G$

$\therefore\ x^{-1} \in Z(G)$.

En consecuencia de (i), (ii), (iii), tenemos que $Z(G) \leq G$.

Proposición: Sea $(G, \cdot)$ un grupo. Entonces $H = \{ g^n : n \in \mathbb{Z} \}$ es un subgrupo de G.

Demostración:

Se tiene $H \subseteq$ G y $H \neq \varnothing$, donde $e_G \in H$

i) Dados $x, y \in H$, por demostrar $x \cdot y \in H$

Si $x, y \in H \Rightarrow x = g^k$, $y = g^r$, donde $k, r \in \mathbb{Z}$

Luego tenemos $x \cdot y = g^k \cdot g^r = g^{k+r} = g^{\lambda}$, donde $\lambda = k + r \in \mathbb{Z}$

$\therefore x \cdot y \in H$

ii) Dado $x \in H$ por demostrar $x^{-1} \in H$

Si $x \in H \Rightarrow x = g^k$, $k \in \mathbb{Z}$

Luego $x^{-1} = \left(g^k\right)^{-1} = g^{-k}$; $-k \in \mathbb{Z}$

$$\therefore x^{-1} \in H$$

Finalmente por i) y ii) podemos asegurar que $H \leq G$

Teorema : "Todo subgrupo de un grupo cíclico es cíclico"

Demostración: *(John B. Fraleigh; "Algebra Abstracta"; página 58")*

Hipótesis: $G = \langle g \rangle$ y $H \leq G$

Tesis: H es cíclico.

Si $H = \{e_G\}$, entonces H es cíclico (Trivial)

Consideremos a $H \neq \{e_G\}$, Como $H \leq G = \langle g \rangle$, los elementos de H son de la forma g^s y consideremos m el menor entero positivo tal que $g^m \in H$. Aplicamos "principio de la división" a s y m (con $m < s$) se tiene que existen enteros q y r tales que :

$$s = m\,q + r \quad ; \quad \text{con } 0 \leq r < m$$

$$r = s - m\,q \quad ; \quad 0 < r < m$$

$$\Rightarrow g^r = g^{s-mq} = g^s \cdot (g^m)^{-q}$$

Como $g^s \in H$ y $g^m \in H$ con lo cual $(g^m)^{-q} \in H$ se tiene que:

$g^s \cdot (g^m)^{-q} \in H$. Luego $g^r \in H$ donde $0 < r < m$, esto es una contradicción, pues m es el menor entero positivo tal que $g^m \in H$.

Luego $r = 0$, así $s = m\,q$. En consecuencia $g^s = g^{mq} = (g^m)^q \in H$

$$\therefore H = \langle g^m \rangle \text{ es cíclico.}$$

Proposición: Si $G = \langle g \rangle$ es un grupo cíclico finito de orden n, entonces los subgrupos de G, son exactamente los subgrupos generados por g^m, donde $"m\ divide\ a\ n"$, esto es:

Corolario: $H \leq G = \langle g \rangle$, $|G| = n$

$\Rightarrow H = \langle g^m \rangle$, donde $m \Big|_n$ luego

Ejemplo 5:

$\mathbb{Z}_{12} = \langle \bar{1} \rangle$

$\Rightarrow H = \langle \bar{1}^m \rangle \leq \mathbb{Z}_{12}$, donde $m \Big|_{12}$

$m = 1 \quad ; \quad H_1 = \langle \bar{1} \rangle = \mathbb{Z}_{12}$

$m = 12 \quad ; \quad H_2 = \langle \bar{1}^{12} \rangle = \langle \bar{0} \rangle$

