***módulo 1*:**

1.1.- GRUPOS: DEFINICION Y EJEMPLOS

En este capítulo veremos las propiedades de la teoría de grupos y algunos ejemplos. Destacando que las propiedades tales como; asociatividad, conmutatividad, existencia de elemento neutro, existencia de elemento inverso se ven especificadas en los Contenidos Mínimos Obligatorios del primer año de enseñanza media en la unidad de “Algebra”.

Definición 1: Dado G un conjunto no vacío y $*$ una ley de composición interna en G. Diremos que $(G, *)$ es un grupo si se verifica lo siguiente: $*: G \times G \to G$

(G.1) $*$ es cerrada en G (es l.c.i)

$\forall\ a, b \in G, \exists\ c \in G$ tal que $a * b = c$

(G.2) $*$ es asociativo

$\forall\ a, b, c \in G$ se cumple $a * (b * c) = (a * b) * c$

(G.3) Existencia de elemento neutro e

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

(G.4) Para cada elemento de G existe elemento inverso

$\forall\ a \in G, \exists\ b \in G$ tal que $a * b = e = b * a$

Nota: Anotaremos el inverso de a como a^{-1}, en G.4, $a^{-1} = b$

Debemos tener presente que un grupo no es simplemente un conjunto G, sino que el par $(G,*)$, o dicho en forma más rigurosa, un grupo es un conjunto G dotado de una operación $*$ que verifica las cuatro propiedades antes mencionadas. Sin embargo, abusando un poco del lenguaje matemático, en adelante nos referiremos al grupo G, queriendo significar con esto $(G,*)$.

Si además en el grupo (G, $*$) se verifica que $*$ es conmutativo en G, es decir, $\forall a,b \in G : a*b = b*a$, se dice que el grupo es grupo conmutativo, o bien, grupo abeliano.

Niels Henrik Abel (1802-1829)

Los grupos abelianos son así llamados en honor al matemático noruego Niels Henrik l (Findö, Noruega, 5 de agosto de 1802 - Froland, Noruega, 6 de abril de 1829). Su primer aporte fue la prueba de la imposibilidad de resolución algebraica de la ecuación de grado 5 mediante radicales.

Debemos considerar que un grupo no es simplemente un conjunto denominado por la letra G, sino que es una dupla (G, $*$), donde $*$ verifica las condiciones G.1, G.2, G.3, G.4 nombradas anteriormente. Sin embargo más adelante abusando del lenguaje matemático nos referiremos al grupo G, queriendo decir (G, $*$).

Dentro de los ejemplos clásicos de grupos se tienen los siguientes, dentro de otros $(\mathbb{Z},+)$, $(\mathbb{R},+)$, $(\mathbb{Q},+)$, $(\mathbb{R}-\{0\}, \cdot)$, $(\mathbb{R}^{nxn},+)$.

A continuación se presenta un resumen de estructuras algebraicas, donde la “x” indica la propiedad que debe cumplir.

Propiedades / Estructuras	Cerrada	Asociativa	Elemento Neutro	Elemento Inverso	Conmutativa
Grupoide	x				
Semigrupo	x	x			
Monoide	x	x	x		
Grupo	x	x	x	x	
Grupo Abeliano	x	X	x	x	x

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

A continuación veremos algunos ejemplos de grupos.

Ejemplo 1: ¿Es $(\mathbb{R}-\{1\}, *)$ un grupo?, donde $a * b = a + b - a \cdot b$; $\forall\, a, b \in \mathbb{R}-\{1\}$ ¿Es abeliano?

Respuesta:

i) Claramente se observa que si $a, b \in \mathbb{R}$, entonces $a \cdot b \in \mathbb{R}$ y $a + b \in \mathbb{R}$, luego podemos asegurar que $a + b - a \cdot b \in \mathbb{R}$.

Basta probar que $a + b - a \cdot b \neq 1$ con $a, b \in \mathbb{R}-\{1\}$, es decir, supongamos que:

$$a + b - a \cdot b = 1 \text{ con } a, b \in \mathbb{R}-\{1\}$$

Luego, tenemos

$$\begin{aligned} a - a \cdot b + b - 1 &= 0 \\ a \cdot (1 - b) - (1 - b) &= 0 \\ (1 - b) \cdot (a - 1) &= 0 \end{aligned}$$

$$\Rightarrow a - 1 = 0 \quad \vee \quad 1 - b = 0$$

$$\Rightarrow a = 1 \quad \vee \quad b = 1$$

$$\Rightarrow\!\Leftarrow$$

Contradicción pues $a, b \in \mathbb{R}-\{1\}$

Luego podemos asegurar que $a + b - a \cdot b \in \mathbb{R}-\{1\}$

$\therefore\ *$ es cerrada en $\mathbb{R}-\{1\}$

ii) Por ver que $*$ es asociativo en $\mathbb{R}$ - $\{1\}$, $\forall\ a, b, c \in \mathbb{R}$ - $\{1\}$

$$\begin{aligned}
a * (b * c) &= a * (b + c - b \cdot c) \\
&= a + (b + c - b \cdot c) - a \cdot (b + c - b \cdot c) \\
&= a + b + c - b \cdot c - a \cdot b - a \cdot c + a \cdot b \cdot c \\
&= (a + b - a \cdot b) + c - a \cdot c - b \cdot c + a \cdot b \cdot c \\
&= (a + b - a \cdot b) + c - (a + b - a \cdot b) \cdot c \\
&= (a + b - a \cdot b) * c \\
&= (a * b) * c
\end{aligned}$$

$\therefore\ *$, es asociativa en $\mathbb{R}$ - $\{1\}$

iii) Por ver si existe elemento neutro.

