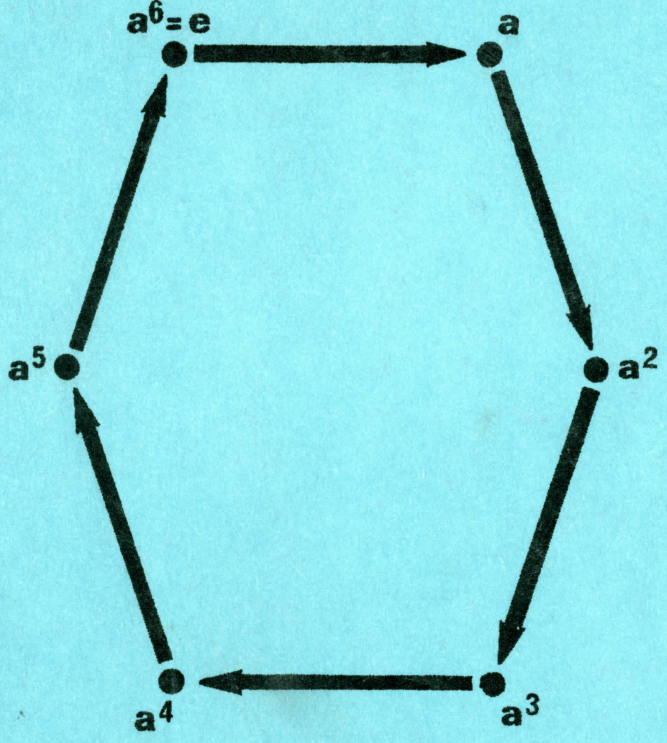
REPUBLICA DE CHILE
MINISTERIO DE EDUCACION
CENTRO DE PERFECCIONAMIENTO, EXPERIMENTACION
E INVESTIGACIONES PEDAGOGICAS
DEPARTAMENTO DE MATEMATICA

GRUPOS CICLICOS



GRUPO CICLICO DE ORDEN SEIS
G $\{e = a^6, a, a^2, a^3, a^4, a^5\}$

material complementario

Prof.: Alicia Labra Jeldres

1976

Isomorfismos

Subgrupos de un grupo cíclico

GRUPOS CICLICOS

Subgrupo engendrado por un elemento

Potencias en un grupo

Subgrupo

Grupo

1.- GRUPO

1.1.- Definición: Sea G conjunto no vacío, $*$ una ley de composición interna definida en G.

Diremos que el par $(G, *)$ es grupo si

G_1) $*$ es asociativa:

$x * (y * z) = (x * y) * z \qquad \forall\, x, y, z \in G$

G_2) $\exists\, e \in G$ tal que $\forall\, a \in G : a * e = a = e * a$

e es el neutro de G con respecto a $*$

G_3) $\forall\, b \in G \quad \exists\, b' \in G$ tal que $b * b' = e = b' * b$

b' se llama el inverso de b con respecto a $*$

Si además se cumple:

G_4) $*$ es conmutativa: $x * y = y * x \qquad \forall\, x, y \in G$

El par $(G, *)$ se llama grupo conmutativo

Observación: G debe ser no vacío pues $e \in G$.

1.2.- Propiedades:

1) El neutro es único
2) El inverso de cada elemento es único
3) $(a')' = a \qquad \forall a \in G$
4) $(a * b)' = b' * a' \qquad \forall a, b \in G$

Demostración:

1.- Sean e_1, e_2 dos neutros. Por demostrar que: $e_1 = e_2$

e_2 neutro $\Longrightarrow e_1 = e_1 * e_2$ por G_2

e_1 neutro $\Longrightarrow e_2 = e_1 * e_2$ por G_2

$\therefore\ e_1 = e_2$

2.- Sean a_1, a_2 dos inversos de a. Por demostrar que: $a_1 = a_2$

Consideremos $a_1 * a * a_2$

$$a_1 * a * a_2 = a_1 * (a * a_2) = a_1 * e = a_1 \qquad \text{(por } G_1, G_3, G_2\text{)}$$

$$a_1 * a * a_2 = (a_1 * a) * a_2 = e * a_2 = a_2 \qquad \text{(por } G_1, G_3, G_2\text{)}$$

