MATEMÁTICA DISCRETA
Estructuras Algebraicas

Prof. Sergio Salinas

Facultad de Ingeniería
Universidad Nacional de Cuyo

Segundo semestre 2024

Contenido

Subgrupos

Subgrupos

Definición

Sea $< G, * >$ *un grupo, entonces un subconjunto* $H \subset G$ *es un subgrupo de* $< G, * >$ *si satisface las siguientes condiciones:*

1. $e \in H$, *donde* e *es el elemento identidad de* G.
2. *para* $a, b \in H$, *se tiene que* $a * b \in H$.
3. *para todo* $a \in H$, *se tiene que* $a^{-1} \in H$.

Subgrupos

Definición

Sea $< G, * >$ un grupo, entonces un subconjunto $H \subset G$ es un subgrupo de $< G, * >$ si satisface las siguientes condiciones:

1. *$e \in H$, donde e es el elemento identidad de G.*
2. *para $a, b \in H$, se tiene que $a * b \in H$.*
3. *para todo $a \in H$, se tiene que $a^{-1} \in H$.*

Es posible observar que $< H, * >$ es un grupo en sí mismo, con el mismo elemento identidad e y la misma operación binaria $*$.

Subgrupos

Definición

Sea $< G, * >$ *un grupo, entonces un subconjunto* $H \subset G$ *es un subgrupo de* $< G, * >$ *si satisface las siguientes condiciones:*

1. $e \in H$*, donde* e *es el elemento identidad de* G.
2. *para* $a, b \in H$*, se tiene que* $a * b \in H$.
3. *para todo* $a \in H$*, se tiene que* $a^{-1} \in H$.

Es posible observar que $< H, * >$ es un grupo en sí mismo, con el mismo elemento identidad e y la misma operación binaria $*$.

Como e y G son subconjuntos de G y satisface las tres condiciones anteriores, entonces $< e, * >$ y $< G, * >$ son subgrupos de $< G, * >$. Estos subgrupos son llamados **subgrupos triviales**. Los demás subgrupos, si los hay, son llamados **subgrupos propios**.

Ejemplos:

1. Sea $< \mathbb{Z}, + >$ un grupo entonces $\mathbb{H} = 2\mathbb{Z}$ es un subgrupo de $\mathbb{Z}$.
2. $H = \mathbb{Q}$ es un subgrupo de $< \mathbb{R}, + >$
3. $H = \{[0], [2], [4]\}$ es un subgrupo de $< \mathbb{Z}_6, + >$
4. $H = \{[0], [2], [4], [6]\}$ es un subgrupo de $< \mathbb{Z}_8, + >$
5. Sea $< GL(2, \mathbb{R}), \cdot >$ el grupo lineal general, esto es, el conjunto de matrices invertibles de tamaño 2. Entonces, el subconjunto H de matrices diagonales invertibles definido por: $H = \{\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \mid a, b \in \mathbb{R}^*, a \neq 0, b \neq 0\}$ es un subgrupo de $< GL(2, \mathbb{R}), \cdot >$.

Clases Laterales

Clases laterales

Definición

Sea $< H, * >$ *un subgrupo de* $< G, * >$, *entonces el conjunto* $aH \subset G$ *con* $a \in G$, *definido por*

$$aH = \{a * h : h \in H\},$$

se denomina **clases lateral izquierda** *o* **agregación izquierda** *de* H *en* G *generada por* $a \in G$. *A veces el elemento* $a \in G$ *recibe el nombre de representativo de la clase lateral izquierda* aH.

Definición

Sea $< H, * >$ *un subgrupo de* $< G, * >$*, entonces el conjunto* $Ha \subset G$ *con* $a \in G$*, definido por*

$$Ha = \{h * a : h \in H\},$$

se denomina **clases lateral derecha** *o* **agregación derecha** *de* H *en* G *generada por* $a \in G$*. A veces el elemento* $a \in G$ *recibe el nombre de representativo de la clase lateral derecha* Ha*.*

Lema 1

Si H es un subgrupo del grupo G, entonces las clases laterales izquierda y derecha de H en G forman una partición de G.

Lema 1

Si H es un subgrupo del grupo G, entonces las clases laterales izquierda y derecha de H en G forman una partición de G.

Lema 2

Si H es un subgrupo del grupo G, entonces las clases laterales izquierda y derecha de H en G tienen el mismo número de elemento que H.