} Subgrupos Triviales

$m = 2 \quad ; \quad H_3 = \langle \bar{1}^2 \rangle = \langle \bar{2} \rangle$

$m = 3 \quad ; \quad H_4 = \langle \bar{1}^3 \rangle = \langle \bar{3} \rangle$

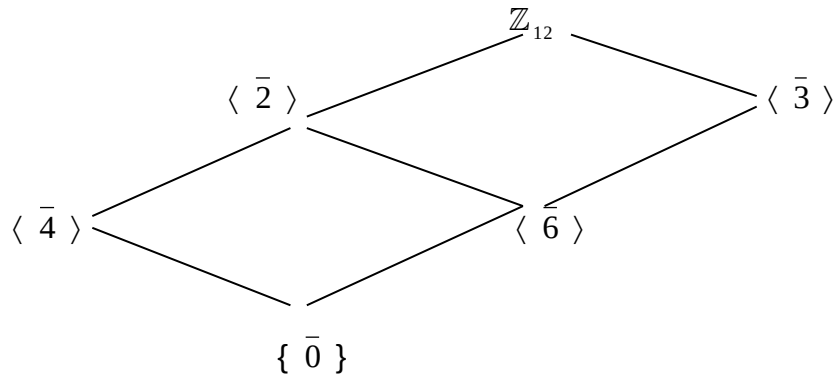
} Subgrupos

$m = 4 \;;\; H_5 = \langle \bar{1}^{\,4} \rangle = \langle \bar{4} \rangle$

$m = 6 \;;\; H_6 = \langle \bar{1}^{\,6} \rangle = \langle \bar{6} \rangle$

Propios

La red de subgrupos de $\mathbb{Z}_{12}$



2.4.- Guía nº2

1.- Establecer si H es subgrupo de G con la multiplicación ordinaria:

$H=\{2^n / n\in\mathbb{Z}\}; G=Q-\{0\}$

¿($H=\{2^n / n\in\mathbb{Z}\}, \cdot$) $\leq G$?

(i) $H\neq\varnothing$

El neutro de $Q-\{0\}$ es 1, luego el neutro de H es $2^0 = 1$, pues $0\in\mathbb{Z}$, entonces $H\neq\varnothing$

$$\therefore\ H\subseteq G$$

(ii) Sean $x,y\in H$, por demostrar: $x\cdot y\in H$.

si

$x\in H \rightarrow x = 2^n$

$y\in H \rightarrow y = 2^m$

luego $x\cdot y = 2^n\cdot 2^m$

$= 2^{n+m}$ $,(m+n)\in\mathbb{Z}$

$$\therefore\ x\cdot y\in H$$

(iii) Si $x\in H$, por demostrar: $x^{-1}\in H$

si

$$x \in H \rightarrow \quad x = 2^n \quad ,(\ )^{-1}$$

$$x^{-1} = (2^n)^{-1}$$

$$x^{-1} = 2^{-n} \quad ,-n \in \mathbb{Z}$$

$$\therefore \quad x^{-1} \in H$$

En consecuencia de (i), (ii) y (iii) $H \leq G$

2.- Demostrar que todo subgrupo de un grupo abeliano es también abeliano.

Demostración:

Hipótesis: $H \leq G \quad ,G \ abeliano$

Tesis: $H \ es \ abeliano$

$\forall a,b \in H \ \ , por \ \ demostrar \ a \cdot b = b \cdot a$

Por hipótesis se tiene que $H \leq G$, luego $H \subseteq G$ entonces:

si $a,b \in H \subseteq G \rightarrow a,b \in G$, como G es grupo abeliano

$a \cdot b \in G \rightarrow b \cdot a \in G$, lo que demuestra que $H \ es \ abeliano$

3.- Demostrar que todo subgrupo cíclico es abeliano.

Demostración:

Hipótesis: si $|G| = n \ \rightarrow g^n = e \ , g \in G \ \ tal que \ G = \langle g \rangle$, luego:

$\forall x \in G, \exists k \in \mathbb{Z} \ \ tal \ que \ x = g^k$

Tesis: $\forall x,y \in G \ \ por \ demostrar \ x \cdot y = y \cdot x$

$$si \ x \in G \quad \rightarrow \quad x = g^k \quad ,k \in \mathbb{Z}$$

$$si \ y \in G \quad \rightarrow \quad y = g^l \quad ,l \in \mathbb{Z}$$

$$\text{luego} \quad x \cdot y = g^k \cdot g^l$$

$= \quad g^{k+l} \qquad , k+l \in \mathbb{Z}$, + en $\mathbb{Z}$ es conmutativa

$= \quad g^{l+k}$

$= \quad g^{l} \cdot g^{k}$

$\therefore \; x \cdot y = y \cdot x$

4.- Encontrar todos los subgrupos de $\mathbb{Z}_{60}$; confeccionar la red.

