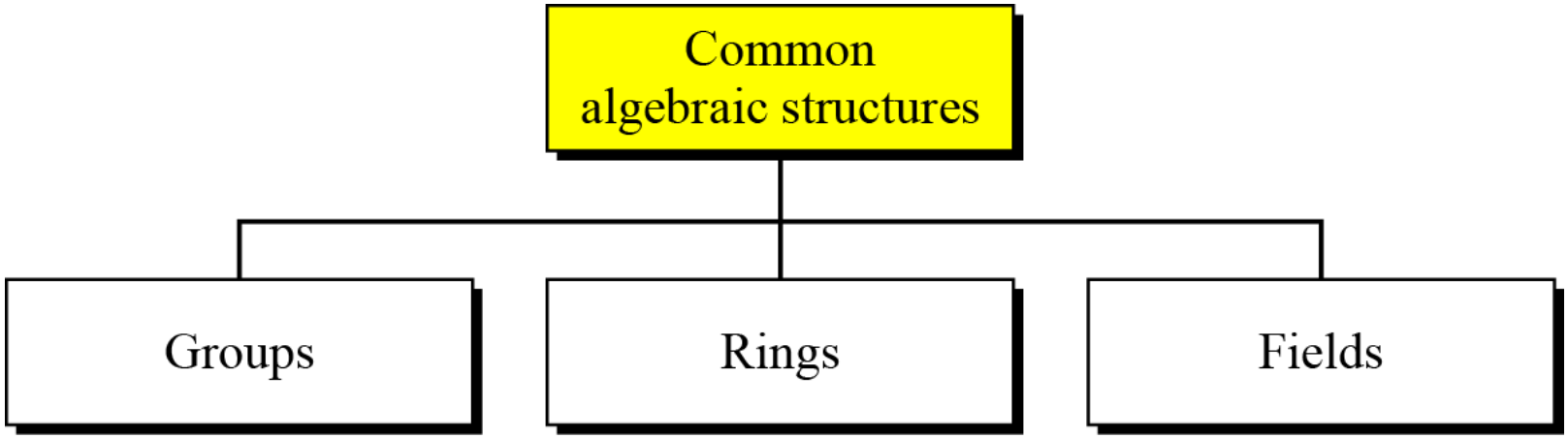
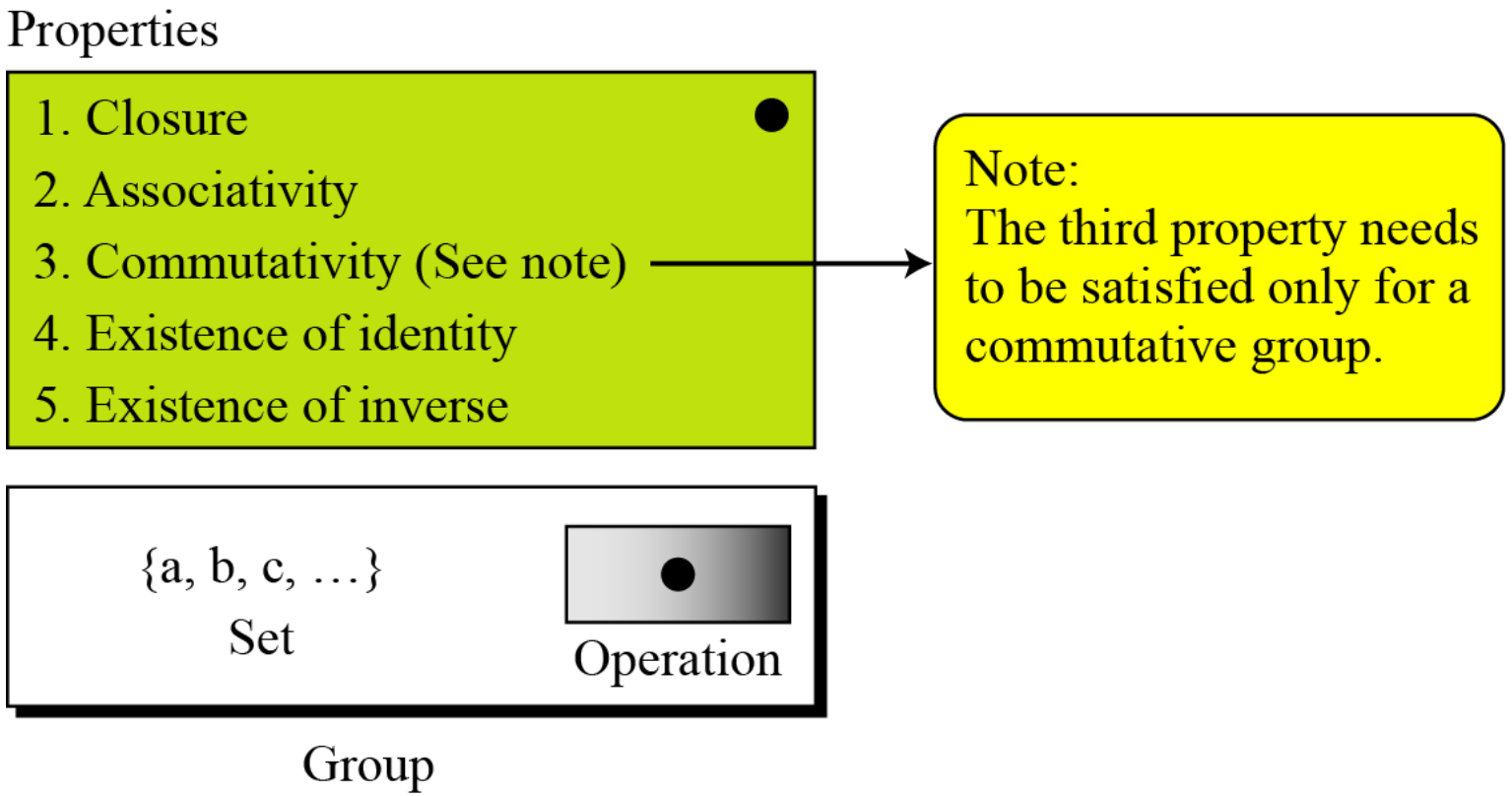
GRUPOS