Debe existir $e \in \mathbb{R}$ - $\{1\}$ tal que $a * e = e * a = a$, $\forall\ a \in \mathbb{R}$ - $\{1\}$

Supongamos

$$\begin{aligned}
a * e &= a \\
\Rightarrow\ a + e - a \cdot e &= a \\
\Rightarrow\ e \cdot (1 - a) &= 0
\end{aligned}$$

Como $1 - a \neq 0$, pues $a \neq 1 \Rightarrow e = 0$

Se verifica también por la derecha.

$\therefore$ Existe elemento neutro para *

iv) Por ver si todo elemento posee inverso.

$\forall\ a \in \mathbb{R} - \{1\}$, debe existir $u \in \mathbb{R} - \{1\}$, tal que $a * u = u * a = 0$

Supongamos

$$a * u = 0$$

$$\Rightarrow \quad a + u - a \cdot u = 0$$
$$\Rightarrow \quad u \cdot (1 - a) = -a$$

Pero sabemos que $1 - a \neq 0$, pues $a \neq 1$

Entonces;

$$u = \frac{-a}{1-a} \quad \text{o bien} \quad u = \frac{a}{a-1}, \ \forall \ a \in \mathbb{R} - \{1\}$$

Se verifica inverso por la izquierda.

$\therefore$ Existe inverso de $a \in \mathbb{R} - \{1\}$, que es $\dfrac{a}{a-1}$

Hasta aquí $(\mathbb{R} - \{1\}, *)$ es un grupo.

v) Por ver si es conmutativo

$\forall \ a, b \in \mathbb{R} - \{1\}$, se cumple $a * b = b * a$

Luego

$$a * b = a + b - a \cdot b$$
$$\Rightarrow \quad a * b = b + a - b \cdot a \text{; Conmutatividad en } \mathbb{R}$$
$$\Rightarrow \quad a * b = b * a$$

$\therefore$ $(\mathbb{R} - \{1\}, *)$ es un Grupo Abeliano.

Ejemplo 2: El conjunto constituido por los múltiplos de un entero a con la adición, constituyen un grupo abeliano, donde $G = \{n \cdot a \ / \ a, n \in \mathbb{Z}$, a fijo$\}$

En este ejemplo ya no es tan evidente aceptar que $(G, +)$ es realmente un grupo abeliano, por lo que probaremos esta afirmación.

i) Claramente $G \neq \varnothing$, pues $a \in G$ por definición.

ii) Por ver si la operación + es cerrada en G

Para probarlo basta sumar dos múltiplos de a y ver si su resultado es también un múltiplo de a. Luego tenemos $n_1 \cdot a$ y $n_2 \cdot a \in G$.

Sumando obtenemos $n_1 \cdot a + n_2 \cdot a = (n_1 + n_2) \cdot a$, donde $(n_1 + n_2) \cdot a \in G$.

$\therefore$ + es cerrada en G.

iii) Por ver si + es asociativa.

Esto queda garantizado por la asociatividad de la adición en $\mathbb{Z}$.

$\therefore$ + es asociativa en G

iv) Por ver si existe elemento neutro.

Tenemos $0 \in G$, pues $0 = 0 \cdot a$

$\therefore$ Existe elemento neutro.

v) Por ver si para todo elemento existe su elemento inverso.

Claramente el inverso de $n \cdot a$ es $-n \cdot a$ ya que al sumar $n \cdot a + (-n \cdot a) = 0$, 0 neutro en G.

$\therefore$ Existe elemento inverso.

Hasta acá podemos decir que $(G, +)$ es un grupo.

Como además se verifica que la adición en $\mathbb{Z}$ es conmutativa, tenemos que $(G, +)$ es grupo abeliano.

1.2.- El grupo multiplicativo de las raíces n-ésimas de la unidad en $\mathbb{C}$.

$$(G=\{z\in\mathbb{C} : z^n = 1, \text{ con } n\in\mathbb{Z}^+\}, \bullet)$$

1.2.1: Para *n* = 1, se tiene el grupo trivial $(H_1=\{1\}, \bullet)$

1.2.2: Para *n* = 2, Raíces cuadradas de la unidad

$$x^2 = 1$$
$$\Rightarrow (x-1)\cdot(x+1) = 0$$
$$\Rightarrow x_1 = 1 \vee x_2 = -1$$

Se tiene que $(H_2=\{1,-1\}, \cdot)$, ahora elaboraremos la tabla de doble entrada.

