Universidad de Valparaíso
CHILE

Teoría de Grupos

Daniel Jiménez Briones.

Marzo de 2017.

Índice general

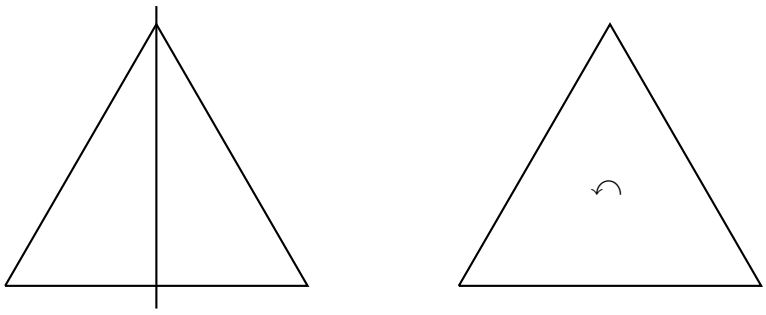
Capítulo 1

Grupos

1.1. Introducción

La noción de grupo la podemos encontrar en distintas área de la matemática o en la naturaleza.

Un primer tipo consiste en las simetrías de un objeto, por ejemplo los polígonos regulares, para evidenciar las simetrías es conveniente marcar los objetos de alguna manera, aunque esta marcas no son partes del objeto, en el caso de los polígonos regulares, pueden ser los vértices o las aristas, en particular para el triángulo equilátero tenemos las siguientes simetrías:

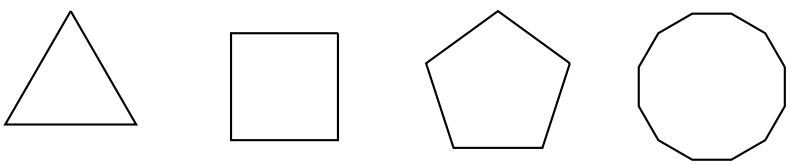


J R

Sea G el conjunto de todas las simetrías de esta figura, en este conjunto es fácil definir una **operación binaria**, que corresponde aplicar una después la otra de estas simetrías, y es claro que obtendremos una nueva simetría.

Podemos describir todas las simetrías de esta figura y la denotamos por *Sim(Triángulo)*.

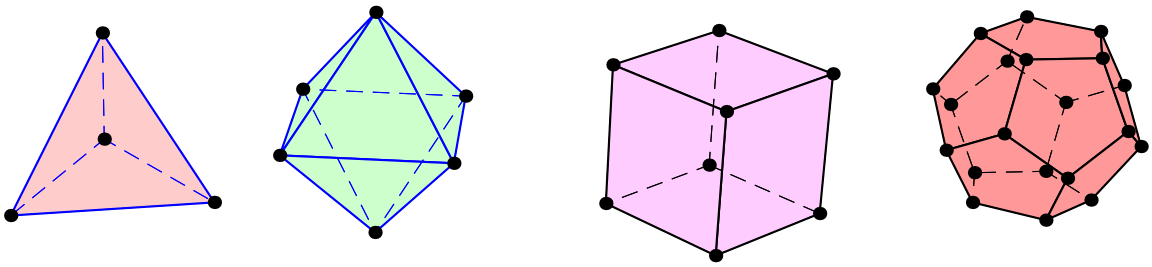
Para otros polígonos regulares también se puede determinar el mismo conjunto de simetrías.



Los objetos también puedes ser tridimensionales, como los poliedros regulares, en cuyo

caso podemos incorporar marcas en las caras.

Tetraedro, **Octaedro**, **Cubo**, **Dodecaedro**.



Otro tipo de conjunto donde existe una operación binaria, es en el siguiente, sea G el conjunto potencia de $A = \{a, b, c\}$ y la correspondiente operación binaria dada por diferencia simétrica, de otro modo,

$$\begin{array}{rccl} \triangle: & G \times G & \longrightarrow & G \\ & (X, Y) & \longmapsto & X \triangle Y := X \cup Y - X \cap Y \end{array}$$

En el ejemplo anterior tenemos la siguiente tabla de la diferencia simétrica u operación binaria

$\triangle$	ϕ	$\{a\}$	$\{b\}$	$\{c\}$	$\{a,b\}$	$\{a,c\}$	$\{b,c\}$	$\{a,b,c\}$
ϕ	ϕ	$\{a\}$	$\{b\}$	$\{c\}$	$\{a,b\}$	$\{a,c\}$	$\{b,c\}$	$\{a,b,c\}$
$\{a\}$	$\{a\}$	ϕ	$\{a,b\}$	$\{a,c\}$	$\{b\}$	$\{c\}$	$\{a,b,c\}$	$\{b,c\}$
$\{b\}$	$\{b\}$	$\{a,b\}$	ϕ	$\{b,c\}$	$\{a\}$	$\{a,b,c\}$	$\{c\}$	$\{a,c\}$
$\{c\}$	$\{c\}$	$\{a,c\}$	$\{b,c\}$	ϕ	$\{a,b,c\}$	$\{a\}$	$\{b\}$	$\{a,b\}$
$\{a,b\}$	$\{a,b\}$	$\{b\}$	$\{a\}$	$\{a,b,c\}$	ϕ	$\{b,c\}$	$\{a,c\}$	$\{c\}$
$\{a,c\}$	$\{a,c\}$	$\{c\}$	$\{a,b,c\}$	$\{a\}$	$\{b,c\}$	ϕ	$\{a,b\}$	$\{b\}$
$\{b,c\}$	$\{b,c\}$	$\{a,b,c\}$	$\{c\}$	$\{b\}$	$\{a,c\}$	$\{a,b\}$	ϕ	$\{a,b,c\}$
$\{a,b,c\}$	$\{a,b,c\}$	$\{b,c\}$	$\{a,c\}$	$\{a,b\}$	$\{c\}$	$\{b\}$	$\{a\}$	ϕ

En forma natural se puede generalizar el ejemplo anterior del siguiente modo, dado un conjunto X no vacío y $G = \mathcal{P}(X)$ el conjunto potencia, entonces tenemos que la diferencia simétrica $\triangle$ es una operación binaria en G.

En cada uno de estos conjuntos con las respectivas operaciones binarias, podemos buscar o escudriñar, que propiedades básicas cumplen o satisfacen.

1.2. Nociones Básicas

Definición 1 *Sea G un conjunto no vacío.*

1. *Se dice que $(G, *)$ es un* ***Grupoide*** *si y sólo si*

$$\begin{array}{rccl} *: & G \times G & \longrightarrow & G \\ & (a, b) & \longmapsto & a * b \end{array} \qquad \textit{es una función}$$

Otra manera de referirse a esta propiedad es ***Clausura u Operación Binaria***

2. *Se dice que* $(G,*)$ *es un* **`Semigrupo`** *si y sólo si,* $(G,*)$ *es un grupoide y además* $(*)$ *es asociativa*
$$(\forall a,b,c\in G)((a*b)*c=a*(b*c)).$$

3. *Se dice que* $(G,*)$ *es un* **`Monoide`** *si y sólo si* $(G,*)$ *es un semigrupo y además* $(*)$ *tiene neutro*
$$(\exists e\in G)(\forall a\in G)(a*e=e*a=a).$$

4. *Se dice que* $(G,*)$ *es un* **`Grupo`** *si y sólo si* $(G,*)$ *es un monoide y además* $(*)$ *tiene la propiedad del inverso*
$$(\forall a\in G)(\exists b\in G)(a*b=b*a=e).$$

5. *Se dice que* $(G,*)$ *es un* **`Grupo Abeliano`** *si y sólo si* $(G,*)$ *es un grupo y además* $(*)$ *tiene la propiedad conmutativa*
$$(\forall a\in G)(\forall b\in G)(a*b=b*a).$$

Observación: No se debe confundir "grupo puro" con "puro grupo"

Ejemplo 1 *Los siguientes conjuntos con la operación que se indica son grupos:*

$(\mathbb{Q},+)$
$(\mathbb{R},+)$
$(\mathbb{C},+)$
$(\mathbb{Q}^*,\cdot)$
$(\mathbb{R}^*,\cdot)$
$(\mathbb{C}^*,\cdot)$
$(M_n(\mathbb{K}),+)$ *con* $\mathbb{K}=\mathbb{Z},\mathbb{Q},\mathbb{R},\mathbb{C},\mathbb{Z}_n$
$(GL_n(K),\cdot)$ *con* $\mathbb{K}=\mathbb{Z},\mathbb{Q},\mathbb{R},\mathbb{C},\mathbb{Z}_n$
$(\mathbb{Z}/n\mathbb{Z},+)$
$(U(\mathbb{Z}/n\mathbb{Z}),\cdot)$
$(\mathbb{Z}/p\mathbb{Z},\cdot)$, *con* p *número primo*
$(\mathbb{K}[x],+)$ *con* $\mathbb{K}=\mathbb{Z},\mathbb{Q},\mathbb{R},\mathbb{C},\mathbb{Z}_n$
$(F(X,G),*)$*el conjunto de la funciones de* X *en el grupo* $(G,*)$
$(Biy(X),\circ)$*el conjunto de las biyecciones de* X *en* X

Ejemplo 2 *Sea* $G=\mathbb{Z}$*, y se define* $a\oplus b=a+b+1$.
Demostrar que $(G,\oplus)$ *es grupo.*
Solución: *Claramente* $(\mathbb{Z},\oplus)$ *es un grupoide, pues* $\oplus:\mathbb{Z}\times\mathbb{Z}\longrightarrow\mathbb{Z}$ *donde* $\oplus(a,b)=a\oplus b=a+b+1$ *es un único valor, luego es una función bien definida.*

Ahora veamos que $\oplus$ es asociativa, sean $a, b, c \in \mathbb{Z}$ se tiene que

$$\begin{aligned}(a \oplus b) \oplus c &= (a + b + 1) \oplus c \\ &= a + b + 1 + c + 1 \\ &= a + (b + c + 1) + 1 \\ &= a \oplus (b + c + 1) \\ &= a \oplus (b \oplus c)\end{aligned}$$

Lo cual prueba que $\oplus$ es asociativa, y por tanto $(\mathbb{Z}, \oplus)$ es Semigrupo.

Ahora para encontrar el elemento neutro, nos basaremos en suponer que existe, es decir, supongamos que para todo $a \in \mathbb{Z}$ existe $b \in \mathbb{Z}$ tal que

$$\begin{aligned}& a \oplus b &=& \ a \\ \Leftrightarrow \quad & a + b + 1 &=& \ a \\ \Leftrightarrow \quad & b + 1 &=& \ 0 \\ \Leftrightarrow \quad & b &=& -1\end{aligned}$$

Luego, como $-1 \in \mathbb{Z}$, y se puede comprobar que -1, es el neutro por la derecha de $(\mathbb{Z}, \oplus)$, y análogamente también es el neutro por la izquierda, por lo tanto -1 es el elemento neutro de $(\mathbb{Z}, \oplus)$, luego $(\mathbb{Z}, \oplus)$ es un Monoide.

Por último, supongamos que para cada $a \in \mathbb{Z}$ existe $c \in \mathbb{Z}$ tal que

$$\begin{aligned}& a \oplus c &=& -1 \\ \Leftrightarrow \quad & a + c + 1 &=& -1 \\ \Leftrightarrow \quad & c &=& -2 - a\end{aligned}$$

De este modo, obtenemos que $-2 - a$ es el inverso por la derecha de a, de forma análoga tendremos que $-2 - a$ es el inverso por la izquierda y por tanto $-2 - a$ es el inverso de a, luego $(\mathbb{Z}, \oplus)$ es un Grupo.

Más aún, tenemos que $(\mathbb{Z}, \oplus)$ es un Grupo abeliano, ya que para todo $a, b \in \mathbb{Z}$ se tiene que

$$\begin{aligned}a \oplus b &= a + b + 1 \\ &= b + a + 1 \\ &= b \oplus a\end{aligned}$$

□

Ejercicio 3 *Sean A un conjunto, $G = \mathcal{P}(A)$ el conjunto potencia y $\triangle$ la diferencia simétrica.*
Demostrar que $(G, \triangle)$ es grupo abeliano.

Ejercicio 4 *Sea $G = \mathbb{Z}$, se define $a \odot b = a + b + ab$.*
Determinar si $(G, \odot)$ es semigrupo, monoide, grupo.

Grupo Diedral

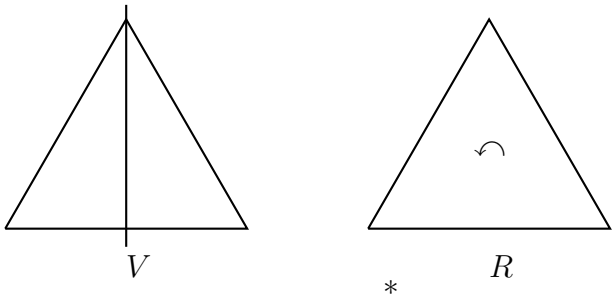
Sea $n \in \mathbb{N}$, entonces $D_n = Sim(n - \text{agono regular})$

Enumeremos los vértices del 1 al n en el sentido del reloj, de manera referencial. Al realizar una simetría obtenemos una biyección del conjunto de vértice en si mismo. Además notemos que una simetría envía vértices adyacente en vértices adyacentes. De este modo podemos contar las posibles simetrías, el vértice 1 tiene n, posibilidades y el vértices 2 sólo tiene dos posibilidades, los adyacentes a la imagen del vértice 1, los demás quedan únicamente determinados.

Por lo tanto hay a lo más $2n$ simetrías.

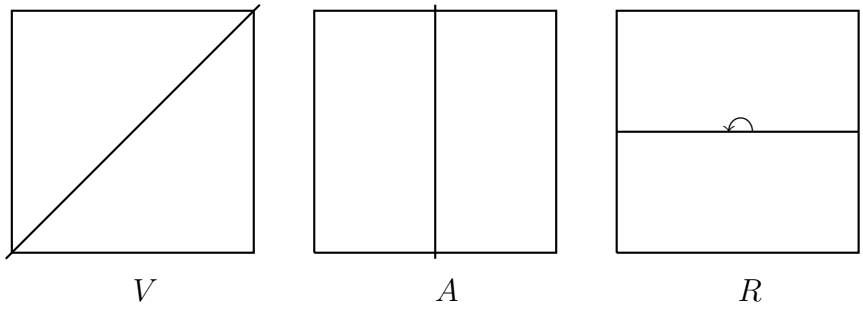
Ahora construiremos las simetrías, cada n-agono regular, se puede rotar en $360/n$ grados, luego existe n rotaciones denotemos por R_1 esta rotación, note que las rotaciones no dejan fija ningún vértices. Además existe las reflexiones, para ello debemos diferenciar casos.

Caso n impar:



El lado opuesto a un vértice es una arista, buscando el punto medio, se construye la reflexión, cada una de las cuales deja un punto fijo distinto, luego existe otras n reflexiones.

Caso n Par:



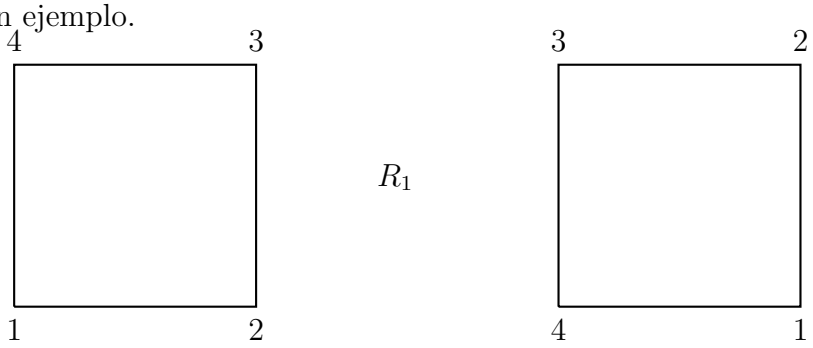
El lado opuesto a un vértice es otro vértice, luego esta reflexiones dejan fija dos vértices, de este modo hay $n/2$ reflexiones, pero existe otro tipo, dada una arista existe la arista opuesta, buscando los puntos medios, se construye la reflexión, cada una de las cuales deja dos arista, luego existe otras $n/2$ reflexiones.

De este modo existen $2n$ simetrías en un n-agono regular

Es importante comprender, que la anterior demostración lleva implícita la construcción, pero no la notación mas conveniente. Para ello enumeraremos los vértices en el sentido contrario del reloj correlativamente. R_1 la rotación en el sentido de la enumeración en un ángulo de $360/n$, V_i la reflexión que deja fijo el vértice i y cuando corresponda $A_{i,i+1}$ la

reflexión que deja fijo la arista $\{i, i+1\}$

Veamos un ejemplo.

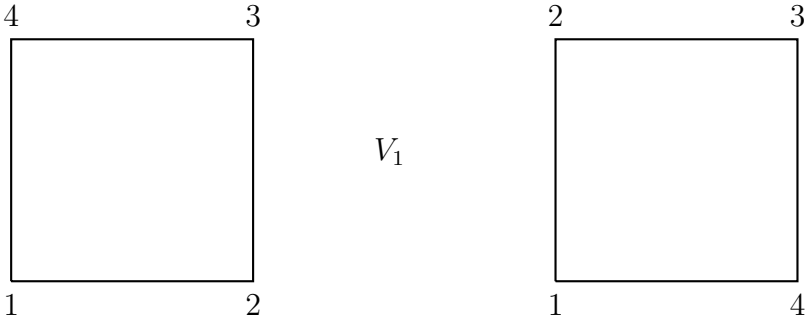


A lo menos hay dos posible forma de describir esta función, es importante entender las implicancia de cada una de ellas. En este texto optaremos por "**donde esta**" por ello tenemos lo siguiente:

$$R_1(1) = 2;\ R_1(2) = 3;\ R_1(3) = 4;\ R_1(4) = 1.$$

Lo cual lo denotaremos por

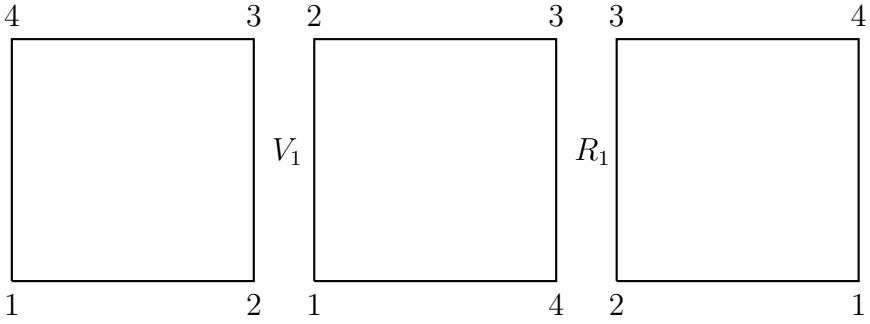
$$R_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ R_1(1) & R_1(2) & R_1(3) & R_1(4) \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$$



Lo cual corresponde a

$$V_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}$$

Ahora operaremos ambas simetrías



Lo cual significa que primero hemos realizado la simetría V_1 y después hemos rotado.

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} * \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

Lo cual corresponde a a compuesta de funciones.
Observación: Recuerde que la enumeración no pertenece a la figura sólo es referencia, y la notación no debe depender de las circunstancias.

Ejercicio 5 *Sea $n \in \mathbb{N}$, entonces $D_n = Sim(n - agono\ regular)$ es un grupo.*

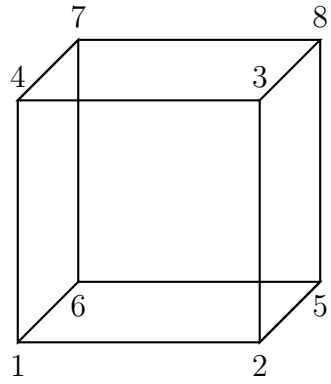
Simetrías del Cubo

Es importante tener presente que al describir esto grupo, involucran varias decisiones que llevan a distintas visualización del mismo este. Una de ella es que enumeramos las caras, las aristas o los vértices, son 6 caras, 12 arista y 4 vértices. cada una de ella bien de a pares ya que se distingue claramente el opuesto en la figura. y toda simetrías debe respetar lo opuesto.

Argumentemos de dos formas distintas, si enumeramos las caras de modo que la opuesta sume 7, siempre sabremos que dado una la otra tiene una única posibilidad, por ello para la primera cara tenemos 6 posibilidades, adyacente a ella a cuatro, luego la otra tiene dos posibilidades y finalmente la tercera tiene dos posibilidades, entonces a lo mas hay 48 simetrías, una argumento similar lo obtenemos con los vértices, para el primero hay 8, para el segundo hay 3 y para el tercero hay 2, total 48.
Observación: Lo anterior nos lleva "interpretar" que entendemos por simetría. Hay a lo menos forma de entender una primera y más general que consiste en preservar los elementos notable del objeto (vértices en vértices, aristas en arista, caras en cara, etc). y otra en que realizable sin deformar la figura)

La discusión es mas profunda, ya que involucra el espacio en que se encuentra la figura, para más información mirar la teoría de grafos.

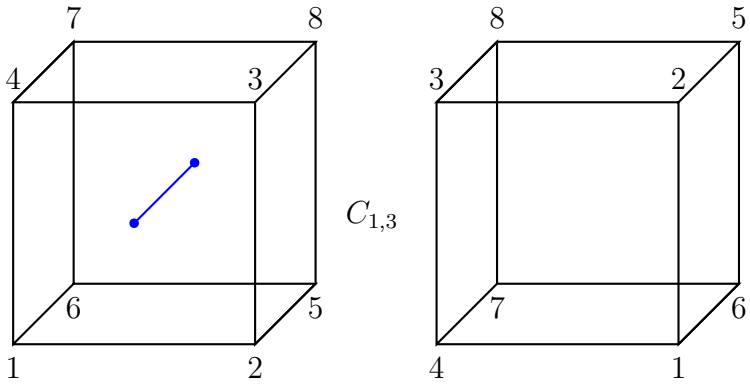
Para el desarrollo del curso, sólo trabajaremos con las simetrías realizables en el espacio tridimensional. Una forma de reconocer este hecho, es mirar desde el exterior a la cara principal $\{1, 2, 3, 4\}$ debe ser contraria al movimientos de las manecillas del reloj.



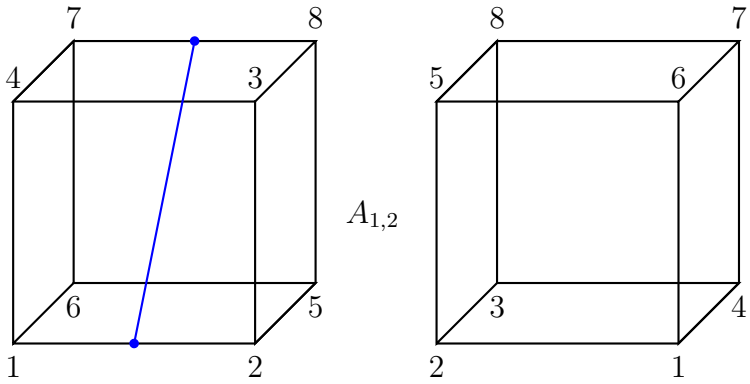
De este modo son sólo 24 simetrías realizables, ya que el tercer vértices tiene una sola posibilidad de mantener la orientación.

Los tipos de movimientos son tres,

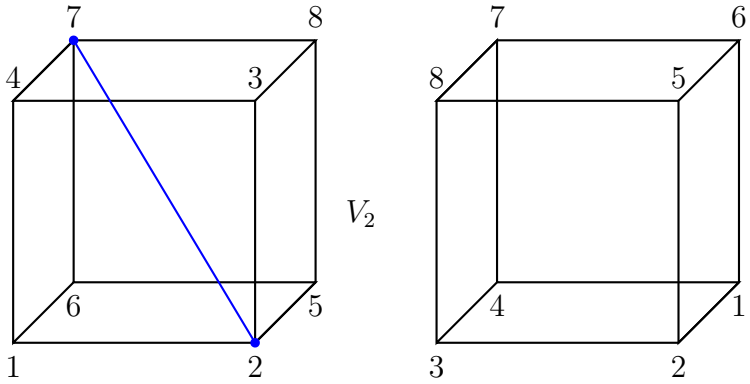
Movimiento de Caras $C_{i,j}$, donde i, j son opuestos en una cara. Consiste en dejar fija la cara y mover en un cuarto de vuelta 90° el cubo en el sentido contrario al reloj.



Movimiento de Arista $A_{i,j}$, donde $\{i, j\}$ es una arista. Consiste en dejar fija la arista y mover en 180° el cubo.



Movimiento de Vértices V_i, donde i es un vértices. Consiste en dejar fijo el vértices y mover en 120° el cubo en el sentido contrario al reloj.



1.2.1. Propiedades Básicas

En todo lo que sigue G representa un grupo y la notación empleada sera multiplicativa.

Teorema 1 *Sea G un grupo, entonces*

1. *El elemento neutro es único.*

2. *El elemento inverso de cada elemento es único.*

Demostración: Si e es el neutro, entonces para todo $a \in G$ se cumple que $ae = ea = a$. Supongamos entonces, que existe $e, e' \in G$ que también satisface la condición anterior. Luego

$$ee' = e'e = e' \tag{1.1}$$

y por otro lado

$$e'e = ee' = e \tag{1.2}$$

Por (1.1) y (1.2) se tiene que

$$e = ee' = e'$$

es decir

$$e = e'.$$

La segunda parte de la demostración se deja de ejercicio, puesto que es una consecuencia inmediata de la siguiente proposición. □

Notación: El elemento neutro también se llama la identidad de G, en notación multiplicativa se denota por 1 y en notación aditiva por 0.

El elemento inverso de a se denota en notación multiplicativa por a^{-1} y en notación aditiva por $-a$.

Propiedad 2 (Cancelación) *Sea G un grupo*

1. $(\forall a \in G)(\forall b \in G)(\forall c \in G)(ab = ac \Leftrightarrow b = c)$ *cancelación izquierda*

2. $(\forall a \in G)(\forall b \in G)(\forall c \in G)(ba = ca \Leftrightarrow b = c)$ *cancelación derecha*

Demostración: Sólo demostraremos la primera equivalencia.

Supongamos que $ba = ca$, luego como G es grupo, existe $a^{-1} \in G$ tal que $aa^{-1} = a^{-1}a = e$, entonces tenemos que

$$b = be = b(aa^{-1}) = (ba)a^{-1} = (ca)a^{-1} = c(aa^{-1}) = ce = c$$

es decir,

$$b = c$$

En la otra dirección es inmediata teniendo presente que la operación binaria es una función, sea $b = c$, luego $(a, b) = (a, c)$ por lo tanto tiene igual imagen $ab = ac$. □

Una consecuencia de la propiedad de cancelación es la siguiente proposición

Propiedad 3 *Sea G un grupo y $a, b \in G$ entonces*

1. *La ecuación $ax = b$ tiene única solución en G y es $x = a^{-1}b$*

2. *La ecuación $xa = b$ tiene única solución en G y es $x = ba^{-1}$.*

Demostración de ejercicio □

Ejemplo 6 *Resolver la siguiente ecuación (si tiene sentido).*

$$11x = 4 \quad en\ \mathcal{U}(\mathbb{Z}_{3157})$$

Solución: Recordemos que un elemento en $\mathbb{Z}_n$ es invertible (tiene inverso multiplicativo) si y sólo si es primo relativo con n. Ahora, como $MCD(11, 3157) = 11$, entonces 11 y 3157 **no** son primos relativos y por tanto 11 no es invertible en $\mathbb{Z}_{3157}$, luego la ecuación no tiene sentido en este grupo. □

Ejemplo 7 *Resolver la siguiente ecuación (si tiene sentido).*

$$25x = 3 \quad en\ \mathcal{U}(\mathbb{Z}_{3157})$$

Solución: Por la observación hecha en el ejemplo anterior, esta vez la ecuación sentido y por ende tiene solución $\mathcal{U}(\mathbb{Z}_{3157})$, ya que $MCD(3, 3157) = 1$ y $MCD(25, 3157) = 1$.