Cap. 16 (Grimaldi)


Common
algebraic structures
Groups
Rings
Fields

GRUPO

- Un grupo (**G**) es un conjunto de elementos con una operación binaria (**.**) que satisface cuatro propiedades o axiomas y una propiedad extra, conmutativa



GRUPO

- **Definición 16.1**
  - Si G es un conjunto no vacío y ° es una operación binaria en G, entonces (G, °) es un grupo si cumple las siguientes condiciones.
    1) **G es cerrado mediante °**
       Para todo a, b ∈ G, a°b ∈ G
    2) **Propiedad asociativa**
       Para todo a, b, c ∈ G, a°(b °c) = (a°b)°c.
    3) **Existencia de un elemento identidad o neutro**
       Existe un **e** ∈ G tal que a°e = e°a=a, para todo a ∈ G.
    4) **Existencia de inversos.**
       Para a ∈ G existe un elemento b ∈ G tal que a°b=b °a=**e**.
    5) **Grupo conmutativo abeliano**
       Si, a°b=b °a para todo a,b ∈ G.

GRUPO

- Ejemplo: G=({a,b,c,d},•)

•	*a*	*b*	*c*	*d*
a	*a*	*b*	*c*	*d*
b	*b*	*c*	*d*	*a*
c	*c*	*d*	*a*	*b*
d	*d*	*a*	*b*	*c*

Cerradura:
Asociatividad: (a+b) + c = a+ (b + c)
Conmutativa: a+b=b+a (Grupo abeliano)
Elemento Identidad: a
Existencia de inversos: (a,a), (b,d), (c,c)

GRUPO

- Ejemplo: G={e,a,b,c}

°	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

Elemento Identidad:

Existencia de inversos:

Grupo abeliano:

GRUPO

- Ejemplo: $(Z_6,+)$

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

Elemento Identidad:

Existencia de inversos:

Grupo abeliano:

GRUPO

- Ejemplo: Si p es primo (Z^*_7 , .)