$\cdot$	1	-1
1	1	-1
-1	-1	1

Se verifica claramente que la operación es cerrada y asociativa, el elemento neutro es 1, el inverso de 1 es 1 y el inverso de -1 es -1.

1.2.3: Para *n* = 3, Raíces cúbicas de la unidad

$$x^3 = 1$$
$$\Rightarrow x^3 - 1 = 0$$
$$\Rightarrow (x-1)(x^2+x+1) = 0$$
$$\Rightarrow x-1 = 0 \vee x^2+x+1 = 0$$

$$\Rightarrow \quad x_0 = 1 \quad \vee \quad x_1 = \frac{-1}{2} + \frac{\sqrt{3}i}{2} \;;\; x_2 = \frac{-1}{2} - \frac{\sqrt{3}i}{2}$$

$\cdot$	x_0	x_1	x_2
x_0	x_0	x_1	x_2
x_1	x_1	x_2	x_0
x_2	x_2	x_0	x_1

Es cerrada la operación, además se observa que ($H_3=\{x_0, x_1, x_2\}$, $\cdot$) es un grupo abeliano o conmutativo por la simetría de la tabla.

1.2.4: Para *n* = 4; El grupo $(H_4=\{1,-1,i,-i\},\cdot)$ de las raíces cuarta de la unidad, donde $H_4 \subseteq \mathbb{C}$

Para verificar que G es realmente un grupo es conveniente elaborar la Tabla de Cayley o de doble entrada, pues los elementos del grupo G no son abstractos.

$\cdot$	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

Se observa en la tabla que la operación es cerrada, la asociatividad se hereda de $\mathbb{C}$, el elemento neutro es 1, y además cada elemento del grupo tiene su inverso, estos son:

- El inverso de 1 es 1
- El inverso de -1 es -1
- El inverso de i es $-i$
- El inverso de $-i$ es i

Notemos además que $(G=\{1,-1,i,-i\},\cdot)$ es un grupo abeliano, pues sólo basta observar si existe o no simetría en la tabla elaborada.

1.2.5: Para $n = 5$, Raíces quinta de la unidad

$$x^5 = 1$$

Sea $w = 1 + 0\,i \quad \Rightarrow \quad \|w\| = 1$

$$\alpha_w = \arg(w) = \operatorname{tg}^{-1}\left(\frac{0}{1}\right) = 0$$

Luego tenemos:

$$x_k = \|w\|^{\frac{1}{5}}\left[\cos\left(\frac{\alpha+2k\pi}{5}\right)+i\ sen\left(\frac{\alpha+2k\pi}{5}\right)\right]$$

Con $k = 0,1,2,3,4$

Si $k = 0$; $x_0 = 1$

Si $k = 1$; $x_1 = cis\left(\frac{2\pi}{5}\right) = \cos 72^\circ + i\ sen\ 72^\circ$

Si $k = 2$; $x_2 = cis\left(\frac{4\pi}{5}\right) = \cos 144^\circ + i\ sen\ 144^\circ$

Si $k = 3$; $x_3 = cis\left(\frac{6\pi}{5}\right) = \cos 216^\circ + i\ sen\ 216^\circ$

Si $k = 4$; $x_4 = cis\left(\frac{8\pi}{5}\right) = \cos 288^\circ + i\ sen\ 288^\circ$

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

$\cdot$	x_0	x_1	x_2	x_3	x_4
x_0	x_0	x_1	x_2	x_3	x_4
x_1	x_1	x_2	x_3	x_4	x_0
x_2	x_2	x_3	x_4	x_0	x_1
x_3	x_3	x_4	x_0	x_1	x_2
x_4	x_4	x_0	x_1	x_2	x_3

Se observa en la tabla claramente que la operación es cerrada y asociativa, además el elemento neutro es x_0 y cada uno de los elementos del grupo tiene su propio inverso, como se señala a continuación.

- El inverso de x_0 es x_0
- El inverso de x_1 es x_4
- El inverso de x_2 es x_3
- El inverso de x_3 es x_2
- El inverso de x_4 es x_1

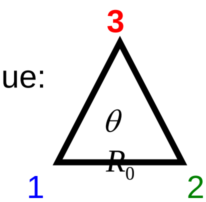
En general las raíces n-ésimas de la unidad determinan o definen un grupo multiplicativo abeliano cuyas raíces determinan los vértices de un polígono regular de n-lados.

1.3.- El Grupo geométrico de las transformaciones de un polígono regular que lo dejan invariante (Grupo Diédrico *D_n* o Grupo de las Simetrías*).*

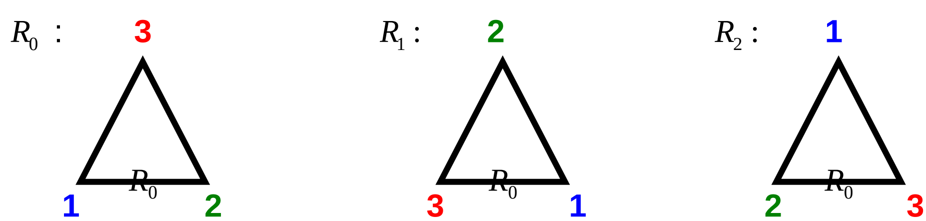
Sea τ_n (o bien, $\tau_{pol(n)}$) el conjunto de los movimientos de un polígono regular que lo dejan invariante como tal, y $\bullet$ una ley de composición interna definida en τ_n representada por el movimiento.