$\therefore\ a_1 = a_2$

3.- Tenemos que $(a')' * a' = e$ por G_3

y $a' * (a')' = e$ pero $e = a * a'$

$\therefore (a')' * a' = e \Rightarrow (a')' * a' = a * a'$

$\Rightarrow (a')' * a' * a = a * a' * a \Rightarrow (a')' * e = a * e$

$\Rightarrow (a')' = a$

4.- Por demostrar: i) $(a * b) * (b' * a') = e$

ii) $(b' * a') * (a * b) = e$

i) $(a * b) * (b' * a') = a * (b * b') * a' = a * e * a' = a * a' = e$

ii) En forma análóga a i)

Ejemplo: recordemos que en Z podemos definir la siguiente relación de equivalencia: $a \, R \, b \Leftrightarrow a - b = 2\lambda, \quad \lambda \in Z$

(la diferencia es múltiplo de 2)

$$\bar{0} = cl(0) = \{ x \in Z / x - 0 = 2\lambda, \lambda \in Z \}$$
$$= \{ x \in Z / x = 2\lambda, \lambda \in Z \}$$
$$= \{ \ldots, -2, 0, 2, 4, 6 \ldots\ldots\ldots\ldots \}$$

$$\bar{1} = cl(1) = \{ x \in Z / x - 1 = 2\lambda, \lambda \in Z \}$$
$$= \{ x \in Z / x = 2\lambda + 1, \lambda \in Z \}$$
$$= \{ \ldots, -1, 1, 3, 5, 7, \ldots\ldots\ldots \}$$

$\bar{2} = \bar{0}$, $\bar{3} = \bar{1}$, ...

$Z_2 = Z/R = \{ \bar{0}, \bar{1} \}$

en Z_2 definamos las siguientes tablas:

$+_2$	$\bar{0}$	$\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{1}$
$\bar{1}$	$\bar{1}$	$\bar{0}$

$\cdot_2$	$\bar{0}$	$\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$

$(Z_2, +_2)$ es grupo, $(Z_2 - \{0\}, \cdot 2)$ es grupo.

$\bar{0}$ podemos identificarla con los enteros pares

$\bar{1}$ podemos identificarla con los enteros impares

Entonces las tablas $+_2$, $\cdot 2$ mos dan las reglas ya conocidas:

par + par = par
par + impar = impar
impar + par = impar
impar + impar = par

par . par = par
par . impar = par
impar . par = par
impar . impar = impar

Ejercicio 1: a) ¿ Es $(\mathbb{N}, +)$ grupo ?
b) ¿ Es $(\mathbb{R}, +)$ grupo ?
c) ¿ Es $(\mathbb{R}, .)$ grupo ?
d) ¿ Es $(\mathbb{R}^*, .)$ grupo ? donde $\mathbb{R}^* = \mathbb{R} - \{0\}$

1.3.- Definición:

Llamaremos orden de un grupo G al número de elementos de G y lo denotaremos por: $|G|$

Ejercicio 2: ¿Cuántos grupos de orden 1, 2, 3, 4 hay?
Use tablas de doble entrada

Ejemplo: $G = \{e, a, b\}$; $|G| = 3$

$*$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

luego hay un único grupo de orden 3

$(a * a) = \begin{cases} b \\ \text{ó} \\ e \end{cases}$ si $a * a = e \implies a * b = b \longrightarrow\!\!\leftarrow$
(no pueden existir dos elementos repetidos en una misma columna)

- 0 --- 0 --- 0 --- 0 -

Ejercicio 3: En el grupo de Klein $(K_4 = \{e, a, b, c\}, *)$

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Considere los siguientes conjuntos:

a) $\{e, a, b\}$ b) $\{e, a, b, c\}$ c) $\{e\}$
d) $\{e, b\}$ e) $\{e, a\}$ f) $\{e, c\}$
g) $\{e, a, c\}$

¿Cuáles de todos ellos con grupos con la operación $*$?

2.- SUBGRUPO

2.1.- **Definición:** Sea $(G, *)$ grupo y sea $H \subset G$. Diremos que $(H, *)$ es subgrupo de $(G, *)$ $\Leftrightarrow$

$S_1)$ $H \neq \emptyset$

$S_2)$ $a, b \in H \Rightarrow a * b \in H$

$S_3)$ $a \in H \Rightarrow a' \in H$; donde a' es el inverso de a.

Note que un subgrupo es un grupo más pequeño contenido en otro grupo.

Ejercicio 4: Considere el grupo $(\mathbb{R}, +)$

a) ¿Es $(\mathbb{N}, +)$ subgrupo de $(\mathbb{R}, +)$?

b) ¿Es $(\mathbb{Z}, +)$ subgrupo de $(\mathbb{R}, +)$?