Para resolver la ecuación sólo debemos encontrar el inverso de 25 en $\mathbb{Z}_{3157}$, y para esto recurriremos al algoritmo de Euclides (de la división). Tenemos

$$\begin{aligned} 3157 &= 25 \cdot 126 + 7 \\ 25 &= 7 \cdot 3 + 4 \\ 7 &= 4 \cdot 1 + 3 \\ 4 &= 3 \cdot 1 + 1 \end{aligned}$$

De otro modo

$$\begin{aligned} 7 &= 3157 - 25 \cdot 126 \\ 4 &= 25 - 7 \cdot 3 \\ 3 &= 7 - 4 \cdot 1 \\ 1 &= 4 - 3 \cdot 1 \end{aligned}$$

Así tenemos que

$$\begin{aligned} 1 &= 4 - 3 \cdot 1 \\ &= 4 - (7 - 4 \cdot 1) \cdot 1 \\ &= 4 \cdot 2 - 7 \\ &= (25 - 7 \cdot 3) \cdot 2 - 7 \\ &= 25 \cdot 2 - 7 \cdot 7 \\ &= 25 \cdot 2 - 7(3157 - 25 \cdot 126) \\ &= 25 \cdot 2 - 7 \cdot 3157 + 25 \cdot 882 \\ &= 25(884) + 3157(-7) \end{aligned}$$

es decir

$$1 = 25(884) + 3157(-7)$$

aplicando módulo 3157 en la ecuación anterior tenemos:

$$25(884) = 1 \pmod{3157}$$

Luego 884 es el inverso de 25 en $\mathbb{Z}_{3157}$. Finalmente tenemos que

$$x = 884 \cdot 3 = 2652 \quad \text{en } U(\mathbb{Z}_{3157})$$

□

Ejemplo 8 *Considere las siguientes funciones $f, g, h \in Biy(\mathbb{R})$ tales que*

$$f(x) = 3x + 1; \quad g(x) = 2 - x; \quad h(x) = 5x + 1.$$

Resolver $f \circ Z \circ g = h$.

Solución: Note que las funciones son biyectiva y que

$$f^{-1}(x) = \frac{x-1}{3}; \quad g^{-1}(x) = 2 - x; \quad h^{-1}(x) = \frac{x-1}{5}.$$

Luego despejando tenemos

$$Z = f^{-1} \circ h \circ g^{-1}$$

De lo cual obtenemos $Z(x) = \frac{10-5x}{3}$. Por lo tanto

$$\begin{array}{rccc} Z: & \mathbb{R} & \to & \mathbb{R} \\ & x & \rightsquigarrow & \frac{10-5x}{3} \end{array}$$

□

Ejemplo 9 *Sea D_{15} el grupo de las simetrías del polígono regular de 15 lados, donde V_i es la reflexión que no mueve el vértice i y R es la rotación en 24 grados en el sentido de la enumeración.*

Resolver las siguientes ecuaciones, de modo de reconocer el tipo de movimiento.

1. $V_3 = V_1 X_1$
2. $V_9 = V_1 X_2 V_1$

Solución: Para la primera ecuación tenemos que $X_1 = V_1^{-1} V_3$, para reconocer el elemento, verifiquemos la imagen dos elementos adyacentes.

$$X_1(3) = V_1^{-1} V_3(3) = V_1^{-1}(3) = 14 \text{ y } X_1(2) = V_1^{-1} V_3(2) = V_1^{-1}(4) = 13$$

Luego $X_1(1) = 12$, luego es una rotación en 264 grados.

La segunda ecuación $V_9 = V_1 X_2 V_1$, luego se tiene que $X_2 = V_1^{-1} V_9 V_1^{-1} = V_1 V_9 V_1$, ya que es su propio inverso, ahora verifiquemos la imagen dos elementos adyacentes

$$X_2(1) = V_1 V_9 V_1(1) = V_1 V_9(1) = V_1(2) = 15 \text{ y } X_2(2) = V_1 V_9 V_1(2) = V_1 V_9(15) = V_1(3) = 14$$

Luego $X_2(3) = 13$, luego es una reflexión en el vértice 8. □

Ejemplo 10 *Sea G el grupo de las simetrías del cubo.*

Sean $V_6 = V_6^+$ la rotación en 120 grados que no mueve el vértice 6, $A_{1,4}$ la rotación en 180 grados que no mueve el arista $\{1,4\}$ y $C = C_{1,5}^+$ es la rotación en 90 grado que no mueve la cara $\{1,2,5,6\}$.

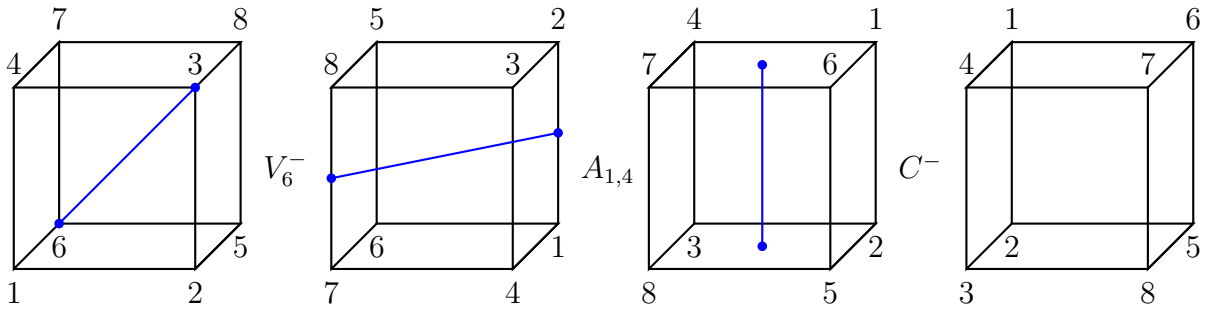
Resolver explícitamente la siguiente ecuación:

$$C \circ X \circ V_6 = A_{1,4}$$

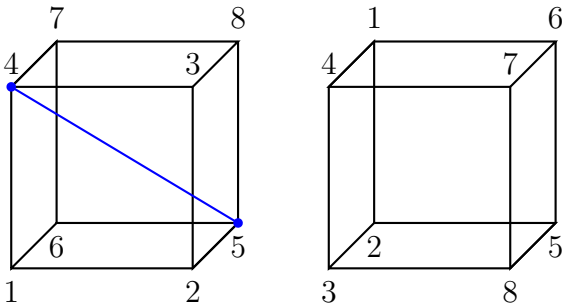
Solución: Para la primera parte, despejando obtenemos que

$$X = C^{-1} \circ A_{1,4} \circ V_6^{-1}$$

Para determinar que tipo de movimiento es podemos



Para reconocer el movimiento buscamos vértices aristas o caras fijas, en este caso tenemos los vértices 4,5 están fijos.



$$X = V_5^+ = V_4^-$$

□

Corolario 4 *Sea G un grupo y $a, b \in G$ entonces*

1. $(a^{-1})^{-1} = a$
2. $(ab)^{-1} = b^{-1}a^{-1}$

Demostración: Para la primera afirmación, sea $a \in G$, luego existe $a^{-1} \in G$, de igual modo existe el inverso de a^{-1}, denotado por $(a^{-1})^{-1}$, es decir se tiene que

$$aa^{-1} = e \qquad a^{-1}(a^{-1})^{-1} = e$$

Luego se tiene

$$a = ae = a(a^{-1}(a^{-1})^{-1}) = (aa^{-1})(a^{-1})^{-1} = e(a^{-1})^{-1} = (a^{-1})^{-1}$$

Para la segunda parte, notemos que

$$ab(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aa^{-1} = e$$

y

$$(b^{-1}a^{-1})ab = b^{-1}(a^{-1}a)b = b^{-1}b = e$$

Luego, $b^{-1}a^{-1}$ es el inverso de ab. Por lo tanto, por la segunda parte del teorema 1 tenemos que

$$(ab)^{-1} = b^{-1}a^{-1}$$

□

Observación: Sean $g_1, g_2, g_3, g_4 \in G$.

Notemos que podemos tener distinto tipo de agrupación

$$(g_1g_2)(g_3g_4) = ((g_1g_2)g_3)g_4 = (g_1(g_2g_3))g_4 = g_1((g_2g_3)g_4)$$

luego e producto $g_1g_2g_3g_4$ esta únicamente determinado.

Teorema 5 (Ley de Asociatividad Generalizada) *Sean $g_1, g_2, \ldots, g_n$ elementos de G, el producto de ellos, está únicamente determinado, sin importar el orden en que se agrupen los productos cuidando si, de no alterar el orden de los factores.*

Observación: Teniendo presente el teorema anterior y el corolario podemos escribir sin ambigüedad la siguiente expresión:

$$(g_1 \cdots g_n)^{-1} = g_n^{-1} \cdots g_1^{-1}.$$

Además podemos omitir los paréntesis en una expresión algebraica, ya que obtendremos el mismo resultado, no importando como agrupemos el producto, pero no demos cambiar el orden.

Definición 2 (Potencia) *Sean $g \in G$, $n \in \mathbb{N}_0$. Se define por recurrencia*

$$g^0 = 1$$
$$g^{n+1} = g^n \cdot g, \forall n \in \mathbb{N}_0$$

Observación: Note que no es ambiguo escribir

$$g^n = \prod_{i=1}^{n} g = \underbrace{g \cdots g}_{n-veces}$$

Así, también podemos ampliar la definición, a exponente entero

$$g^{-n} = (g^{-1})^n.$$

Propiedad 6 *Sea G un grupo entonces*

1. $(\forall n \in \mathbb{Z})(\forall g \in G)(g^{n+1} = g \cdot g^n.)$
2. $(\forall n \in \mathbb{Z})(\forall g \in G)(g^{-n} = (g^n)^{-1}.)$
3. $(\forall n \in \mathbb{Z})(\forall m \in \mathbb{Z})(\forall g \in G)(g^{m+n} = g^m \cdot g^n)$
4. $(\forall n \in \mathbb{Z})(\forall m \in \mathbb{Z})(\forall g \in G)((g^n)^m = g^{nm})$

Demostración: Sólo haremos la prueba de [3] y las otras quedan de ejercicios, para ello usaremos inducción sobre $n \in \mathbb{N}_0$.

Sea

$$p(n) := (\forall m \in \mathbb{N}_0)(\forall g \in G)(g^{m+n} = g^m \cdot g^n),$$

luego

a) $p(0) := (\forall m \in \mathbb{N}_0)(\forall g \in G)(g^{m+0} = g^m \cdot g^0)$, al reescribirlo obtenemos

$$p(0) := (\forall m \in \mathbb{N}_0)(\forall g \in G)(g^m = g^m \cdot e),$$

que es la propiedad del neutro.

b) Ahora debemos demostrar que $(\forall k \in \mathbb{N}_0)(p(k) \Rightarrow p(k+1))$, para ello suponemos que

$$p(k) := (\forall m \in \mathbb{N}_0)(g^{m+k} = g^m \cdot g^k)$$

es verdadero y debemos demostrar que

$$p(k+1) := (\forall m \in \mathbb{N}_0)(g^{m+(k+1)} = g^m \cdot g^{k+1}) \qquad \text{es verdadero}$$

Sea $m \in \mathbb{N}$,

$$\begin{array}{lll} g^{m+(k+1)} & = g^{(m+k)+1} & \\ & = g^{m+k} \cdot g & \text{por definición} \\ & = (g^m \cdot g^k) \cdot g & \text{por hipótesis} \\ & = g^m \cdot (g^k \cdot g) & \text{asociatividad} \\ & = g^m \cdot g^{k+1} & \text{por definición} \end{array}$$

luego tenemos que $p(k+1)$ es verdadero y por teorema de inducción se obtiene lo deseado.

$$(\forall n \in \mathbb{N}_0)(\forall m \in \mathbb{N}_0)(\forall g \in G)(g^{m+n} = g^m \cdot g^n).$$

Para completar la demostración veremos los otros casos:

c) Cuando los dos elementos son negativos basta factorizar. Sea $n, m \in \mathbb{N}$

$$g^{-n-m} = g^{-(n+m)} = (g^{-1})^{n+m} = (g^{-1})^n (g^{-1})^m = g^{-n} g^{-m}$$

d) Ahora veremos cuando uno es negativo y el otro es positivo, de modo que la suma sea positiva. Sean $n, m \in \mathbb{N}$, notemos que

$$g^n = g^{n-m+m} = g^{n-m}g^m$$

Luego

$$g^n g^{-m} = g^{n-m}$$

e) El último caso, reemplazamos g por g^{-1}

$$(g^{-1})^n (g^{-1})^{-m} = (g^{-1})^{n-m}$$

Luego se tiene

$$g^{-n}g^m = g^{-n+m}$$

Por lo tanto se tiene

$$(\forall n \in \mathbb{Z})(\forall m \in \mathbb{Z})(\forall g \in G)(g^{m+n} = g^m \cdot g^n).$$

□

Teorema 7 (Ley de Conmutatividad Generalizada) *Sean G un grupo conmutativo y $g_1, g_2, \ldots, g_n \in G$, entonces*

$$g_1 \cdot g_2 \cdots g_n = g_{\sigma(1)} \cdot g_{\sigma(2)} \cdots g_{\sigma(n)}. \tag{1.3}$$

para todo σ biyección de $I_n = \{1, 2, \ldots, n\}$.

Demostración: La demostración será realizada por inducción en el número de elementos.

$$p(n) := (\forall \sigma \in Biy(I_n))(g_1 \cdot g_2 \cdots g_n = g_{\sigma(1)} \cdot g_{\sigma(2)} \cdots g_{\sigma(n)})$$

Claramente tenemos que $p(1) := g_1 = g_1$ es verdadero.

Para la segunda parte suponemos $p(k)$ y demostraremos $p(k+1)$

Sea σ una biyección de $k+1$ elementos,

Supongamos que $\sigma^{-1}(k+1) = j \neq k+1$ y $\sigma(k+1) = i$ luego definimos

$$\omega(l) = \begin{cases} \sigma(l) & l \neq j; k+1 \\ i & l = j \\ k+1 & l = k+1 \end{cases}$$

$$\begin{aligned}(g_1 \cdots g_k)g_{k+1} &= (g_{\omega(1)} \cdots g_{\omega(k)})g_{k+1} \\ &= (g_{\omega(1)} \cdots g_{\omega(j-1)})g_{\omega(j)}(g_{\omega(j+1)} \cdots g_{\omega(k)})g_{k+1} \\ &= (g_{\omega(1)} \cdots g_{\omega(j-1)})g_{k+1}(g_{\omega(j+1)} \cdots g_{\omega(i)})g_{\omega(j)} \\ &= g_{\sigma(1)} \cdots g_{\sigma(j-1)} \cdot g_{\sigma(j)} \cdot g_{\sigma(j+1)} \cdots g_{\sigma(k)} \cdot g_{\sigma(k+1)}\end{aligned}$$

□

Definición 3 *Sea G un grupo.*

Se dice que G es un ***grupo finito*** *si y sólo si el conjunto G es finito, en caso contrario se dice que G es infinito.*

Se dice que el ***orden*** *de G es n, si y sólo si el cardinal de G es n, lo denotamos por*

$$\sharp(G) = |G| = n.$$

Ejemplo 11 *Determinar el orden de los siguiente grupos:*

1. *El orden de $\mathbb{Z}_5$ es 5.*
2. *El orden de $\mathbb{Z}_n$ es n.*
3. *El orden de $U(\mathbb{Z}_6)$ es 2.*
4. *Recuerde que, en general, el orden de $U(\mathbb{Z}_n) = \phi(n)$, donde ϕ es la función de Euler.*
5. *El orden de D_n es $2n$.*
6. *El orden de $Sim(tetraedro)$ es 24*
7. *El orden de $(\mathcal{P}(A), \triangle)$ es $2^{|A|}$.*

además tenemos que $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ son grupos infinitos

1.2.2. Problemas Propuestos

Problema 1.

Sea D_9 el grupo de las simetrías, del polígono regular de 9 lados, donde V_i es la reflexión que no mueve el vértice i y R es la rotación en 40 grados en el sentido de la enumeración.

Resolver explícitamente las siguientes ecuaciones:

a) $V_5 = V_2 \circ X_1$

b) $V_7 = V_1 \circ X_2 \circ V_1$

Problema 2.

Sea D_{10} el grupo de las simetrías, del polígono regular de 10 lados, donde V_i es la reflexión que no mueve el vértice i y R es la rotación en 36 grados en el sentido de la enumeración.

Resolver explícitamente las siguientes ecuaciones:

$$V_5 = V_2 \circ X_1 \circ R$$

Problema 3.

Sea D_{24} el grupo de las simetrías, del polígono regular de 24 lados, donde V_i es la reflexión que no mueve el vértice i, A_i es la reflexión que no mueve la arista $\{i, i+1\}$, y R es la rotación en 15 grados en el sentido de la enumeración.

Resolver explícitamente las siguientes ecuaciones:

a) $V_6 = V_2 \circ X_1$

b) $V_7 = R \circ X_2 \circ A_1$

Problema 4.

Sea D_{25} el grupo de las simetrías, del polígono regular de 25 lados, donde V_i es la reflexión que no mueve el vértice i y R es la rotación en 14.4 grados en el sentido de la enumeración.

Resolver explícitamente las siguientes ecuaciones:

(a) $V_3 = V_1 \circ X_1$

(b) $V_{15} = V_1 \circ X_2 \circ V_3$

Problema 5.

Sea G el grupo de las simetrías del cubo.

Sean $A = A_{1,2}$ la rotación que no mueve la arista $\{1, 2\}$, $V = V_4^+$ la rotación en 120 grados que no mueve el vértice 4 y $C = C_{1,7}^+$ es la rotación en 90 grado que no mueve la cara $\{1, 4, 7, 6\}$.

Resolver explícitamente las siguiente ecuación:

$$V \circ X \circ C = A$$

Problema 6.

Sea G el grupo de las simetrías del cubo.

Sean $V_6 = V_6^+$ la rotación en 120 grados que no mueve el vértice 6, $A_{1,4}$ la rotación en 180 grados que no mueve el arista $\{1, 4\}$ y $C = C_{15}^+$ es la rotación en 90 grado que no mueve la cara $\{1, 2, 5, 6\}$.

Resolver explícitamente la siguiente ecuación:

$$C \circ X \circ V_6 = A_{1,4}$$

Problema 7.

Sea G el grupo de las simetrías del cubo.

Sean $A = A_{1,2}$ la rotación que no mueve la arista $\{1, 2\}$, $V = V_4^+$ la rotación en 120 grados que no mueve el vértice 4 y $C = C_{3,7}^+$ es la rotación en 90 grado que no mueve la cara $\{3, 8, 7, 4\}$.

Resolver explícitamente las siguiente ecuación:

$$V \circ X \circ C = A$$

Problema 8.

Determinar el valor de verdad de las siguientes proposiciones. JUSTIFIQUE

a) Si E es un conjunto, entonces $(\mathcal{P}(E), \cap)$ es un grupo.

b) $(\mathbb{R}^+, \cdot)$ es un grupo.

c) La ecuación $2 \oplus x = 3$ en $(\mathbb{Z}, \oplus)$, no tiene solución.(Ejemplo 2)

Problema 9.

Sean H un subgrupo del grupo G y

$$H^g = \{x \in G \mid (\exists h \in H)(\ x = ghg^{-1}\ )\}.$$

Demostrar que, para todo $g \in G$, H^g es un subgrupo de G.

Problema 10.

Sea $H = \{1, -1\} \subseteq \mathbb{R}^*$, se define en $G = \mathbb{Z} \times H$, la siguiente operación binaria

$$(a, b) \star (c, d) = (a + bc, bd).$$

Demostrar que $(G, \star)$ es un grupo.

1.3. Subgrupo

Definición 4 *Sea $H \subseteq G$, no vacío. Se dice que H es un* ***subgrupo*** *de G si y sólo si H es un grupo con la misma operación, y lo denotamos por:*

$$H \leq G \text{ o bien } (H, *) \leq (G, *).$$

es decir, si $(G, *)$ es un grupo, entonces $(H, *)$ es un subgrupo si cumple con

1. *Clausura u Operación Binaria*

$$\begin{array}{rccc} * : & H \times H & \longrightarrow & H \\ & (a, b) & \longmapsto & a * b \end{array}$$

2. *Propiedad Asociativa*

$$(\forall a, b, c \in H)((a * b) * c = a * (b * c))$$

3. *Propiedad del Neutro*

$$(\exists e \in H)(\forall a \in H)(a * e = e * a = a)$$

4. *Propiedad del Inverso*

$$(\forall a \in H)(\exists b \in H)(a * b = b * a = e.)$$

Ejemplo 12

1. $(\mathbb{Q}, +)$ *es un subgrupo de* $(\mathbb{R}, +)$
2. $(\mathbb{R}, +)$ *es un subgrupo de* $(\mathbb{C}, +)$
3. $(\mathbb{Q}^*, \cdot)$ *es un subgrupo de* $(\mathbb{R}^*, \cdot)$
4. $(M_n(\mathbb{R}), +)$ *es un subgrupo de* $(M_n(\mathbb{C}), +)$

Propiedad 8 *Sea $H \subseteq G$, no vacío, entonces H es un subgrupo de G si y sólo si*

1. $(\forall a, b \in H)\,(ab \in H)$
2. $(\forall a \in H)\,(a^{-1} \in H)$

Demostración:
$\Rightarrow$) Supongamos que H es un subgrupo de G, luego H es un grupo y por tanto se cumplen [1] y [2].
$\Leftarrow$) Supongamos que se cumplen [1] y [2], por demostrar que H es un subgrupo de G. Por [1] vemos que H cumple la clausura y además la asociatividad la hereda de G, pues $H \subseteq G$, luego H es un Semigrupo. Como H es no vacío, se tiene que existe$a \in H$, luego por [1] y [2] se tiene que

$$aa^{-1} = a^{-1}a = e \in H$$

Luego, H es un Monoide. Finalmente, por [2] se tiene que H es un grupo y por tanto un subgrupo de G. □

Propiedad 9 *Sea $H \subseteq G$, no vacío, entonces H es un subgrupo de G si y sólo si*

$$(\forall a, b \in H)(ab^{-1} \in H). \tag{1.4}$$

Demostración:
$\Rightarrow$) Supongamos que H es un subgrupo de G, luego H es un grupo y por tanto se cumplen que dado $a, b \in H$, se tiene que $b^{-1} \in H$, luego $ab^{-1} \in H$
$\Leftarrow$) Verificaremos la propiedad 1.4, sea $a \in H$, ya que es no vacío, luego se tiene que $e = aa^{-1} \in H$. Sean $a, b \in H$, luego $b^{-1} = eb^{-1} \in H$, es decir $a, b^{-1} \in H$ y por lo tanto

$$ab = a(b^{-1})^{1-} \in H$$

Luego, H cumple las condiciones de la propiedad anterior, por tanto H un subgrupo de G. □

Ejemplo 13 *Sean $\mathbb{Z}[i] = \{a + bi \in \mathbb{C} \mid a, b \in \mathbb{Z}\}$ y $\mathbb{Q}[i] = \{a + bi \in \mathbb{C} \mid a, b \in \mathbb{Q}\}$*
Demostrar que $\mathbb{Z}[i], \mathbb{Q}[i]$ son subgrupos de $\mathbb{C}$
Solución: *Es claro que $\mathbb{Z}[i] \neq \emptyset$, pues $0 = 0 + 0i \in \mathbb{Z}[i]$, además $\mathbb{Z}[i] \subset \mathbb{C}$ por definición.*
Sean $u = a + bi, v = c + di \in \mathbb{Z}[i]$, por demostrar que $u - v \in \mathbb{Z}[i]$. Notemos que

$$u - v = a + bi - (c + di) = (a - c) + (b - d)i$$

luego $u - v \in \mathbb{Z}[i]$, pues $(a - c), (b - d) \in \mathbb{Z}$. Así concluimos que $\mathbb{Z}[i] \leq \mathbb{C}$.
Demostrar que $\mathbb{Q}[i] \leq \mathbb{C}$ es análogo al ejercicio anterior.

□

Ejemplo 14 *Sea* $\mathbb{Q}(i) = \{a + bi \in \mathbb{Q}[i] \mid a \neq 0 \ \vee \ b \neq 0\}$
Demostrar que $\mathbb{Q}(i)$ *es un subgrupo de* $\mathbb{C}^*$.
Solución: *Vemos que* $\mathbb{Q}(i) \neq \emptyset$, *pues* $1 = 1 + 0i \in \mathbb{Q}(i)$. *Notemos que* $\mathbb{Q}(i) \subset \mathbb{Q}[i] \subset \mathbb{C}$, *además* $0 \notin \mathbb{Q}(i)$ *por definición, entonces* $\mathbb{Q}(i) \subset \mathbb{C}^*$.
Sean $u = a + bi, v = c + di \in \mathbb{Q}(i)$, *por demostrar que* $uv^{-1} \in \mathbb{Q}(i)$. *Notemos que*

$$uv^{-1} = (a + bi)(\frac{c - di}{c^2 + d^2}) = \frac{ac + bd}{c^2 + d^2} + \frac{bc - ad}{c^2 + d^2}i$$

Ahora, supongamos que $uv^{-1} \notin \mathbb{Q}(i)$, *es decir*

$$ac + bd = 0 \ \wedge \ bc - ad = 0$$

estudiemos entonces los casos

1. *Si* $a = 0 \ \wedge \ b \neq 0$, *se tiene que* $c = d = 0$ *lo cual es una contradicción, pues* $v = c + di \in \mathbb{Q}(i)$.

2. $\sharp(\{b, c, d\} \cap \{0\}) = 1$ *son casos similares al caso 1, es decir, en todos existen contradicciones (se deja de ejercicio su verificación).*

3. *Para el caso* $\{a, b, c, d\} \cap \{0\} = \emptyset$ *estudiemos el sistema*

$$\begin{array}{rcll} ac + bd & = & 0 & /b \\ bc - ad & = & 0 & / - a \end{array}$$

entonces

$$d(a^2 + b^2) = 0 \ \Leftrightarrow d = 0 \ \vee \ a^2 + b^2 = 0$$

lo cual es una contradicción.

Así concluimos que $uv^{-1} \in \mathbb{Q}(i)$ *y por tanto* $\mathbb{Q}(i) \leq \mathbb{C}^*$. □

Ejercicio 15 *Sea* $A = \{a + b\sqrt[3]{5} \in \mathbb{R} \mid a, b \in \mathbb{Q}\}$
Determinar si A *es un subgrupo de* $\mathbb{R}^*$

Definición 5 *Sean* G *un grupo y* H *un subgrupo de* G.
Se dice que H *es* ***subgrupo propio*** *de* G *si y sólo si* $\{e\} \neq H \neq G$.