Construyamos a $\tau_{pol(3)}$, grupo de las simetrías de un polígono regular de 3 lados (triángulo equilátero). Observamos que hay movimientos Rotacionales respecto a un punto fijo θ (centro del pol(3)) y movimientos rotacionales respecto de ejes de simetría, que los identificamos como movimientos axiales.

Nuestro pol(3) rotulado como sigue:

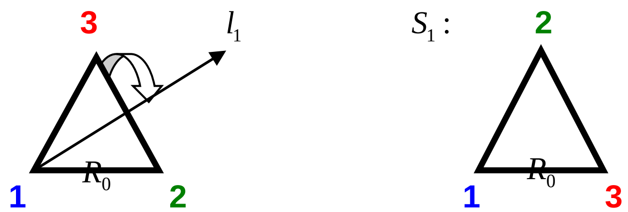


Tomando en cuenta el triángulo descrito anteriormente, se muestran a continuación los *movimientos rotacionales* con respecto al origen θ . Estas son: R_0 rotación en 0º, R_1 rotación en 120º y R_2 rotación en 240º

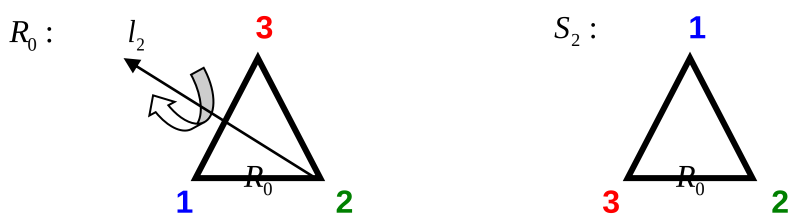


A continuación, se describirán los *movimientos axiales*:

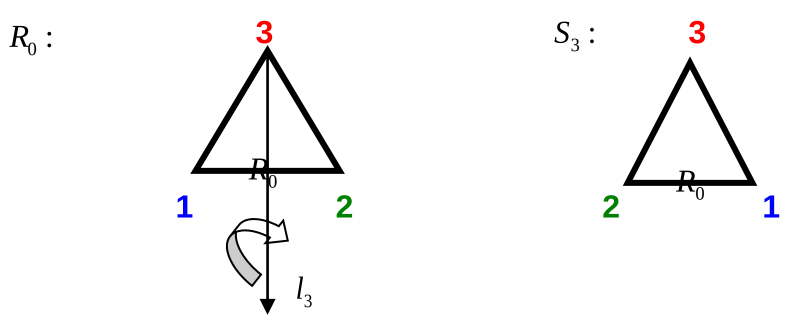
Con respecto al eje axial l_1 o eje de simetría l_1, como se observa en la figura inmediata, notamos que triángulo "original" a quedado transformado, bajo este movimiento axial, en S_1. Note en este caso, que la simetría al eje l_1, deja fijo el vértice inferior izquierdo del triángulo.



Con respecto al eje axial l_2 o eje de simetría l_2, como se observa en la figura inmediata, notamos que el triángulo "original" a quedado transformado, bajo este movimiento axial, en S_2. Note en este caso, que la simetría al eje l_2, deja fijo el vértice inferior derecho del triángulo.



Con respecto al eje axial l_3 o eje de simetría l_3, como se observa en la figura inmediata, notamos que el triángulo "original" a quedado transformado, bajo este movimiento axial, en S_3. Note en este caso, que la simetría al eje l_3, deja fijo el vértice superior del triángulo.



Luego formamos el conjunto $\tau_\Delta = \{R_0, R_1, R_2, S_1, S_2, S_3\}$, donde sus elementos tienen el significado que indica la figura, es decir, por ejemplo R_2 significa rotar el triángulo, desde su posición normal, en un ángulo de 240°, en torno de su centro de gravedad y en sentido de los punteros de un reloj.

Los movimientos rotacionales con respecto a θ del triángulo equilátero quedan definidos como R_0 R_1 R_2, donde:

$$R_0 := Rot\ (\theta,\ 0^\circ) \qquad R_1 := Rot\ (\theta, 120^\circ) \qquad R_2 := Rot\ (\theta, 240^\circ)$$

Considerando la rotación como el movimiento de un cuerpo que gira entorno a su eje.

Aquí tenemos $\tau_\Delta = \{R_0, R_1, R_2, S_1, S_2, S_3\}$, ahora nos queda verificar que

$(\tau_\Delta, \cdot)$ es un grupo, para esto elaboraremos la siguiente tabla.

$\cdot$	R_0	R_1	R_2	S_1	S_2	S_3
R_0	R_0	R_1	R_2	S_1	S_2	S_3
R_1	R_1	R_2	R_0	S_3	S_1	S_2
R_2	R_2	R_0	R_1	S_2	S_3	S_1
S_1	S_1	S_2	S_3	R_0	R_1	R_2
S_2	S_2	S_3	S_1	R_2	R_0	R_1
S_3	S_3	S_1	S_2	R_1	R_2	R_0

Podemos observar claramente que este grupo no es abeliano, ya que por ejemplo $S_2 \circ R_1 \neq R_1 \circ S_2$.