Ejercicio 5: Sea A el conjunto formado por todos los enteros pares. Muestre que $(A, +)$ es subgrupo de $(Z, +)$.

Ejercicio 6: Sea $Z_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$, entonces

Z_4 con la ley de composición interna definida por la tabla siguiente es un grupo.

Encuentre subgrupos de $(Z_4, +_4)$

$+_4$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$

- 0 --- 0 --- 0 --- 0 -

3.- POTENCIAS EN UN GRUPO

3.1.- **Definición:** Sea $(G, *)$ grupo. Para todo $a \in G$ definamos $a^{(n)}$, $n \in Z$ de la siguiente manera:

$$\begin{cases} a^{(n)} = a * a * \overbrace{\cdots}^{n} * a & \text{si } n \in Z^+ \\ a^{(0)} = e \quad ; \quad e = \text{neutro de } G \\ a^{(-n)} = a' * a' * \overbrace{\cdots}^{n} * a' & \text{si } n \in Z^+ \end{cases}$$

Ejercicio 7 A: Verifique la definición para el grupo $(\mathbb{R}^*, .)$

Ejercicio 7 B: Verifique la definición para el grupo $(Z, +)$

3.2.- Propiedades de la potenciación

Sea $(G, *)$ grupo, $a \in G$ entonces:

P_1.- $a^{(n+m)} = a^{(n)} * a^{(m)}$ $\quad \forall n, m \in Z$

P_2.- $(a^{(n)})' = a^{(-n)} = (a')^{(n)}$ $\quad \forall n \in Z$

P_3.- $a^{(nm)} = (a^{(n)})^{(m)}$ $\quad \forall n, m \in Z$

Demostración:

P_1.- i) Por demostrar: $a^{(n)} * a^{(m)} = a^{(n+m)}$ $\quad \forall n, m \in Z^+$

$$a^{(n)} * a^{(m)} = a * a * \overbrace{\cdots}^{n} * a * a * \overbrace{\cdots}^{m} * a = a * a * \overbrace{\cdots}^{n+m} * a$$
$$= a^{(n+m)}.$$

ii) Por demostrar: $a^{(n)} * a^{(m)} = a^{(n+m)}$ $\quad \forall n \in Z^-, \forall m \in Z^+$

$n \in Z^- \implies n = -t$, $t \in Z^+$ y supongamos que $t < m$.

$$a^{(n)} * a^{(m)} = a^{(-t)} * a^{(m)} = a' * a' * \overbrace{\cdots}^{t} * a' * a * \overbrace{\cdots}^{m} * a$$
$$a * a * \overbrace{\cdots}^{m-t} * a = a^{(m-t)} = a^{(-t+m)} = a^{(n+m)}.$$

iii) $n \in Z^+$, $m \in Z^-$ se reduce al caso ii)

iv) $n \in Z^-$, $m \in Z^- \implies n = -t$, $t \in Z^+$ y $m = -k$, $k \in Z^+$

$$a^{(n)} * a^{(m)} = a^{(-t)} * a^{(-k)} = a' * \overbrace{\cdots}^{t} * a' * a' * \overbrace{\cdots}^{k} * a'$$
$$= a' * a' * \overbrace{\cdots}^{t+k} * a' = a^{(-(t+k))}$$
$$= a^{(-t-k)} = a^{(n+m)}$$

$\therefore a^{(n)} * a^{(m)} = a^{(n+m)}$ $\quad \forall n, m \in Z$

P_2.- i) $n \in Z^+$

$$(a^{(n)})' = (a * \overset{n}{\ldots} * a)' = a' \times \overset{n}{\ldots} \times a' = a^{(-n)}$$

$$(a')^{(n)} = a' * \overset{n}{\ldots} * a' = a^{(-n)}$$

ii) $n = 0$ $(a^{(0)})' = e' = e$

$$a^{(-0)} = a^{(0)} = e \quad \forall \quad (a')^{(0)} = e$$

iii) $n \in Z^- \Longrightarrow n = -t,\ t \in Z^+$

$$(a^{(n)})' = (a^{(-t)})' = (a' * \overset{t}{\ldots} a')' = a * \overset{t}{\ldots} * a = a^{(t)} = a^{(-n)}$$

$$(a')^{(n)} = (a')^{(-t)} = (a')' * \overset{t}{\ldots} * (a')' = a * \overset{t}{\ldots} * a = a^{(t)} = a^{(-n)}$$

$$\therefore (a^{(n)})' = a^{(-n)} = (a')^{(n)} \quad \forall\, n \in Z$$

P_3.- Ejercicio.