Propiedad 10 *Sea* G *un grupo entonces se tiene que*

1. *Sean* H *y* K *subgrupos de* G, *entonces* $H \cap K$ *es un subgrupo de* G.

2. *Sea* $\{H_\lambda\}_{\lambda \in L}$ *una familia de subgrupos de* G, *entonces* $\bigcap\limits_{\lambda \in L} H_\lambda$ *es un subgrupo de* G.

Demostración: Haremos la demostración [1] y la de [2] se deja de ejercicio.

Notemos que $H \cap K \neq \emptyset$, pues $e \in H$ y $e \in K$ (por el hecho de ser subgrupos de G) y por tanto $e \in H \cap K$. Además, es fácil ver que $H \cap K \subseteq G$. Ahora sólo nos resta probar que si $a, b \in H \cap K$, entonces $ab^{-1} \in H \cap K$.

Como $a, b \in H \cap K$, entonces $a, b \in H$ y $a, b \in K$, luego como ambos son grupos se tiene que $ab^{-1} \in H$ y $ab^{-1} \in K$, de modo que

$$ab^{-1} \in H \cap K$$

Por lo tanto $H \cap K \leq G$. □

Observación: Si H, K son subgrupos de G, entonces $H \cup K$ no necesariamente es un subgrupo de G.

Un Ejemplo de ello es $H = 3\mathbb{Z}; K = 4\mathbb{Z}$ subgrupos de $\mathbb{Z}$, en la unión se encuentra el 3 y el 4 pero $7 = 3 + 4$ no pertenece a la unión.

Luego necesitamos construir el más pequeño de los subgrupos que contiene a H y también a K.

1.3.1. Problemas Propuestos

Problema 11.

Determinar en cada caso, si las siguientes proposiciones son verdaderas o falsas.

1. $\mathbb{Q} \leq \mathbb{R}^*$
2. $\mathbb{R}^+ \leq \mathbb{R}^*$.
3. $\mathcal{U} = \{u \in \mathbb{C} \mid (\exists n \in \mathbb{N})(u^n = 1)\} \leq \mathbb{C}^*$.
4. $\mathcal{H} = \left\{ \begin{pmatrix} a & b \\ b & a \end{pmatrix} \mid a, b \in \mathbb{Q} \right\} \leq M_2(\mathbb{Q})$.
5. $\mathcal{H} = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{R}) \mid ad - bc = 1 \right\} \leq GL_2(\mathbb{R})$.
6. $\mathcal{L}_{x_0} = \{f \in \mathcal{F}(\mathbb{R}, \mathbb{R}) \mid f(x_0) = 0\} \leq \mathcal{F}(\mathbb{R}, \mathbb{R})$; x_0 fijo.
7. $\mathcal{L} = \{f \in \mathcal{F}(\mathbb{R}, \mathbb{R}) \mid (\forall t \in \mathbb{Z})(f(t) = 0)\} \leq \mathcal{F}(\mathbb{R}, \mathbb{R})$.
8. $\mathcal{H} = \{f \in \mathcal{F}(\mathbb{R}, \mathbb{R}) \mid (\forall x \in \mathbb{R})\,(f(x) = 0)\} \leq \mathcal{F}(\mathbb{R}, \mathbb{R})$.
9. $\mathcal{H} = \{f \in \mathcal{F}(\mathbb{R}, \mathbb{R}) \mid (\exists x \in \mathbb{R})\,(f(x) = 0)\} \leq \mathcal{F}(\mathbb{R}, \mathbb{R})$.
10. $\mathcal{K} = \{T_a \in \mathcal{F}(\mathbb{R}, \mathbb{R}) \mid T_a$ es una traslación, con $a \in \mathbb{R}\} \leq \mathcal{F}(\mathbb{R}, \mathbb{R})$, donde $T_a(x) = x + a$.
11. $\mathcal{H} = \{h_t \in \mathcal{F}(\mathbb{R}, \mathbb{R}) \mid h_t$ es una homotecia, con $t \in \mathbb{R}\} \leq Biy(\mathbb{R})$.

Problema 12.

Sean $G = Biy(\mathbb{R}) = \{f \in F(\mathbb{R},\mathbb{R}) \quad | \quad f \text{ es biyectiva}\}$.

Determinar el valor de verdad de las siguientes proposiciones.

(a) $H_0 = \{h_t \in F(\mathbb{R},\mathbb{R}) \mid h_t \text{ es una homotecia, con } t \in \mathbb{R}\} \leq G$, (es decir, $h_t(x) = tx$).

(b) $H_1 = \{t_a \in F(\mathbb{R},\mathbb{R}) \mid t_a \text{ es una traslación, con } a \in \mathbb{R}\} \leq G$, (es decir, $t_a(x) = x + a$).

(c) $H_2 = \{f \in G \mid (\forall x \in \mathbb{R})\,(f(-x) = -f(x)\} \leq G$

Problema 13.

Demuestre que un grupo no puede ser unión de dos subgrupos propios.

1.4. Generado

Sea S un subconjunto de G, el grupo `generado` por S, es el subgrupo más pequeño de G que contiene a S y se denota por $\langle S\rangle$.

Caso particular si $S = \{x_1, x_2, ..., x_n\}$ es un conjunto finito entonces

$$\langle S\rangle = \langle\{x_1, x_2, ..., x_n\}\rangle = \langle x_1, x_2, ..., x_n\rangle$$

Propiedad 11 *Sea G un grupo y $a \in G$*

$$\langle\{a\}\rangle = \langle a\rangle = \{a^n \in G \mid n \in \mathbb{Z}\}$$

Solución: Sean $a \in G$ y $H = \{a^n \in G \mid n \in \mathbb{Z}\}$, notemos que $a^0 = e \in H$, y $a^n \in G$, luego H es no vacío y $H \subset G$. Además, dado $a^n, a^m \in H$, se tiene que

$$a^n(a^m)^{-1} = a^n a^{-m} = a^{n-m} \in H$$

Luego H es un subgrupo que contiene a, por otro lado se tiene que $< a >$ es el subgrupo más pequeño que contiene al elemento a, por lo tanto $< a > \subset H$, dado $a^m \in H$ se tiene que $a^m \in < a >$, de lo cual obtenemos

$$H = < a >$$

□

Ejemplo 16 *Determinar $\langle 2\rangle$ en $G = \mathbb{Z}_6$.*

Solución: Por propiedad 11 tenemos que

$$\langle 2\rangle = \{2n \in \mathbb{Z}_6 \mid n \in \mathbb{Z}\} = \{0, 2, 4\}$$

□

Ejemplo 17 *Determinar $\langle 2\rangle$ en $G = \mathbb{Z}_7{}^*$.*

Solución: Nuevamente, por propiedad 11 tenemos que

$$\langle 2\rangle = \{2^n \in \mathbb{Z}_7{}^* \mid n \in \mathbb{Z}\} = \{1, 2, 4\}$$

□

Ejemplo 18 *Sea $S = \{f\}$, donde f esta definida por $f(x) = x + 1$.*
Determinar $\langle S\rangle$ en el grupo $(Biy(\mathbb{R}), \circ)$.

Solución: Dada la función $f(x) = x + 1$, tenemos $f^2(x) = f(x + 1) = x + 2$, de lo cual podemos obtener generalizar que

$$f^{n+1}(x) = f(x + n) = x + n + 1$$

es decir, por inducción se tiene que $f^n(x) = x + n$, y las funciones inversas esta dada por, $f^{-n}(x) = x - n$. de este modo se tiene que

$$\langle f\rangle = \{\ g \in Biy(\mathbb{R}) \mid (\exists n \in \mathbb{Z})\forall x \in \mathbb{R})(g(x) = x + n)\}$$

□

Ejemplo 19 *Sea $S = \{f\}$, donde f esta definida por $f(x) = x + 1$.*
Determinar $\langle S\rangle$ en el grupo $(F(\mathbb{R}, \mathbb{R}), +)$.

Solución: Dada la función $f(x) = x + 1$, tenemos $(f + f)(x) = f(x) + f(x) = 2x + 2$, de lo cual podemos obtener generalizar que

$$(n + 1)f(x) = nf(x) + f(x) = nx + n + x + 1$$

es decir, por inducción se tiene que $nf(x) = nx + n$, y las funciones inversas aditiva esta dada por, $-(nf)(x) = -nx - n$. de este modo se tiene que

$$\langle f\rangle = \{\ g \in F(\mathbb{R}, \mathbb{R}) \mid (\exists n \in \mathbb{Z})\forall x \in \mathbb{R})(g(x) = nx + n)\}$$

□

Propiedad 12 *Sean $a \in S \subset G$, luego se tiene que*

$$\langle a\rangle \leq \langle S\rangle \leq G$$

Ejemplo 20 *Determinar $\langle\{2, 3\}\rangle = \langle 2, 3\rangle$ en el grupo $\mathbb{Z}_6$, es decir, $(\mathbb{Z}_6, +)$.*

Solución: Note que $\langle 2\rangle = \{2, 4, 0\}$ y $\langle 3\rangle = \{3, 0\}$, pero como $H = \langle 2, 3\rangle$ es un subgrupo, se tiene que $1 = 3 - 2 \in H$, luego se tiene que

$$n = n1 \in H$$

De lo cual obtenemos $\langle 2, 3\rangle = \mathbb{Z}_6$ □

Ejemplo 21 *Determinar $\langle\{2, 3\}\rangle = \langle 2, 3\rangle$ en el grupo $G = \mathbb{Z}_7{}^*$, es decir, $(\mathbb{Z}_7{}^*, \cdot)$.*

Solución: Sea $\langle 2\rangle = \{2, 4, 1\}$, $\langle 3\rangle = \{3, 2, 6, 4, 5, 1\}$ Por lo tanto $\langle 2, 3\rangle = \mathcal{U}(\mathbb{Z}_7)$. □

Propiedad 13 *Sea $S \subseteq G$, entonces*

$$\langle S\rangle = \bigcap_{\substack{H\leq G\\ S\subseteq H}} H$$

Demostración: Sea

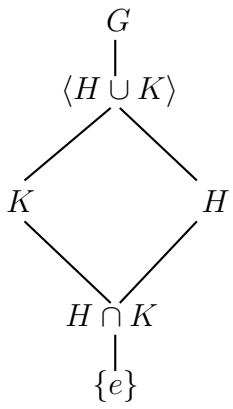
$$K = \bigcap_{\substack{H\leq G\\ S\subseteq H}} H$$

Por la propiedad 10, se tiene que K es un subgrupo de G. Además $S \subset K$, luego $\langle S\rangle \subset K$, por otro lado tenemos que $S \subset \langle S\rangle$, luego es un subgrupo que contiene a S, por lo tanto

$$K = \bigcap_{\substack{H\leq G\\ S\subseteq H}} H \subset \langle S\rangle,$$

es decir, $K = \langle S\rangle$. □

Observación: Sean $H, K \leq G$, entonces tenemos que $\langle H \cup K\rangle$ es el subgrupo más pequeño que contiene a H y K y se cumple el siguiente diagrama de inclusiones.



Propiedad 14 *Sea $\phi \neq S \subseteq G$, entonces*

$$H = \{s_1 \cdots s_n \mid (\forall n \in \mathbb{N})(\forall i \in \{1, 2, ..., n\})(s_i \in S \vee s_i^{-1} \in S)\}$$

es el subgrupo de G generado por S.

1.4.1. Problemas Propuestos

Problema 14.

Sea G =Biy($\mathbb{Z}$) y

$$f: \begin{array}{ccc}\mathbb{Z} & \longrightarrow & \mathbb{Z}\\ x & \rightsquigarrow & x+1\end{array} \quad ; \qquad g: \begin{array}{ccc}\mathbb{Z} & \longrightarrow & \mathbb{Z}\\ x & \rightsquigarrow & -x\end{array}$$

Describir $H =< f, g >\leq G$, es decir, dada $h \in H$ entonces $h \in$Biy($\mathbb{Z}$) y $h(x) = ...$

Problema 15.

Sean $G = Sim(\triangle)$ y V_i la reflexión que deja fijo el vértice i). Determinar $\langle V_3, V_2\rangle$.

1.5. Grupos Cíclicos

Definición 6 *Sea G un grupo, se dice que G es un grupo* `cíclico` *si y sólo si existe $g \in G$ tal que*

$$G = \langle g \rangle$$

Ejemplo 22

1. *$\mathbb{Z}$ es un grupo cíclico infinito generado por 1 o por -1.*
2. *$\mathbb{Z}_n$ es un grupo cíclico generado por 1, más aún, generado por cualquier $r \in \mathbb{Z}_n$ tal que $MCD(n, r) = 1$.*
3. *$U(\mathbb{Z}_5)$ es un grupo cíclico generado por 2.*
4. *$\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$ no son cíclicos.*

Propiedad 15 *Todo Grupo Cíclico es Abeliano*

Demostración de ejercicio □

Observación: Notemos que el recíproco de la proposición anterior no es válido, por ejemplo, $\mathbb{R}$ es un grupo abeliano, pero no es cíclico.

Teorema 16 *Todo subgrupo de un Grupo Cíclico es Cíclico.*

Demostración: Sea G un grupo cíclico generado por a y sea $H \leq G$, veamos que si $H = \{e\}$ entonces $H = \langle e \rangle$, por lo tanto es cíclico.

Supongamos que $H \neq \{e\}$, entonces existe $e \neq a^m \in G$ tal que $a^m \in H$ para algún $m \in \mathbb{Z}^+$. Ahora, consideremos m como el menor entero positivo tal que $a^m \in H$. El objetivo es demostrar que $H = \langle a^m \rangle$, pero sabemos que $\langle a^m \rangle \subseteq H$, luego basta demostrar que $H \subseteq \langle a^m \rangle$.

Sea $b \in H \leq G$, como G es cíclico entonces $b = a^n$ para algún $n \in \mathbb{Z}$. Ahora, como es costumbre, utilicemos el algoritmo de la división para m y n.

$$\begin{array}{rcll} n & = & mq + r & 0 \leq r < m \\ a^n & = & a^{mq+r} & \\ a^n(a^m)^{-q} & = & a^r & \end{array}$$

Ahora como $a^n, a^m \in H$ y H es grupo entonces $a^n(a^m)^{-q} = a^r \in H$, pero como m es el menor entero positivo tal que $a^m \in H$ y además $0 \leq r < m$, entonces $r = 0$. Por lo tanto $n = mq$, luego

$$b = a^n = (a^m)^q$$

Entonces b es una potencia de a^m (es decir, $b \in \langle a^m \rangle$) y por tanto $H \subseteq \langle a^m \rangle$. Así concluimos que H es cíclico. □

Ejemplo 23 *Determine todos los subgrupo de* $\mathbb{Z}_6$.
Solución: *Es claro que*

$$\langle 1\rangle = \langle 5\rangle = \mathbb{Z}_6$$

Por la proposición precedente, los subgrupos de $\mathbb{Z}_6$ *son:*

1. *Los subgrupos triviales* $\langle 0\rangle = \{0\}$ *y* $\mathbb{Z}_6$.
2. $H_1 = \langle 2\rangle = \langle 4\rangle = \{0, 2, 4\}$.
3. $H_2 = \langle 3\rangle = \{0, 3\}$.

□

Ejemplo 24 *Determine todos los subgrupos de* $U(\mathbb{Z}_9)$.

Solución: Los subgrupos de $U(\mathbb{Z}_9)$ son:

1. Los triviales $\langle 1\rangle = \{1\}$ y $\langle 2\rangle = \langle 5\rangle = U(\mathbb{Z}_9)$. Note que el grupo es cíclico
2. $H_1 = \langle 4\rangle = \langle 7\rangle = \{1, 4, 7\}$.
3. $H_2 = \langle 8\rangle = \{1, 8\}$

□

Teorema 17 *Sea* $g \in G$, *entonces el subgrupo generado por* g, *es decir,* $\langle g\rangle$ *es*

1. *infinito o bien*
2. *Existe* $k \in \mathbb{N}$ *tal que* $\langle g\rangle = \{1, g, \ldots, g^{k-1}\}$, *todos distintos,* $|\langle g\rangle| = k$

Demostración: Sean $n, m \in \mathbb{Z}$, entonces

$$g^n \neq g^m \quad \vee \quad g^n = g^m$$

1. Si para todo $n, m \in \mathbb{Z}$ tenemos $g^n \neq g^m$, entonces todos los elementos g^n son distintos, es decir:

$$\begin{array}{ccc} \mathbb{Z} & \longrightarrow & \langle g\rangle \\ m & \longmapsto & g^m \end{array}$$

   esta aplicación es biyectiva, es decir, G es infinito.

2. Si existen n, m distintos tal que $g^n = g^m$, luego

$$g^{n-m} = 1 \quad \wedge \quad g^{m-n} = 1.$$

   Así tenemos que $\{l \in \mathbb{N} \mid g^l = 1\}$ es un conjunto no vacío y acotado inferiormente.
   Luego existe

$$k = min\{l \in \mathbb{N} \mid g^l = 1\},$$

Sea $m \in \mathbb{Z}$, por algoritmo de la división tenemos $m = k \cdot s + r$, donde $0 \leq r < k$

$$g^m = g^{ks} \cdot g^r = (g^k)^s \cdot g^r = 1 \cdot g^r = g^r,$$

Así

$$g^m \in \{1, g, \ldots, g^{k-1}\}.$$

Veamos ahora que los elementos son distintos, dado $m, n\mathbb{N}$, menores que k, supongamos que $mgeqn$ tales que $g^m = g^n$, luego $g^{m-n} = 1$, pero $m - n < k$, luego $m = n$, luego tenemos

$$\langle g \rangle = \{1, g, \ldots, g^{k-1}\}.$$

□

Definición 7 *Sea $g \in G$,*

1. *Se dice que el* **orden** *de g es infinito si y sólo si $\langle g \rangle$ es infinito.*
2. *Se dice que el* **orden** *de g es n si y sólo si $|\langle g \rangle| = n$.*

Notación:

$$|\langle g \rangle| = |g| = o(g) = ord(g)$$

Corolario 18 *Sean G un grupo y $g \in G$ de orden n.*
Si $g^m = e$ entonces m es múltiplo de n.

Ejemplo 25 *Sea $A = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \in GL_2(\mathbb{Z}_5)$. Entonces el orden de A es 4.*

Ya que

$$\left\langle \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \right\rangle = \left\{ \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 4 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 3 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\}$$

Ejemplo 26 *Sea $B = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \in GL_2(\mathbb{Z}_5)$. Entonces el orden de B es 5.*

Ya que

$$\left\langle \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \right\rangle = \left\{ \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 4 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\}$$

Observación: Note que AB y BA del ejemplo anterior tienen orden 4, y no es el producto de los ordenes.

$$AB = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 4 \\ 0 & 1 \end{pmatrix}$$

$$\langle AB \rangle = \left\{ \begin{pmatrix} 2 & 4 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 4 & 2 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 3 & 3 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\}$$

$$BA = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 2 \\ 0 & 1 \end{pmatrix}$$

$$\langle BA \rangle = \left\{ \begin{pmatrix} 2 & 2 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 4 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 3 & 4 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\}$$

Propiedad 19 *Sea $G = \langle g \rangle$ finito de orden n, entonces para todo $k \in \mathbb{N}$, tal que $1 \leq k < n$, se tiene que*

$$|g^k| = \frac{n}{MCD(n,k)}$$

Demostración: Sean $G = \langle g \rangle$ finito de orden n, y $k \in \mathbb{N}$, tal que $1 \leq k < n$, luego

$$(g^k)^{\frac{n}{MCD(n,k)}} = (g^n)^{\frac{k}{MCD(n,k)}} = e$$

Además, se tiene que

$$(g^k)^r = e \Leftrightarrow g^{kr} = e$$

De lo cual tenemos, existe m, tal que $nm = kr$, por lo tanto

$$\frac{n}{MCD(n,k)}m = \frac{k}{MCD(n,k)}r,$$

es decir

$$\frac{n}{MCD(n,k)} \left| \frac{k}{MCD(n,k)}r \right.$$

de este modo $\frac{n}{MCD(n,k)}|r$. □

1.5.1. Problemas Propuestos

Problema 16.

Determine todos los subgrupos de $U(\mathbb{Z}_{13})$.

Problema 17.

Determine todos los subgrupos de $U(\mathbb{Z}_4) \times \mathbb{Z}_7$

Problema 18.

Determine todos los subgrupos de $\{1, -1\} \times \mathbb{Z}_5$.

Problema 19.

Sean $g, h \in G$ tales que $|g| = m$; $|h| = r$.
Si g, h conmutan entonces $|gh| = MCM(m, r)$.

Problema 20.

Sean G un grupo y $a \in G$ de orden finito entonces para todo $x \in G$ se tiene que

$$|a| = |a^{-1}| = |xax^{-1}|$$

1.6. Subgrupos Notables

Sea $\phi \neq S \subseteq G$, se define

1. El `Centro` de G
$$Z(G) = \{g \in G \mid g \cdot h = h \cdot g \quad \forall h \in G\}$$

Ejemplo 27 *El centro de $\mathbb{Z}$ es $\mathbb{Z}$, pues para todo $x \in \mathbb{Z}$ se tiene que*
$$x + y = y + x$$
para todo $y \in \mathbb{Z}$

Ejemplo 28 *El centro de D_3 es $\{Id\}$.*

2. El `Centralizador` de S en G:
$$C_G(S) = \{g \in G \mid g \cdot s = s \cdot g \quad \forall s \in S\}.$$

Observación: El centralizador de G en G es el centro de G, es decir,
$$Z(G) = C_G(G).$$

3. El `Normalizador` de S en G:
$$N_G(S) = \{g \in G \mid g \cdot S = S \cdot g\}.$$
donde
$$g \cdot S = \{x \in G \mid (\exists s \in S)\,(x = gs)\}$$
$$S \cdot g = \{x \in G \mid (\exists s \in S)\,(x = sg)\}$$

4. El `Conmutador` de G
$$[G,\ G] = \left\langle \{ghg^{-1}h^{-1} \in G \mid g, h \in G\} \right\rangle$$
denotamos $[g, h] = ghg^{-1}h^{-1}$
$$[G,\ G] = \langle \{[g, h] \in G \mid g, h \in G\} \rangle$$

Ejemplo 29 *El conmutador de D_3 es $\langle R \rangle = \{Id, R, R^2\}$, donde R es la rotación en 60 grados en sentido de la enumeración.*

Observación: Con las herramientas que poseemos hasta el momento, el conmutador de un grupo G cualquiera no es fácil de calcular, ya que en general debemos considerar dos elementos arbitrarios $g, h \in G$ y debemos calcular explícitamente el elemento $[g, h]$ el cual es un elemento de $[G, G]$ (y como $[G, G]$ es grupo, entonces también están sus potencias), y así sucesivamente. Sin embargo, en las siguientes secciones conoceremos dos herramientas que nos serán de utilidad para el calcular este importante subgrupo.

Ejemplo 30 *Sean* $G = GL_2(\mathbb{R})$ *y sea* $S = \left\{ \begin{pmatrix} 1 & 0 \\ 1 & 3 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix} \right\}$. *Determinar* $C_G(S)$ *y* $N_G(S)$.

Solución: Sea $\begin{pmatrix} x & y \\ z & w \end{pmatrix} \in C_S(G)$, luego

$$\begin{pmatrix} x & y \\ z & w \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 3 \end{pmatrix}\begin{pmatrix} x & y \\ z & w \end{pmatrix}$$
$$\begin{pmatrix} x & y \\ z & w \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 0 & 2 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 2 \end{pmatrix}\begin{pmatrix} x & y \\ z & w \end{pmatrix}$$

Del cual tenemos el siguiente sistema de ecuaciones

$$\begin{array}{rcl} x+y & = & x \\ 3y & = & y \\ z+w & = & x+3z \\ 3w+y & = & 3w \\ 2y & = & z \\ x & = & y \\ 2w & = & 2x \\ z & = & 2y \end{array}$$

el cual tiene como soluciones

$$x = w \quad , \quad y = z = 0$$

Así tenemos que

$$C_G(S) = \left\{ \begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix} \in G \;\middle|\; x \in \mathbb{R}^* \right\}$$

De manera análoga, sea $\begin{pmatrix} x & y \\ z & w \end{pmatrix} \in N_G(S)$, luego

$$\begin{pmatrix} x & y \\ z & w \end{pmatrix}\left\{ \begin{pmatrix} 1 & 0 \\ 1 & 3 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix} \right\} = \left\{ \begin{pmatrix} 1 & 0 \\ 1 & 3 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix} \right\}\begin{pmatrix} x & y \\ z & w \end{pmatrix}$$

$$\left\{ \begin{pmatrix} x & y \\ z & w \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 1 & 3 \end{pmatrix}, \begin{pmatrix} x & y \\ z & w \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix} \right\} = \left\{ \begin{pmatrix} 1 & 0 \\ 1 & 3 \end{pmatrix}\begin{pmatrix} x & y \\ z & w \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix}\begin{pmatrix} x & y \\ z & w \end{pmatrix} \right\}$$

Entonces tenemos dos casos:

1.
$$\begin{pmatrix} x & y \\ z & w \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 3 \end{pmatrix}\begin{pmatrix} x & y \\ z & w \end{pmatrix}$$
$$\begin{pmatrix} x & y \\ z & w \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 0 & 2 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 2 \end{pmatrix}\begin{pmatrix} x & y \\ z & w \end{pmatrix}$$

el cual es el caso que estudiamos para calcular el centralizador.

2.
$$\begin{pmatrix} x & y \\ z & w \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 1 & 3 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix}\begin{pmatrix} x & y \\ z & w \end{pmatrix}$$
$$\begin{pmatrix} x & y \\ z & w \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 3 \end{pmatrix}\begin{pmatrix} x & y \\ z & w \end{pmatrix}$$

Del cual tenemos el siguiente sistema de ecuaciones

$$\begin{array}{rcl} x+y & = & z \\ 3y & = & w \\ z+w & = & 2x \\ 3w & = & 2y \\ 2y & = & x \\ x & = & y \\ 2w & = & x+3z \\ z & = & y+3w \end{array}$$

el cual tiene como solución

$$x = y = z = w = 0$$

pero $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \notin G$, luego este caso no puede ocurrir. Así concluimos que

$$N_G(S) = C_G(S)$$

□

Propiedad 20 *Sean G un grupo y $S \subseteq G$ no vacío, entonces*

1. $C_G(S) \leq G$
2. $N_G(S) \leq G$
3. $C_G(S) \leq N_G(S)$
4. $N_G(S) \leq N_G(C_G(S))$

Demostración: Sean G un grupo y $S \subseteq G$ no vacío, por definición se tiene que

$$e \in C_G(S) \subset G.$$

Veamos ahora, sean $g, h \in C_G(S)$, luego para todo $s \in S$ se tiene que $gs = sg$ y $hs = sh$.

$$(gh)s = g(hs) = (gs)h = s(gh)$$

luego $gh \in C_G(S)$.

Por otro lado tenemos

$$hs = sh \Leftrightarrow sh^{-1} = h^{-1}s$$

es decir, $h^{-1} \in C_G(S)$.

Por lo tanto $C_G(S)$ es un subgrupo G.

Veamos ahora que

$$e \in N_G(S) \subset G.$$

Sean $g, h \in N_G(S)$, luego se tiene que $gS = Sg$ y $hS = Sh$.

$$(gh)S = g(hS) = g(Sh) = (gS)h = S(gh)$$

luego $gh \in N_G(S)$.