.	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

Elemento Identidad:

Existencia de inversos:

Grupo abeliano:

GRUPO

- Para n $\in Z^+$, n>1, (Zn,+) es un grupo abeliano.
- Si p es primo $(Z^*_p, .)$ es un grupo abeliano.

- Definición 16.2:
  - Para cualquier grupo G, el número de elementos de G es el **orden** de G que se denota con |G|.

- Ejemplo:
  - Para cualquier n $\in Z^+$, $|(Z_n,+)| = n$
  - Para cualquier p primo $|(Z^*_p, .)| = p-1$

GRUPO

- Ejemplo:
  - $(Z_9, +, .)$
  - $U_9 = \{a \in Z_9 \mid a \text{ es una unidad en } Z_9\} = \{a \in Z_9 \mid a^{-1} \text{ existe}\}$

GRUPO

- $U_9 = \{1,2,4,5,7,8\} = \{a \in Z+ \mid 1 \leq a \leq 8 \text{ y } mcd(a,9)=1\}$

.	1	2	4	5	7	8
1	1	2	4	5	7	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	4	2
8	8	7	5	4	2	1

Elemento Identidad:
Existencia de inversos:
Grupo abeliano:
Orden

U9=Grupo de unidades del anillo
U9= es cerrado mediante la operación binaria de multiplicación módulo n.

GRUPO

- Teorema 16.1: Para cualquier grupo G.
  a) El neutro o identidad de G es único.
  b) El inverso de cada elemento de G es único.
  c) Si a,b,c ∈ G y ab=ac, entonces b=c.
     (**Propiedad cancelativa por la izquierda**).
  d) Si a,b,c ∈ G y ba=ca, entonces b=c.
     (**Propiedad cancelativa por la derecha**)

GRUPO

- Definición 16.3:
  - Sea G un grupo y $\emptyset \neq H$ incluido G. Si H es un grupo mediante la operación binaria de G, entonces H es un subgrupo de G.
- Ejemplo:
  - Sea G $=(Z_5,+)$. Si H $= \{0,2,4\}$, entonces H es un subconjunto no vacío de G.

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

+	0	2	4
0	0	2	4
2	2	4	0
4	4	0	2

SUB-GRUPO

- Teorema 16.3
  - Si G es un grupo y Ø≠H incluido G, con H finito, entonces H es un **Subgrupo** de G si y solo si H es cerrado mediante la operación binaria G.

SUB-GRUPOS

- Un subconjunto H de un grupo G es un sub-grupo de G si H es grupo con respecto a la operación en G.
  - Si a y b son miembros de ambos grupos, entonces c=a*b es también miembro de ambos grupos.
  - El grupo comparte el mismo elemento identidad.
  - Si a es un elemento de ambos grupos, la inversa de a es también miembro de ambos grupos
  - El grupo obtenido del elemento identidad de G, H=<[e],*> es un sub-grupo de G.
  - Cada grupo es un sub-grupo de si mismo.

SUB-GRUPOS

- Es el grupo $H=(Z_{10},+)$ un subgrupo del grupo $G(Z_{12},+)$?

GRUPO

- Ejemplo:
  - G={e,a,b,c}
  - H={e,b}

.	e	b
e	e	b
b	b	e

Operación binaria cerrada.
Elemento neutro:
Inverso:

EJERCICIOS

- Cuál de los siguientes sub-conjuntos (H) de G Z_{13} son grupos con la operación de multiplicación?
  - H={1,3,5,7,9,11}
  - H={1,2,3,4,5,6,8,9,10,11}
  - H={1,3,5,8,9}
  - H={1,5,8,12}

GRUPO FINITO

- Grupo Finito
  - Un grupo es llamado de finito si el conjunto tiene un número finito de elementos, de lo contrario es un grupo infinito.

Grupo cíclico

- Definición 16.6
  - Un grupo G es cíclico si existe un elemento x ∈ G tal que a ∈ G, $a = x^n$ para algún n ∈ Z.