Lema 1

Si H es un subgrupo del grupo G, entonces las clases laterales izquierda y derecha de H en G forman una partición de G.

Lema 2

Si H es un subgrupo del grupo G, entonces las clases laterales izquierda y derecha de H en G tienen el mismo número de elemento que H.

El conjunto de todas las clases laterales a la derecha se denota como $G/H_{\sim} = \{hg|h \in G\}$ para toda $g \in G$, análogamente el conjunto de clases laterales a la izquierda $G/_{\sim}H = \{gh|h \in G\}$ para toda $g \in G$. En el caso de de que $G/H_{\sim} = G/_{\sim}H$ se denota como G/H y se denominan conjuntos cocientes derecho, izquierdo y conjunto cociente respectivamente.

Sea $H = \{[0], [3]\} \subset \mathbb{Z}_6$ entonces:

Sea $H = \{[0], [3]\} \subset \mathbb{Z}_6$ entonces:

$+$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$
$[0]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$
$[1]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$	$[0]$
$[2]$	$[2]$	$[3]$	$[4]$	$[5]$	$[0]$	$[1]$
$[3]$	$[3]$	$[4]$	$[5]$	$[0]$	$[1]$	$[2]$
$[4]$	$[4]$	$[5]$	$[0]$	$[1]$	$[2]$	$[3]$
$[5]$	$[5]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$

Clases laterales

Sea $H = \{[0], [3]\} \subset \mathbb{Z}_6$ entonces:

Clases laterales

Sea $H = \{[0], [3]\} \subset \mathbb{Z}_6$ entonces:

Clases laterales izquierda:

Clases laterales

Sea $H = \{[0], [3]\} \subset \mathbb{Z}_6$ entonces:

Clases laterales izquierda:

$[0] + H = \{[0], [3]\}$

Sea $H = \{[0], [3]\} \subset \mathbb{Z}_6$ entonces:

Clases laterales izquierda:

$[0] + H = \{[0], [3]\}$
$[1] + H = \{[1], [4]\}$

Sea $H = \{[0], [3]\} \subset \mathbb{Z}_6$ entonces:

Clases laterales izquierda:

$[0] + H = \{[0], [3]\}$
$[1] + H = \{[1], [4]\}$

$[2] + H = \{[2], [5]\}$

Clases laterales

Sea $H = \{[0], [3]\} \subset \mathbb{Z}_6$ entonces:

Clases laterales izquierda:

$[0] + H = \{[0], [3]\}$
$[1] + H = \{[1], [4]\}$

$[2] + H = \{[2], [5]\}$

$[3] + H = \{[3], [0]\}$

Clases laterales

Sea $H = \{[0],[3]\} \subset \mathbb{Z}_6$ entonces:

Clases laterales izquierda:

$[0] + H = \{[0],[3]\}$
$[1] + H = \{[1],[4]\}$

$[2] + H = \{[2],[5]\}$

$[3] + H = \{[3],[0]\}$

$[4] + H = \{[4],[1]\}$

Sea $H = \{[0], [3]\} \subset \mathbb{Z}_6$ entonces:

Clases laterales izquierda:

$[0] + H = \{[0], [3]\}$
$[1] + H = \{[1], [4]\}$

$[2] + H = \{[2], [5]\}$

$[3] + H = \{[3], [0]\}$

$[4] + H = \{[4], [1]\}$

$[5] + H = \{[5], [2]\}$

Sea $H = \{[0], [3]\} \subset \mathbb{Z}_6$ entonces:

Clases laterales izquierda:

$[0] + H = \{[0], [3]\}$

$[1] + H = \{[1], [4]\}$

$[2] + H = \{[2], [5]\}$

$[3] + H = \{[3], [0]\}$

$[4] + H = \{[4], [1]\}$

$[5] + H = \{[5], [2]\}$

Clases laterales derecha:

Clases laterales

Sea $H = \{[0],[3]\} \subset \mathbb{Z}_6$ entonces:

Clases laterales izquierda:

$[0] + H = \{[0],[3]\}$

$[1] + H = \{[1],[4]\}$

$[2] + H = \{[2],[5]\}$

$[3] + H = \{[3],[0]\}$

$[4] + H = \{[4],[1]\}$

$[5] + H = \{[5],[2]\}$

Clases laterales derecha:

$H + [0] = \{[0],[3]\}$

Clases laterales

Sea $H = \{[0], [3]\} \subset \mathbb{Z}_6$ entonces:

Clases laterales izquierda:

$[0] + H = \{[0], [3]\}$
$[1] + H = \{[1], [4]\}$

$[2] + H = \{[2], [5]\}$

$[3] + H = \{[3], [0]\}$

$[4] + H = \{[4], [1]\}$

$[5] + H = \{[5], [2]\}$

Clases laterales derecha:

$H + [0] = \{[0], [3]\}$
$H + [1] = \{[1], [4]\}$

Clases laterales

Sea $H = \{[0], [3]\} \subset \mathbb{Z}_6$ entonces:

Clases laterales izquierda:

$[0] + H = \{[0], [3]\}$

$[1] + H = \{[1], [4]\}$

$[2] + H = \{[2], [5]\}$

$[3] + H = \{[3], [0]\}$

$[4] + H = \{[4], [1]\}$

$[5] + H = \{[5], [2]\}$

Clases laterales derecha:

$H + [0] = \{[0], [3]\}$

$H + [1] = \{[1], [4]\}$

$H + [2] = \{[2], [5]\}$

Clases laterales

Sea $H = \{[0],[3]\} \subset \mathbb{Z}_6$ entonces:

Clases laterales izquierda:

$[0] + H = \{[0],[3]\}$
$[1] + H = \{[1],[4]\}$
$[2] + H = \{[2],[5]\}$
$[3] + H = \{[3],[0]\}$
$[4] + H = \{[4],[1]\}$
$[5] + H = \{[5],[2]\}$

Clases laterales derecha:

$H + [0] = \{[0],[3]\}$
$H + [1] = \{[1],[4]\}$
$H + [2] = \{[2],[5]\}$
$H + [3] = \{[3],[0]\}$

Sea $H = \{[0], [3]\} \subset \mathbb{Z}_6$ entonces:

Clases laterales izquierda:

$[0] + H = \{[0], [3]\}$
$[1] + H = \{[1], [4]\}$

$[2] + H = \{[2], [5]\}$

$[3] + H = \{[3], [0]\}$

$[4] + H = \{[4], [1]\}$

$[5] + H = \{[5], [2]\}$

Clases laterales derecha:

$H + [0] = \{[0], [3]\}$
$H + [1] = \{[1], [4]\}$

$H + [2] = \{[2], [5]\}$

$H + [3] = \{[3], [0]\}$

$H + [4] = \{[4], [1]\}$

Clases laterales

Sea $H = \{[0], [3]\} \subset \mathbb{Z}_6$ entonces:

Clases laterales izquierda:

$[0] + H = \{[0], [3]\}$
$[1] + H = \{[1], [4]\}$
$[2] + H = \{[2], [5]\}$
$[3] + H = \{[3], [0]\}$
$[4] + H = \{[4], [1]\}$
$[5] + H = \{[5], [2]\}$

Clases laterales derecha:

$H + [0] = \{[0], [3]\}$
$H + [1] = \{[1], [4]\}$
$H + [2] = \{[2], [5]\}$
$H + [3] = \{[3], [0]\}$
$H + [4] = \{[4], [1]\}$
$H + [5] = \{[5], [2]\}$

Clases laterales

Sea $H = \{[0],[3]\} \subset \mathbb{Z}_6$ entonces:

Clases laterales izquierda:

$[0]+H = \{[0],[3]\}$
$[1]+H = \{[1],[4]\}$
$[2]+H = \{[2],[5]\}$
$[3]+H = \{[3],[0]\}$
$[4]+H = \{[4],[1]\}$
$[5]+H = \{[5],[2]\}$

Clases laterales derecha:

$H+[0] = \{[0],[3]\}$
$H+[1] = \{[1],[4]\}$
$H+[2] = \{[2],[5]\}$
$H+[3] = \{[3],[0]\}$
$H+[4] = \{[4],[1]\}$
$H+[5] = \{[5],[2]\}$

Se cumple que $G/H_{\sim} = G/_{\sim}H$ entonces el conjunto cociente es:

Sea $H = \{[0], [3]\} \subset \mathbb{Z}_6$ entonces:

Clases laterales izquierda:

$[0] + H = \{[0], [3]\}$
$[1] + H = \{[1], [4]\}$
$[2] + H = \{[2], [5]\}$
$[3] + H = \{[3], [0]\}$
$[4] + H = \{[4], [1]\}$
$[5] + H = \{[5], [2]\}$

Clases laterales derecha:

$H + [0] = \{[0], [3]\}$
$H + [1] = \{[1], [4]\}$
$H + [2] = \{[2], [5]\}$
$H + [3] = \{[3], [0]\}$
$H + [4] = \{[4], [1]\}$
$H + [5] = \{[5], [2]\}$

Se cumple que $G/H_{\sim} = G/_{\sim}H$ entonces el conjunto cociente es:

$G/H = \{\{[0], [3]\}, \{[1], [4]\}, \{[5], [2]\}\}$

Clases laterales

Ejemplo 2

Sea H el subgrupo de S_3 definido por las permutaciones:

Sea H el subgrupo de S_3 definido por las permutaciones:

$$H = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\}$$

Las clases laterales izquierdas y derecha son iguales (1):

Sea H el subgrupo de S_3 definido por las permutaciones:

$$H = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\}$$

Las clases laterales izquierdas y derecha son iguales (1):

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} H = H \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\}$$
$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} H = H \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\}$$
$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} H = H \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\}$$

Sea H el subgrupo de S_3 definido por las permutaciones:

Sea H el subgrupo de S_3 definido por las permutaciones:

$$H = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\}$$

Las clases laterales izquierdas y derecha son iguales (2):

Sea H el subgrupo de S_3 definido por las permutaciones:

$$H = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\}$$

Las clases laterales izquierdas y derecha son iguales (2):

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} H = H \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \right\}$$
$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} H = H \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \right\}$$
$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} H = H \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \right\}$$

El conjunto cociente es:

$$G/H = \left\{\left\{\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}\right\}, \left\{\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}\right\}\right\}$$

Sea K el subgrupo de S_3 definido por:

$$K = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right\}$$

Las clases laterales por izquierda de K son:

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} K = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} K = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right\}$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} K = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} K = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \right\}$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} K = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} K = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\}$$

Sea K el subgrupo de S_3 definido por:

$$K = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right\}$$

Las clases laterales por derecha son distintas de la izquierda:

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} K = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} K = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right\}$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} K = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 2 \end{pmatrix} K = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\}$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} K = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} K = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \right\}$$

Clases laterales

Ejemplo 3

El conjunto cociente izquierdo es:

$$G/_{\sim}K = \left\{\left\{\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}\right\}, \left\{\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}\right\}, \left\{\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}\right.\right.$$

El conjunto cociente derecho es:

$$G/K_{\sim} = \left\{\left\{\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}\right\}, \left\{\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}\right\}, \left\{\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}\right.\right.$$

Subgrupos Normales

Definición

Sea $< H, * >$ un subgrupo de $< G, * >$ decimos que H es un subgrupo normal si para todo $a \in G$ se cumple que

$$aH = Ha,$$

es decir, las clases laterales izquierdas y derechas generadas por a coinciden para todo $a \in G$.

Observación 1

$aH = Ha$ no significa $a * h = h * a$ para toda $h \in H$, pero si quiere decir que $a * h_1 = h_2 * a$ para algunas $h_1, h_2 \in H$.

Observación 2

Sea $< G, * >$ un grupo abeliano, esto es, conmutativo entonces todo subgrupo H de G es subgrupo normal.

Subgrupos normales

Theorem

Sea $< G, * >$ *un grupo y sea* $< H, * >$ *un subgrupo, entonces* H *es un subgrupo normal de* $< G, * >$ *si y sólo si* $a^{-1} * h * a \in H$ *para todo* $a \in G$ *y* $h \in H$.

Teorema de Lagrange

Teorema de Lagrange

Theorem

Sea $< G, * >$ *un grupo finito y sea* $< H, * >$ *un subgrupo, entonces* $O(H)$ *es un divisor de* $O(G)$*, en otras palabras, el orden de un subgrupo* H *es divisor del orden de* G*.*

Teorema de Lagrange

Theorem

Sea $< G, * >$ *un grupo finito y sea* $< H, * >$ *un subgrupo, entonces* $O(H)$ *es un divisor de* $O(G)$*, en otras palabras, el orden de un subgrupo* H *es divisor del orden de* G*.*

Ejemplo

Un grupo de orden 50 sólo puede tener subgrupos de orden $1, 2, 5, 10$ o 25.

Teorema de Lagrange

Corolario 1

Si G es un grupo finito de orden n y g un elemento de G entonces $g^n = e$.

Corolario 1

Si G es un grupo finito de orden n y g un elemento de G entonces $g^n = e$.