Notamos que R_0 es el neutro del grupo y cada elemento del grupo posee su propio inverso como veremos a continuación:

- El inverso de R_0 es R_0
- El inverso de R_1 es R_2
- El inverso de R_2 es R_1
- El inverso de S_1 es S_1
- El inverso de S_2 es S_2
- El inverso de S_3 es S_3

Además, $R_1{}^3 = R_2{}^3 = R_0$, $S_1{}^2 = S_2{}^2 = S_3{}^2 = R_0$ esto nos dice que R_1 y R_2 son de orden 3 y S_1, S_2 y S_3 son de orden 2, también $R_1{}^2 = R_2$, $R_1 S_1 = S_3$ y $R_1{}^2 S_1 = S_2$. De lo precedente $\tau_\Delta = \langle R_1, S_1 \rangle$ generado por R_1 y S_1 ambos.

1.4.- Modelos de grupos de igual orden salvo isomorfismo.

En este capítulo estudiaremos los grupos de orden 1, 2, 3, 4, 5, 6 y 7. Nuestro análisis será "salvo isomorfismo", con lo que queremos decir que si conocemos un grupo de un cierto orden no entraremos a analizar lo demás grupos que son isomorfos a el, pues los "*Isomorfismos"* los estudiaremos en capítulos posteriores.

Determinemos cuantos modelos distintos de grupos salvo isomorfismo existen de orden 1, 2, 3, 4, 5, 6 y 7:

1.4.1.- De orden 1:

Sea $G = \{e\}$, donde e es el elemento neutro del grupo G.

$*$	e
e	e

Luego el grupo de orden 1 queda representado por un único modelo.

$\therefore$ Existe un modelo de grupo de orden 1, salvo isomorfismo.

1.4.2- De orden 2:

Consideremos $G = \{e, a\}$, con e neutro del grupo G y $a \neq e$. Sabemos que e es el neutro del grupo entonces:

$$e * e = e \qquad e * a = a \qquad a * e = a.$$

Ahora veamos las posibilidades que existen para $a * a$, tenemos:

$$a * a = e \quad \vee \quad a * a = a.$$

Supongamos que $a * a = a$, esto es una contradicción pues el neutro del grupo es e, luego $a * a = e$.

$*$	e	a
e	e	a
a	a	e

Luego el grupo de orden 2 queda representado por este modelo.

$\therefore$ Existe un modelo de grupo de orden 2, salvo isomorfismo.

1.4.3.- De orden 3:

Consideremos $G=\{ e, a, b \}$, con e neutro del grupo y $e \neq a \neq b$. Sabemos que e es el neutro del grupo entonces:

$$e * e = e \qquad e * a = a \qquad e * b = b$$

Ahora veamos las posibilidades que existen para $a * a$, tenemos:

$$a * a = e \quad \vee \quad a * a = a \quad \vee \quad a * a = b$$

- $a * a \neq a$, pues a no es neutro en el grupo G.
- Luego supongamos que: $a * a = e$, esto es una contradicción pues "a" no puede tener dos inversos, lo que implica que $a * a = b$.

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

Luego el grupo de orden 3 queda representado por este modelo.

$\therefore$ Existe un modelo de grupo de orden 3, salvo isomorfismo.

1.4.4.- De orden 4:

Consideremos $G = \{ e, a, b, c \}$, con e neutro del grupo y $e \neq a \neq b \neq c$, ¿Cuántas tablas distintas pueden definirse?

Como e es el neutro del grupo G, entonces:

$$e * e = e \quad , \quad e * a = a \quad , \quad e * b = b \quad \wedge \quad e * c = c.$$

Ahora ¿Qué posibilidades existen para: $a * a$, $a * b \wedge a * c$?

- $a * a$:

  $a * a = b \quad \vee \quad a * a = c \quad \vee \quad a * a = e$
- $a * b$:

  $a * b = c \quad \vee \quad a * b = e$

- $a * c$:

  $a * c = e \quad \vee \quad a * c = b$

¿Qué posibilidades existen para: $b * b \wedge b * c$?

- $b * b$:

  $b * b = a \quad \vee \quad b * b = c \quad \vee \quad b * b = e$

- $b * c$:

  $b * c = a \quad \vee \quad b * c = e$

¿Qué posibilidades existen para: $c * c$?

- $c * c$:

  $c * c = e \quad \vee \quad c * c = a \quad \vee \quad c * c = b$

Luego a partir de estos datos podemos definir las siguientes tablas:

G_1 :

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

G_2 :

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

G_3 :

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

G_4 :

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

Notemos que:

- Hay 2 modelos de grupos salvo isomorfismo de orden 4 a saber:

  $G_4 \wedge G_3$, pues $G_3 \cong G_2 \cong G_1$.

- G_4 recibe el nombre de grupo de ***Klein***: K.