Nota: $a^0 = e$

- **G = <Z6, +>**

$0^0 \bmod 6 = 0$

$1^0 \bmod 6 = 0$
$1^1 \bmod 6 = 1$
$1^2 \bmod 6 = (1 + 1) \bmod 6 = 2$
$1^3 \bmod 6 = (1 + 1 + 1) \bmod 6 = 3$
$1^4 \bmod 6 = (1 + 1 + 1 + 1) \bmod 6 = 4$
$1^5 \bmod 6 = (1 + 1 + 1 + 1 + 1) \bmod 6 = 5$

$2^0 \bmod 6 = 0$
$2^1 \bmod 6 = 2$
$2^2 \bmod 6 = (2 + 2) \bmod 6 = 4$

$3^0 \bmod 6 = 0$
$3^1 \bmod 6 = 3$

$4^0 \bmod 6 = 0$
$4^1 \bmod 6 = 4$
$4^2 \bmod 6 = (4 + 4) \bmod 6 = 2$

$5^0 \bmod 6 = 0$
$5^1 \bmod 6 = 5$
$5^2 \bmod 6 = 4$
$5^3 \bmod 6 = 3$
$5^4 \bmod 6 = 2$
$5^5 \bmod 6 = 1$

Grupo cíclico

- Elemento generador
  - Si g es un generador, los elementos en un finito grupo cíclico puede ser escrito como:

$$\{e, g, g^2, \ldots, g^{n-1}\}, \text{ where } g^n = e$$

    - Denotado por G ‹g›

  - **G = <Z6, +> = Z6= ‹[1]›,‹[5]›**

Grupo cíclico

- Definición 16.7: Orden de un elemento
  - Si G es un grupo y a Є G, el orden de a, que denotamos como ȯ(a), es |‹a›|.
  - **G = <Z6, +>**
    - ȯ(0)= 1
    - ȯ(1)= 6
    - ȯ(2)= 3
    - ȯ(3)= 2
    - ȯ(4)= 3
    - ȯ(5)= 6

Sub-Grupos cíclicos

- Si un sub-grupo de un grupo puede ser generador usando la potencia de un elemento, el sub-grupo es llamado sub-grupo cíclico

$$a^n \rightarrow a \bullet a \bullet \ldots \bullet a \quad (n \text{ times})$$

Sub-Grupos cíclicos: Ejemplo

- 4 subgrupos cíclicos pueden obtenerse del grupo
  - G = <Z6, +>.
    - H1 = <{0}, +>,
    - H2 = <{0, 2, 4}, +>,
    - H_3 = <{0, 3}, +>,
    - H4 = G.

Sub-Grupos cíclicos: Ejemplo

- G = <Z10*, ×>.
  - G has only four elements: 1, 3, 7, and 9.
  - Los subgrupos cíclicos son
    - H1 = <{1}, ×>,
    - H2 = <{1, 9}, ×>,
    - H3 = G

$1^0 \bmod 10 = 1$

$3^0 \bmod 10 = 1$
$3^1 \bmod 10 = 3$
$3^2 \bmod 10 = 9$
$3^3 \bmod 10 = 7$

$7^0 \bmod 10 = 1$
$7^1 \bmod 10 = 7$
$7^2 \bmod 10 = 9$
$7^3 \bmod 10 = 3$

$9^0 \bmod 10 = 1$
$9^1 \bmod 10 = 9$

Teorema de Lagrange

- Asume que si G es un grupo, y H es un sub-grupo. Si el orden de G y H son |G| y |H|, entonces |H| divide |G|.
- $G = <Z_6, +>$.
  - $|Z_6|=6$
  - $|H1| = 1$
  - $|H2| = 3$
  - $|H3| = 2$
  - $|H4| = 6$
- Dado un grupo G de |G|, los ordenes de los sub-grupos potencias se determinan si los divisores de G pueden ser encontrados
- $G = <Z_{17}, +>$.
  - $|Z_{17}|=17$. Los divisores son 1 y 17. Tiene dos sub-grupos H1=identidad y H2=G

HOMOMORFISMO, ISOMORFISMO

- Definición 16.4:
  - Si $(G,^{o})$, $(H,*)$ son grupos y $f: G \rightarrow H$, entonces f es un homomorfismo de grupos si para todos $a,b \in G$,
    - $f(a \, ^{o} \, b) = f(a) * f(b)$

- Teorema 16.5
  - Sean $(G,^{o})$, $(H,*)$ grupos con neutros respectivos e_g y e_h. Si $f: G \rightarrow H$ es un homomorfismo, entonces:
    - $f(e_g) = e_h$
    - $f(a^{-1}) = [f(a)]^{-1}$ par todo $a \in G$.
    - $f(a_n) = [f(a)]^{n}$ para todo $a \in G$ y todo $n \in Z$.
    - f(S) es un subgrupo de H para cada subgrupo S de G.