- O --- O --- O --- O -

4.- SUBGRUPO CICLICO GENERADO POR UN ELEMENTO

4.1.- Definición 1: Sea $(G, *)$ grupo y sea $a \in G$

definamos: $\langle a \rangle = \{ a^{(n)} / n \in Z \}$ = subgrupo generado por a.

Ejercicio 8: $\langle a \rangle$ es el subgrupo más pequeño que contiene a

Ejercicio 9: Considere el grupo $(Z, +)$.

¿Cuál es el subgrupo $\langle 3 \rangle$?

¿Cuál es el subgrupo $\langle -5 \rangle$?

Definición 2: orden de un elemento $a \in G$ es el menor entero positivo m tal que $a^{(m)} = e$.

Si no hay tal entero m diremos que a tiene orden infinito.

Notación: $|a|$

4.2.- Propiedades:

1.- $|a| = |a'| \quad \forall a \in G$

2.- $|a| = |\langle a \rangle| \quad \forall a \in G$

3.- $|a| = |b * a * b'| \quad \forall a, b \in G$

4.- $|a * b| = |b * a$ (use 3)

5.- $|a| = m$ y si $a^{(p)} = e$ entonces m divide a p. $(m \mid p)$

6.- $a^{(i)} = a^{(j)} \Rightarrow m \mid i-j$, donde $m = |a|$

Demostración:

1.- Sea $m = |a|$

Por demostrar que $m = |a'|$

i) $(a')^{(m)} = a^{(-m)} = (a^{(m)})' = e' = e.$

ii) Supongamos que existe $k \in Z^+$ tal que

$(a')^{(k)} = e \quad y \quad k < m.$

$(a')^{(k)} = e \Rightarrow (a^{(k)})' = e \Rightarrow a^{(k)} = e \rightarrow\leftarrow |a| = m.$

$\therefore \quad m = |a'|$

2.- Ejercicio

3.- Sea $|a| = m$. Por demostrar que $|b * a * b'| = m$

i) $(b * a * b')^{(m)} = (b * a * b') * (b * a * b') * \overset{m}{\smile}\!\!\cdots (b * a * b')$

$= b * a * a * \overset{m}{\smile}\!\!\cdots * a * b'$

$= b * a^{(m)} * b' = b * e * b'$

$= b * b' = e$

ii) Supongamos que existe $k \in Z^+$ tal que

$(b * a * b')^{(k)} = e \quad y \quad k < m$

$(b * a * b')^{(k)} = e \Rightarrow b * a^{(k)} * b' = e$

$\Rightarrow b * a^{(k)} = e * b = b$

$\Rightarrow a^{(k)} = b' * b = e$

$\Rightarrow a^{(k)} = e$

$\rightarrow\leftarrow |a| = m.$

$\therefore \quad |b * a * b'| = m$

4.- $|a * b| = m$. Por demostrar que $|b * a| = m$.

Se tiene: $b * a = b * (a * b) * b'$

Apliquemos 3) y nos queda:

$|b * (a * b) * b'| = |a * b| = m$

$\therefore |b * a| = |a * b|$

5.- Sea $|a| = m$, $a^{(p)} = e$. Por demostrar: $m \mid p$

Sea $m \in Z^+$, $p \in Z$. Por algoritmo de división $\exists!$ $q, r \in Z$ tales que:

$p = m \cdot p + r$ con $0 \leq r < m$

Por demostrar que $r = 0$

Si $r \neq 0$ tenemos: $a^{(p)} = a^{(m\,q + r)} = a^{(m\,q)} * a^{(r)}$

$= (a^{(m)})^{(q)} * a^{(r)} = e * a^{(r)} = a^{(r)}$

$\therefore e = a^{(r)}$ y $r < m \rightarrow\leftarrow |a| = m$

luego $r = 0$

y por lo tanto $p = m \cdot q$, $q \in Z$

$\therefore m \mid p$

- 0 --- 0 --- 0 --- 0 -

Ejercicio: (Motivación para la definición de grupo cíclico)

a) Consideremos el grupo $(Z_3, +_3)$

$Z_3 = \{\bar{0}, \bar{1}, \bar{2}\}$

$\langle \bar{0} \rangle = \{\bar{0}\}$

$\langle \bar{1} \rangle = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}, \ldots\} = \{\bar{1}, \bar{2}, \bar{0}, \bar{1}, \bar{2}, \bar{0}\} = \{\bar{0}, \bar{1}, \bar{2}\} = Z_3$