Por otro lado tenemos que si $hS = Sh$, entonces $Sh^{-1} = h^{-1}S$.

Dado $x = sh^{-1}$, por lo cual $xh = s$, es decir $hxh = hs = s'h$, por lo tanto cancelando $hx = s'$, es decir $x = h^{-1}s' \in h^{-1}S$.

En el otro sentido $x = h^{-1}s$, por lo cual $hx = s$, es decir $hxh = sh = hs'$, por lo tanto cancelando $xh = s'$, es decir $x = s'h^{-1} \in Sh^{-1}$.

$$Sh^{-1} = h^{-1}S,$$

es decir, $h^{-1} \in N_G(S)$

Por lo tanto $N_G(S)$ es un subgrupo G.

Para la tercera proposición tenemos que $C_G(S)$ y $N_G(S)$ son grupos solo falta ver la contención Dado $g \in C_G(S)$

□

Propiedad 21 *Sea G un grupo.*

G es conmutativo si y sólo si $[G,\ G] = \{e\}$.

Demostración: Si G es conmutativo, entonces se tiene que dado $a, b \in G$ se cumple $ab = ba$ es decir, $aba^{-1}b^{-1} = e$.

De lo cual se tiene que $[a, b] = e$, para todo $a, b \in G$.

Luego $[G, G] = \langle e \rangle = \{e\}$.

En el otro sentido se tiene que $[G, G] = \{e\}$ por lo tanto, para todo $a, b \in G$ $[a, b] = e$, de lo cual se tiene

$$aba^{-1}b^{-1} = e \Leftrightarrow ab = ba$$

luego G es conmutativo. □

Propiedad 22 *Sea G un grupo*

G es conmutativo si y sólo si $Z(G) = G$.

Definición 8 *Sea $\phi \neq S \subseteq G$, y sea $g \in G$. Se define*

$$S^g = \{gsg^{-1} \mid s \in S\},$$

se llama el conjugado de S, en particular si $H \leq G$, se define el conjugado de H.

$$H^g = \{ghg^{-1} \mid h \in H\},$$

Propiedad 23 *Sean $\phi \neq S \subseteq G$, $H \leq G$. Demostrar que:*

$$H^g \leq G.$$

Demostración: Notemos que $H^g \neq \phi$, pues $e = geg^{-1} \in H^g$, además es claro que $H^g \subseteq G$.
Sean $x = ghg^{-1}, y = gh'g^{-1} \in H^g$, por demostrar que $xy^{-1} \in H^g$. Tenemos:

$$\begin{aligned} xy^{-1} &= ghg^{-1}(gh'g^{-1})^{-1} \\ &= ghg^{-1}g(h')^{-1}g^{-1} \\ &= gh(h')^{-1}g^{-1} \end{aligned}$$

Ahora, como H es grupo se tiene que $h, (h')^{-1} \in H$, por lo tanto $xy^{-1} \in H^g$. Así concluimos que $H^g \leq G$.

□

Propiedad 24 *Sean $\phi \neq S \subseteq G$, $H \leq G$. Demostrar que:*

$$C_G(S^g) = (C_G(S))^g$$

Demostración: La demostración la haremos por contención

i) Primero veamos $(C_G(S))^g \subseteq C_G(S^g)$.

Sea $x \in (C_G(S))^g$, luego $x = ghg^{-1}$ con $h \in C_G(S)$.

Por demostrar que $x \in C_G(S^g)$ si y sólo si $xm = mx \quad (\forall\, m \in S^g)$.

Para ello notemos que:

$$\begin{aligned} xm &= (ghg^{-1})(gkg^{-1}) && \text{con } k \in S,\ h \in C_G(S) \\ &= g(hk)g^{-1} && h \in C_G(S), \text{ entonces conmuta con } k \\ &= g(kh)g^{-1} \\ &= (gkg^{-1})(ghg^{-1}) \\ &= mx \end{aligned}$$

Luego $x \in C_G(S^g)$, y por tanto

$$(C_G(S))^g \subseteq C_G(S^g)$$

ii) Veamos ahora que $C_G(S^g) \subseteq (C_G(S))^g$.

Sea $y \in C_G(S^g)$, entonces tenemos que $y(gsg^{-1}) = (gsg^{-1})y \quad (\forall\, s \in S)$.

Por demostrar que $y \in (C_G(S))^g$ si y sólo si $y = gng^{-1}$ con $n \in C_G(S)$. Notemos que $y = g(g^{-1}yg)g^{-1}$, entonces sólo basta demostrar que $g^{-1}yg \in C_G(S)$.

Para todo $s \in S$ tenemos que:

$$\begin{aligned} (g^{-1}yg)s &= (g^{-1}yg)s(g^{-1}g) && \text{aplicamos una identidad} \\ &= g^{-1}[y(gsg^{-1})]g \\ &= g^{-1}[(gsg^{-1})y]g \\ &= s(g^{-1}yg) \end{aligned}$$

es decir, $g^{-1}yg \in C_G(S)$, entonces $y \in (C_G(S))^g$. Por lo tanto

$$C_G(S^g) \subseteq (C_G(S))^g$$

Por (i) y (ii) queda demostrado que

$$(C_G(S))^g = C_G(S^g).$$

□

Propiedad 25 *Sean $\phi \neq S \subseteq G$, $H \leq G$, entonces*

1. $\langle S^g \rangle = \langle S \rangle^g$
2. $N_G(S^g) = (N_G(S))^g$

Ejercicio 31 *Determinar el centro de los siguientes grupos.*

1. $G = GL_n(K)$
2. $G = \mathbb{R}$
3. $G = D_4$

Ejercicio 32 *Calcular el conmutador para*

1. $G = Biy(\{1, 2, 3\})$
2. $G = GL_2(K)$
3. $G = D_n$
4. $G = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \middle| \, a, b \in K \right\}$

1.6.1. Problemas Propuestos

Problema 21.

Sea $G = Sim(\triangle)$ y $S = \{V_3, V_2\}$ (V_i la reflexión que deja fijo el vértice i).
Determinar el $Z(G)$ y $C_G(S)$.

Problema 22.

Sea $G = Biy(\mathbb{Z})$, $f(x) = x + 1$. y $g(x) = -x$
Determinar el $C_G(\{f\})$ y $N_G(\{f, g\})$

Problema 23.

Sea $G = GL_2(\mathbb{R})$ y $H = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \quad | \quad b \in \mathbb{R} \right\}$.
Determinar el $C_G(H)$ y $N_G(H)$.

Problema 24.

Sea $G = GL_2(\mathbb{R})$ y $H = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \quad | \quad a, b \in \mathbb{R}^* \right\}$.
Determinar $N_G(H)$.

Problema 25.

Sea $G = GL_2(\mathbb{R})$ y $H = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \quad | \quad a \in \mathbb{R}^*, b \in \mathbb{R} \right\}$.
Determinar $N_G(H)$.

Problema 26.

Sean G y G' dos grupos.
Demuestre que

$$Z(G \times G') = Z(G) \times Z(G').$$

Problema 27.

Sea G un grupo y H un subgrupo de G
Demostrar que $[H, H]$ es un subgrupo de $[G, G]$.

1.7. Clases Laterales

Sea G un grupo y $H \leq G$. Se define la siguiente relación derecha en G, dada por, si $a, b \in G$

$$a \sim_H b \Leftrightarrow ab^{-1} \in H$$

Propiedad 26 *$\sim_H$ es una relación de equivalencia.*

Demostración: Sean $a, b, c \in G$.

1. $\sim_H$ es Refleja.

   Por demostrar $a \sim_H a$, esto es, si y sólo si $aa^{-1} \in H$, pero $aa^{-1} = e \in H$ ya que H es un subgrupo de G

2. $\sim_H$ es Simétrica.

   Por demostrar $a \sim_H b \Rightarrow b \sim_H a$. Como $ab^{-1} \in H$, y además H es grupo tenemos que $(ab^{-1})^{-1} = ba^{-1} \in H$

3. $\sim_k$ es Transitiva.

   Por demostrar $(a \sim_H b \wedge b \sim_H c) \Rightarrow a \sim_H c$. Como $(ab^{-1} \in H) \wedge (bc^{-1} \in H)$, y además H es grupo, tenemos que $(ab^{-1})(bc^{-1}) = ac^{-1} \in H$. Lo cual prueba que $\sim_H$ es transitiva.

Entonces, por [1], [2] y [3] queda demostrado que $\sim_H$ es una relación de equivalencia. □

Así $\sim_H$ define una partición sobre G, dada por la clase que están definida del siguiente modo

$$\begin{aligned} cl(a) &= \{b \in G \mid b \sim_H a\} \\ &= \{b \in G \mid ba^{-1} \in H\} \\ &= \{b \in G \mid (\exists h \in H)\left(ba^{-1} = h\right)\} \\ &= \{b \in G \mid (\exists h \in H)\,(b = ha)\} \\ &= Ha. \end{aligned}$$

Luego

$$a \sim_H b \Leftrightarrow Ha = Hb,$$

por lo tanto

$$G = \dot{\bigcup_{a \in \mathfrak{R}}} Ha$$

donde $\mathfrak{R}$ es un sistema de representante de las clases.

Propiedad 27 *Sean $a, b \in G$ y $H \leq G$, entonces*

$$\begin{array}{rccc} f: & Ha & \longrightarrow & Hb \\ & ha & \longmapsto & hb \end{array}$$

es una biyección.

Demostración: Notemos que esta bien definida, ya que., $x = ha = h'a$ cancelando obtenemos que $h = h'$, luego hb es único. Es inyectiva de manera análoga, se tiene que $f(ha) = f(ka)$ entonces $hb = kb$, luego cancelando se tiene $h = k$, es decir $ha = ka$.

Es epiyectivas, ya que,dado $y \in Hb$, luego $y = hb = f(ha)$. □

Observación: Análogamente también se define la relación de equivalencia izquierda en G. Dada por:

$$a \ {}_H\!\sim b \Leftrightarrow a^{-1}b \in H$$

y las clases

$$\begin{aligned} cl(a) &= \{b \in G \mid b \ {}_H\!\sim a\} \\ &= \{b \in G \mid a^{-1}b \in H\} \\ &= \{b \in G \mid (\exists h \in H)\left(a^{-1}b = h\right)\} \\ &= \{b \in G \mid (\exists h \in H)\,(b = ah)\} \\ &= aH. \end{aligned}$$

Fácilmente se demuestra que

$$\begin{array}{rccc} f: & aH & \longrightarrow & Hb \\ & ax & \to & xb \end{array}$$

es una biyección.

Definición 9 *Sea $H \leq G$, $g \in G$*

1. *gH se llama la clase* **`lateral izquierda`** *de g.*
2. *Hg se llama la clase* **`lateral derecha`** *de g.*

Notación: Denotaremos por:

$$G/H = \{aH \mid a \in G\}$$

$$H\backslash G = \{Ha \mid a \in G\}$$

el conjunto de las clases laterales izquierdas y el conjunto de las clases laterales derechas respectivamente.

Ejemplo 33 *Consideremos D_3 y $K = \{V_3, Id\}$, con V_i es la reflexión que fija el vértice i.*

Solución: Por definición tenemos:

$$D_3/K = \{\sigma \circ \{V_3, Id\} \mid \sigma \in D_3\}$$

luego, podemos escoger elementos de D_3 para conocer explícitamente los elementos (clases laterales) de G/K, por ejemplo

$$V_2 \circ \{V_3, Id\} = \{V_2 \circ V_3, V_2 \circ Id\} = \{R, V_2\}$$

$$V_1 \circ \{V_3, Id\} = \{V_1 \circ V_3, V_1 \circ Id\} = \{R^2, V_1\}$$

Luego

$$D_3/K = \{\{V_3, Id\}\ , \{R^2, V_1\},\ \{R, V_2\}\}.$$

A modo de observación

$$D_3 = \{V_3, Id\} \dot{\cup} \{R^2, V_1\} \dot{\cup} \{R, V_2\}$$

□

Teorema 28 *Sea G un grupo, $H \leq G$, entonces*

1. *Todo elementos g de G está contenido en una sola clase lateral derecha (izquierda).*
2. *Las funciones*

$$\begin{array}{rcl} H & \longrightarrow & Ha \\ h & \longmapsto & ha \end{array} \qquad \begin{array}{rcl} H & \longrightarrow & aH \\ h & \longmapsto & ah \end{array}$$

son biyectivas.

3. *G es la unión disjunta de sus clases laterales derechas (izquierda).*

4. *Existe una función biyectiva entre el conjunto de las clases laterales derechas y el conjunto de las clases laterales izquierda.*

Definición 10 *Se define el* **índice** *de H en G, denotado por $[G : H]$, es el número de clases laterales derechas o izquierdas.*

Observación: En el ejemplo 33 tenemos que $[D_3 : K] = 3$.

Teorema 29 (Lagrange) *Si $H \leq G$, entonces*

$$|G| = [G : H] \cdot |H|$$

Además si $|G| < \infty$

1. *$|H|$ divide a $|G|$*

2. *$|g|$ divide a $|G|$*

Demostración: Sea G un grupo finito, de la tercera parte del teorema 28 sabemos que

$$G = \dot{\bigcup_{a \in R}} Ha$$

donde R es un sistema de representante de clases. Entonces tenemos que

$$|G| = \sum_{a \in R} |Ha| = \sum_{i=1}^{[G:H]} |Ha_i|$$

luego, por la segunda parte del teorema 28 se tiene que

$$|G| = \sum_{i=1}^{[G:H]} |Ha_i| = \sum_{i=1}^{[G:H]} |H| = [G : H] \cdot |H|$$

es decir

$$|G| = [G : H] \cdot |H|$$

□

Corolario 30 *Sea G un grupo finito*

1. *Si G tiene orden primo entonces es cíclico y no tiene subgrupos no triviales.*

2. *Si $|G| = n$, entonces $g^n = 1$, para todo $g \in G$.*

Demostración: Sea $K \leq G$, tal que $\{e\} \neq K$, luego tenemos que

$$|G| = [G : K]|K|$$

de lo cual, $|K|$ divide a un primo y no es unidad, por lo tanto $|G| = |K|$, y como son conjuntos finitos, se tiene que $G = K$. Dado $e \neq g \in G$, luego $\{e\} \neq < g >$, y por lo tanto $G = < g >$, es decir, el grupo G es cíclico.

Para la segunda parte, dado $g \in G$, se tiene que $K = \langle g \rangle$, luego $ord(g) = |g| = |K|$, divide a $|G| = n$, por lo tanto $n = |g|t$.

$$g^n = g^{|g|t} = (g^{|g|})^t = 1^t = 1$$

□

Teorema 31 *Sean $K \leq H \leq G$, tales que $[G : H], [H : K]$ son finitos, entonces*

$$[G : K] = [G : H] \cdot [H : K]$$

Demostración: Sean $K \leq H \leq G$, tales que $[G : H], [H : K]$ son finitos, entonces se tiene:

$$G = \dot{\bigcup_{i \in I}} Ha_i; \quad H = \dot{\bigcup_{j \in J}} Kb_j \text{ con } a_i \in G,\ b_j \in H$$

reemplazando se obtiene

$$G = \bigcup_{(i,j) \in I \times J} Kb_j a_i$$

y

$$|I \times J| = |I| \cdot |J| = [G : H] \cdot [H : K].$$

Luego basta demostrar que la unión es disjunta, es decir,

$$Kb_j a_i = Kb_r a_s \Rightarrow j = r \wedge i = s$$

para ello, recuerde que las clases laterales son iguales o disjunta.

Sea $b_j a_i \in Kb_r a_s$

$$\begin{aligned}
&\Rightarrow b_j a_i = kb_r a_s \\
&\Rightarrow a_i = b_j^{-1} kb_r a_s, \text{ como } b_j^{-1} kb_r \in H \\
&\Rightarrow a_i \sim_H a_s, \text{ es decir, } i = s \\
&\Rightarrow a_i = a_s
\end{aligned}$$

reemplazando y cancelando obtenemos $kb_r = b_j$, luego están relacionado, y como pertenecen a un sistema de representante, se tiene que

$$b_r = b_j \Rightarrow r = j$$

□

Ejemplo 34 *Determine un sistema de representante de clases para el conjunto $\mathbb{R}/\mathbb{Z}$.*

Solución: Sabemos que

$$\mathbb{R}/\mathbb{Z} = \{x + \mathbb{Z} \mid x \in \mathbb{R}\}$$

Además notemos que para todo $a \in \mathbb{Z}$

$$a + \mathbb{Z} = \mathbb{Z}$$

Luego, si tomamos, por ejemplo el real $12,154782$ vemos que

$$12,154782 + \mathbb{Z} = 0,154782 + \mathbb{Z}$$

pues $12 = 12,154782 - 0,154782 \in \mathbb{Z}$.

Más generalmente, para todo $x \in \mathbb{R}$ existen únicos $a \in \mathbb{Z}$ y $b \in [0,1[$ tales que

$$x = a + b$$

Así tenemos que un sistema de representantes para el conjunto $\mathbb{R}/\mathbb{Z}$ es $[0,1[$.

□

1.7.1. Problemas Propuestos

Problema 28.

Demuestre que $\mathbb{Z}$ es un sistema de representante de clases para el conjunto $\mathbb{Z}\times\mathbb{Z}/\langle(3,5)\rangle$.

Problema 29.

Determine un sistema de representantes para el conjunto $\mathbb{Z}_4 \times U(\mathbb{Z}_5)/\langle(2,4)\rangle$.

Problema 30.

Sea $G = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \quad | \quad a \in \mathbb{R}^*, b \in \mathbb{R} \right\}$ y $H = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \quad | \quad b \in \mathbb{R} \right\}$.

Determinar el conjunto cuociente G/H

1.8. Subgrupo Normal

Sea G grupo y $H \leq G$, luego al conjunto de las clases laterales izquierda, se desea definir una operación binaria natural, de modo de obtener una estructura natural de grupo, de manera similar a la construida en $\mathbb{Z}_n$, para ello

$$G/H = \{aH \mid a \in G\}$$

Luego la multiplicación natural debería ser:

$$aH \cdot bH = abH$$

¿Pero esta bien definido? para poder responder afirmativamente, debemos averiguar si depende o no de los representantes, es decir,

$$ah_1H \cdot bh_2H = ah_1bh_2H = ah_1bH$$

Luego debe cumplirse que

$$(\forall h \in H)(abH = ah_1bH)$$

es decir, los elementos deben estar relacionados

$$ah_1b = abh \Leftrightarrow h_1b = bh$$

con lo cual se tiene que

$$(\forall h \in H)(b^{-1}hb \in H) \quad \text{o bien} \quad Hb = bH$$

Definición 11 *Sea G un grupo y H un subgrupo de G entonces*
Se dice que H es un subgrupo `normal` *de G, denotado por $H \trianglelefteq G$ si y sólo si*

$$(\forall g \in G)(Hg = gH).$$

Propiedad 32 *Sea H un subgrupo del grupo G, tal que $(\forall g \in G)(gHg^{-1} \subseteq H)$ entonces $H \trianglelefteq G$.*

Demostración: Sean $g \in G$, y $x = gh \in gH$, luego $xg^{-1} = ghg^{-1} \in gHg^{-1} \subset H$, por lo tanto $xg^{-1} = k \in H$, de lo cual se tiene $x = kg \in Hg$.

En el otro sentido se tiene que, dado $g \in G$, y $x = hg \in Hg$, luego $g^{-1}x = g^{-1}hg \in g^{-1}Hg \subset H$, por lo tanto $g^{-1}x = k \in H$, de lo cual se tiene $x = gk \in gH$. □

Propiedad 33 *Si G es conmutativo, entonces todos los subgrupos son normales.*

Demostración: Sea G un grupo conmutativo, y H un subgrupo, entonces

$$gHg^{-1} = \{ghg^{-1} \mid h \in H\} = \{gg^{-1}h \mid h \in H\} = H$$

Luego H es un subgrupo normal □

Propiedad 34 *Sea G un grupo, entonces $Z(G) \trianglelefteq G$.*

Demostración: Sea G un grupo conmutativo, y $Z(G)$ el centro de G, entonces

$$gZ(G)g^{-1} = \{gkg^{-1} \mid k \in Z(G)\} = \{gg^{-1}k \mid k \in Z(G)\} = Z(G)$$

Luego $Z(G)$ es un subgrupo normal □

Propiedad 35 *Sea $S \subseteq G$, entonces $C_G(S) \trianglelefteq N_G(S)$,*

Demostración: Recordemos que $C_G(S) = \{g \in G \mid (\forall s \in S)(gs = sg)\}$ y $N_G(S) = \{g \in G \mid gS = Sg\}$.

Dado $g \in N_G(S)$ y $h \in C_G(S)$, por demostrar que $ghg^{-1} \in C_G(S)$, dado $s \in S$, note que $g^{-1}sg \in S$, ya que $Sg = gS$.

$$(ghg^{-1})s(gh^{-1}g^{-1}) = g(h(g^{-1})sg)h^{-1})g^{-1} = gg^{-1}sgg^{-1} = s.$$

□

Propiedad 36 *Sea G un grupo entonces $[G,\ G] \trianglelefteq G$*

Demostración: Recordemos la propiedad 25, $\langle S^g \rangle = \langle S \rangle^g$, con $g \in G$, ya que el conmutador esta generado por $[a, b]$, conjugamos y obtenemos

$$\begin{aligned} c[a,b]c^{-1} = &\ (cab)(a^{-1}b^{-1}c^{-1}) \\ &= (cab)a^{-1}c^{-1}b^{-1}bca(a^{-1}b^{-1}c^{-1}) \\ &= (cab)(ca)^{-1}b^{-1}bca(a^{-1}b^{-1}c^{-1}) \\ &= (ca)b(ca)^{-1}b^{-1}bcb^{-1}c^{-1} \\ &= (ca)b(ca)^{-1}b^{-1} \cdot bcb^{-1}c^{-1} \\ &= [cab, b] \cdot [b, c], \end{aligned}$$

luego se tiene que, $c[a, b]c^{-1} \in [G, G]$ y por lo tanto es un subgrupo normal. □

Ejemplo 35 *Demostrar que*

$$\left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \mid b \in \mathbb{R} \right\} \trianglelefteq \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \mid a \in \mathbb{R}^*, b \in \mathbb{R} \right\}$$

Solución: Queda como ejercicio verificar que uno es subgrupo del otro.

Veamos ahora la condición de normalidad

$$\begin{aligned} \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & d \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}^{-1} &= \begin{pmatrix} a & da+b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a^{-1} & -a^{-1}b \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & da \\ 0 & 1 \end{pmatrix} \end{aligned}$$

Luego se tiene que

$$\begin{pmatrix} 1 & da \\ 0 & 1 \end{pmatrix} \in \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \middle| \, b \in \mathbb{R} \right\}$$

De lo cual es un subgrupo normal. □

Ejemplo 36 *Demostrar que el conjunto*

$$O_2(\mathbb{R}) = \{A \in GL_2(\mathbb{R}) \mid |\det(A)| = 1\}$$

es un subgrupo normal de $GL_2(\mathbb{R})$.

Solución: Demostrar que $O_2(\mathbb{R})$ es un subgrupo de $GL_2(\mathbb{R})$ se deja de ejercicio. Luego, según la proposición 32 debemos demostrar que

$$(\forall B \in GL_2(\mathbb{R}))(B \cdot O_2(\mathbb{R}) \cdot B^{-1} \subseteq O_2(\mathbb{R}))$$

Entonces sea $M \in B \cdot O_2(\mathbb{R}) \cdot B^{-1}$, por demostrar que $M \in O_2(\mathbb{R})$ (es decir $|\det(M)| = 1$). Tenemos

$$\begin{aligned}
|\det(M)| &= |\det(B \cdot A \cdot B^{-1})| && \text{para algún } A \in O_2(\mathbb{R}) \\
&= |\det(B) \cdot \det(A) \cdot \det(B)^{-1}| \\
&= |\det(B)| \cdot |\det(A)| \cdot |\det(B)^{-1}| && \text{pero } |\det(A)| = 1 \\
&= |\det(B)| \cdot |\det(B)|^{-1} \\
&= 1
\end{aligned}$$

es decir,

$$|\det(M)| = 1$$

Por lo tanto

$$O_2(\mathbb{R}) \trianglelefteq GL_2(\mathbb{R})$$

□

Ejercicio 37 *Demostrar que*

$$SL_2(K) \trianglelefteq GL_2(K)$$

Definición 12 *Sean $K, H \leq G$, entonces*

$$HK = \{hk \in G \quad | \quad h \in H, k \in K\}$$

Propiedad 37 *Sea $K \leq G$, $H \trianglelefteq G$, entonces*

1. *$HK \leq G$*
2. *$\langle H \cup K \rangle = HK$*
3. *$H \cap K \trianglelefteq K$*
4. *$H \trianglelefteq \langle H \cup K \rangle$*
5. *Si $K \trianglelefteq G$ y $H \cap K = \{e\}$, entonces*

$$(\forall h \in H)(\forall k \in K)(\ kh = hk\ )$$

1.8.1. Problemas Propuestos

Problema 31.

Dados los siguientes grupos

$$G = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \quad | \quad a \in \mathbb{R}^{\times}, b \in \mathbb{R} \right\}, \qquad H = \left\{ \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} \quad | \quad a \in \mathbb{R}^{\times} \right\}$$

Determinar si H es un subgrupo normal de G

Problema 32.

Demostrar que: Si $H \leq G$ tal que $[G : H] = 2$ entonces $H \trianglelefteq G$

Problema 33.

Sea V_i la reflexión sobre el vértice i del triángulo equilátero.
Demostrar que $< T_2, T_3 > \trianglelefteq D_3$

Problema 34.

Sea G el grupo de las simetrías, del polígono regular y H es el subgrupo de las rotaciones
Demostrar que: $H \trianglelefteq G$

Problema 35.

Sean $H \trianglelefteq G, K \trianglelefteq G$ si

$$HK = \{hk \in G \mid h \in H, k \in K\}$$

Demostrar que $HK \trianglelefteq G$

1.9. Grupo Cuociente

Propiedad 38 *Sea $H \trianglelefteq G$, entonces la multiplicación dada por*

$$(xH) \cdot (yH) = xyH,$$

esta bien definida y $(G/H, \cdot)$ tiene estructura de grupo.

Definición 13 *Si $H \trianglelefteq G$, entonces $(G/H, \cdot)$ se llama* `grupo cuociente` *de G por H.*

Ejemplo 38

1. $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$,
2. $\mathbb{R}/\mathbb{Z}$,
3. $\mathbb{R}^2/\mathbb{Z}^2$,

4. $PGL_2(K) = GL_2(K)/Z(GL_2(K))$.