HOMOMORFISMO, ISOMORFISMO

- Definición 16.5:
  - Si $f: G \rightarrow H$ es un homomorfismo, f es un isomorfismo si es inyectiva y sobre. En este caso, G y H son grupos isomorfos.

HOMOMORFISMO, ISOMORFISMO

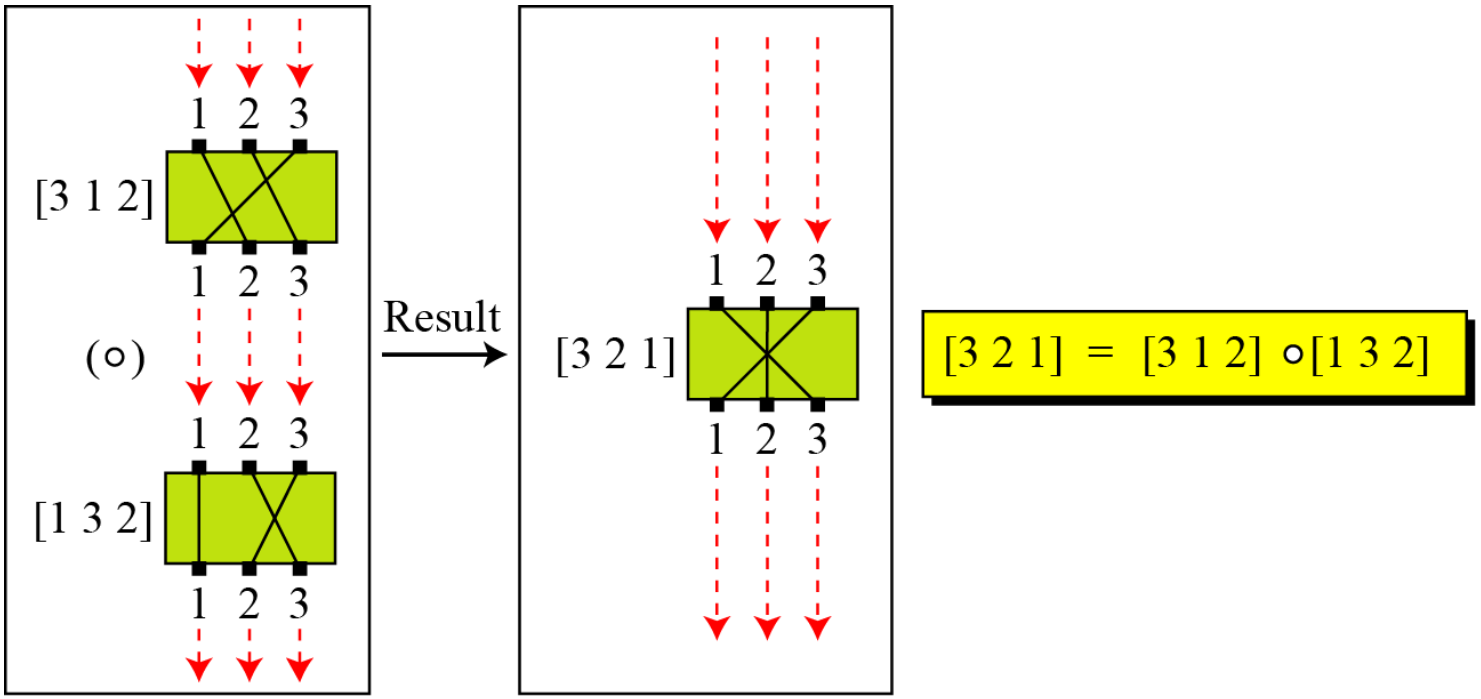
- Ejemplo:
  - Sea G el grupo de números complejos {1,-1,i,-i} mediante el producto. Si $H=(Z_4,+)$, consideremos la función f: G⟶H dada por

    f(1) =[0] f(-1) =[2] f(i) =[1] f(-i) =[3]