Corolario 2

Si H es un subgrupo propio de un grupo finito G entonces $|H| \leq |G|/2$.

Corolario 1

Si G es un grupo finito de orden n y g un elemento de G entonces $g^n = e$.

Corolario 2

Si H es un subgrupo propio de un grupo finito G entonces $|H| \leq |G|/2$.

Corolario 3

Todo grupo de orden primo es cíclico.

Definición

Si G es un grupo finito, entonces el **<u>número de clases</u>** *se llama* **índice de** *H en G y se denota $|G : H| = \frac{|G|}{|H|}$. Donde el teorema de Lagrange afirma que sea G un grupo finito y H un* **<u>subgrupo propio/no triviales</u>** *de G entonces $|H|$ divide a $|G|$.*

Teorema de Lagrange

Definición

Si G es un grupo finito, entonces el **número de clases** *se llama* **índice de** *H en G y se denota $|G:H| = \frac{|G|}{|H|}$. Donde el teorema de Lagrange afirma que sea G un grupo finito y H un* **subgrupo propio/no triviales** *de G entonces $|H|$ divide a $|G|$.*

Corolario 4

Si G es un grupo finito, $|G| = [G:H] \cdot [H]$.

Teorema de Lagrange

Theorem

Si G es un grupo abeliano y H es un subgrupo de G, entonces toda clase lateral a la derercha de H es también una clase lateral a la izquierda de H.

Teorema de Lagrange

Theorem

Si G es un grupo abeliano y H es un subgrupo de G, entonces toda clase lateral a la derercha de H es también una clase lateral a la izquierda de H.

El teorema de Lagrange limita el número de subgrupos que puede tener un grupo. Por ejemplo, un grupo de orden primo no puede tener ningún subgrupo propio, recordemos que un número primo es sólo divisible por 1 y por sí mismo. El recíproco del teorema de Lagrange no es necesariamente cierto, el hecho que k sea un divisor de $|G|$ no quiere decir que G tenga que tener un subgrupo de orden k o que no pueda tener más de uno.

Sea $< G, * >$ un grupo finito y H y K subgrupos de G. Si $|H| = 38$ y $|K| = 55$. Demostrar que $|H \cap K| = \{e\}$.

Sea $< G, * >$ un grupo finito y H y K subgrupos de G. Si $|H| = 38$ y $|K| = 55$. Demostrar que $|H \cap K| = \{e\}$.

Demostración

$|H \cap K|$ es un subgrupo tanto de H como de K, por el teorema de Lagrange, deducimos que $|H \cap K|$ tiene que dividir tanto a $|H| = 38$ como a $|K| = 55$. Pero $38 = 2.19$ y $55 = 5.11$ son coprimos, el $mcd(38, 55) = 1$ luego la única posibilidad es $|H \cap K| = 1$, es decir $|H \cap K| = \{e\}$.

Encuentre las clases laterales de H en G donde $H = \{[0], [2], [4], [6]\}$ y $G =< \mathbb{Z}_8, + >$

Encuentre las clases laterales de H en G donde $H = \{[0],[2],[4],[6]\}$ y $G = <\mathbb{Z}_8, + >$

- $\mathbb{Z}_8 = \{[0],[1],[2],[3],[4],[5],[6],[7]\}$

Encuentre las clases laterales de H en G donde $H = \{[0], [2], [4], [6]\}$ y $G =< \mathbb{Z}_8, + >$

- $\mathbb{Z}_8 = \{[0], [1], [2], [3], [4], [5], [6], [7]\}$
- Por definición, sea $< G, * >$ entonces las clases laterales derecha son $Ha = \{h * a | h \in H\}$ e izquierda son $aH = \{a * h | h \in H\}$ donde $a \in G$ donde $H < G$.

Encuentre las clases laterales de H en G donde $H = \{[0], [2], [4], [6]\}$ y $G =< \mathbb{Z}_8, + >$

- $\mathbb{Z}_8 = \{[0], [1], [2], [3], [4], [5], [6], [7]\}$
- Por definición, sea $< G, * >$ entonces las clases laterales derecha son $Ha = \{h * a | h \in H\}$ e izquierda son $aH = \{a * h | h \in H\}$ donde $a \in G$ donde $H < G$.
  - $[0] + H = H + [0] = \{[0], [2], [4], [6]\}$ (1)

Encuentre las clases laterales de H en G donde $H = \{[0], [2], [4], [6]\}$ y $G =< \mathbb{Z}_8, + >$