Ejercicio 39 *Sea $H \trianglelefteq G$, y $H \subseteq K \leq G$, entonces*

$$K/H \leq G/H$$

Ejercicio 40 *Todo grupo cociente de un grupo cíclico es cíclico.*

Ejercicio 41 *Si G es un grupo generado por $\{s_i, i \in I\}$, $H \trianglelefteq G$, entonces G/H esta generado por $\{\overline{s_i}, i \in I\}$.*

Teorema 39 (Correspondencia) *Sea $H \trianglelefteq G$, entonces existe una correspondencia biunívoca entre los subgrupos K de G que contiene a H y los subgrupos de G/H, es decir*

$$\begin{array}{ccc} \{K \leq G \mid H \subseteq K\} & \longrightarrow & \{L \leq G/H\} \\ K & \longmapsto & K/H \\ I = \{g \in G \mid gH \in L\} & \leftarrow & L \end{array}$$

Además esta correspondencia satisface

1. $L_1 \subset L_2 \Leftrightarrow H \subset I_1 \subset I_2$
2. $[L_1 : L_2] = [I_1 : I_2]$
3. $L_1 \trianglelefteq L_2 \Leftrightarrow I_1 \trianglelefteq I_2$

Ejemplo 42 *Determinar los subgrupos de $\mathbb{Z}/6\mathbb{Z}$.*

Solución: Notemos que los subgrupo K de $\mathbb{Z}$ tales que $6\mathbb{Z} \subseteq K$ son:

$$\mathbb{Z}\,,\ 2\mathbb{Z}\,,\ 3\mathbb{Z}\,,\ 6\mathbb{Z}$$

Así, por el teorema de la correspondencia tenemos que los subgrupo de $\mathbb{Z}/6\mathbb{Z}$ son:

$$\mathbb{Z}/6\mathbb{Z}\,,\ 2\mathbb{Z}/6\mathbb{Z}\,,\ 3\mathbb{Z}/6\mathbb{Z}\,,\ 6\mathbb{Z}/6\mathbb{Z}$$

□

Ejercicio 43 *Generalizar el ejemplo anterior, es decir, determine los subgrupo de $\mathbb{Z}/n\mathbb{Z}$, con $n \in \mathbb{N}$*

Propiedad 40 *Sean H y K subgrupos normales de G, entonces*

1. *G/H es un grupo abeliano si y solo si $[G, G] \subseteq H$.*
2. *Si $K \subseteq Z(G)$ y G/K es cíclico, entonces G es abeliano.*

Demostración: Para la primera parte, se tiene que $aH, bH \in G/H$, luego

$$aHbH = abH = baH = bHaH,$$

es decir, $b^{-1}a^{-1}ba = [b^{-1}, a^{-1}] \in H$, luego

$$[G, G] = \langle [a, b] \mid a, b \in G \rangle \subset H$$

En el otro sentido, se tiene que $[G, G] \subset H \trianglelefteq G$, como $b^{-1}a^{-1}ba = (ab)^{-1}(ba) \in H$, por lo tanto

$$abH = baH$$

Para la segunda parte $K \subseteq Z(G)$ y G/K es cíclico. es decir, $(\forall k \in K)(\forall g \in G)(gk = kg)$, además $G/K = \langle gK \rangle$.

Sean $x, y \in G$, luego $xK = g^iK,\ yK = g^jK$, de lo cual se obtiene que $x = g^ik_1,\ y = g^jk_2$.

Veamos ahora

$$xy = g^ik_1g^jk_2 = g^ig^jk_2k_1 = g^{i+j}k_2k_1 = g^jg^ik_2k_1 = g^jk_2g^ik_1 = yx$$

□

Observación: Esta propiedad nos ayuda a determinar el conmutador, ya que si encontramos un subgrupo H que cumpla la parte [1], entonces ya sabemos que $[G, G]$ está limitado por H. Por ejemplo:

Sea $G = D_3$ y consideremos el subgrupo $K = \langle R \rangle = \{Id, R, R^2\}$ (subgrupo de rotaciones). Como $[G : K] = 2$, entonces K es un subgrupo normal de G y además G/K es cíclico (pues tiene orden primo) y por tanto abeliano, luego por la parte [1] de la proposición anterior se tiene que

$$[G, G] \subseteq \langle R \rangle$$

Además, es fácil ver que $\langle R \rangle \subseteq [G, G]$, por lo tanto

$$[G, G] = \langle R \rangle$$

La segunda parte de la proposición nos será de gran utilidad en la sección del teorema de Sylow.

1.9.1. Problemas Propuestos

Problema 36.

Sea $G = \mathbb{Z}_{12} \times \mathbb{Z}_{15} \times \mathbb{Z}_{24}$ y $H = < \overline{(5, 10, 4)} >$

Determinar el orden del elemento $\overline{(4, 2, 8)}$ en G/H

Problema 37.

Determinar si es verdadero o falso

Sea V_i la reflexión sobre el vértice i del triángulo equilátero entonces

a) $< V_2, V_3 > \trianglelefteq D_3$

b) $< V_1 > \trianglelefteq D_3$

Problema 38.

Sea $G = \mathbb{Z}_{36} \times \mathbb{Z}_{60}$ y $H =< (5, 10) >$
Determinar el orden del elemento $\overline{(4, 2)}$ en G/H

1.10. Homomorfismo

Sean $(G, \cdot)$ y $(G', *)$ dos grupos y $f : G \longrightarrow G'$ una función.
Se dice que f es un `homomorfismo` de grupo si y sólo si

$$(\forall x \in G)(\forall y \in G)(f(x \cdot y) = f(x) * f(y)).$$

El conjunto de los homomorfismo lo denotamos por

$$Hom(G, G') = \{f \in F(G, G') \mid f \text{ es un homomorfismo } \}$$

Además tenemos

1. f es `endomorfismo` si y sólo si $G = G'$ y f es un homomorfismo

$$End(G) = \{f \in Hom(G, G) \mid f \text{ es un edomorfismo } \}$$

2. f es `monomorfismo` si y sólo si f es un homomorfismo y es inyectiva
3. f es `epimorfismo` si y sólo si f es un homomorfismo y es epiyectiva
4. f es `isomorfismo` si y sólo si f es un homomorfismo y es biyectiva
5. f es `automorfismo` si y sólo si f es endomorfismo y es biyectiva.

$$Aut(G) = \{f \in End(G) \mid f \text{ es biyectiva } \}$$

Ejemplo 44

1. *La función exponencial* $Exp_a : \mathbb{R} \longrightarrow \mathbb{R}^*,\ Exp_a(x) = a^x$ *es un homomorfismo.*
2. *El conjugado complejo* $J : \mathbb{C} \longrightarrow \mathbb{C},\ J(z) = \overline{z}$ *es un homomorfismo.*
3. *El Determinante dado por:*

$$det : GL_n(K) \longrightarrow K^\times$$

es un homomorfismo.

4. *La Traza definida por:*

$$tr : M_n(K) \longrightarrow K$$

es un homomorfismo.

5. *Sea $H \trianglelefteq G$, entonces la proyección o* **epimorfismo canónico** *esta dado por:*

$$\begin{array}{rccc} \pi: & G & \longrightarrow & G/H \\ & a & \longmapsto & \overline{a} \end{array}$$

6. *Sea G un grupo y $g \in G$*

$$\begin{array}{rccc} f: & \mathbb{Z} & \longrightarrow & \langle g \rangle \\ & n & \longmapsto & g^n \end{array}$$

es un homomorfismo.

Observación: Note que $\begin{array}{rccc} \pi: & \mathbb{Z}_n & \longrightarrow & \mathbb{Z}_m \\ & \overline{a} & \longmapsto & \overline{a} \end{array}$ en general no es una función, y en los casos afirmativos es homomorfismo.

Propiedad 41 *Sean $(G, \cdot)$ un grupo abeliano y $(G', \cdot')$ un grupo entonces $(Hom(G', G), \cdot)$ es un grupo, donde $\cdot$ está definido por:*

Dado $f, h \in Hom(G', G)$, entonces $(f \cdot h)(x) = f(x) \cdot h(x)$.

Demostración: Ya que $(G, \cdot)$, entonces $f(x) \cdot h(x)$, esta bien definido para cada $x \in G'$.

Veamos que $f \cdot h$ es homomorfismo

$$\begin{aligned} (fh)(xy) &= f(xy)h(xy) \\ &= f(x)f(y)h(x)h(y) \\ &= f(x)h(x)f(y)h(y) \\ &= (fh)(x)(fh)(y) \end{aligned}$$

Luego

$$\begin{array}{rccc} \cdot & Hom(G', G) \times Hom(G', G) & \to & Hom(G', G) \\ & (f, h) & & f \cdot h \end{array}$$

es una operación binaria.

La asociatividad se hereda de G

$$\begin{aligned} ((fh)k)(x) &= (fh)(x)k(x) \\ &= (f(x)h(x))k(x) \\ &= f(x)(h(x)k(x)) \\ &= (f)(x)(hk)(x) \\ &= (f(hk))(x) \end{aligned}$$

El elemento neutro, es la función constante igual a e.

$$\begin{aligned} (f\widehat{e})(x) &= f(x)\widehat{e}(x) \\ &= f(x)e \\ &= f(x) \\ &= e(f)(x) \\ &= \widehat{e}(x)(f)(x) \\ &= (\widehat{e}f)(x) \end{aligned}$$

Dada $f \in Hom(G', G)$, se tiene que $f(x) \in G$, para todo $x \in G'$, es decir, $(f(x))^{-1} \in G$. Se define $f^{-1}(x) = (f(x))^{-1}$ y cumple con

$$(ff^{-1})(x) = f(x)f^{-1}(x) = f(x)(f(x))^{-1} = e = \widehat{e}(x) = (f(x))^{-1}f(x) = (f^{-1}(x))f(x) = (f^{-1}f)(x)$$

Por lo tanto $Hom(G', G)$, es un grupo. □

Corolario 42 *Sea $(G, \cdot)$ un grupo abeliano entonces $(End(G), \cdot)$ es un grupo.*
Note que $End(G) = Hom(G, G)$

Propiedad 43 *Sea G un grupo entonces $(Aut(G), \circ)$ es un grupo.*

Demostración: Sea G un grupo y como $Biy(G), \circ)$ es un grupo tal que $Aut(G) \subset Biy(G)$, luego basta probar que es un subgrupo.

La identidad es un automorfismo, de lo cual tenemos que $Id \in Aut(G) \neq \phi$.

Sean $f, h \in Aut(G)$, por demostrar que $f \circ h \in Aut(G)$.

$$\begin{aligned}(f \circ h)(xy) &= f(h(xy)) \\ &= f(h(x)g(y)) \\ &= f(h(x))f(h(y)) \\ &= (f \circ h)(x)f \circ h)(y)\end{aligned}$$

De lo cual se tiene la pertenencia.

Para el inverso. Sea $f \in Aut(G)$, dado $x, y \in G$, luego existen únicos $x', y' \in G$, tales que $f(x') = x; f(y') = y$.

$$f^{-1}(xy) = f^{-1}(f(x')f(y')) = f^{-1}(f(x'y')) = x'y' = f^{-1}(x)f^{-1}(y)$$

De lo cual $f^{-1} \in Aut(G)$.

Por lo tanto $Aut(G)$ es un grupo. □

1.10.1. Problemas Propuestos

Problema 39.

Sean X e Y conjuntos no vacíos y $\phi : X \longrightarrow Y$ una función biyectiva. Demostrar que

$$\begin{array}{rccc} T: & Biy(X) & \longrightarrow & Biy(Y) \\ & f & \mapsto & T(f) = \phi \circ f \circ \phi^{-1} \end{array}$$

es un isomorfismo.

Problema 40.

Determinar $Hom(SL_2(\mathbb{R}), \mathbb{R})$

Problema 41.

Determinar el valor de verdad de las siguientes proposiciones. JUSTIFIQUE

1. Sea $n \in \mathbb{N}$, $F_n : \mathbb{R}^+ \to \mathbb{R}^+$; con $F_n(x) = x^n$ entonces F_n es un homomorfismo de grupo
2. Sea $n \in \mathbb{N}$, un número impar y $F_n : \mathbb{R}^* \to \mathbb{R}^*$; con $F_n(x) = \sqrt[n]{x}$, entonces F_n es un homomorfismo de grupo.
3. $L : F(\mathbb{R}^*, \mathbb{R}) \to \mathbb{R}$; con $L(f) = f(1)$ es un homomorfismo de grupo
4. $T : \{t_a \in F(\mathbb{R}, \mathbb{R}) \mid t_a$ es una traslación, con $a \in \mathbb{R}\} \to \mathbb{R}$. tal que $T(t_a) = a$ es un homomorfismo de grupo
5. $T : \{h_a \in Biy(\mathbb{R}) \mid h_a$ es una homotecia, con $a \in \mathbb{R}^*\} \to \mathbb{R}^*$, con $T(h_a) = a$ es un homomorfismo de grupo.
6. $det : GL_2(\mathbb{R}) \to \mathbb{R}$ es un homomorfismo de grupo.
7. $L : GL_2(\mathbb{R}) \to \mathbb{R}$ donde $L([b_{ij}]) = b_{11} + b_{22}$ es un homomorfismo de grupo.
8. $L : \mathcal{H} = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \mid a \in \mathbb{R}^*, b \in \mathbb{R} \right\} \to \mathbb{R}^*$ donde $L([b_{ij}]) = b_{11}$ es un homomorfismo de grupo.
9. $L : \mathcal{H} = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{R}) \mid a = d; c = -b \right\} \to \mathbb{C}^*$ donde $L([b_{ij}]) = b_{11} + b_{12}i$ es un homomorfismo de grupo.

Problema 42.

Dados los siguientes grupos

$$B = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \quad : \quad a, c \in \mathbb{R}^\times, b \in \mathbb{R} \right\} \quad , \quad D = \left\{ \begin{pmatrix} a & 0 \\ 0 & c \end{pmatrix} \quad : \quad a, c \in \mathbb{R}^\times \right\}$$

Determinar si las siguientes funciones, son homomorfismo de grupo

(a) $f : B \to \mathbb{R}^\times; \quad f \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} = a$

(b) $g : B \to \mathbb{R}; \quad g \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} = b$

(c) $h : B \to D; \quad h \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & c \end{pmatrix}$

Definición 14 *Sea $f \in Hom(G, G')$.*

Se define el **Kernel** *o Núcleo de f como*

$$ker(f) = \{x \in G \mid f(x) = e\}$$

Se define la **Imagen** *o Recorrido de f como*

$$Im(f) = \{y \in G' \mid (\exists x \in G)(f(x) = y)\}$$

Ejemplo 45 *Determinar el kernel y la imagen, de los siguientes homomorfismo*

1. *La función exponencial* $Exp_a : \mathbb{R} \longrightarrow \mathbb{R}^*,\ Exp_a(x) = a^x$.
   El kernel es $\{0\}$ *y la imagen es* $\mathbb{R}^+$
2. *El conjugado complejo* $J : \mathbb{C} \longrightarrow \mathbb{C},\ J(z) = \overline{z}$.
   El kernel es $\{0\}$ *y la imagen es* $\mathbb{C}$
3. *El Determinante dado por:*
   $$det : GL_n(K) \longrightarrow K^\times$$
   es un homomorfismo.
   El kernel es $SL_n(K)$ *y la imagen es* K^*

Propiedad 44 *Sea* $f : G \longrightarrow G'$ *un homomorfismo de grupo.*

1. $f(e) = e$
2. $(\forall x \in G)((f(x))^{-1} = f(x^{-1}))$
3. $H \leq G \Rightarrow f(H) \leq G'$
4. $K \leq G' \Rightarrow f^{-1}(K) \leq G$
5. $H \trianglelefteq G \Rightarrow f(H) \trianglelefteq f(G)$
6. f *es monomorfismo* $\Leftrightarrow ker(f) = \{e\}$
7. $ker(f) \trianglelefteq G$

Demostración: Sea e el neutro, luego

$$\begin{aligned} f(e) &= f(ee) \\ f(e) &= f(e)f(e) \\ e &= f(e) \end{aligned}$$

Sea $x \in G$, luego tenemos que

$$\begin{aligned} e = f(e) &= f(xx^{-1}) \\ e &= f(x)f(x^{-1}) \\ (f(x))^{-1}e &= f(x^{-1}) \\ (f(x))^{-1} &= f(x^{-1}) \end{aligned}$$

Probaremos ahora 4, para ello sea $K \leq G'$ y recordemos como esta definido

$$f^{-1}(K) = \{x \in G \mid f(x) \in K\}$$

Notemos que $e' \in K$, luego $f(e') = e$, por lo tanto $e \in f^{-1}(K)$, para la segunda parte, sea $x, y \in f^{-1}(K)$, luego tenemos que demostrar que $xy^{-1} \in f^{-1}(K)$, es decir, $f(xy^{-1}) \in K$.

Para ello sabemos que $f(x), f(y) \in K$, ahora veremos

$$\begin{aligned} f(xy^{-1}) &= f(x)f(y^{-1}) \\ &= f(x)f(y)^{-1} \in K \end{aligned}$$

Veamos la última afirmación, $Ker(f) = f^{-1}(\{e'\}$, luego es un subgrupo, veamos ahora la contención, para ello sea $g \in G$, y $h \in ker(f)$debemos justificar que $ghg^{-1} \in ker(f)$.

$$\begin{aligned} f(ghg^{-1}) &= f(g)f(h)f(g^{-1}) \\ &= f(g)ef(g^{-1}) \\ &= f(g)f(g^{-1}) \\ &= f(gg^{-1}) \\ &= f(e) = e \end{aligned}$$

Luego $ker(f) \trianglelefteq G$. □

Propiedad 45 *Sea $f : G \longrightarrow H$ un homomorfismo, entonces f es un Isomorfismo si y sólo si existe un homomorfismo $f^{-1} : H \longrightarrow G$ tal que $f \circ f^{-1} = I_H$ y $f^{-1} \circ f = I_G$*

Demostración:
⇒) Esta demostración la dejaremos de ejercicio.
⇐) Supongamos que existe un homomorfismo $f^{-1} : H \longrightarrow G$ tal que $f \circ f^{-1} = I_H$ y $f^{-1} \circ f = I_G$, por demostrar que f es un Isomorfismo.

Por el enunciado tenemos que f es un homomorfismo, ahora basta demostrar que f es una función biyectiva.

1. Demostremos que f es inyectiva. Sean $x, y \in G$ tales que $f(x) = f(y)$, por demostrar que $x = y$

$$\begin{aligned} f(x) &= f(y) && /f^{-1} \\ (f^{-1} \circ f)(x) &= (f^{-1} \circ f)(y) && \text{por hipótesis tenemos que } f^{-1} \circ f = I_G \\ x &= y \end{aligned}$$

   Por lo tanto f es inyectiva.

2. Demostremos que f es epiyectiva. Sea $h \in H$, por demostrar que $h \in Imf$. Veamos que $f^{-1}(h) \in G$ y además por hipótesis sabemos que $ff^{-1} = I_H$, entonces nos queda lo siguiente:

$$f(f^{-1}(h)) = (ff^{-1})(h) = I_H(h) = h$$

   Luego $f^{-1}(h)$ es una preimagen para h, es decir $h \in Imf$, entonces $H \subseteq Imf$.

   Por lo tanto f es una función epiyectiva.

   Así tenemos que f es un Isomorfismo.

□

Ejemplo 46 *la función* $ln : \mathbb{R}^+ \longrightarrow \mathbb{R}$ *es un isomorfismo, pues la función* exp_e *es su inversa y además es un homomorfismo.*

Propiedad 46 (Producto Directo) *Sean* $H, K \lhd G$*, tales que* $H \cap K = \{e\}$ *y* $HK = G$ *entonces* $G \simeq H \times K$

Demostración: Sean $H, K \lhd G$, y consideremos la función

$$\begin{array}{rccc} f: & H \times K & \longrightarrow & G \\ & (h,k) & \mapsto & hk \end{array}$$

la cual es un isomorfismo por propiedad 37. Luego $G \simeq H \times K$. □

Propiedad 47 (Producto Directo) *Sea* $G \simeq H \times K$*, entonces existen* $H', K' \lhd G$*, tales que* $H' \cap K' = \{e\}$ *y* $H'K' = G$*.*

Demostración: Sean H, K grupos consideremos el isomorfismo

$$\begin{array}{rccc} f: & H \times K & \longrightarrow & G \\ & (h,k) & \mapsto & f(h,k) \end{array}$$

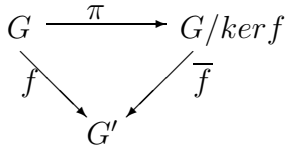
luego tenemos $H \times \{e\} \lhd H \times K$ y $\{e\} \times K \lhd H \times K$, tales que $H \times \{e\} \cap \{e\} \times H = \{(e,e)\}$ y $H \times \{e\}\{e\} \times K = H \times K$, por lo tanto

$$H' = f(H \times \{e\}), K' = f(\{e\} \times K) \lhd G$$

y cumplen con $H' \cap K' = \{e\}$ y $H'K' = G$. □

1.11. Teorema del Homomorfismo

Teorema 48 (Teorema del Homomorfismo) *Si* $f : G \longrightarrow G'$ *homomorfismo de grupo, entonces existe un único homomorfismo* $\overline{f} : G/ker f \longrightarrow G'$ *tal que* $\overline{f} \circ \pi = f$



Además si f *es epiyectiva se tiene que* $\overline{f}$ *es isomorfismo.*

Demostración: Sabemos que $ker f \trianglelefteq G$, luego tenemos que $G/ker f$ es un grupo.

Sea $\overline{x}, \overline{y} \in G/ker f$, tales que

$$\overline{x} = \overline{y},$$

de lo cual

$$\begin{aligned} \overline{x} &= \overline{y} \\ x^{-1}y &\in ker f \\ f(x^{-1}y) &= e \\ f(x) &= f(y). \end{aligned}$$

Por lo anterior podemos de definir $\overline{f}(\overline{x}) = f(x)$, la cual esta bien definida, es decir, $\overline{f}$ es una función.

Además es homomorfismo

$$\begin{aligned}\overline{f}(\overline{xy}) &= f(xy)\\ &= f(x)f(y)\\ &= \overline{f}(\overline{x})\overline{f}(\overline{y})\end{aligned}$$

y finalmente, sea $x \in G$

$$\overline{f}(\pi(x)) = \overline{f}(\overline{x}) = f(x)$$

Si f es epiyectiva, por definición de $\overline{f}$ tenemos que es epiyectiva.

Nos falta la inyectividad, para ello, si $\overline{x} \in ker\overline{f}$ luego tenemos que $\overline{f}(\overline{x}) = f(x) = e$, es decir, $x \in kerf$ y por lo tanto $\overline{x} = \overline{e}$. Con lo cual hemos demostrado que $ker\overline{f} = \{\overline{e}\}$ y por ende $\overline{f}$ es un isomorfismo. □

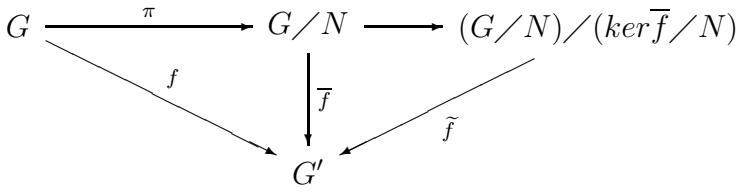
Corolario 49 (Primer Teorema del Isomorfismo) *En particular se tiene*

$$G/kerf \simeq Imf.$$

Teorema 50 (Generalización del Teorema del Homomorfismo) *Sea $N \trianglelefteq G$, $\pi : G \longrightarrow G/N$ el epimorfismo canónico y $f : G \longrightarrow G'$ homomorfismo tal que $N \subset kerf$, entonces existe un homomorfismo canónico $\overline{f}$ de G/N en G' y además se tiene*

$$f(G) \simeq (G/N)/(kerf/N)$$

Es decir, los diagramas conmutan.



Teorema 51 (de la Correspondencia) *Sea $f : G \longrightarrow G'$ epimorfismo, entonces existe una correspondencia biunívoca entre los subgrupos de G que contiene al $kerf$ y el conjunto de subgrupos de G'. Más precisamente*

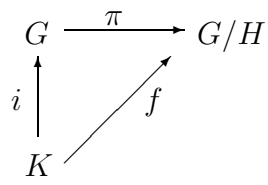
$$\psi : \{H \leq G \mid kerf \subset H\} \longrightarrow \{H' \subseteq G' \mid H' \leq G'\}$$

$$\begin{array}{ccc} H & \to & f(H) \\ f^{-1}(H') & \leftarrow & H' \end{array}$$

Teorema 52 (Segundo Teorema del Isomorfismo) *Si $H, K \leq G$ y $H \trianglelefteq G$, entonces*

$$K/H \cap K \simeq HK/H$$

Demostración: Sean $H, K \leq G$ y $H \trianglelefteq G$ y π proyección, i la inclusión.



Luego tenemos el homomorfismo $\pi \circ i : K \longrightarrow G/H$.
Es fácil determinar su kernel, ya que

$$ker(\pi \circ i) = \{k \in K \mid k \in H\} = K \cap H.$$

Y la Imagen esta dada por

$$Im(\pi \circ i) = \{kH \mid k \in K\} = HK/H$$

luego, por primer teorema del isomorfismo tenemos

$$K/H \cap K \simeq HK/H$$

Recuerde que $H \trianglelefteq G, K \leq G$, luego tenemos

$$\begin{aligned} HK &= \{hk \mid h \in H, k \in K\} \\ &= \{k(k^{-1}hk) \mid h \in H, k \in K\} \\ &= \{kh' \mid h' \in H, k \in K\} \\ &= KH \end{aligned}$$

Note que el teorema también puede escribirse

$$K/H \cap K \simeq HK/H \simeq KH/H$$

□

Corolario 53 *Si $H, K \leq G$ y $H \trianglelefteq G$, con G finito entonces*

$$|HK| = \frac{|H||K|}{|H \cap K|}.$$

Teorema 54 (Tercer Teorema del isomorfismo) *Si $H, K \trianglelefteq G$, donde $K \subset H$, entonces*

$$(G/K)/(H/K) \simeq G/H$$

Demostración: Sean $H, K \trianglelefteq G$ y $K \subseteq H$
Construiremos la función de G/K en G/H, para ello dados $\overline{x}, \overline{y} \in G/K$, tales que

$$\begin{aligned} \overline{x} &= \overline{y} \in G/K \\ y^{-1}x &\in K \subset H \\ \overline{x} &= \overline{y} \in G/H \end{aligned}$$

De lo cual tenemos

$$\begin{array}{rccc} f: & G/K & \to & G/H \\ & xK & \mapsto & xH \end{array}$$

es un homomorfismo, ya que

$$f(xKyK) = f(xyK) = xyH = xHyH = f(xK)f(yK)$$

Veamos ahora el kernel,

$$ker(f) = \{xK \in G/K \mid xH = H\} = H/K.$$

Y la Imagen esta dada por

$$Im(f) = \{xH \mid x \in G\} = G/H$$

luego, por primer teorema del isomorfismo tenemos

$$(G/K)/(H/K) \simeq G/H$$

□

1.11.1. Problemas Propuestos

Problema 43.

Dada $n \in \mathbb{N}$ y la función

$$G_n : \mathbb{R}^* \to \mathbb{R}^*; \text{ con } G_n(x) = x^{2n}$$

1. Demostrar que G_n es un homomorfismo de Grupo.
2. Determinar el Kernel y la Imagen.

Problema 44.

Se define la función conjugación de G en G por $T_g(x) = gxg^{-1}$ y el conjunto de todas ellas por $Int(G) = \{T_g \in Aut(G) \mid g \in G\}$,

Demostrar que:

$$Int(G) \trianglelefteq Aut(G)$$

Problema 45.

Si H, K son grupos. Demostrar que:

$$(H \times K)/(\{e\} \times K) \simeq K$$

Problema 46.

Consideremos los subgrupos $a\mathbb{Z}, b\mathbb{Z}$ de $\mathbb{Z}$. Demuestre que

$$a\mathbb{Z}/MCM(a,b)\mathbb{Z} \simeq MCD(a,b)\mathbb{Z}/b\mathbb{Z}$$

Problema 47.