  El Grupo de ***Klein*** es sólo de orden 4, además es abeliano y no cíclico, pues $\forall \ x \in G_4, \ x^2 = e$, esto nos dice que todos sus elementos son de orden 2.

> **Félix Klein** (1849-1925)
>
> Matemático alemán, En 1872 presentó una notable clasificación de la geometría, el "programa de Erlangen", que puso fin a la escisión entre geometría pura y geometría analítica. En esta clasificación el concepto de grupo desempeña un papel fundamental, ya que el objeto de cada geometría se convierte en el estudio del grupo de transformaciones que la caracteriza. Profesor de la universidad de Gotinga (1886), fue el fundador de la "Gran Enciclopedia de las matemáticas" (1895) y uno de los abogados y artífices de la renovación de la enseñanza de las matemáticas en los estudios secundarios.

1.4.5.- De orden 5:

Por ser 5 un número primo resulta que todo grupo de orden 5 es cíclico, y por consiguiente será isomorfo a $\mathbb{Z}_5$. Así podemos afirmar que existe un único modelo de grupo de orden 5, este es $\mathbb{Z}_5$.

1.4.6.- De orden 6:

En este caso resultaría demasiado complicado y extenso tratar de deducir los posibles modelos de grupos de orden 6 a partir de la construcción de tablas. Por esta razón lo haremos de una manera diferente, analizando dos casos:

1º).- Si G posee un elemento de orden 6, entonces G es cíclico e isomorfo a $\mathbb{Z}_6$.

2º).- Si G no tiene ningún elemento de orden 6, debe tener elementos de orden 1,2, o 3, y no de otros órdenes (corolario del Teorema de Lagrange).

Además G no puede tener todos sus elementos de orden 2, pues si así ocurriera G sería abeliano y encontraríamos un subgrupo de G de orden 4: e, a, b, ab .

Por lo tanto existe un elemento $a \in G$ de orden 3, de esta manera tenemos 3 elementos distintos de G:

$$e,\ a,\ a^2 \qquad con\ a^3 = e$$

Por otro lado, sea $b \in G$ otro elemento distinto de lo tres anteriores, entonces podemos afirmar que el grupo G está constituido por los siguientes elementos.

$$e,\ a,\ a^2,\ b,\ ab,\ a^2b$$

Evidentemente todos ellos son distintos, por ejemplo si suponemos:

$a^2 \cdot b = a \to ab = e \to b = a^{-1} = a^2$, se produce una contradicción.

Ahora veamos que pasa con el elemento b^2, como no puede ser de la forma ab (pues llegaríamos a una contradicción), existen 3 posibilidades:

(a) $b^2 = e$ (b) $b^2 = a$ (c) $b^2 = a^2$

En los últimos casos resulta que b es de orden 3, entonces:

(c) $\to b^3 = e = a^2b$, lo que es una contradicción.

Luego debemos verificar (a), es decir:

$$b^2 = e$$

Consideremos ahora el elemento ba, para el se tiene:

(d) $ba = ab$ (e) $ba = a^2b$

Pues las otras posibilidades producen contradicciones.

En el caso (d), G sería abeliano, entonces;

$$\begin{array}{ccccccc} (ab)^2 & = & a^2b^2 & = & a^2 & \neq & e \\ (ab)^3 & = & a^3b^3 & = & b & \neq & e \end{array}$$

Así el orden de ab debe ser 6, lo que es una contradicción, por lo tanto:

$$ba = a^2 b$$

de donde:

$$(ab)^2 = ab \cdot ab = a \cdot a^2 b \cdot b = a^3 b^2 = e \cdot e = e$$

Confirmando que se verifica la asociatividad, podemos afirmar que:

$G = \{e, a, b, a^2, ab, a^2 b\}$, donde $a^3 = b^2 = (ab)^2 = e$

Así podemos concluir que si G no es cíclico, entonces es único.

Luego existen 2 modelos de grupos de orden 6, a saber:

$\mathbb{Z}_6$, cíclico S_3, no cíclico ni abeliano

Cuadro resumen

Modelos de grupos de orden dado

Orden del grupo	**Nº de grupos con este orden**	**Representantes**
1	1	$\mathbb{Z}_1$
2	1	$\mathbb{Z}_2$
3	1	$\mathbb{Z}_3$
4	2	$\mathbb{Z}_4$ y Klein
5	1	$\mathbb{Z}_5$
6	2	$\mathbb{Z}_6 \cong \mathbb{Z}_2 \times \mathbb{Z}_3$, S_3 ,
7	1	$\mathbb{Z}_7$

1.5.- Guía nº1

1.- Identificar cuáles de las siguientes estructuras constituyen un grupo. En caso de no serlo justifique su respuesta.

a) $(\mathbb{Z},-)$

Claramente no es grupo pues falla la asociatividad.
Ejemplo:

$$\begin{aligned}(5-2)-3 &\neq 5-(2-3)\\(3)-3 &\neq 5-(-1)\\0 &\neq 6\end{aligned}$$

b) $(\mathbb{N},\cdot)$

No es grupo, ya que falla el elemento inverso.
Ejemplo: Sabemos que el neutro es 1

$$
\begin{aligned}
5 \cdot x &= 1 \quad / \cdot \left(\frac{1}{5}\right) \\
x &= \frac{1}{5} \notin \mathbb{N}
\end{aligned}
$$

c) $(\mathbb{Q}*,+)$ donde $\mathbb{Q}*$ es el conjunto de los números racionales con denominador impar.