.	1	-1	i	-i
1	1	-1	i	-i
-1	-1	1	-i	i
i	i	-i	-1	1
-i	-i	i	1	-1

Grupo: Permutación

- Conjunto de datos: Permutaciones
- Operación: Composición: una permutación después de otra



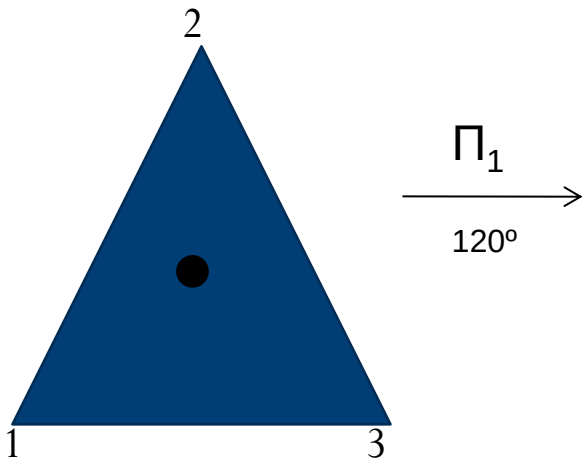
Grupo: Permutación

- Conjunto de datos: Permutaciones
- Operación: Composición: una permutación después de otra

°	[1 2 3]	[1 3 2]	[2 1 3]	[2 3 1]	[3 1 2]	[3 2 1]
[1 2 3]	[1 2 3]	[1 3 2]	[2 1 3]	[2 3 1]	[3 1 2]	[3 2 1]
[1 3 2]	[1 3 2]	[1 2 3]	[2 3 1]	[2 1 3]	[3 2 1]	[3 1 2]
[2 1 3]	[2 1 3]	[3 1 2]	[1 2 3]	[3 2 1]	[1 3 2]	[2 3 1]
[2 3 1]	[2 3 1]	[3 2 1]	[1 3 2]	[3 1 2]	[1 2 3]	[2 1 3]
[3 1 2]	[3 1 2]	[2 1 3]	[3 2 1]	[1 2 3]	[2 3 1]	[1 3 2]
[3 2 1]	[3 2 1]	[2 3 1]	[3 1 2]	[1 3 2]	[2 1 3]	[1 2 3]