Sean G_1, G_2 dos grupos y $H_i \trianglelefteq G_i$ entonces
Demostrar que

$$(G_1 \times G_2)/(H_1 \times H_2) \simeq (G_1/H_1) \times (G_2/H_2)$$

Problema 48.

Determinar si

$$\mathbb{Z}_{12}/ < \overline{2} > \simeq \mathbb{Z}_6$$

Problema 49.

Demostrar que

$$\mathbb{R}^*/\{1,-1\} \simeq \mathbb{R}^+$$

1.12. Clasificación Grupos Cíclicos

Propiedad 55 *Si $G = \langle g \rangle$ es finito de orden n, entonces para todo $k \in \mathbb{N}$ tal que $k|n$, se tiene*

1. *G contiene un único subgrupo de índice k.*
2. *$[G : \langle g^k \rangle] = k$.*
3. *Existe un único subgrupo de orden k.*

Demostración: Sea $G = \langle g \rangle$ finito de orden n, luego el orden de $k|pn$, notemos lo siguiente

$$|g^k| = \frac{n}{MCD(k,n)} = \frac{n}{kMCD(1,\frac{n}{k})} = \frac{n}{k} \qquad |g^{\frac{n}{k}}| = \frac{n}{MCD(n,\frac{n}{k})} = \frac{n}{\frac{n}{k}MCD(k,1)} = \frac{n}{\frac{n}{k}} = k$$

Sea H un subgrupo de orden k, luego se tiene que

$$H = \langle g^t \rangle$$

luego se tiene que $g^{tk} = e$, por lo tanto, $n|tk$, es decir

$$\frac{n}{MCD(n,k)} \left| \left(t\frac{k}{MCD(n,k)} \right) \right.$$

Por lo tanto $\frac{n}{MCD(n,k)}|t$, luego

$$g^t = (g^{\frac{n}{k}})^{l\frac{k}{MCD(n,k)}} \in \langle g^{\frac{n}{k}} \rangle$$

es decir, $H = \langle g^t \rangle \subseteq \langle g^{\frac{n}{k}} \rangle$ y además tiene igual cardinal, por lo tanto $H = \langle g^{\frac{n}{k}} \rangle$. □

Propiedad 56 *Si G es un grupo finito de orden n que tiene a lo más un subgrupo de orden k para todo $k \in \mathbb{N}$ que divide a n, entonces G es cíclico.*

Demostración: Sea $k|n$ y $\eta(k)$ es igual al número de elementos de G de orden k.

$$\sum_{k|n} \eta(k) = n.$$

Sea $x \in G$ de orden k, entonces $\langle x \rangle$ es un subgrupo de orden k. Además todo elemento de orden k pertenece a $\langle x \rangle$.

Así

$$\eta(k) = 0 \quad \vee \quad \eta(k) = \phi(k)$$

donde $\phi(k)$ es el número de elementos de orden k en el grupo cíclico de orden k, ϕ es la función de Euler. Pero

$$\sum_{k|n} \phi(k) = n$$

Luego, se tiene que

$$\phi(k) = \eta(k), \qquad \forall k|n$$

En particular se tiene que $\phi(n) = \eta(n) > 0$, por lo tanto G contiene un elemento de orden n, es decir G es cíclico.

□

Propiedad 57 *Todo grupo cíclico **infinito** es isomorfo a $\mathbb{Z}$, y todo grupo cíclico **finito** de orden n es isomorfo a $\mathbb{Z}_n$.*

Demostración: Sea $G = \langle g \rangle$, para algún $g \in G$.

Consideremos la siguiente función:

$$\begin{array}{rccc} \phi_g : & \mathbb{Z} & \longrightarrow & G \\ & k & \rightsquigarrow & g^k \end{array}$$

Veamos que ϕ_g es un homomorfismo, ya que, dado m, $n \in \mathbb{Z}$, se tiene que

$$\phi(m+n) = g^{m+n} = g^m g^n = \phi(m)\phi(n)$$

por lo cual ϕ es un homomorfismo.

Sabemos que ϕ es epiyectiva si y sólo si $G \subseteq Im\phi_g$, pero esto es fácil de verificar, pues para todo $g^k \in G$ con algún $k \in \mathbb{Z}$, luego existe una preimagen, la cual es exactamente k, entonces $G \subseteq Im\phi_g$.

Ahora veamos el Kernel, es un subgrupo de $\mathbb{Z}$, $\ker\phi \leq \mathbb{Z}$, por lo cual $\ker\phi = \{0\} \vee \ker\phi = n\mathbb{Z}$ con algún $n \in \mathbb{Z}^+$.

Luego tenemos dos casos

1. Si G es infinito $\ker\phi = \{0\}$, y no existe $m \neq 0$ tal que $g^m = e$, entonces se tiene que

$$\mathbb{Z} \simeq G$$

2. Por otro lado, si G en finito de orden n, entonces $\ker\phi = n\mathbb{Z}$, donde n es el menor entero positivo que cumple con $g^n = e$, luego por *primer teorema del isomorfismo* tenemos que
$$\mathbb{Z}_n \simeq \mathbb{Z}/n\mathbb{Z} \simeq G.$$

□

1.13. Grupo Hom

En esta sección describiremos explícitamente los grupos de homomorfismos

$$Hom(\mathbb{Z}_n, \mathbb{Z}_m);\ Hom(\mathbb{Z}_n \times \mathbb{Z}_r, \mathbb{Z}_m);\ Hom(\mathbb{Z}_n, \mathbb{Z}_m \times \mathbb{Z}_r)$$

Notemos la siguiente propiedad, que dado $f : G \to G'$ un homomorfismo de grupo se tiene que:
$$(\forall n \in \mathbb{N})(\forall g \in G))(f(g^n) = f(g)^n)$$
Resultado que se demuestra por inducción.

1.13.1. $Hom(\mathbb{Z}_n, \mathbb{Z}_m)$

Ejercicio 47 *Determinar explícitamente todos los elementos homomorfismos de $\mathbb{Z}_n$ en $\mathbb{Z}_m$, es decir, describir el grupo $Hom(\mathbb{Z}_n, \mathbb{Z}_m)$.*

Para ello, sea ϕ un elemento de $Hom(\mathbb{Z}_n, \mathbb{Z}_m)$, es decir

$$\begin{array}{rccc} h: & \mathbb{Z}_n & \longrightarrow & \mathbb{Z}_m \\ & \overline{x} & \mapsto & h(\overline{x}) \end{array}$$

y de tiene
$$h(\overline{x}) = h(x\overline{1}) = xh(\overline{1})$$
De lo cual tenemos que, h queda únicamente determinado si conocemos $h(1)$, el cual denotaremos por $a \in \mathbb{Z}_m$.

Pero además notemos que $0 = n$, luego $h(0) = h(n)$, es decir $na = 0 \in \mathbb{Z}_m$ luego, veamos que, existe $t \in \mathbb{Z}$ tal que $na = mt$.

Sea $d = MCD(n, m)$, entonces tenemos que $\frac{n}{d}a = \frac{m}{d}t$ y como $\frac{n}{d}$ y $\frac{m}{d}$ son primos relativos, obtenemos que $\frac{m}{d}|a$, lo cual implica que $a \in \frac{m}{d}\mathbb{Z}$ (a es múltiplo de $\frac{m}{d}$).

De este modo concluimos que

$$\begin{array}{rccc} h_a: & \mathbb{Z}_n & \longrightarrow & \mathbb{Z}_m \\ & \overline{x} & \rightsquigarrow & \overline{ax} \end{array}$$

esta bien definida si y sólo si a es múltiplo de $\frac{m}{d}$.

Ahora dados $x,\ y \in \mathbb{Z}_n$, tenemos que

$$h_a(x + y) = a(x + y) = ax + ay = h_a(x) + h_a(y)$$

Lo que nos dice, que para cada múltiplo de $\frac{m}{d}$ obtenemos un elemento de $Hom(\mathbb{Z}_n, \mathbb{Z}_m)$.

Y por la primera parte tenemos que todo los elementos de $Hom(\mathbb{Z}_n, \mathbb{Z}_m)$ son de la formar h_a, con $a \in (\frac{m}{d})\mathbb{Z}$.

Propiedad 58 *Sean* $n, m \in \mathbb{N},\ d = MCD(n, m)$.

$$Hom(\mathbb{Z}_n, \mathbb{Z}_m) = \{\ h_a \mid a \in \left\langle \frac{m}{d} \right\rangle \leq \mathbb{Z}_m\ \} \simeq \mathbb{Z}_d$$

Ejemplo 48 *Determinemos* $Hom(\mathbb{Z}_6, \mathbb{Z}_{12})$ *. Por el estudio anterior tenemos que*

$$Hom(\mathbb{Z}_6, \mathbb{Z}_{12}) = \{\ h_a \mid a \in < 2 > \leq \mathbb{Z}_{12}\}$$

Luego, nos queda $Hom(\mathbb{Z}_6, \mathbb{Z}_{12}) = \{h_0, h_2, h_4, h_6, h_8, h_{10}\}$*. Donde vemos claramente que* h_0 *es el elemento neutro y no está demás decir que, es un grupo con la operación suma.*

1.13.2. $Hom(\mathbb{Z}_r, \mathbb{Z}_n \times \mathbb{Z}_m)$

De forma análoga al problema anterior, si $\rho \in Hom(\mathbb{Z}_r, \mathbb{Z}_n \times \mathbb{Z}_m)$, entonces, ρ está únicamente determinada si conocemos $\rho(1)$, luego podemos escribir $\rho(1) = (a, b)$ y determinar las condiciones necesarias para que ρ este bien definida.

$$\begin{array}{ccccc} \mathbb{Z}_r & \longrightarrow & \mathbb{Z}_n \times \mathbb{Z}_m & \longrightarrow & \mathbb{Z}_n \\ \overline{x} & \mapsto & \rho(\overline{x}) & \mapsto & \pi(\rho(x)) = xa \end{array}$$

Luego de algunos cálculos similares al problema anterior obtendremos que los elementos de $Hom(\mathbb{Z}_r, \mathbb{Z}_n \times \mathbb{Z}_m)$, los cuales denotaremos por $\rho_{(a,b)}$, donde $a \in (\frac{n}{d})\mathbb{Z}$, $b \in (\frac{m}{c})\mathbb{Z}$, $d = MCD(r, n)$ y $c = MCD(r, m)$, son de la siguiente forma:

$$\begin{array}{rccc} \rho_{(a,b)}: & \mathbb{Z}_r & \longrightarrow & \mathbb{Z}_n \times \mathbb{Z}_m \\ & x & \mapsto & (ax, bx) \end{array}$$

Si notamos, es una definición análoga al caso anterior, sólo esta vez trabajamos con un par (a, b) y en donde restringimos ambas coordenadas por separado, para obtener las condiciones necesarias para ser homomorfismos. *Se deja al lector detallar los cálculos intermedios.*

Propiedad 59 *Sean* $r, n, m \in \mathbb{N},\ c = MCD(r, n),\ d = MCD(r, m)$.

$$Hom(\mathbb{Z}_r, \mathbb{Z}_n \times \mathbb{Z}_m) = \{\rho_{(a,b)} \mid a \in \langle \frac{n}{c} \rangle \leq \mathbb{Z}_n,\ b \in \langle \frac{m}{d} \rangle \leq \mathbb{Z}_m\} \simeq \mathbb{Z}_c \times \mathbb{Z}_d$$

Ejemplo 49 *Determinemos, el grupo* $Hom(\mathbb{Z}_3, \mathbb{Z}_4 \times \mathbb{Z}_6)$*. Tenemos que*

$$Hom(\mathbb{Z}_3, \mathbb{Z}_4 \times \mathbb{Z}_6) = \{\rho_{(a,b)} \mid a \in < 4 > \leq \mathbb{Z}_4\ ,\ b \in < 3 > \leq \mathbb{Z}_6\}$$

Luego $a = 0$*,y para* b *tiene las siguientes posibilidades* $0, 3$*. Por lo tanto, el grupo es*

$$Hom(\mathbb{Z}_3, \mathbb{Z}_4 \times \mathbb{Z}_6) = \{\rho_{(0,0)}, \rho_{(0,3)}\}$$

1.13.3. $Hom(\mathbb{Z}_n \times \mathbb{Z}_m, \mathbb{Z}_r)$

Encontrar explícitamente este grupo, significa razonar de manera análoga a los casos anteriores, tomemos $\phi \in Hom(\mathbb{Z}_n \times \mathbb{Z}_m, \mathbb{Z}_r)$, luego

$$\begin{array}{rccc} \psi: & \mathbb{Z}_n \times \mathbb{Z}_m & \longrightarrow & \mathbb{Z}_r \\ & (x,y) & \mapsto & x\psi((1,0)) + y\psi((0,1)) \end{array}$$

Ahora, llamemos $\psi((1,0)) = a$ y $\psi((0,1)) = b$. Como ψ es un homomorfismo, entonces el neutro de $\mathbb{Z}_n \times \mathbb{Z}_m$ es enviado al neutro de $\mathbb{Z}_r$, es decir,

$$\begin{array}{rccccc} \psi \circ i: & \mathbb{Z}_n & \longrightarrow & \mathbb{Z}_n \times \mathbb{Z}_m & \longrightarrow & \mathbb{Z}_r; \\ & x & \mapsto & (x,e) & \mapsto & xa \end{array} \qquad \begin{array}{rccccc} \psi \circ i: & \mathbb{Z}_n & \longrightarrow & \mathbb{Z}_m \times \mathbb{Z}_m & \longrightarrow & \mathbb{Z}_r \\ & y & \mapsto & (e,y) & \mapsto & by \end{array}$$

Consideremos $c = MCD(r,n)$ y $d = MCD(r,m)$, obtenemos que a debe ser múltiplo de $\frac{r}{c}$ y que b debe ser múltiplo de $\frac{r}{d}$. (*se deja de ejercicio su verificación*)

Propiedad 60 *Sean $r,n,m \in \mathbb{N}$, $c = MCD(r,n)$, $d = MCD(r,m)$.*

$$Hom(\mathbb{Z}_n \times \mathbb{Z}_m, \mathbb{Z}_r) = \{\psi_{(a,b)} \mid (a \in \langle \frac{r}{c} \rangle \leq \mathbb{Z}_r \ \wedge \ b \in \langle \frac{r}{d} \rangle \leq \mathbb{Z}_r\}$$

donde $\psi_{(a,b)}((x,y)) = ax + by$ para todo $(x,y) \in \mathbb{Z}_n \times \mathbb{Z}_m$.

Ejemplo 50 *Determine explícitamente el grupo $Hom(\mathbb{Z}_3 \times \mathbb{Z}_9, \mathbb{Z}_{12})$. Según lo precedente tenemos que*

$$Hom(\mathbb{Z}_3 \times \mathbb{Z}_9, \mathbb{Z}_{12}) = \{\psi_{(\overline{a},\overline{b})} \mid a \in < 4 > \leq \mathbb{Z}_{12} \ \wedge \ b \in < 4 > \leq \mathbb{Z}_{12}\}$$

Luego, tenemos las siguientes posibilidades; $a = 0,4,8$ y $b = 0,4,8$, es decir, el grupo $Hom(\mathbb{Z}_3 \times \mathbb{Z}_9, \mathbb{Z}_{12})$ tiene 9 elementos.

$$Hom(\mathbb{Z}_3 \times \mathbb{Z}_9, \mathbb{Z}_{12}) = \{\psi_{(0,0)}, \psi_{(0,4)}, \psi_{(0,8)}, \psi_{(4,0)}, \psi_{(4,4)}, \psi_{(4,8)}, \psi_{(8,0)}, \psi_{(8,4)}, \psi_{(8,8)}\}$$

Propiedad 61 *Sean G, G' grupos, H, K grupos abelianos entonces*

1. $Hom(G, H \times K) \simeq Hom(G,H) \times Hom(G,K)$
2. $Hom(G \times G', K) \simeq Hom(G,K) \times Hom(G',K)$

1.13.4. Problemas Propuestos

Problema 50.

Sea $a \in \mathbb{Z}$ y la función definida por

$$\begin{array}{rccc} h_a: & \mathbb{Z}_n & \longrightarrow & \mathbb{Z}_n \\ & \overline{x} & \rightsquigarrow & \overline{ax} \end{array}$$

1. Demostrar que h_a es un homomorfismo
2. Si $n = 20, a = 5$. Determinar el $\ker h_5$, $\operatorname{Im} h_5$ explícitamente
3. Si $n = p$ (primo). Demostrar que h_a es un automorfismo $a \in \{1, 2, ..., p-1\}$

Problema 51.

Sea $d = MCD(n, m)$, entonces

$$\mathbb{Z}_d \cong Hom(\mathbb{Z}_n, \mathbb{Z}_m)$$

Observación: Esta proposición, nos indica que el grupo $Hom(\mathbb{Z}_n, \mathbb{Z}_m)$, es cíclico y su cardinal.
Sugerencia: Considere la función $\phi : (\frac{m}{d})\mathbb{Z} \longrightarrow Hom(\mathbb{Z}_n, \mathbb{Z}_m)$, dada por $\phi(a) = \phi_a$.

Problema 52.

Determinar explícitamente el grupo $Hom(\mathbb{Z}_a \times \mathbb{Z}_b, \mathbb{Z}_c \times \mathbb{Z}_d)$.

Problema 53.

Determinar explícitamente el grupo $Hom(\mathbb{Z}, \mathbb{Z}_n)$.

1.13.5. Automorfismos

Un caso particular de lo anteriores grupos, son los grupos **automorfismos** de los grupos cíclicos $\mathbb{Z}_n$ y conocer algunos propiedades básicos de estos grupos de automorfismos.

Para lo anterior necesitamos recordar la función ϕ de Euler, vista en la asignatura de aritmética, la cual proporciona el orden del grupo $Aut(\mathbb{Z}_n)$ como lo veremos a continuación.

Función ϕ de Euler

Definición 15 *Sea $n \in \mathbb{N}$, entonces la función φ de Euler se define como*

$$\phi(n) = \{m \in \mathbb{N} \mid m \leq n,\ MCD(n, m) = 1\}$$

Teorema 62 (Fundamental de la Aritmética) *Sea $n \in \mathbb{N}$, entonces existen únicos $\alpha_i \in \mathbb{N}$ y p_i primos distintos, con $1 \leq i \leq k$, tales que*

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

Propiedad 63 *Sea p un número primo, entonces*

1. $\phi(1) = 1$
2. $\phi(p) = p - 1$.
3. $\phi(p^t) = (p-1)p^{t-1}$, *con* $t \in \mathbb{N}$.

4. Sean $n, m \in \mathbb{N}$ tales que $MCD(n, m) = 1$, entonces

$$\phi(nm) = \phi(n)\phi(m)$$

Otro resultado que utilizaremos es el siguiente

Propiedad 64 *Sean G y G' dos grupos tales que G es isomorfo a G', entonces*

$$Aut(G) \simeq Aut(G')$$

Demostración de ejercicio □

Luego de estos resultados podemos comenzar a estudiar uno de nuestros propósitos del apartado

Ejercicio 51 *Determinar explícitamente el grupo $Aut(\mathbb{Z}_n)$.*

Sabemos que $h \in Aut(\mathbb{Z}_n)$ si y sólo si $h \in Hom(\mathbb{Z}_n, \mathbb{Z}_n)$ biyectivo, es decir, es de la forma h_a, con $a \in \mathbb{Z}_n$ y como h es invertible, su inversa es del mismo tipo, luego tenemos que el inverso de h_a es h_b, y el cual existe si y sólo si a es invertible en $\mathbb{Z}_n$.

Propiedad 65 *Sea $n \in \mathbb{N}$ entonces*

$$Aut(\mathbb{Z}_n) = \{h_a \mid a \in \mathcal{U}(\mathbb{Z}_n)\} \simeq \mathcal{U}(\mathbb{Z}_n)$$

Demostración: Para mostrar que $Aut(\mathbb{Z}_n) \cong \mathcal{U}(\mathbb{Z}_n)$, basta considerar la función

$$\begin{array}{rccc} \Phi: & \mathcal{U}(\mathbb{Z}_n) & \longrightarrow & Aut(\mathbb{Z}_n) \\ & a & \mapsto & h_a \end{array}$$

y es un Isomorfismo. □

Ejemplo 52 *Determinar explícitamente el grupo $Aut(\mathbb{Z}_{15})$. Como ya sabemos, este problema se reduce a encontrar los $n < 15$ tales que $(n, 15) = 1$ (primos relativos con 15). Luego, inmediatamente obtenemos que*

$$Aut(\mathbb{Z}_{15}) = \{h_1, h_2, h_4, h_7, h_8, h_{11}, h_{13}, h_{14}\}$$

Ejemplo 53 *Determine el orden del grupo $Aut(\mathbb{Z}_{100})$.*

Como ya sabemos el orden de $Aut(\mathbb{Z}_n)$ es $\phi(n)$, luego el problema se reduce a calcular $\phi(100)$. Parra ello tenemos que

$$100 = 2^2 5^2$$

Luego

$$\phi(100) = 100(1 - \frac{1}{2})(1 - \frac{1}{5}) = 100 \cdot \frac{4}{10} = 40$$

De este modo tenemos que

$$|Aut(\mathbb{Z}_{100})| = 40$$

Propiedad 66 *Sea $n \in \mathbb{N}$, entonces las siguientes proposiciones se cumplen:*

1. *Consideremos p un número primo, entonces $Aut(\mathbb{Z}_p)$ es isomorfo a $\mathbb{Z}_{p-1}$.*

2. *$Aut(\mathbb{Z}_{p-1})$ es isomorfo a $Aut(\mathcal{U}(\mathbb{Z}_p))$.*

Demostración: Afirmamos que si p es un número primo, entonces el grupo $\mathcal{U}(\mathbb{Z}_p)$ es un grupo cíclico de orden $p-1$, aplicando la **proposición 57** tenemos que $\mathcal{U}(\mathbb{Z}_p) \cong \mathbb{Z}_{p-1}$, luego por [1] se tiene que $Aut(\mathbb{Z}_p) \cong \mathbb{Z}_{p-1}$.

Como $\mathcal{U}(\mathbb{Z}_p) \cong \mathbb{Z}_{p-1}$, entonces $Aut(\mathbb{Z}_{p-1}) \cong Aut(\mathcal{U}(\mathbb{Z}_p))$ (por **proposición 64**)

□

Ejemplo 54 *Determine si el grupo $Aut(\mathbb{Z}_{30}) \times Hom(\mathbb{Z}_3, \mathbb{Z}_{12})$ es isomorfo al grupo $Aut(\mathcal{U}(\mathbb{Z}_{11}))$.*

Recordemos que $|Aut(\mathbb{Z}_{30}) \times Hom(\mathbb{Z}_3, \mathbb{Z}_{12})| = |Aut(\mathbb{Z}_{30})| \cdot |Hom(\mathbb{Z}_3, \mathbb{Z}_{12})|$. Sabemos que

$$|Aut(\mathbb{Z}_{30})| = \phi(30) = \phi(2 \cdot 3 \cdot 5) = \phi(2)\phi(3)\phi(5) = 1 \cdot 2 \cdot 4 = 8$$

Por otro lado, sabemos que $Hom(\mathbb{Z}_3, \mathbb{Z}_{12}) \cong \mathbb{Z}_3$ obteniendo así que

$$|Hom(\mathbb{Z}_3, \mathbb{Z}_{12})| = 3$$

de esta manera se tiene que

$$|Aut(\mathbb{Z}_{30}) \times Hom(\mathbb{Z}_3, \mathbb{Z}_{12})| = 8 \cdot 3 = 24$$

*Ahora calculemos el orden de $|Aut(\mathcal{U}(\mathbb{Z}_{11}))|$. Por la **proposición 66** parte 3 sabemos que $Aut(\mathcal{U}(\mathbb{Z}_{11})) \cong Aut(\mathbb{Z}_{10})$ y el cual tiene orden $\phi(10) = \phi(2)\phi(5) = 4$, por lo tanto*

$$|Aut(\mathcal{U}(\mathbb{Z}_{11}))| = 4$$

De este modo tenemos que

$$Aut(\mathbb{Z}_{30}) \times Hom(\mathbb{Z}_3, \mathbb{Z}_{12}) \ncong Aut(\mathcal{U}(\mathbb{Z}_{11}))$$

pues sus orden son distintos.

Ejercicio 55 *Determinar el orden de los grupos $Aut(\mathbb{Z}_{1542})$ y $Aut(\mathbb{Z}_{15} \times \mathbb{Z}_{32})$*

Ejercicio 56 *Demuestre que*

$$Aut(\mathbb{Z}_2 \times \mathbb{Z}_3) \cong Aut(\mathcal{U}(\mathbb{Z}_{14}))$$

1.13.6. Automorfismo Interior

Definición 16 *Sea G un grupo, $g \in G$. Se define La siguiente función:*

$$\begin{array}{rccccc} I_g: & G & \longrightarrow & G & & \\ & x & \mapsto & I_g(x) & = & gxg^{-1} \end{array}$$

Afirmamos que I_g es un automorfismo, el cual es conocido como **`Automorfismo Interior`** *asociado a g.*

Observemos que si G es un grupo no abeliano, entonces existe $g \in G$ tal que $I_g(a) = gag^{-1} \neq a$, luego $I_g \neq Id$, donde la identidad es el automorfismo trivial del grupo G. Entonces, para cada grupo no abeliano, siempre existirán automorfismos no triviales.

Veamos que el siguiente conjunto definido como:

$$Int(G) = \{I_g \in Aut(G) \,|\, g \in G\} \subseteq Aut(G),$$

tiene estructura natural de grupo, como la operación compuesta de funciones, es decir,

$$Int(G) \leq Aut(G).$$

Propiedad 67 *Sean G un grupo*

$$G/Z(G) \simeq Int(G)$$

Demostración:

Sea G un grupo. Consideremos la siguiente función:

$$\begin{array}{rccccccc} \mu: & G & \longrightarrow & Aut(G) & & & & \\ & g & \mapsto & I_g: & G & \longrightarrow & G \\ & & & & x & \mapsto & gxg^{-1} \end{array}$$

Demostramos que μ es un homomorfismo, para ello sean $g, h \in G$, por demostrar que

$$\mu(gh) = \mu(g) \circ \mu(h).$$

Sabemos que dos funciones de igual dominio son iguales si y sólo si para todo elemento en su dominio la imagen es la misma.

Sea $x \in G$, luego

$$\begin{array}{rcl} \mu(gh)(x) & = & I_{gh}(x) \\ & = & (gh)x(gh)^{-1} \\ & = & g(hxh^{-1})g^{-1} \\ & = & I_g(hxh^{-1}) \\ & = & I_g(I_h(x)) \\ & = & (I_g \circ I_h)(x) \\ & = & (\mu(g) \circ \mu(h))(x) \end{array}$$

Entonces, $\mu(gh) = \mu(g) \circ \mu(h)$, es decir, μ es un homomorfismo.

Ahora, nos interesa es conocer el $\ker \mu$.

$$\begin{array}{rcrcll} Seak \in ker\mu & \Leftrightarrow & \mu(k) & = & Id & \\ & \Leftrightarrow & I_k(x) & = & Id(x) & \forall\, x \in G \\ & \Leftrightarrow & kxk^{-1} & = & x & \forall\, x \in G \\ & \Leftrightarrow & kx & = & xk & \forall\, x \in G \\ & \Leftrightarrow & k & \in & Z(G) & \end{array}$$

Por pasos de equivalentes tenemos que $ker\mu = Z(G)$.