$\langle \bar{2} \rangle = \{\bar{2}, \bar{4}, \bar{6}, \bar{8}, \bar{10}, \ldots\} = \{\bar{2}, \bar{1}, \bar{0}, \bar{2}, \bar{1}, \bar{0} \ldots\} = \{\bar{2}, \bar{1}, \bar{0}\} = Z_3$

b) Ahora consideremos $(Z_6, +_6)$

$Z_6 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$

$\langle \bar{0} \rangle = \{\bar{0}\}$

$\langle \bar{1} \rangle = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}, \ldots\} = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{1}, \ldots\}$

$= \{\bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{0}\} = Z_6$

$\langle \bar{2} \rangle = \{\bar{2}, \bar{4}, \bar{6}, \bar{8}, \bar{10}\} = \{\bar{2}, \bar{4}, \bar{0}, \bar{2}, \bar{4}, \bar{2}, \bar{0}\} = \{\bar{0}, \bar{2}, \bar{4}\}$

$\langle \bar{3} \rangle = \{\bar{3}, \bar{6}, \bar{9}, \bar{12}, \bar{15}\} = \{\bar{3}, \bar{0}, \bar{3}, \bar{0}, \bar{3}, \bar{0}\} = \{\bar{0}, \bar{3}\}$

$\langle \bar{4} \rangle = \{\bar{4}, \bar{8}, \bar{12}, \bar{16}, \bar{20}\} = \{\bar{4}, \bar{2}, \bar{0}, \bar{4}, \bar{2}, \bar{0}\} = \{\bar{4}, \bar{2}, \bar{0}\} = \{\bar{0}, \bar{4}, \bar{2}\}$

$\langle \bar{5} \rangle = \{\bar{5}, \bar{10}, \bar{15}, \bar{20}, \bar{25}, \bar{30}\} = \{\bar{5}, \bar{4}, \bar{3}, \bar{2}, \bar{1}, \bar{0}, \bar{5}\}$

$= \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\} = Z_6$

c) y finalmente consideremos $(K_4 = \{ e, a, b, c \}, *)$

$\langle e \rangle = \{ e \}$

$\langle a \rangle = \{ a^{(m)} / m \in Z \}$

$= \{ a, a * a, a * a * a, \ldots \}$

$= \{ a, e \}$

$\langle b \rangle = \{ b, e \}$

$\langle c \rangle = \{ c, e \}$

*	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

¿Qué encuentra de diferente en estos 3 casos?

5.- GRUPO CICLICO

5.1.- Definición: Diremos que un grupo $(G, *)$ es cíclico si $\exists\, a \in G$ tal que $G = \langle a \rangle$

Nota: a se llama un generador de G.

En el ejercicio vemos que: $(Z_6, +_6)$ es cíclico, $(Z_3, +_3)$ es cíclico, $(K_4, *)$ no es cíclico.

En $(Z_3, +_3)$ $\overline{1}$, $\overline{2}$ son generadores de Z_3. Observe que $\overline{2}$ es el inverso de $\overline{1}$.

En $(Z_6, +_6)$ $\overline{1}$, $\overline{5}$ son generadores de Z_6 y $\overline{5}$ es el inverso de $\overline{1}$.

Notas: 1) $\langle e \rangle = \{ e \}$ Luego si $G \neq \{ e \}$, e no es generador

2) $G = \langle a \rangle \Rightarrow \forall g \in G : g = a^{(n)}$, algún $n \in Z$

5.2.- Proposición: Sea a generador de un grupo G entonces a' también es un generador de G.

Demostración: Por demostrar que $G = \langle a' \rangle$

Por demostrar que $\forall\, g \in G$, $g = (a')^{(k)}$, algún $k \in Z$

$g \in G \Rightarrow g' \in G$ pero $G = \langle a \rangle$

$\therefore\ g' = a^{(n)}$, algún $n \in Z$

$\therefore\ (g')' = (a^{(n)})'$, algún $n \in Z$

$\therefore\ g = a^{(-n)}$, algún $n \in Z$

$= (a')^{(n)}$, algún $n \in Z$

$\therefore\ g \in \langle a' \rangle$

además: $a \in G \Rightarrow a' \in G \Rightarrow \langle a' \rangle \leq G$

$\therefore\ G = \langle a' \rangle$

Ejercicio 10:

a) ¿ Es $(Z_5^*, \cdot_5)$ grupo cíclico ? donde $Z^*_5 = Z_5 - \{\bar{0}\}$

b) Vea que $G = \{1, -1, i, -i\}$ con la multiplicación es grupo cíclico.