- $\mathbb{Z}_8 = \{[0], [1], [2], [3], [4], [5], [6], [7]\}$
- Por definición, sea $< G, * >$ entonces las clases laterales derecha son $Ha = \{h * a | h \in H\}$ e izquierda son $aH = \{a * h | h \in H\}$ donde $a \in G$ donde $H < G$.
    - $[0] + H = H + [0] = \{[0], [2], [4], [6]\}$ (1)
    - $[1] + H = H + [1] = \{[1], [3], [5], [7]\}$ (2)

Encuentre las clases laterales de H en G donde $H = \{[0],[2],[4],[6]\}$ y $G =< \mathbb{Z}_8, + >$

- $\mathbb{Z}_8 = \{[0],[1],[2],[3],[4],[5],[6],[7]\}$
- Por definición, sea $< G, * >$ entonces las clases laterales derecha son $Ha = \{h * a | h \in H\}$ e izquierda son $aH = \{a * h | h \in H\}$ donde $a \in G$ donde $H < G$.
  - $[0] + H = H + [0] = \{[0],[2],[4],[6]\}$ (1)
  - $[1] + H = H + [1] = \{[1],[3],[5],[7]\}$ (2)
  - $[2] + H = H + [2] = \{[2],[4],[6],[0]\}$ (1)

Encuentre las clases laterales de H en G donde $H = \{[0], [2], [4], [6]\}$ y $G =< \mathbb{Z}_8, + >$

- $\mathbb{Z}_8 = \{[0], [1], [2], [3], [4], [5], [6], [7]\}$
- Por definición, sea $< G, * >$ entonces las clases laterales derecha son $Ha = \{h * a | h \in H\}$ e izquierda son $aH = \{a * h | h \in H\}$ donde $a \in G$ donde $H < G$.
  - $[0] + H = H + [0] = \{[0], [2], [4], [6]\}$ (1)
  - $[1] + H = H + [1] = \{[1], [3], [5], [7]\}$ (2)
  - $[2] + H = H + [2] = \{[2], [4], [6], [0]\}$ (1)
  - $[3] + H = H + [3] = \{[3], [5], [7], [1]\}$ (2)

Encuentre las clases laterales de H en G donde $H = \{[0], [2], [4], [6]\}$ y $G =< \mathbb{Z}_8, + >$

- $\mathbb{Z}_8 = \{[0], [1], [2], [3], [4], [5], [6], [7]\}$
- Por definición, sea $< G, * >$ entonces las clases laterales derecha son $Ha = \{h * a | h \in H\}$ e izquierda son $aH = \{a * h | h \in H\}$ donde $a \in G$ donde $H < G$.
    - $[0] + H = H + [0] = \{[0], [2], [4], [6]\}$ (1)
    - $[1] + H = H + [1] = \{[1], [3], [5], [7]\}$ (2)
    - $[2] + H = H + [2] = \{[2], [4], [6], [0]\}$ (1)
    - $[3] + H = H + [3] = \{[3], [5], [7], [1]\}$ (2)
    - $[4] + H = H + [4] = \{[4], [6], [0], [2]\}$ (1)

Encuentre las clases laterales de H en G donde $H = \{[0], [2], [4], [6]\}$ y $G =< \mathbb{Z}_8, + >$

- $\mathbb{Z}_8 = \{[0], [1], [2], [3], [4], [5], [6], [7]\}$
- Por definición, sea $< G, * >$ entonces las clases laterales derecha son $Ha = \{h * a | h \in H\}$ e izquierda son $aH = \{a * h | h \in H\}$ donde $a \in G$ donde $H < G$.
  - $[0] + H = H + [0] = \{[0], [2], [4], [6]\}$ (1)
  - $[1] + H = H + [1] = \{[1], [3], [5], [7]\}$ (2)
  - $[2] + H = H + [2] = \{[2], [4], [6], [0]\}$ (1)
  - $[3] + H = H + [3] = \{[3], [5], [7], [1]\}$ (2)
  - $[4] + H = H + [4] = \{[4], [6], [0], [2]\}$ (1)
  - $[5] + H = H + [5] = \{[5], [7], [1], [3]\}$ (2)

Encuentre las clases laterales de H en G donde $H = \{[0], [2], [4], [6]\}$ y $G =< \mathbb{Z}_8, + >$