Ahora, sólo nos resta conocer el conjunto $Im\mu$.

$$\begin{array}{rcl} Im\mu & = & \{f \in Aut(G) \,|\, (\exists\, g \in G)(\mu(g) = f)\} \\ & = & \{f \in Aut(G) \,|\, (\exists\, g \in G)(I_g = f)\} \\ & = & \{I_g \in Aut(G) \,|\, g \in G\} \\ & = & Int(G) \end{array}$$

Resumiendo tenemos que μ es un homomorfismo, además que $Ker\mu = Z(G)$ y $Im\mu = Int(G)$, luego si utilizamos el teorema del isomorfismo finalmente tenemos

$$G/Z(G) \simeq Int(G)$$

□

Propiedad 68 *Sean G un grupo y $H \leq G$. Demostrar que*

$$N_G(H)/C_G(H) \simeq Int(H)$$

Demostración: Sea $g \in N_G(H)$, luego $I_g : H \to H$, con $I_g(h) = ghg^{-1}$, esta bien definida.

$$\begin{array}{rccccccc} \mu: & N_G(H) & \longrightarrow & Aut(H) & & & & \\ & g & \mapsto & I_g: & H & \longrightarrow & H \\ & & & & h & \mapsto & ghg^{-1} \end{array}$$

El resto de la demostración es similar a la anterior □

1.14. Producto Semidirecto de Grupos

Sea $Aut(G)$ el grupo de los automorfismo de G y consideremos $F : H \to Aut(G)$, por razones de facilitar la escritura, la imagen la denotamos del siguiente modo $F(h) = F_h$, con ello tenemos

$$\begin{array}{rccccccc} F: & H & \to & Aut(G) & & & & \\ & h & \rightsquigarrow & F(h) & & & & \\ & h & \rightsquigarrow & F_h: & G & \to & G \\ & & & & g & \rightsquigarrow & F_h(g) \end{array}$$

De este modo tenemos $F_h(g) \in G$.

Propiedad 69 *Sean G, H grupos, y $F : H \to Aut(G)$ un homomorfismo.*
El producto cartesiano $G \times H$ dotado de la operación

$$(a, b) *_F (c, d) = (aF_b(c), bd)$$

posee estructura de grupo, y recibe el nombre de producto semidirecto de G y H con respecto a F, y se denota $G \rtimes H$ o $H \ltimes G$

Demostración: Es claro que la operación es cerrada en el producto cartesiano $G \times H$. La asociatividad se demuestra según

$$\begin{aligned}
[(a,b)*(c,d)]*(y,w) &= (aF_b(c),bd)*(y,w)\\
&= (aF_b(c)F_{bd}(y),bdw)\\
&= (aF_b(c)F_b(F_d(y)),bdw)\\
&= (aF_b(cF_d(y)),bdw)\\
&= (a,b)*(cF_d(y),dw)\\
&= (a,b)*[(c,d)*(y,w)]
\end{aligned}$$

El elemento neutro es, claramente, (e_G, e_H), pues

$$(a,b)*(e_G,e_H) = (aF_b(e_G),be_H) = (a,b)$$

El inverso de un elemento (a,b) es $(F_{b^{-1}}(a^{-1}),b^{-1})$. En efecto,

$$\begin{aligned}
(a,b)*(F_{b^{-1}}(a^{-1}),b^{-1}) &= (aF_b(F_{b^{-1}}(a^{-1})),bb^{-1})\\
&= (aF_e(a^{-1}),bb^{-1})\\
&= (aa^{-1},bb^{-1})\\
&= (e_G,e_H)\\
(F_{b^{-1}}(a^{-1}),b^{-1})*(a,b) &= (F_{b^{-1}}(a^{-1})F_{b^{-1}}(a)b^{-1}b)\\
&= (F_{b^{-1}}(a^{-1}a),b^{-1}b)\\
&= (F_{b^{-1}}(e_G),e_H)\\
&= (e_G,e_H)
\end{aligned}$$

□

Propiedad 70 *Sean G, H grupos, y $F : H \to Aut(G)$ un homomorfismo. Entonces,*

1. $G \simeq G' = \{(g, e_H) \mid g \in G\} \trianglelefteq G \rtimes H$
2. $H \simeq H' = \{(e_G, h) \mid h \in H\} \leq G \rtimes H$

Demostración: 1. La aplicación biyectiva $f : G \to G'$ definida según $f(g) = (g, e_H)$ es un homomorfismo, pues

$$f(gg') = (gg', e_H) = (gF_{e_H}(g'), e_H) = (g, e_H) * (g', e_H) = f(g)f(g')$$

Además, para todos $(g, eH) \in G'$, $(a,b) \in G \rtimes H$, se tiene

$$\begin{aligned}
(a,b)*(g,e_H)*(a,b)^{-1} &= (aF_b(g),b)*(F_{b^{-1}}(a^{-1}),b^{-1})\\
&= (aF_b(g)F_b(F_{b^{-1}}(a^{-1})),e_H)\\
= (aF_b(g)a^{-1},e_H) &\in G'
\end{aligned}$$

2. La aplicación biyectiva $f : H \to H$ definida por $f(h) = (e_G, h)$ es un homomorfismo, pues

$$f(hh') = (e_G, hh') = (e_G F_h(e_G), hh') = (e_G, h) * (e_G, h') = f(h) * f(h')$$

□

Propiedad 71 *Sean G un grupo, $M \leq G$, $N \trianglelefteq G$.*

Si $M \cap N = \{e\}$ y $MN = G$, entonces $G \simeq M *_T N$, donde $T : N \to AutM$ y viene dada por $T_n(m) = nmn^{-1}$.

Demostración: Al igual que en la demostración anterior, cada $g \in G$ posee una factorización única $g = mn$. La aplicación $f : G \to M \rtimes N$ dada por $f(g) = (m, n)$ está, por tanto, bien definida, y es biyectiva. Sean $g_1 = m_1 n_1$ y $g_2 = m_2 n_2$. Entonces,

$$g_1 g_2 = m_1 n_1 m_2 n_2 = m_1 n_1 m_2 (n_1^{-1} n_1) n_2 = m_1 T_{n_1}(m_2) n_1 n_2$$

Por tanto,

$$f(g_1 g_2) = (m_1 T_{n_1}(m_2), n_1 n_2) = (m_1, n_1) *_T (m_2, n_2) = f(g_1) * f(g_2)$$

lo cual muestra que f es un isomorfismo. □

Ejemplo 57 *Dado el isomorfismo*

$$\begin{array}{rccc} T: & \mathbb{Z}_4 & \longrightarrow & \mathbb{Z}_4 \\ & x & \longmapsto & -x \end{array}$$

Construir el producto semidirecto $\mathbb{Z}_4 \rtimes \mathbb{Z}_2$ y explícita el grupo

Solución: Notemos que

$$T^2(x) = T(-x) = x$$

tiene orden 2, luego define

$$\begin{array}{rccc} \rho: & \mathbb{Z}_2 & \longrightarrow & Aut(\mathbb{Z}_4) \\ & t & \longmapsto & T^t \end{array}$$

El producto semidirecto asociado $G = \mathbb{Z}_4 \rtimes \mathbb{Z}_2$, es un grupo no abeliano de orden 8. Para ello, el producto

$$(x, z) *_\rho (x', z') \;=\; (x + T^z(x'), z + z') = (x + (-1)^z x', z + z')$$

Veamos el orden de los elementos, dado $(x, z) \in G$ tenemos que

$$\begin{array}{rcl} (x,z)^2 & = & ((1 + (-1)^z)x, 0) \\ (x,z)^3 & = & ((2 + (-1)^z)x, z) \\ (x,z)^4 & = & (0, 0) \end{array}$$

luego tenemos que tiene cinco elementos de orden 2 y dos elementos de orden 4 .

$$G \simeq D_4$$

□

Ejemplo 58 *Dado el isomorfismo*

$$\begin{array}{rccc} T: & \mathbb{Z}_2 \times \mathbb{Z}_2 & \longrightarrow & \mathbb{Z}_2 \times \mathbb{Z}_2 \\ & (x, y) & \longmapsto & (x, x + y) \end{array}$$

Construir el producto semidirecto $(\mathbb{Z}_2 \times \mathbb{Z}_2) \rtimes \mathbb{Z}_2$ y explícita el grupo

Solución: Notemos que

$$T^2(x,y) = T(x,x+y) = (x,2x+y) = (x,y)$$

tiene orden 2, luego define

$$\begin{array}{rccc} \rho: & \mathbb{Z}_2 & \longrightarrow & Aut(\mathbb{Z}_2 \times \mathbb{Z}_2) \\ & t & \longmapsto & T^t \end{array}$$

El producto semidirecto asociado $G = (\mathbb{Z}_2 \times \mathbb{Z}_2) \rtimes \mathbb{Z}_2$, es un grupo no abeliano de orden 8. Para ello, el producto

$$\begin{array}{rcl} ((x,y),z) *_\rho ((x',y'),z') & = & ((x,y) + T^z(x',y'), z+z') = ((x+x', y+zx'+y'), z+z') \\ (x,y,z) * (x',y',z') & = & (x+x', y+zx'+y', z+z') \end{array}$$

Veamos el orden de los elementos, dado $(x,y,z) \in G$ tenemos que

$$\begin{array}{rcl} (x,y,z)^2 & = & (0,zx,0) \\ (x,y,z)^3 & = & (x,zx+y,z) \\ (x,y,z)^4 & = & (0,0,0) \end{array}$$

luego tenemos que tiene dos elementos de orden 4 y cinco elementos de orden 2 .

$$G \simeq D_4$$

□

Ejemplo 59 *Dado el isomorfismo*

$$\begin{array}{rccc} T: & \mathbb{Z}_7 & \longrightarrow & \mathbb{Z}_7 \\ & x & \longmapsto & 2x \end{array}$$

Construir el producto semidirecto $\mathbb{Z}_7 \rtimes \mathbb{Z}_3$ y explícita el grupo.

Solución: Notemos que

$$T^2(x) = T(2x) = 4x \qquad T^3(x) = T(4x) = 8x = x$$

tiene orden 3, luego define

$$\begin{array}{rccc} \rho: & \mathbb{Z}_3 & \longrightarrow & Aut(\mathbb{Z}_7) \\ & t & \longmapsto & T^t \end{array}$$

El producto semidirecto asociado $G = \mathbb{Z}_7 \rtimes \mathbb{Z}_3$, es un grupo no abeliano de orden 21.

Donde el producto esta dada por

$$(a,b) \cdot_\rho (c,d) = (a + 2^b c, b+d)$$

□

1.15. Acción de Grupo en un Conjunto

Definición 17 *Sean G un grupo y X un conjunto no vacío. Se dice que G actúa sobre X, o que X es un G-`espacio` si y sólo si existe una función*

$$\begin{array}{rccc} \cdot : & G \times X & \longrightarrow & X \\ & (g, x) & \to & g \cdot x \end{array}$$

tal que

1. $(\forall g, h \in G)(\forall x \in X)(g \cdot (h \cdot x) = gh \cdot x)$
2. $(\forall x \in X)(e \cdot x = x)$

Ejemplo 60

1. *$GL_n(K)$ actúa en $M_{1\times n}(K)$, dado por*

$$\begin{array}{rccc} \cdot : & GL_n(K) \times M_{1\times n}(K) & \longrightarrow & M_{1\times n}(K) \\ & (A, X) & \to & AX \end{array}$$

2. *$G = Biy(X)$ actúa en X.*

$$\begin{array}{rccc} \cdot : & G \times X & \longrightarrow & X \\ & (f, x) & \to & f(x) \end{array}$$

3. *$G = Sim(poligono)$ actúa en A conjunto de vértices del polígono.*

$$\begin{array}{rccc} \cdot : & G \times A & \longrightarrow & A \\ & (\sigma, x) & \to & \sigma(x) \end{array}$$

4. *$H \leq G$, H actúa sobre G por la derecha*

$$\begin{array}{rccc} \cdot : & H \times G & \longrightarrow & G \\ & (h, g) & \to & h \cdot g = gh^{-1} \end{array}$$

5. *$H \leq G$, H actúa sobre G por la izquierda*

$$\begin{array}{rccc} \cdot : & H \times G & \longrightarrow & G \\ & (h, g) & \to & h \cdot g = hg \end{array}$$

6. *$H \leq G$, H actúa sobre G por conjugación*

$$\begin{array}{rccc} \cdot : & H \times G & \longrightarrow & G \\ & (h, g) & \to & h \cdot g = hgh^{-1} \end{array}$$

7. *$H \trianglelefteq G$, G actúa sobre H por conjugación*

$$\begin{array}{rccc} \cdot : & G \times H & \longrightarrow & H \\ & (g,h) & \to & g \cdot h = ghg^{-1} \end{array}$$

8. *$H \leq G$, G actúa sobre G/H*

$$\begin{array}{rccc} \cdot : & G \times G/H & \longrightarrow & G/H \\ & (g, xH) & \longmapsto & gxH \end{array}$$

Definición 18 *Sean X un G-espacio y $x \in X$, se define el* **`estabilizador`** *de x en G como*

$$Est_G(x) = G_x = \{g \in G \mid g \cdot x = x\}$$

y la **`órbita`** *de x por*

$$O_x = \{y \in X \mid (\exists g \in G)(g \cdot x = y)\}$$
$$O_x = \{g \cdot x \in X \mid g \in G\}$$

Propiedad 72 *Sea X un G-espacio, $x \in X$*

$$G_x \leq G$$

Demostración: Se tiene que $G_X \subseteq G$, además $e \cdot x = x$, luego $e \in G_x$.
Sean $g, h \in G_x$, luego tenemos que

$$gh \cdot x = g(h \cdot x) = g \cdot x = x$$

de lo cual se obtiene que $gh \in G_x$, por otro lado tenemos

$$x = e \cdot x = h^{-1}h \cdot x = h^{-1}(h \cdot x) = h^{-1} \cdot x$$

es decir, $h^{-1} \in G_x$. Por lo tanto $G_x \leq G$. □

Ejercicio 61

1. *Demostrar que $GL_2(K)$ actúa naturalmente por evaluación en K^2*
2. *Demostrar que $GL_2(K)$ actúa naturalmente por evaluación en $\{l \leq K^2 \mid diml = 1\}$*
3. *Demostrar que $GL_2(K)$ actúa naturalmente por evaluación en $\{P \leq K^3 \mid dimP = 2\}$*

Propiedad 73 *Sea X un G-espacio, $x \in X$.*
Si $x \in O_y$ entonces existe $g \in G$ tal que $G_x = gG_yg^{-1}$

Demostración: Si $x \in O_y$, entonces existe $g \in G$ tal que $x = g \cdot y$. Tenemos:

$$\begin{array}{rcrcl} h \in G_x & \Leftrightarrow & h \cdot x & = & x \\ & \Leftrightarrow & h \cdot (g \cdot y) & = & g \cdot y \\ & \Leftrightarrow & g^{-1} \cdot (hg \cdot y) & = & y \\ & \Leftrightarrow & (g^{-1}hg) \cdot y & = & y \\ & \Leftrightarrow & g^{-1}hg & \in & G_y \\ & \Leftrightarrow & h & \in & gG_yg^{-1} \end{array}$$

Por pasos de equivalencia concluimos que

$$G_x = gG_yg^{-1}$$

□

Corolario 74 *Sea X un G-espacio, $x \in X$.*

$$(\forall y \in O_x)(G_x \trianglelefteq G \Rightarrow G_x = G_y).$$

Propiedad 75 *Sea X un G-espacio, $x \in X$ entonces*

$$\begin{array}{rccc} \psi : & G/G_x & \longrightarrow & O_x \\ & gG_x & \longmapsto & g \cdot x \end{array}$$

es una función biyectiva.

Demostración: Sean $gG_x = hG_x$, luego se tiene que $h^{-1}g \in G_x$, por lo tanto

$$h \cdot x = h(h^{-1}g \cdot x) = (hh^{-1}g) \cdot x = g \cdot x$$

Luego esta bien definida ψ.

Claramente es epiyectiva por definición de los elementos de una órbita.

Por último la inyectividad, sean $gG_x, hG_x \in G/G_x$, tales que $g \cdot x = h \cdot x$, por lo tanto

$$h^{-1}g \cdot x = h^{-1}(g \cdot x) = h^{-1}(h \cdot x) = h^{-1}h \cdot x = x$$

es decir $h^{-1}g \in G_x$, por lo cual $gG_x = hG_x$.

□

Corolario 76 *Sea X un G-espacio, entonces*

1. *Si O_x es finito, entonces el cardinal de O_x es $[\, G : G_x \,]$*
2. *Si G es finito, entonces*

$$|G| = |G_x| \cdot |O_x|.$$

Relación de Equivalencia

Sea X un G-espacio, se define la siguiente relación en X

$$x \sim y \quad \Leftrightarrow \quad (\exists g \in G)(g \cdot x = y)$$

Propiedad 77 *$\sim$ es una relación de equivalencia en X.*

Demostración de ejercicio □

Observación: Notemos que las órbitas son las clases de equivalencia de la relación luego tenemos que

$$X = \dot{\bigcup_{x \in R}} O_x$$

donde R es un sistema de representante.

Ejemplo 62 *Sea G un grupo, G actúa por conjugación sobre G*

$$\begin{array}{ccc} G \times G & \longrightarrow & G \\ (h, g) & \longmapsto & hgh^{-1} \end{array}$$

Determinar la órbita y el estabilizador

Solución: Dado $g \in G$, la órbita de g esta dada por

$$O_g = \{hgh^{-1} \mid h \in G\},$$

corresponde a todo los conjugados.

El Estabilizador

$$G_g = \{h \in G \mid hgh^{-1} = g\} = C_G(g),$$

es el centralizador de g en G. □

Teorema 78 (Ecuación de Clases) *Si G es un grupo finito no conmutativo, existe una familia de subgrupos $\{H_i\}_{1 \leq i \leq m}$ tales que*

1. $[G : H_i] > 1$
2. $|G| = |Z(G)| + \sum_{i=1}^{m} [G : H_i]$

Demostración: Sea G un grupo finito y $S = \{g_1, \ldots, g_n\}$ un sistema de representantes de las órbitas de la acción por conjugación, luego tenemos

$$G = \dot{\bigcup_{g \in S}} O_g$$

Como el grupo es finito

$$\begin{aligned} |G| &= \sum_{g\in S}|O_g| \\ &= \sum_{g\in S}[G:G_g] \\ &= \sum_{g\in S}[G:C_G(g)] \end{aligned}$$

La sumatoria se puede reordenar, agrupando las órbitas de cardinal 1 y las de cardinal mayor, ahora bien las de cardinal 1 cumple con

$$\begin{aligned} |O_g| = 1 &\Leftrightarrow hgh^{-1} = g \qquad \forall h \in G \\ &\Leftrightarrow hg = gh \qquad \forall h \in G \\ &\Leftrightarrow g \in Z(G) \end{aligned}$$

Con lo cual obtenemos la `Ecuación de Clases`

$$|G| = |Z(G)| + \sum_{\substack{G\neq G_g \\ g\in S}} [G:C_G(g)]$$

□

Propiedad 79 *Si $|G| = p^n$, entonces $Z(G) \neq \{e\}$.*

Demostración: Por la ecuación de clase tenemos:

$$p^n = |Z(G)| + pt \quad t \in \mathbb{N}$$

aplicando módulo p obtenemos

$$|Z(G)| \equiv 0 \pmod{p}$$

es decir

$$|Z(G)| = pq > 1 \qquad q \in \mathbb{N}$$

y por lo tanto

$$Z(G) \neq \{e\}$$

□

Teorema 80 *Sea X un conjunto no vacío y G un grupo entonces*
X es un G-espacio si y sólo si existe un homomorfismo de G en $Biy(X)$

Demostración: Dada la acción

$$\begin{array}{rccc} \cdot : & G \times X & \longrightarrow & X \\ & (g,x) & \longmapsto & g \cdot x \end{array}$$

se define el homomorfismo

$$\begin{array}{rccccc} \phi : & G & \longrightarrow & Biy(X) & & \\ & g & \longmapsto & \phi_g : & X & \longrightarrow & X \\ & & & & x & \longmapsto & g \cdot x \end{array}$$

Note que $\phi_g \circ \phi_h = \phi_{gh}$, luego es un homomorfismo.

Inversamente tenemos que

$$\begin{array}{rccc} T : & G & \longrightarrow & Biy(X) \\ & g & \longmapsto & T_g \end{array}$$

es un homomorfismo, se define la acción

$$\begin{array}{rccc} \cdot : & G \times X & \longrightarrow & X \\ & (g,x) & \longmapsto & g \cdot x = T_g(x) \end{array}$$

Note que $T(e) = Id$, luego $e \cdot x = T_e(x) = Id(x) = x$.

Además T cumple con

$$T_{gh} = T_g \circ T_h$$

luego se tiene que $(gh) \cdot x = g \cdot (h \cdot x)$. □

Ejemplo 63 *Notemos que*

$$\begin{array}{rccc} h : & \mathbb{R}^* & \longrightarrow & Biy(\mathbb{R}) \\ & a & \mapsto & h_a \end{array}$$

es un homomorfismo, donde h_a es una homotecia. Entonces, por el teorema anterior tenemos:

$$\begin{array}{rccccc} \cdot : & \mathbb{R}^* \times \mathbb{R} & \longrightarrow & \mathbb{R} & & \\ & (a,x) & \mapsto & a \cdot x & = h_a(x) = ax \end{array}$$

es una acción.

Teorema 81 (Cayley) *Todo grupo es isomorfo a un subgrupo de permutaciones*

Demostración: Sabemos que G actúa sobre G por izquierda, por la propiedad anterior tenemos,

$$\begin{array}{rccccc} \phi : & G & \longrightarrow & Biy(G) & & \\ & g & \longmapsto & \phi_g : & G & \to & G \\ & & & & x & \longmapsto & g \cdot x \end{array}$$

es un homomorfismo de grupo.

Calculemos el

$$ker\phi = \{g \in G \mid \phi_g = Id\} = \{e\},$$

entonces ϕ es un monomorfismo, luego se tiene que

$$G \simeq Im\phi \leq Biy(G).$$

Un caso particular lo tenemos cuando G es finito de orden n, entonces

$$G \leq Biy(G) = S_n.$$

□

Observación: Un ejemplo importante a considera, es la acción natural del grupo sobre las clases laterales izquierda, para ello sea $H \leq G$ y la acción sobre G/H, dada por $g \cdot xH = (gx)H$, induce el siguiente homomorfismo.

$$\begin{array}{rccccccc} \phi: & G & \longrightarrow & Biy(G/H) & & & & \\ & g & \longmapsto & \phi_g: & & G/H & \longrightarrow & G/H \\ & & & & & xH & \longmapsto & gxH \end{array}$$

Cuyo kernel esta dado por:

$$\begin{aligned} g \in ker\phi &\Leftrightarrow \phi_g = Id \\ &\Leftrightarrow gxH = xH \quad \forall xH \in G/H \\ &\Rightarrow gH = H \\ &\Rightarrow g \in H \end{aligned}$$

es decir,

$$ker\phi \subseteq H.$$

Propiedad 82 *Sea G un grupo finito y $H < G$, tal que, $[G:H] = p$ y p es el menor primo que divide a $|G|$ entonces*

$$H \trianglelefteq G.$$

Demostración: De la observación anterior tenemos tenemos $K = ker\phi \subset H$, además

$$G/K \simeq Im\phi \leq S_p$$

luego tenemos que $[G:K] \mid p!$, es decir,

$$[G \ : \ K] = (p_1)^{\alpha_1} \cdots (p_r)^{\alpha_r}$$

Supongamos que p_i primos menores que p. Pero cualquier divisor de $[G \ : \ K]$ divide a $|G|$, entonces $[G \ : \ K] = p$ ó 1, pero no es posible que $G = K$, por lo tanto $H = K$, así tenemos $H \trianglelefteq G$. □

Definición 19 *Sean X un G-espacio finito, y $n < |X|$.*

*Se dice que G actúa n-**transitivo** sobre X si y sólo si para cualquier conjunto ordenado $\{x_1, \ldots, x_n\}$ e $\{y_1, \ldots, y_m\}$. Existe $g \in G$ tal que $g \cdot x_i = y_i$.*

*En particular, si $n = 1$ se dice G actúa **transitivamente** en X.*

Ejemplo 64

1. *S_n actúa transitivamente sobre $X = \{1, 2, \ldots, n\}$.*
2. *$GL_2(K)$ actúa transitivamente sobre $K^2 - \{0\}$.*

Observación: En el caso de las acciones transitivas, entonces existe una sola órbita.
Además si G finito, entonces

$$|G| = |G_x| \cdot |X|.$$

1.15.1. Problemas Propuestos

Problema 54.

Sea G un grupo y la función

$$\cdot : \mathbb{Z}_2 \times G \to G,$$
$$\bar{0} \cdot g = g; \quad \bar{1} \cdot g = g^{-1}$$

1. Demostrar que $\cdot$ es un acción
2. ¿Cuántas elementos puede tener una órbitas?
3. Demostrar que, si $|G|$ es par entonces el número de elementos de orden 2 es impar

Problema 55.

Sea G el grupo de simetría del pentágono con la composición

$$X = \{(x, y) \in \mathbb{N}^* \times \mathbb{N}^* \quad : \quad x \leq 5 \wedge y \leq 5\}$$

y la acción

$$\cdot : G \times X \to X, \ g \cdot (x, y) = (g \cdot x, g \cdot y)$$

Determinar la órbita $O_{(1,3)}$ y $Stab_{(1,3)}$.
Determinar el número de órbitas y su cardinal.

Problema 56.

Determinar el valor de verdad de las siguientes proposiciones. JUSTIFIQUE

1. $F : \mathbb{R}^+ \times \mathbb{R} \to \mathbb{R}$; con $F(a, x) = ax$ es una acción
2. Dada la función $F : \mathbb{R} \times Biy(\mathbb{R}) \to Biy(\mathbb{R})$, definida por

$$F(a, f)(x) = f(x + a)$$

entonces F es una acción.

3. Dada la función $F : \mathbb{R}^* \times Biy(\mathbb{R}^*) \to Biy(\mathbb{R}^*)$, definida por

$$F(a, f)(x) = f(ax)$$

entonces F es una acción.

4. Si $H = \{h_t \in F(\mathbb{R}, \mathbb{R}) \mid h_t \text{ homotecia, con } t \in \mathbb{R}\}$ y
$T : \mathbb{R} \times H \to H.$ tal que $T(t, h_a) = h_{ta}$ es una acción

5. $\mathcal{A} = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{C}) \mid d = 1; c = 0 \right\}$ y
$L : \mathcal{A} \times \mathbb{C} \to \mathbb{C}$ donde $L([b_{ij}], x) = b_{11}x + b_{12}$ es una acción

6. Dada la función $T : \mathbb{R} \times M_2(\mathbb{R}) \to M_2(\mathbb{R})$, definida por

$$T\left(t, \begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) = \begin{pmatrix} a+t & b-t \\ c-t & d+2t \end{pmatrix}$$

entonces T es una acción.

7. Sea $A \in M_2(\mathbb{R})$ y la función $T_A : \mathbb{R} \times M_2(\mathbb{R}) \to M_2(\mathbb{R})$, definida por
$T_A(t, B) = B + tA$ entonces T_A es una acción.

Problema 57.