Ejercicio 11: ¿Qué puede decir acerca de los subgrupos de $(Z_3, +_3)$ y de $(Z_6, +_6)$?

5.3.- Proposición: Todo subgrupo de un grupo cíclico es cíclico.

Demostración: Sea $(G, *)$ grupo cíclico, $G = \langle a \rangle$ y sea $(H, *)$ subgrupo de $(G, *)$

1.- $H = G \Rightarrow (H, *)$ es cíclico.

2.- Si $H = \{e\}$; $H = \langle e \rangle$ $\therefore$ H cíclico.

3.- $H \neq G$, $H \neq \{e\}$

Sea m el menor entero positivo tal que $a^{(m)} \in H$.

Afirmación: $H = \langle a^{(m)} \rangle$

$a^{(m)} \in H \Rightarrow \langle a^{(m)} \rangle \subseteq H$.

sólo falta probar que: $H \subseteq \langle a^{(m)} \rangle$

Sea $b \in H$; luego $b \in G$ $\therefore$ $b = a^{(s)}$; algún $s \in Z$

Consideremos: $m \in Z^+$, $s \in Z$; por algoritmo de división existen únicos $q, r \in Z$ tal que $s = m \cdot q + r$ con $0 \leq r < m$

Por demostrar: $r = 0$. Supongamos $r \neq 0$

$a^{(s)} = a^{(mq + r)} = a^{(mq)} * a^{(r)}$

$\therefore$ $a^{(r)} = (a^{(mq)})' * a^{(s)}$

$a^{(m)} \in H \Rightarrow a^{(mq)} \in H \Rightarrow (a^{(mq)})' \in H$. y $a^{(s)} \in H$.

$\therefore$ $a^{(r)} \in H$. $\rightarrow\leftarrow$ m es el menor entero positivo tal que $a^{(m)} \in H$

$\therefore$ $r = 0$ $\therefore$ $s = m \cdot q$

$\therefore$ $b = a^{(s)} = a^{(mq)} = (a^{(m)})^{(q)} \in \langle a^{(m)} \rangle$

$\therefore$ $H = \langle a^{(m)} \rangle$

luego H cíclico

Ejercicio 12: Sea $G = \langle a \rangle$ grupo cíclico y $|G| = n$, entonces los subgrupos H de G son exactamente los subgrupos generados por $a^{(m)}$ con $m \mid n$.

Hint.: $|G| = n \Longrightarrow a^{(n)} = e \in H$. y trabaje con $a^{(n)}$ en lugar de $a^{(s)}$ en la proposición anterior.

Ejercicio 13: Enecuentre todos los subgrupos de $(Z_{16}, +_{16})$

Ejercicio 14 A: Sea $(G, *)$ grupo cíclico entonces $(G, *)$ es abeliano.

Ejercicio 1. B: Vea que el recíproco del ejercicio 11 no es verdadero; es decir encuentre un grupo que sea abeliano pero no cíclico.

Ejercicio 15: Considere el grupo cíclico $(Z, +)$
¿ Cuáles son sus generadores ?

5.4.- Teorema: Sea $(G, *)$ grupo cíclico infinito entonces sus únicos generadores son a y a' donde $G = \langle a \rangle$ y a' es el inverso de a.

Demostración: Sea $G = \langle a \rangle$ G infinito $\therefore$ a tiene orden infinito.
Supongamos $\exists\, b \in G \quad b \neq a, a'$ tal que $G = \langle b \rangle$

$\therefore \quad \langle a \rangle = \langle b \rangle$

$\therefore \quad a \in \langle b \rangle \Longrightarrow a = b^{(k)}; \; k \in Z$

$b \in \langle a \rangle \Longrightarrow b = a^{(t)}; \; t \in Z$

$\therefore \quad a = b^{(k)} = (a^{(t)})^{(k)} = a^{(tk)}$

$\therefore \quad a * a^{(-tk)} = a^{(tk)} * a^{(-tk)} = e$

$\therefore \quad a^{(1-tk)} = e \Longrightarrow$ orden $a \mid 1 - tk$

$\longrightarrow\!\leftarrow$

orden a es infinito

5.5.- Teorema: Sea $(G, *)$ grupo cíclico de orden n. Sea a un generador de G. Entonces los otros generadores de G son de la forma $a^{(k)}$; donde $(k, n) = 1$.