- $\mathbb{Z}_8 = \{[0], [1], [2], [3], [4], [5], [6], [7]\}$
- Por definición, sea $< G, * >$ entonces las clases laterales derecha son $Ha = \{h * a | h \in H\}$ e izquierda son $aH = \{a * h | h \in H\}$ donde $a \in G$ donde $H < G$.
  - $[0] + H = H + [0] = \{[0], [2], [4], [6]\}$ (1)
  - $[1] + H = H + [1] = \{[1], [3], [5], [7]\}$ (2)
  - $[2] + H = H + [2] = \{[2], [4], [6], [0]\}$ (1)
  - $[3] + H = H + [3] = \{[3], [5], [7], [1]\}$ (2)
  - $[4] + H = H + [4] = \{[4], [6], [0], [2]\}$ (1)
  - $[5] + H = H + [5] = \{[5], [7], [1], [3]\}$ (2)
  - $[6] + H = H + [6] = \{[6], [0], [2], [4]\}$ (1)

Encuentre las clases laterales de H en G donde $H = \{[0], [2], [4], [6]\}$ y $G =< \mathbb{Z}_8, + >$

- $\mathbb{Z}_8 = \{[0], [1], [2], [3], [4], [5], [6], [7]\}$
- Por definición, sea $< G, * >$ entonces las clases laterales derecha son $Ha = \{h * a | h \in H\}$ e izquierda son $aH = \{a * h | h \in H\}$ donde $a \in G$ donde $H < G$.
  - $[0] + H = H + [0] = \{[0], [2], [4], [6]\}$ (1)
  - $[1] + H = H + [1] = \{[1], [3], [5], [7]\}$ (2)
  - $[2] + H = H + [2] = \{[2], [4], [6], [0]\}$ (1)
  - $[3] + H = H + [3] = \{[3], [5], [7], [1]\}$ (2)
  - $[4] + H = H + [4] = \{[4], [6], [0], [2]\}$ (1)
  - $[5] + H = H + [5] = \{[5], [7], [1], [3]\}$ (2)
  - $[6] + H = H + [6] = \{[6], [0], [2], [4]\}$ (1)
  - $[7] + H = H + [7] = \{[7], [1], [3], [5]\}$ (2)

Encuentre las clases laterales de H en G donde $H = \{[0], [2], [4], [6]\}$ y $G =< \mathbb{Z}_8, + >$

- $\mathbb{Z}_8 = \{[0], [1], [2], [3], [4], [5], [6], [7]\}$
- Por definición, sea $< G, * >$ entonces las clases laterales derecha son $Ha = \{h * a | h \in H\}$ e izquierda son $aH = \{a * h | h \in H\}$ donde $a \in G$ donde $H < G$.
  - $[0] + H = H + [0] = \{[0], [2], [4], [6]\}$ (1)
  - $[1] + H = H + [1] = \{[1], [3], [5], [7]\}$ (2)
  - $[2] + H = H + [2] = \{[2], [4], [6], [0]\}$ (1)
  - $[3] + H = H + [3] = \{[3], [5], [7], [1]\}$ (2)
  - $[4] + H = H + [4] = \{[4], [6], [0], [2]\}$ (1)
  - $[5] + H = H + [5] = \{[5], [7], [1], [3]\}$ (2)
  - $[6] + H = H + [6] = \{[6], [0], [2], [4]\}$ (1)
  - $[7] + H = H + [7] = \{[7], [1], [3], [5]\}$ (2)

Encuentre las clases laterales de H en G donde $H = \{[0],[2],[4],[6]\}$ y $G =< \mathbb{Z}_8, + >$

- $\mathbb{Z}_8 = \{[0],[1],[2],[3],[4],[5],[6],[7]\}$
- Por definición, sea $< G, * >$ entonces las clases laterales derecha son $Ha = \{h * a | h \in H\}$ e izquierda son $aH = \{a * h | h \in H\}$ donde $a \in G$ donde $H < G$.
  - $[0] + H = H + [0] = \{[0],[2],[4],[6]\}$ (1)
  - $[1] + H = H + [1] = \{[1],[3],[5],[7]\}$ (2)
  - $[2] + H = H + [2] = \{[2],[4],[6],[0]\}$ (1)
  - $[3] + H = H + [3] = \{[3],[5],[7],[1]\}$ (2)
  - $[4] + H = H + [4] = \{[4],[6],[0],[2]\}$ (1)
  - $[5] + H = H + [5] = \{[5],[7],[1],[3]\}$ (2)
  - $[6] + H = H + [6] = \{[6],[0],[2],[4]\}$ (1)
  - $[7] + H = H + [7] = \{[7],[1],[3],[5]\}$ (2)
- De acuerdo a uno de los corolarios del teorema de Lagrange el número de clases laterales es $[G : H] = \frac{|G|}{|H|} = \frac{8}{4} = 2$.