Los subgrupos de $\mathbb{Z}_{60}$. $H \leq \mathbb{Z}_{60}$, tal que $H = \langle \bar{u} \rangle$, *donde u divide a* 60, entonces $u \in \{1,2,3,4,5,6,10,12,15,20,30\}$

luego se tienen:

- subgrupos triviales de $\mathbb{Z}_{60}$: $\{\bar{0}\}$ y $\mathbb{Z}_{60}$

- subgrupos propios de $\mathbb{Z}_{60}$:

$H_1 = \langle \bar{1} \rangle = \mathbb{Z}_{60}$

$H_2 = \langle \bar{2} \rangle$

$H_3 = \langle \bar{3} \rangle$

$H_4 = \langle \bar{4} \rangle$

$H_5 = \langle \bar{5} \rangle$

$H_6 = \langle \bar{6} \rangle$

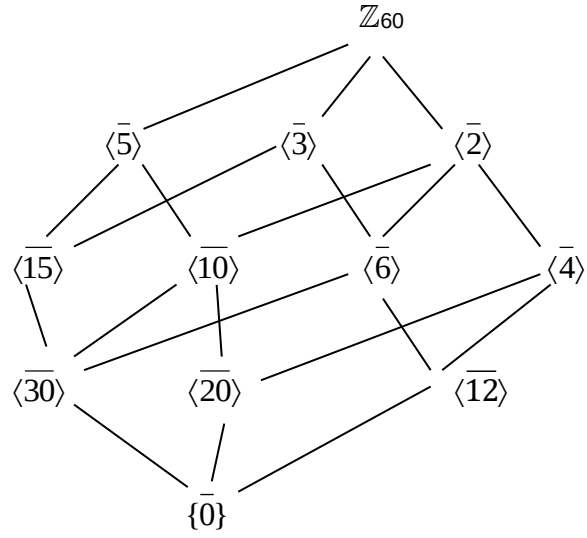
$H_7 = \langle \overline{10} \rangle$

$H_8 = \langle \overline{12} \rangle$

$H_9 = \langle \overline{15} \rangle$

$H_{10} = \langle \overline{20} \rangle$

$H_{11} = \langle \overline{30} \rangle$



2.5.- Autoevaluación 2

1.- Establecer si H es subgrupo de G con la multiplicación ordinaria:

$H = \{a + b \cdot \sqrt{2} \ / \ a,b \in Q \ no \ ambos \ nulos\}$; $G = \mathbb{R}\text{-}\{0\}$.

2.- Encontrar todos los subgrupos del grupo constituido por los enteros múltiplos de 3.

3.- Si $A \ y \ B$ son subgrupos de un grupo G. ¿Es $A \cup B \leq G$?.

4.- Si G es un grupo abeliano y $H \leq G$, demostrar que $S(H) = \{x \in G / x^2 \in H\}$, es un subgrupo de G.

5.- Probar que $G = \{1, -1, i, -i\}$, con la multiplicación, es grupo cíclico. ¿Tiene G algún subgrupo cíclico?.

6.- Determinar el orden de cada elemento del grupo $G = \{1, -1, i, -i\}$, con la multiplicación.

7.- Encontrar todos los generadores de $\mathbb{Z}_{60}$.

8.- Probar que un grupo cíclico con un sólo generador tiene a lo más dos elementos.

9.- Demuestre que en un grupo G, $\forall\ a, b \in G$:

(9.1) $ord(a) = ord(a^{-1})$

(9.2) $ord(a \cdot b) = ord(b \cdot a)$

10.- Hacer una red de subgrupos de $\mathbb{Z}_{64}$, ¿Cuántos generadores posee?, ¿Cuál es el orden de cada uno de sus subgrupos?.