Si es grupo pues verifica todas las condiciones, es decir: la operación es cerrada, es asociativa (esta se hereda de $\mathbb{Q}$), tiene elemento neutro y elemento inverso.

d) $G=\{a_0, a_1, a_3, a_3, a_4, a_5, a_6\}$, con la operación:

$$
\begin{aligned}
a_i \cdot a_j &= a_{i+j} \quad Si\ i+j<7 \\
a_i \cdot a_j &= a_{i+j-7} \quad Si\ i+j \geq 7
\end{aligned}
$$

Para verificarlo realizaremos la tabla de Cayley, aplicando las condiciones dadas:

$\cdot$	a_0	a_1	a_2	a_3	a_4	a_5	a_6
a_0	a_0	a_1	a_2	a_3	a_4	a_5	a_6
a_1	a_1	a_2	a_3	a_4	a_5	a_6	a_0
a_2	a_2	a_3	a_4	a_5	a_6	a_0	a_1
a_3	a_3	a_4	a_5	a_6	a_0	a_1	a_2
a_4	a_4	a_5	a_6	a_0	a_1	a_2	a_3
a_5	a_5	a_6	a_0	a_1	a_2	a_3	a_4
a_6	a_6	a_0	a_1	a_2	a_3	a_4	a_5

i) Claramente la operación es cerrada
ii) Se verifica la asociatividad
iii) El neutro es a_0

iv)
- El inverso de a_0 es a_0
- El inverso de a_1 es a_6
- El inverso de a_2 es a_5
- El inverso de a_3 es a_4
- El inverso de a_4 es a_3
- El inverso de a_5 es a_2
- El inverso de a_6 es a_1

$\therefore$ G es un Grupo.

2.- Se definen las siguientes funciones con dominio $\mathbb{R}$- $\{0,1\}$, donde:

$$f_1(x) = x \; ; \; f_2(x) = \frac{1}{x} \; ; \; f_3(x) = 1 - x \; ; \; f_4(x) = \frac{x-1}{x} \; ; \; f_5(x) = \frac{x}{x-1} \; ; \; f_6(x) = \frac{1}{1-x}$$

Demostrar que este conjunto forma un grupo con la operación de funciones, ¿Es abeliano?

$\circ$	f_1	f_2	f_3	f_4	f_5	f_6
f_1	f_1	f_2	f_3	f_4	f_5	f_6
f_2	f_2	f_1	f_6	f_5	f_4	f_3
f_3	f_3	f_4	f_1	f_2	f_6	f_5
f_4	f_4	f_3	f_5	f_6	f_2	f_1
f_5	f_5	f_6	f_4	f_3	f_1	f_2
f_6	f_6	f_5	f_2	f_1	f_3	f_4

Sea F el grupo formado por todas las funciones nombradas anteriormente, con la operación composición de funciones.

i) Claramente la operación composición de funciones es cerrada, teniendo en cuenta que está definida con dominio $\mathbb{R}$- $\{0,1\}$

ii) Se verifica la asociatividad

iii) El neutro de las funciones es la función identidad $f(x) = x$

iv)
- El inverso de f_1 es f_1 (neutro)
- El inverso de f_2 es f_2
- El inverso de f_3 es f_3
- El inverso de f_4 es f_6
- El inverso de f_5 es f_5
- El inverso de f_6 es f_4

$\therefore$ F , es un Grupo

¿Es conmutativo?

F , claramente no es abeliano, ya que la composición de funciones no lo es.

Ejemplo:

$$f_1 \circ f_2 \neq f_2 \circ f_1$$

$$f_2 \neq f_1$$

$\therefore$ F no es conmutativo.

3.- Dado $\tau_{a,b} : \mathbb{R} \to \mathbb{R}$, tal que $\forall\, x \in \mathbb{R},\ \tau_{a,b}(x) = ax + b$ y sea $G = \{\tau_{a,b} \ / \ a \neq 0\}$. Probar que G es un grupo con la operación composición de funciones.

i) ¿Es cerrada la operación?

Dados $\tau_{a,b}$, $\tau_{c,d} \in G$, por demostrar que $\tau_{a,b} \cdot \tau_{c,d} \in G$, con $a \neq 0$ y $c \neq 0$, luego tenemos:

$$\begin{aligned}
\forall\, x \in \mathbb{R} \; ; \; (\tau_{a,b} \cdot \tau_{c,d})(x) &= \tau_{a,b}(\tau_{c,d}(x)) \\
&= \tau_{a,b}(cx+d) \\
&= a(cx+d)+b \\
&= (ac)x+(ad+b)
\end{aligned}$$

Luego $\tau_{a,b} \cdot \tau_{c,d} = \tau_{ac,ad+b}$, donde $ac \neq 0$ y $\tau_{ac,ad+b} \in G$

$\therefore$ La operación composición de funciones es cerrada.

ii) ¿Es asociativa?