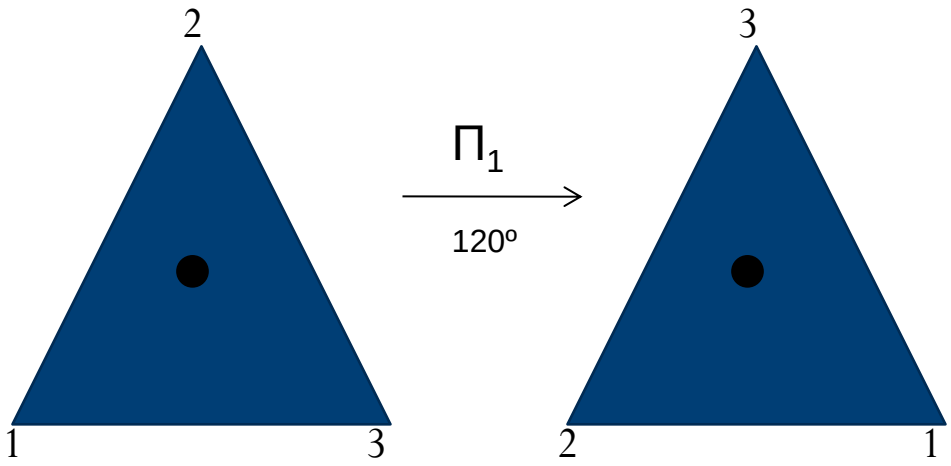
GRUPOS: ejemplo

- Considere el triángulo equilátero



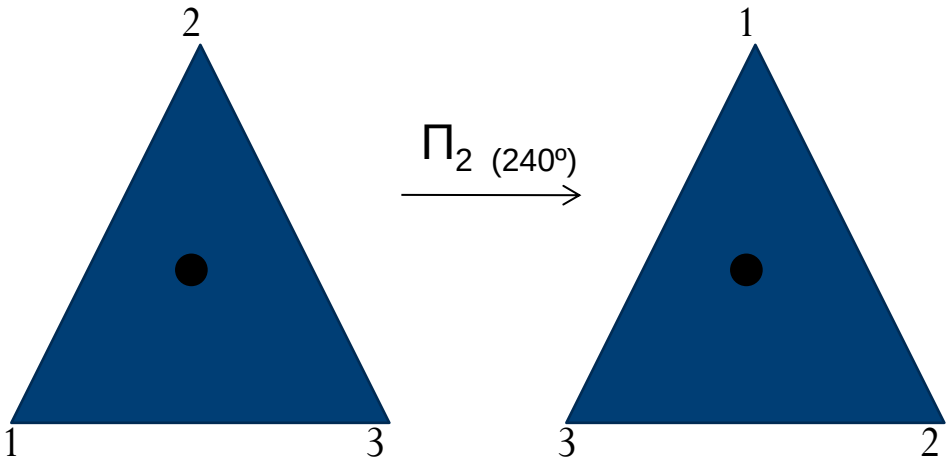
GRUPOS: ejemplo

- Considere el triángulo equilátero



GRUPOS: ejemplo

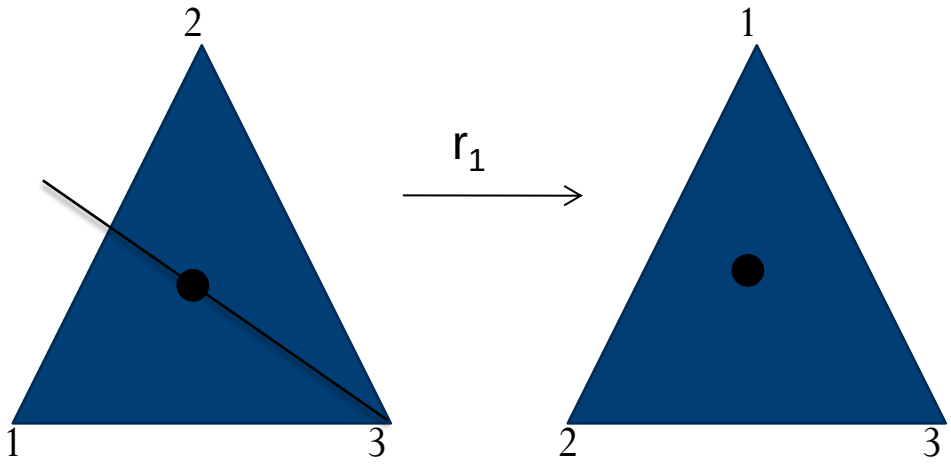
- Considere el triángulo equilátero



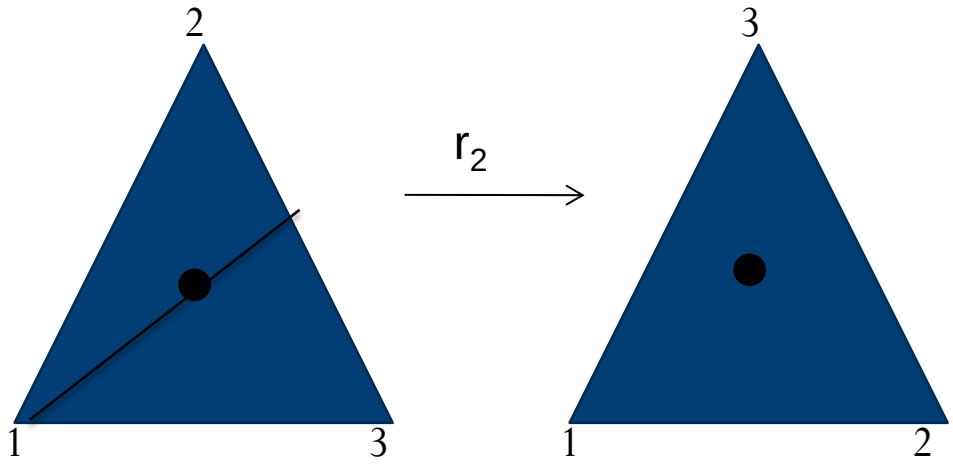
Movimientos rígidos del triángulo: Conservan fijo el centro y preservan la forma.