Observación: La notación (k, n) significa máximo común devisor de k y n.

Demostración: Por demostrar que:

$a^{(k)}$ generador de G $\langle\Longrightarrow\rangle$ (k, n) = 1

$a^{(k)}$ generador de G $\langle\Longrightarrow\rangle$ $G = \langle a^{(k)} \rangle \langle\Longrightarrow\rangle \langle a \rangle = \langle a^{(k)} \rangle$

$\langle\Longrightarrow\rangle$ $a \in \langle a^{(k)} \rangle \langle\Longrightarrow\rangle$ $a = (a^{(k)})^{(t)}$; algún $t \in Z$.

$\langle\Longrightarrow\rangle$ $a = a^{(kt)}$, algún $t \in Z$

$\langle\Longrightarrow\rangle$ $a^{(1-kt)} = e$, algún $1 - kt \in Z$

$\langle\Longrightarrow\rangle$ $n \mid 1 - kt$

$\langle\Longrightarrow\rangle$ $1 - kt = n\lambda$; algún $\lambda \in Z$

$\langle\Longrightarrow\rangle$ $1 = kt + n\lambda$ algún $t \in Z$, algún $\lambda \in Z$

$\langle\Longrightarrow\rangle$ $1 = (k, n)$.

Observación: basta considerar $n, k \in Z^+$, $k < n$.

Ejercicio 16: Encuentre todos los generadores de $(Z_{16}, +_{16})$ y de todos sus subgrupos.

Por ejercicio 12 los subgrupos de Z_{16} son

Z_{16}; $\langle \overline{2} \rangle$; $\langle \overline{4} \rangle$; $\langle \overline{8} \rangle$; $\langle \overline{0} \rangle$

1) otros generadores de Z_{16} son: $\overline{1}^k$ con (k, 16) = 1

$\therefore Z_{16} = \langle \overline{1} \rangle = \langle \overline{3} \rangle = \langle \overline{5} \rangle = \langle \overline{7} \rangle = \langle \overline{9} \rangle = \langle \overline{11} \rangle = \langle \overline{13} \rangle = \langle \overline{15} \rangle$

2) otros generadores de $\langle \overline{2} \rangle$ son de la forma $\overline{2}^k$; $(k, |\langle 2 \rangle|) = 1$

$\langle \overline{2} \rangle = \{ \overline{0}, \overline{2}, \overline{4}, \overline{6}, \overline{8}, \overline{10}, \overline{12}, \overline{14} \}$, $|\langle \overline{2} \rangle| = 8$

luego los otros generadores de $\langle \overline{2} \rangle$ son: $\overline{2}^k$; (k, 8) = 1

(k = 1, 3, 5, 7)

$\langle \overline{2} \rangle = \langle \overline{6} \rangle = \langle \overline{10} \rangle = \langle \overline{14} \rangle$

3) $\langle \overline{4} \rangle = \{ \overline{0}, \overline{4}, \overline{8}, \overline{12} \}$ $\therefore$ $\langle \overline{4} \rangle = \langle \overline{12} \rangle$

4) $\langle \overline{8} \rangle = \langle \overline{8} \rangle$

5) $\langle \overline{0} \rangle = \langle \overline{0} \rangle$

Ejercicio 17: a) Encuentre todos los subgrupos de $(Z_{18}, +_{18})$

b) Encuentre todos los generadores de Z_{18} y de todos sus subgrupos.

c) Encuentre todos los generadores de $(Z_{11}^*, +_{11})$ donde

$Z_{11}^* = Z_{11} - \{ \overline{0} \}$

Ejercicio 18: Demuestre ó de un contraejemplo del enunciado: "Si todos los subgrupos (no triviales) de un grupo G son cíclicos entonces G es cíclico".

Ejercicio 19: Encuentre todos los subgrupos de $(Z_{36}, +_{36})$

Ejercicio 20: Sea $G = \langle a \rangle$ y sea $b = a^{(s)} \in G$
Demuestre que $|\langle b \rangle| = \frac{n}{(n,s)}$ donde $n = |G|$

- O --- O --- O --- O --- O -

6.- ISOMORFISMOS

6.1.- Definición: Diremos que dos grupos $(G, *)$ y $(G', \square)$ son isomorfos y lo denotaremos por $(G, *) \simeq (G', \square)$ sí y sólo sí existe $f: G \longrightarrow G'$ tal que:

1) f es homomorfismo:
$f(a * b) = f(a) \square f(b) \quad \forall a, b \in G$
2) f es biyección.