Sean $\tau_{a,b}(x) = ax+b;\; a \neq 0, \tau_{c,d}(x) = cx+d;\; c \neq 0, \tau_{e,f}(x) = ex+f;\; e \neq 0$, por demostrar que $(\tau_{a,b} \cdot \tau_{c,d}) \cdot \tau_{e,f} = \tau_{a,b} \cdot (\tau_{c,d} \cdot \tau_{e,f})$.

Se tiene:

$$\begin{aligned}
\forall\, x \in \mathbb{R} \; ; \; \tau_{a,b} \cdot (\tau_{c,d} \cdot \tau_{e,f})(x) &= \tau_{a,b} \cdot (\tau_{c,d}(\tau_{e,f}(x))) \\
&= \tau_{a,b} \cdot (\tau_{c,d}(ex+f)) \\
&= \tau_{a,b} \cdot (c(ex+f)+d) \\
&= \tau_{a,b} \cdot (cex+cf+d)) \\
&= a(cex+cf+d)+b \\
&= acex+acf+ad+b \\
&= ac(ex+f)+ad+b \\
&= \tau_{ac,ad+b}(ex+f) \\
&= \tau_{ac,ad+b}(\tau_{e,f}) \\
&= (\tau_{a,b} \cdot \tau_{c,d}) \cdot \tau_{e,f}
\end{aligned}$$

$\therefore$ Es asociativa

iii) ¿Existe elemento neutro?

$\exists\ \tau_{w,u} \in G$, talque $\tau_{a,b} \in G$, por demostrar que $\tau_{w,u} \cdot \tau_{a,b} = \tau_{a,b}$.
Supongamos que:

$$\begin{aligned}
(\tau_{w,u} \cdot \tau_{a,b})(x) &= \tau_{a,b}(x) \\
\tau_{w,u}(\tau_{a,b}(x)) &= ax+b \\
\tau_{w,u}(ax+b) &= ax+b \\
w(ax+b)+u &= ax+b \\
(wa)x+(wb+u) &= ax+b
\end{aligned}$$

Se tiene:

$$wa = a \Rightarrow w = 1 \quad \wedge \quad wb+u = b \Rightarrow u = 0$$

$\therefore\ \tau_{1,0}$, es el neutro en G

iv) Elemento inverso

$\forall\ \tau_{a,b} \in G, \exists\ \tau_{p,q} \in G,$ Talque $\tau_{a,b} \cdot \tau_{p,q} = \tau_{1,0}$
Supongamos que:

$$\begin{aligned}
(\tau_{a,b} \cdot \tau_{p,q})(x) &= \tau_{1,0}(x) \\
(\tau_{a,b} \cdot \tau_{p,q}(x)) &= x+0 \\
\tau_{a,b}(px+q) &= x \\
apx+aq+b &= x \qquad / \ ap \neq 0
\end{aligned}$$

Se tiene: $ap = 1 \Rightarrow p = \dfrac{1}{a} \quad \wedge \quad qa+b = 0 \Rightarrow q = \dfrac{-b}{a}$

$\therefore\ \tau_{\frac{1}{a},\frac{-b}{a}}$, es el inverso de $\tau_{a,b}$

$\therefore$ G, es grupo.

1.6.- Autoevaluación 1

1.- Demostrar que el conjunto $\left\{a+b\sqrt{2}\ /\ a,\ b\in\mathbb{Q},\ \text{no ambos nulos}\right\}$, forma un grupo con la multiplicación ordinaria.

2.- Sea $G=\{\ (a,b)/\,a,\,b\ \in\ \mathbb{R},\ \ a\neq 0\}$ y la operación definida en G sea la siguiente: $(a,b)\cdot(c,d)=(ac,bc+d)$. Demostrar que $(G\ ,\ \cdot)$ es grupo. ¿Es abeliano?

3.- Probar que las matrices:

$$\begin{bmatrix}1&0\\0&1\end{bmatrix},\ \begin{bmatrix}w&0\\0&w^2\end{bmatrix},\ \begin{bmatrix}w^2&0\\0&w\end{bmatrix},\ \begin{bmatrix}0&1\\1&0\end{bmatrix},\ \begin{bmatrix}0&w^2\\w&0\end{bmatrix},\ \begin{bmatrix}0&w\\w^2&0\end{bmatrix}$$

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

En las que $w^3 = 1,\ w \neq 1$, forman un grupo con la operación multiplicación de matrices, definida por:

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \begin{bmatrix} p & q \\ r & s \end{bmatrix} = \begin{bmatrix} ap+br & aq+bs \\ cp+dr & cq+ds \end{bmatrix}$$

4.- Sea $G = \mathbb{R} \times \mathbb{R}$, donde su operación $*$ está dada por: $(a,b)*(c,d) = (a+c, b+d+2bd), \forall (a,b),(c,d) \in G$. Verificar si $(G\ ,\ *)$ es grupo. Justificar su respuesta.

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