GRUPOS: Ejemplo

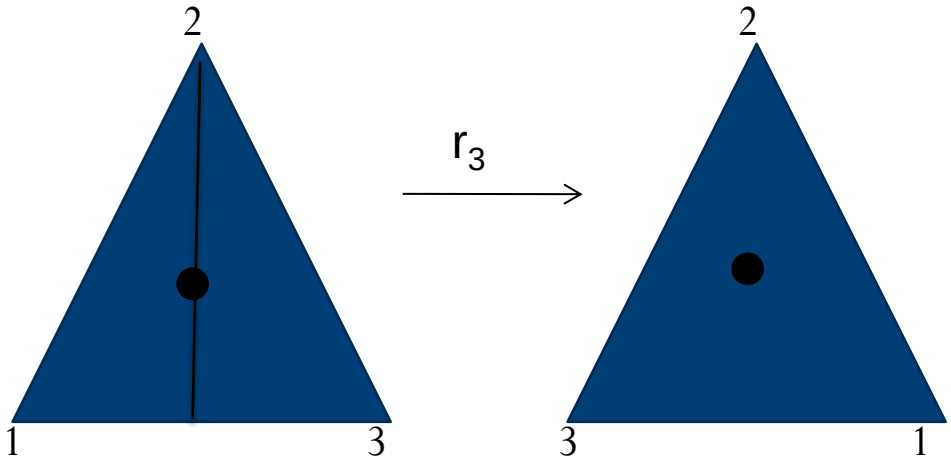
- **Reflejar el triángulo** a lo largo de un eje que pasa por un vértice y por el punto medio del lado opuesto.



GRUPOS: Ejemplo



GRUPOS: Ejemplo



GRUPOS: Ejemplo

- Sea G={Π_0, Π_2, Π_3, r_1, r_2, r_3,}
- G un grupo que define el movimiento rígido $\alpha\beta \in$ G, como el movimiento obtenido de aplicar primero α y después β.

.	Π_0	Π_1	Π_2	r_1	r_2	r_3
Π_0						
Π_1				r_3		
Π_2						
r_1						
r_2						
r_3						

$\Pi_1\, r_1$

$1 \rightarrow 3 \rightarrow 3$

$2 \rightarrow 1 \rightarrow 2$

$3 \rightarrow 2 \rightarrow 1$

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

GRUPOS: Ejemplo

- Sea G={Π_0, Π_2, Π_3, r_1, r_2, r_3,}
- G un grupo que define el movimiento rígido $\alpha\beta \in$ G, como el movimiento obtenido de aplicar primero α y después β.

.	Π_0	Π_1	Π_2	r_1	r_2	r_3
Π_0	Π_0	Π_1	Π_2	r_1	r_2	r_3
Π_1	Π_1	Π_2	Π_0	r_3	r_1	r_2
Π_2	Π_2	Π_0	Π_1	r_2	r_3	r_1
r_1	r_1	r_2	r_3	Π_0	Π_1	Π_2
r_2	r_2	r_3	r_1	Π_2	Π_0	Π_1
r_3	r_3	r_1	r_2	Π_1	Π_2	Π_0

Elemento neutro:

Inversa:

Abeliano:

Ejercicios Grimaldi

- Ejercicios 16.1
- Ejercicios 16.2

Referencias

- Discrete and Combinatorial Matemathics. 5ta ed. Ralph P. Grimaldi. Ch. 16 Groups, Coding, Theory, and Polya´s Method of enumeration

- Algebra Abstracta Primer Curso John B. Fraleigh Caps. 2,3,4,5,6 y 7

- Cryptography and Network Security (Behrouz Forouzan) Mathematics of Cryptography. Ch. 4