Intuitivamente dos grupos son isomorfos si tienen las mismas propiedades; los elementos se nominan en forma distinta.

Ejercicio 21: a) ¿ Es $(\mathbb{R}, +) \simeq (\mathbb{R}_+, .)$?

b) Demuestre que: $(Z/n\,Z, +) \simeq (Z_n, +_n)$

6.2.- Teorema: Sea $(G, *)$ grupo cíclico de generador a.
Entonces:

1) G finito, $|G| = n \Longrightarrow (G, *) \simeq (Z_n, +_n)$
2) G infinito $\Longrightarrow (G, *) \simeq (Z, +)$

En virtud de este teorema se dice que $(Z, +)$ y $(Z_n, +_n)$ son los prototipos de los grupos cíclicos.

Demostración:

1) $G = \{ e, a, a^{(2)}, a^{(3)}, \ldots\ldots, a^{(n-1)} \}$

Sea $f: G \longrightarrow Z_n$

$a^{(k)} \longmapsto \overline{k} \qquad 0 \leq k < n$

f es homomorfismo:

$$f(a^{(k)} * a^{(t)}) = f(a^{(k+t)}) = \overline{k+t} = \overline{k} +_n \overline{t}$$
$$= f(a^{(k)}) +_n f(a^{(t)})$$

f inyectiva:

Por demostrar que: $f(a^{(k)}) = f(a^{(t)}) \Rightarrow a^{(k)} = a^{(t)}$

$f(a^{(k)}) = f(a^{(t)}) \Rightarrow \overline{k} = \overline{t}$

$\Rightarrow k - t = \lambda n$, algún $\lambda \in Z$

$\Rightarrow a^{(k-t)} = a^{(\lambda n)}$, algún $\lambda \in Z$

$\Rightarrow a^{(k)} * a^{(-t)} = (a^{(n)})^{\lambda}$, algún $\lambda \in Z$

$\Rightarrow a^{(k)} * (a^{(t)})' = e$

$\Rightarrow a^{(k)} = a^{(t)}$.

f epiyectiva: : Sea $\overline{t} \in Z_n$

Por encontrar $g \in G$ tal que $f(g) = \overline{t}$

tomando $g = a^{(t)}$ se tiene:

$a^{(t)} \in G$ y $f(a^{(t)}) = \overline{t}$

$\therefore (G, *) \simeq (Z_n, +_n)$

2) Sea $f: G \longrightarrow Z$

$a^{(m)} \longmapsto m$

entonces f es homomorfismo biyectivo.

$\therefore (G, *) \simeq (Z, +)$.

A continuación veremos una manera más elegante de demostrar este último teorema usando el teorema del homomorfismo:

Sea $f: G \longrightarrow G'$ homomorfismo del grupo $(G, *)$ en el grupo $(G', \square)$ entonces: $(G / \text{núcleo } f, *) \simeq (f(G), \square)$.

Sea $(G, *)$ grupo y sea $a \in G$

Construyamos un homomorfismo

$f : Z \longrightarrow G$

$k \longmapsto a^{(k)}$

$f(Z) = \{ f(t) / t \in Z \}$

$= \{ a^{(t)} / t \in Z \} = \langle a \rangle$

núcleo $f = \{ k \in Z / f(k) = e \}$

$= \{ k \in Z / a^{(k)} = e \}$

1) Si núcleo $f = \{0\}$ se tiene por teorema de homomorfismo:

$$(Z, +) \simeq (\langle a \rangle , *)$$

y en este caso $|a| = \infty$ luego parte 2) del teorema.

2) Si núcleo $f \neq \{0\}$ entonces hay $t \neq 0$, $t \in Z$ tal que $a^{(t)} = e$.

Consideremos el menor entero positivo k tal que $a^{(k)} = e$

$\therefore$ núcleo $f = kZ$

luego por terema del homomorfismo se tiene:

$$(Z / kZ, +) \simeq (\langle a \rangle , *)$$

pero

$$(Z / kZ, +) \simeq (Z_k, +_k)$$

luego

$$(Z_k, +_k) \simeq (\langle a \rangle , *)$$

y en este caso a tiene orden k luego parte 1) del teorema.

- 0 --- 0 --- 0 --- 0 -

7.- BIBLIOGRAFIA

7.1.- DAVID BURTON : Introduction to Modern Abstract Algebra.

7.2.- FRALEIGH : A first course in Abstract Algebra.

7.3.- HERSTEIN : Topics in Modern Algebra.

/ecpm.