Homomorfismos

Definición

Sean $< G, * >$ *y* $< G', \triangle >$ *y una función* $f : G \to G'$ *se dice que es un* **homomorfismo de grupos** *si*

$$f(a * b) = f(a) \triangle f(b),$$

para todo $a, b \in G$.

Sean $< G, * >$ y $< G', \triangle >$ y sea $f : G \to G'$ un homomorfismo de grupos, entonces:

1. **Monomorfismo de grupos:** si f es inyectiva.
2. **Epimorfismo de grupos:** si f es sobreyectiva.
3. **Isomorfismo de grupos:** si f es biyectiva.
4. **Endomorfismo de grupos:** si $G \subset G'$.
5. **Automorfismo de grupos:** si $G = G'$.

Theorem

Sean $< G, * >$ *y* $< G', \triangle >$ *y sea* $f : G \to G'$ *un homomorfismo de grupos, entonces*

1. $f(e) = e'$, *donde* e *y* e' *son los elementos identidad de* G *y* G' *respectivamente*
2. *para cualquier* $a \in G$, *se tiene que* $f(a^{-1}) = [f(a)]^{-1}$
3. *si* H *es un subgrupo de* G, *entonces*

$$f(H) = f(h) : h \in H,$$

es un subgrupo de G'.

Demostración

Como G es un grupo entonces $e = e * e$ y por ser f un homomorfismo

$$f(e) = f(e * e) = f(e)\triangle f(e)$$

Premultiplicando por $[f(e)]^{-1}$ y asociando
$[f(e)]^{-1}\triangle f(e) = ([f(e)]^{-1}\triangle f(e))\triangle f(e)$
y por definición de inverso

$$e' = e'\triangle f(e) = f(e)$$

esto es lo que se quería demostrar.

Demostración

Como G es un grupo entonces $e = a * a^{-1}$ y por ser f un homomorfismo

$$e' = f(e) = f(a * a^{-1}) = f(a) \triangle f(a^{-1})$$

Como $e = a^{-1} * a$ y por ser f un homomorfismo

$$e' = f(e) = f(a^{-1} * a) = f(a^{-1}) \triangle f(a)$$

De la definición de inverso se tiene que

$$f(a^{-1}) = [f(a)]^{-1}$$

Kernel

Definición

Sean $< G, * >$ *y* $< G', \triangle >$ *grupos y sea* $f : G \to G'$ *un homomorfismo de grupos, entonces*

$$Ker(f) = \{g : f(g) = e'\},$$

se denomina **kernel** *o* **núcleo** *del homomorfismo*

$$f(a * b) = f(a) \triangle f(b),$$

para todo $a, b \in G$.

Imagen

La imagen de un homomorfismo de grupo es el conjunto de todos los elementos en el grupo objetivo que pueden ser alcanzados aplicando el homomorfismo a los elementos del grupo de partida.

Definición

Formalmente, si $\phi : G \to H$ es un homomorfismo de grupos, donde G y H son grupos, la imagen de ϕ se denota como $Im(\phi)$ y se define como:

$$Im(\phi) = \{\phi(g) \mid g \in G\}$$

Esto significa que la imagen de ϕ incluye todos los elementos de H que son de la forma $\phi(g)$ para algún g en G. La imagen es un subgrupo de H si ϕ es un homomorfismo de grupos.

Ejemplo:

Determinar, si h es un homomorfismo de grupo, hallar el núcleo y la imagen.

1. $h :< \mathbb{R} - \{0\}, . > \rightarrow < \mathbb{R} - \{0\}, . >$ donde $h(x) = x^2$.
(a) Verificar si $f(ab) = f(a)f(b)$

- $f(ab) = (ab)^2$
- $f(a)f(b) = a^2b^2 = (ab)^2$
- Es un homomorfismo.

(b) Cálculo del núcleo:

- $ker(f) = \{1\}$

(c) Imágen del homomorfismo es:

- $f(\mathbb{R} - \{0\}) = \mathbb{R}^+ \subseteq \{\mathbb{R} - \{0\}\}$

Fin