Dado el grupo de las matrices triangulares superiores invertibles, es decir

$$\mathcal{B} = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{R}) \;\middle|\; c = 0 \right\}$$

y la acción dada por

$$\begin{array}{rccc} \cdot : & \mathcal{B} \times \mathbb{R}^2 & \to & \mathbb{R}^2 \\ & \left(\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}, (x, y) \right) & \to & (ax + by, dy) \end{array}$$

Determinar la cantidad o el número de órbitas, es decir, un sistema de representante de las clases de equivalencia.

Problema 58.

Dado el subgrupo

$$\mathcal{U}(\mathbb{C}) = \{u \in \mathbb{C} \mid (\exists n \in \mathbb{N})(u^n = 1)\} \leq \mathbb{C}^*$$

y la función

$$\begin{array}{rccc} \cdot & \mathcal{U}(\mathbb{C}) \times \mathbb{C} & \to & \mathbb{C} \\ & (x, y) & \to & xy \end{array}$$

Demostrar $\cdot$ es una acción.

Problema 59.

Dado la acción dada por

$$\begin{array}{rccc} \cdot & \mathbb{R}^* \times \mathbb{R} & \to & \mathbb{R} \\ & (a,x) & \to & ax \end{array}$$

Determinar la cantidad o el número de órbitas, es decir, un sistema de representante de las clases de equivalencia.

Problema 60.

Dada la acción definida por

$$\begin{array}{rccc} \cdot : & \mathbb{R}^+ \times \mathbb{R}^2 & \to & \mathbb{R}^2 \\ & (a,(x,y)) & \to & (x+\ln(a), ay) \end{array}$$

Determinar un sistema de representante de las órbitas o clases.

Problema 61.

Sea $G = Aut(\mathbb{Z}_6)$ el grupo de automorfismo de $\mathbb{Z}_6$ con la composición y la acción

$$\cdot : G \times \mathbb{Z}_6 \to \mathbb{Z}_6,\ g \cdot x = g(x)$$

Determinar el número de órbitas y su cardinal de cada una de ellas..

1.16. Grupo de Permutación

Sea X un conjunto no vacío. El grupo $(Biy(X), \circ)$ es llamado grupo `simétrico` o de `permutaciones` de X.

Propiedad 83 *Si $\rho : X \longrightarrow Y$ es una biyección, entonces*

$$\overline{\rho} : Biy(Y) \longrightarrow Biy(X),\ \text{con } \overline{\rho}(f) = \rho^{-1} \circ f \circ \rho$$

es un isomorfismo de grupo

Observación: En particular, sean $J_n = \{1, 2, \ldots, n\}$ e Y un conjunto de cardinal n, luego tenemos que

$$Biy(J_n) \simeq Biy(Y)$$

es decir, todos los grupo de permutaciones de un conjunto de n elementos son isomorfos.

Por lo anterior, estudiaremos en forma especial el Grupo de Permutaciones

$$S_n = \sigma_n = Biy(J_n)$$

el cual es llamado grupo simétrico y su cardinal es $n! = |S_n|$.
Notación: Si $\sigma \in S_n$, la denotaremos por

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$$

Estructura de Ciclos Sea $\sigma \in S_n$ y

$$H = \langle \sigma \rangle = \{\sigma^i \mid i \in \mathbb{N}\}$$

basta considerar el exponente un número natural, ya que el grupo S_n es finito.

Entonces H actúa en $J_n = \{1, 2, \ldots, n\}$, en forma natural. Es decir

$$\begin{array}{rccc} \cdot \ : & H \times J_n & \longrightarrow & J_n \\ & (\sigma^i, x) & \longmapsto & \sigma^i(x) \end{array}$$

Sean $O_1, \ldots O_r$ las órbitas distintas de esta acción. Para cada una de las órbitas O_i, construimos una permutación σ_i de S_n, definida por

$$\sigma_i(x) = \begin{cases} \sigma(x) & x \in O_i \\ x & x \notin O_i \end{cases}$$

llamada ciclo asociado a σ.

Notemos que $x \in O_i$

$$\sigma_i^j(x) = \sigma^j(x).$$

Luego

$$\begin{array}{rcl} O_i & = & \{x, \sigma_i(x), \sigma_i^2(x), \ldots\} \\ O_i & = & \{x, \sigma(x), \sigma^2(x), \ldots\} \end{array}$$

Además, si $|O_i| = r_i$, entonces

$$O_i = \{x, \sigma_i(x), \sigma_i^2(x), \ldots, \sigma_i^{r_i - 1}(x)\}.$$

Propiedad 84 *Sea $\sigma \in S_n$ y con las notaciones anteriores, entonces*

1. $|\sigma_i| = r_i \Leftrightarrow |O_i| = r_i$
2. $i \neq j \Rightarrow \sigma_i \sigma_j = \sigma_j \sigma_i$
3. $\sigma = \sigma_1 \sigma_2 \cdots \sigma_r$
4. $|\sigma| = MCM\{|\sigma_i|\}$

Observación: note que los σ_i están únicamente determinado por las órbitas.
Notación: El ciclo σ_i se denota por:

$$\sigma_i = (x \ \sigma_i(x) \ \sigma_i^2(x) \cdots \sigma_i^{r_i - 1}(x))$$

Ejemplo 65 *Sea* $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 1 & 5 & 7 & 4 & 6 \end{pmatrix} \in S_7$, *luego*

Veremos sus órbitas, las cuales son dos y están dadas por

1. $O_1 = \{1, 2, 3\}$

2. $O_2 = \{4, 5, 6, 7\}$

Con las cuales construimos los ciclos

1. $\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 1 & 4 & 5 & 6 & 7 \end{pmatrix} = (1\ 2\ 3)$

2. $\sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 2 & 3 & 5 & 7 & 4 & 6 \end{pmatrix} = (4\ 5\ 7\ 6)$

Luego $\sigma = (1\ 2\ 3)(4\ 5\ 7\ 6)$ *y* $|\sigma| = 12$.

Propiedad 85 *En el grupo* S_n *y* $m \leq n$*, tenemos*

$$(x_1\ x_2\ \cdots\ x_m)^{-1} = (x_1\ x_m\ \cdots\ x_2)$$

Demostración: Basta evaluar para obtener la igual funcional □

Propiedad 86 *Toda permutación es producto de transposiciones (ciclos de largo* 2*).*

Demostración: Basta considerar un ciclo

$$(x) = (x\ x_1)(x_1\ x) = (1\ x)(x\ 1), \quad x \neq 1$$

$$(x_1\ x_2 \quad x_m) = (x_1\ x_m)(x_1\ x_{m-1}) \cdots (x_1\ x_2).$$

□

Propiedad 87 *Sea* $\sigma \in S_n$ *y* $m \leq n$*, entonces*

$$\sigma(x_1\ x_2\ \cdots x_m)\sigma^{-1} = (\sigma(x_1)\ \sigma(x_2)\ \cdots \sigma(x_m))$$

Demostración: Evaluemos ne z

$$\sigma(x_1\ x_2\ \cdots x_m)\sigma^{-1}(z)$$

La demostración, lo obtenemos en tres caso.

Primera parte $z \neq \sigma(x_i)$, luego $\sigma^{-1}(z) \neq x_i$

$$\sigma(x_1\ x_2\ \cdots x_m)\sigma^{-1}(z) = \sigma\sigma^{-1}(z) = z$$

Segundo caso $z = \sigma(x_m)$

$$\sigma(x_1\ x_2\ \cdots x_m)\sigma^{-1}(z) = \sigma(x_1\ x_2\ \cdots x_m)(x_m) = \sigma(x_1)$$

Tercer caso $z = \sigma(x_i),\ i \neq m$.

$$\sigma(x_1\ x_2\ \cdots x_m)\sigma^{-1}(z) = \sigma(x_1\ x_2\ \cdots x_m)(x_i) = \sigma(x_{i+1})$$

Luego tenemos

$$\sigma(x_1\ x_2\ \cdots x_m)\sigma^{-1} = (\sigma(x_1)\ \sigma(x_2)\ \cdots \sigma(x_m))$$

□

Propiedad 88 *Sean $\sigma,\ \tau \in S_n$. σ es conjugado con τ si y sólo si tienen la misma estructura de ciclos.*

Demostración: Supongamos que σ es conjugado con τ, luego existe γ, tal que

$$\gamma\sigma\gamma^{-1} = \tau$$

además, σ tiene una estructura de ciclos, propiedad 84, luego existe

$$\sigma = \sigma_1\sigma_2\sigma_3\cdots\sigma_r$$

Aplicando la propiedad anterior $\gamma\sigma_i\gamma^{-1}$ es un ciclos y son disjuntos, ya que γ es biyectiva.

$$\tau = (\gamma\sigma_1\gamma^{-1})(\gamma\sigma_2\gamma^{-1})(\gamma\sigma_3\gamma^{-1})\cdots(\gamma\sigma_r\gamma^{-1})$$

luego τ, tiene la misma estructura de ciclos.

En la otra dirección, Sean $\sigma y \tau$, dos tenga la misma estructura de ciclos, como los ciclos disjuntos conmutan ordenemos de modo que los ordenes sean iguales $|\tau_i| = |\sigma_i|$. es decir

$$\sigma_i = (x_{i,1}\ x_{i,2}\ \cdots x_{i,m}) = (y_{i,1}\ y_{i,2}\ \cdots y_{i,m}) = \tau_i$$

Luego $z \in J_n$, luego $z \in \cup O_i$, propiedad 84, existe único j, tal que $z \in O_j$, así $z = x_{j,s}$ único, por lo cual, se define $\gamma(z) = y_{j,s}$, claramente γ es biyectiva.

De lo cual se obtiene que

$$\gamma\sigma\gamma^{-1} = \tau$$

□

Ejemplo 66 *Determinar las clases de conjugación de S_4.*
Solución: *Por la propiedad anterior tenemos que un sistema de representantes es:*

$$R = \{(1\ 2\ 3\ 4), (1\ 2\ 3), (1\ 2)(3\ 4), (1\ 2), (1)\}$$

es decir,

$$S_4 = O_{(1\ 2\ 3\ 4)} \dot\cup O_{(1\ 2\ 3)} \dot\cup O_{(1\ 2)(3\ 4)} \dot\cup O_{(1\ 2)} \dot\cup O_{(1)}$$

donde, por ejemplo

$$O_{(\ 1\ 2\ 3)} = \{(\ 1\ 2\ 3), (\ 1\ 3\ 2), (\ 1\ 2\ 4), (\ 1\ 4\ 2), (\ 1\ 3\ 4), (\ 1\ 4\ 3), (\ 2\ 3\ 4), (\ 2\ 4\ 3)\}$$

la cual es la órbita que contiene los 3-ciclos de S_4. □

Observación: Para determinar todas las estructuras cíclicas de S_n con facilidad, necesitamos definir una partición de n, lo cual corresponde a una $m-upla$ formada por numeros naturales no nulos, decrecientes, tales que su suma es n. por ejemplo las particiones de 4 son $(4), (3,1), (2,2), (2,1,1), (1,1,1,1)$.

Propiedad 89 *Las estructuras cíclicas de S_n están únicamente determinadas por las particiones de n.*

Ejemplo 67 *Determinar las estructuras cíclicas de S_4.*

Solución: Notemos que

$$\begin{aligned} 4 &= 4 \\ 4 &= 3+1 \\ 4 &= 2+2 \\ 4 &= 2+1+1 \\ 4 &= 1+1+1+1 \end{aligned}$$

luego, las estructuras cíclicas de S_4 son:

$$\begin{aligned} (4) &\longleftrightarrow (\cdot\cdot\cdot\cdot) \\ (3,1) &\longleftrightarrow (\cdot\cdot\cdot)(\cdot) \\ (2,2) &\longleftrightarrow (\cdot\cdot)(\cdot\cdot) \\ (2,1,1) &\longleftrightarrow (\cdot\cdot)(\cdot)(\cdot) \\ (1,1,1,1) &\longleftrightarrow (\cdot)(\cdot)(\cdot)(\cdot) \end{aligned}$$

es decir,

$$S_4 = O_{(1\ 2\ 3\ 4)} \dot{\cup} O_{(1\ 2\ 3)} \dot{\cup} O_{(1\ 2)(3\ 4)} \dot{\cup} O_{(1\ 2)} \dot{\cup} O_{(1)}$$

□

Ejercicio 68 *Determinar las órbitas de la acción*

$$\begin{array}{rccc} \cdot : & S_5 \times S_5 & \longrightarrow & S_5 \\ & (\sigma, \tau) & \mapsto & \sigma\tau\sigma^{-1} \end{array}$$

Ejercicio 69 *Considere la acción por conjugación sobre S_9.*
Calcular el cardinal de la orbita $O_{(124)(35)(87)}$.

Propiedad 90

$$S_n = \langle\ (1\ 2\ \cdots\ n),\ (1\ 2)\ \rangle$$

Demostración: Sea $\tau = (1\ 2\ \cdots\ n)$ y $\sigma = (1\ 2)$, luego $\tau^{-1} = (n\ n-1\ \cdots\ 2\ 1)$, definimos $H =< \tau, \sigma >$.

Recordemos que por la propiedad 84, se tiene que toda permutación es producto de ciclos y por la propiedad 86, se tiene que son producto de transposiciones, luego basta probar que las transposiciones pertenecen a H.

Para ello veamos los siguientes productos

i) Conjugando obtenemos los siguientes elementos

$$\begin{aligned} \tau(1\ 2)\tau^{-1} &= (2\ 3) \\ \tau(2\ 3)\tau^{-1} &= (3\ 4) \\ (\tau)^{s-1}(1\ 2)(\tau^{-1})^{s-1} &= (s\ s+1) \quad s < n \\ \tau(n-1\ n)\tau^{-1} &= (n\ 1) \end{aligned}$$

es decir

$$(1\ 2), (2\ 3),\ \cdots\ , (n-1\ n), (n\ 1) \in H$$

ii) Además

$$(1\ 2)(2\ 3)(1\ 2) = (1\ 3)$$
$$(1\ 3)(3\ 4)(1\ 3) = (1\ 4)$$
$$(1\ r)(r\ r+1)(1\ r) = (1\ r+1).$$

con lo cual obtenemos

$$(1\ 2), (1\ 3), \cdots, (1\ n) \in H$$

iii) Finalmente sean $x \neq 1 \neq y$ luego

$$(x\ y) = (y\ 1)(1\ x) \in H$$

Con lo cual hemos obtenido que todas las transposiciones pertenece a H y como ellas generan el grupo simétrico entonces obtenemos $G = H$.

□

Ejercicio 70 *Demostrar que S_n actúa por permutación en las variables sobre $K[x_1, \ldots, x_n]$, es decir,*

$$\sigma \cdot p(x_1, x_2, \ldots, x_n) = p(x_{\sigma(1)}, \ldots, x_{\sigma(n)}).$$

y respeta el producto polinomial

Observación: Con la acción anterior y el polinomio

$$q(x_1, \ldots, x_n) = \prod_{i<j}(x_i - x_j)$$

podemos verificar que

$$\sigma \cdot q(x_1, \ldots, x_n) = \prod_{i<j}(x_{\sigma(i)} - x_{\sigma(j)}) = \pm q(x_1, \ldots, x_n)$$

Ya que, no hay elementos repetido, la cantidad es la correcta. Con lo cual obtenemos que la órbita

$$O_{q(x_1,\ldots,x_n)} = \{q(x_1, \ldots, x_n), -q(x_1, \ldots, x_n)\}$$

y el estabilizador

$$Est_{q(x_1,\ldots,x_n)} = \{\sigma \in S_n \mid \sigma \cdot q(x_1, \ldots, x_n) = q(x_1, \ldots, x_n)\}$$

al reescribir obtenemos que

$$Est_{q(x_1,\ldots,x_n)} = \left\{ \sigma \in S_n \quad \middle| \quad \frac{\prod_{i<j}(x_{\sigma(i)} - x_{\sigma(j)})}{\prod_{i<j}(x_i - x_j)} = 1 \right\} = A_n$$

Con lo anterior hemos demostrado que

Propiedad 91 *A_n es un subgrupo de S_n, llamado* ***grupo alternado***

Definición 20 *Con las notaciones anteriores y el hecho $(\{1,-1\},\cdot)$ es un grupo, definimos la función* ***signo*** *dada por:*

$$\begin{array}{rccl} Sg: & S_n & \longrightarrow & \{1,-1\} \\ & \sigma & \longmapsto & Sg(\sigma)=\frac{\sigma\cdot q}{q} \end{array}$$

Observación: La función signo es un homomorfismo, es decir,

$$Sg(\sigma\circ\tau)=Sg(\sigma)Sg(\tau).$$

Note que el grupo alternado es igual a $A_n=\ker(Sg)$

Definición 21

1. *Se dice que $\sigma\in S_n$ es* ***par*** *si y sólo si $Sg(\sigma)=1$*
2. *Se dice que $\sigma\in S_n$ es* ***impar*** *si y sólo si $Sg(\sigma)=-1$*

Propiedad 92 *En el grupo S_n y $m\leq n$, entonces*

1. *$Sg(x_1\ x_2\ \cdots\ x_m)=(-1)^{m+1}$*
2. *$\sigma\in S_n$ es par si y sólo si σ es producto par de transposiciones*
3. *$\sigma\in S_n$ es impar si y sólo si σ es producto impar de transposiciones*

Propiedad 93

$$A_n=\langle\ \sigma^2\mid\sigma\in S_n\ \rangle$$

Demostración:
$\subseteq$) $\sigma^2\in A_n$, entonces

$$H=\langle\ \sigma^2\ \mid\ \sigma\in S_n\ \rangle\subseteq A_n$$

$\supseteq$) Como todo elemento de A_n se escribe como un producto par de transposiciones, basta demostrar que $(x\ y)(z\ w)\in H$, para ello veremos los siguientes casos

i) Si $|\{x,y,z,w\}|=4$, entonces $(x\ y)(z\ w)=(x\ z\ y\ w)^2\in H$

ii) Si $|\{x,y,z,w\}|=3$, entonces $(x\ y)(z\ x)=(x\ y\ z)^2\in H$

Así tenemos que

$$A_n=\langle\ \sigma^2\mid\sigma\in S_n\ \rangle$$

□

Propiedad 94 *Sean $x,y,z\in\{1,\ldots,n\}$ distintos*

1. *A_n esta generado por los 3-ciclos*

$$A_n = \langle \{(x\ y\ z\ ) \mid |\{x,y,z\}| = 3\} \rangle$$

2. *Si x, y fijos, entonces*

$$A_n = \langle \{(x\ y\ z\ ) \mid 1 \leq z \leq n,\ x \neq z \neq y\} \rangle$$

Demostración: Recordemos que toda permutación de A_n es producto part de transposiciones, luego tenemos que, verificar $(x\ y)(z\ w)$.

Si hay una valor repetido tenemos salvo orden

$$(x\ y)(z\ x) = (x\ z\ y)$$

Si no hay un valor repetido tenemos

$$(x\ y)(z\ w) = [(x\ y)(z\ y)][(z\ y)(z\ w)] = (x\ y\ z)(z\ w\ y).$$

Sea $H = \langle\ (x\ y\ z\ ) \mid 1 \leq z \leq n,\ x \neq z \neq y \rangle$, entonces por la primera parte basta demostrar que todo 3-ciclo $(a\ b\ c)$ pertenece a H.

Para esto veremos los casos pertinentes, salvo variable

1. Si hay dos repetido, sea $a \notin \{x, y\}$

$$(y\ x\ a) = (x\ y\ a)^2 = (x\ a\ y)$$

luego tenemos los elementos

$$(x\ y\ a), (y\ x\ a), (x\ a\ y), (y\ a\ x)$$

2. Si hay un elemento repetido, $\{x, y\} \cap \{a, b\} = \emptyset$

a)

$$(x\ a\ b) = (x\ y\ b)(x\ a\ y) = (x\ y\ b)(x\ y\ a)^2$$

b)

$$(y\ a\ b) = (x\ y\ b)^2(x\ y\ a)$$

3. Si no hay elementos repetidos, $\{x, y\} \cap \{a, b, c\} = \emptyset$

$$(a\ b\ c) = (x\ y\ a)^2(x\ y\ c)(x\ y\ b)^2(x\ y\ a)$$

□

Propiedad 95 *Sea $n > 3$, entonces*

$$[S_n, S_n] = A_n$$

Solución: Por demostrar que $[S_n, S_n] \subseteq A_n \quad \wedge \quad A_n \subseteq [S_n, S_n]$.

1. Sea $x \in [S_n, S_n]$, entonces veamos que:

   i) Si $x = [a, b] = aba^{-1}b^{-1}$

   $$Sg(x) = Sg(a)Sg(b)Sg(a)^{-1}Sg(b)^{-1} = Sg(a)^2Sg(b)^2 = 1$$

   Luego, $x \in A_n$.

   ii) Si $x = [a_1, b_1][a_2, b_2] \cdots [a_r, b_r]$

   $$Sg(x) = Sg([a_1, b_1])Sg([a_2, b_2]) \cdots Sg([a_r, b_r]) = 1$$

   Luego, $x \in A_n$.

   Por lo tanto $[S_n, S_n] \subseteq A_n$.

2. Nótese que para todo $1 \neq x \neq 2$ tenemos:

   $$(1\ 2)(1\ 2\ x)(1\ 2)(1\ x\ 2) = (1\ 2\ x) \in [S_n, S_n]$$

   luego, el conjunto $\{(1\ 2\ x) \mid 2 < x \leq n\}$ está contenido en $[S_n, S_n]$, entonces

   $$\langle\{(1\ 2\ x) \mid 2 < x \leq n\}\rangle \subseteq [S_n, S_n]$$

   pero, por la segunda parte de la proposición anterior tenemos:

   $$A_n = \langle\{(1\,2\,x) \mid 2 < x \leq n\}\rangle \subseteq [S_n, S_n]$$

□

Propiedad 96 *Demostrar que*

$$[A_n, A_n] = A_n \qquad n \geq 5$$

1.16.1. Problemas Propuestos

Problema 62.

Determinar el orden de

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 5 & 8 & 7 & 1 & 3 & 4 & 6 & 10 & 2 & 9 & 12 & 11 \end{pmatrix} \in S_{12}$$

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 5 & 8 & 7 & 1 & 3 & 4 & 6 & 10 & 11 & 9 & 2 \end{pmatrix}^2 \in S_{11}.$$

Problema 63.

Sean

$$\begin{aligned}\alpha &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 8 & 9 & 7 & 10 & 11 & 12 & 1 & 5 & 2 & 6 & 3 & 4 \end{pmatrix} \text{ y} \\ \beta &= \begin{pmatrix} 1 & 5 & 3 & 9 & 10 & 12 \end{pmatrix}\begin{pmatrix} 1 & 6 & 9 & 7 & 12 & 2 \end{pmatrix}\end{aligned}$$

a) Exprese α como producto de ciclos disjuntos

b) Determine el orden de α

c) Resolver en S_{12}; $\beta\alpha Z = \alpha\beta$

Problema 64.

Sean

$$\begin{aligned}\alpha &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 8 & 9 & 7 & 10 & 11 & 12 & 1 & 5 & 2 & 6 & 3 & 4 \end{pmatrix} \text{ y} \\ \beta &= \begin{pmatrix} 1 & 4 & 3 & 5 & 10 & 12 \end{pmatrix}\begin{pmatrix} 1 & 6 & 9 & 7 & 12 & 3 \end{pmatrix}\end{aligned}$$

a) Exprese α como producto de ciclos disjuntos.

b) Determine el orden de α.

c) Resolver en S_{12}; $\beta\alpha Z = \alpha\beta$.

Problema 65.

Sean

$$\begin{aligned}\alpha &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 8 & 9 & 7 & 10 & 11 & 4 & 12 & 5 & 2 & 6 & 1 & 3 \end{pmatrix} \text{ y} \\ \beta &= \begin{pmatrix} 1 & 4 & 3 & 5 & 10 & 12 \end{pmatrix}\begin{pmatrix} 1 & 6 & 9 & 7 & 12 & 3 \end{pmatrix}\end{aligned}$$

a) Exprese α como producto de ciclos disjuntos.

b) Determine el orden de α.

c) Resolver en S_{12}; $\beta\alpha Z = \alpha\beta$.

Problema 66.

Sea $\alpha \in S_9$ tal que

$$(1\ 2\ 5\ 6\ 8\ 9)\,\alpha\,(1\ 7\ 8\ 9)^2 = (1\ 2)\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 8 & 7 & 1 & 3 & 4 & 6 & 9 & 2 \end{pmatrix}$$

Determine el orden y el signo de α

Problema 67.

Sean $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 5 & 2 & 6 & 4 \end{pmatrix}$, $\beta = \begin{pmatrix} 2 & 3 & 4 & 5 & 1 \end{pmatrix}$, $\gamma = \begin{pmatrix} 1 & 3 & 6 & 5 & 2 \end{pmatrix}$.

Resolver ecuación en S_6

$$\alpha \circ Z \circ \gamma = \beta$$

Problema 68.

Sea $\alpha \in S_9$ tal que

$$(1\ 2\ 5\ 6\ 8\ 9)\,\alpha\,(1\ 7\ 8\ 9)^2 = (1\ 2)\,(3\ 4\ 6\ 7\ 1\ 8)$$

Exprese α como producto de ciclos disjuntos y determine el orden y el signo.

Problema 69.

Resolver la siguiente ecuación en S_9

$$(1\ 3\ 4\ 5\ 6)(2\ 3\ 4\ 1)\alpha(9\ 5\ 8\ 3)^2(1\ 2) = (1\ 5\ 9\ 2)(3\ 7\ 1\ 4)$$

Además calcular el orden y el signo del elemento α

Problema 70.

Sean $n \geq 4$, $H \trianglelefteq S_n$ y H contiene un 3-ciclo.

Demuestre que

$$A_n \subseteq H.$$

Problema 71.

Dada la acción por conjugación

$$\begin{array}{rccc} \cdot : & S_5 \times S_5 & \to & S_5 \\ & (g, x) & \to & gxg^{-1} \end{array}$$

Determinar un sistema de representante de las órbitas o clases.

Problema 72.

Sea $G = S_4$ el grupo de permutaciones de 4 elementos

$$X = \{(x, y, z) \in \mathbb{N}^* \times \mathbb{N}^* \times \mathbb{N}^* \quad : \quad x \leq 4 \wedge y \leq 4 \wedge z \leq 4\}$$

y la acción

$$\cdot : G \times X \to X,\ g \cdot (x, y, z) = (g \cdot x, g \cdot y, g \cdot z)$$

Determinar el número de órbitas y su cardinal

1.17. Grupos Abelianos Finitos

Propiedad 97 *Sea G un grupo abeliano finito entonces*

i) Existen números primos $p_1, p_2, ..., p_r$ y números naturales $n_1, n_2, ..., n_r$ tales que

$$G \simeq \mathbb{Z}_{p_1^{n_1}} \times \mathbb{Z}_{p_2^{n_2}} \times \cdots \times \mathbb{Z}_{p_r^{n_r}}$$

además si existen números primos $q_1, q_2, ..., q_s$ y números naturales $m_1, m_2, ..., m_s$ tales que

$$G \simeq \mathbb{Z}_{q_1^{m_1}} \times \mathbb{Z}_{q_2^{m_2}} \times \cdots \times \mathbb{Z}_{q_s^{m_s}}$$

entonces $r = s$ y existe $\sigma \in S_r$ tal que $p_i^{n_i} = q_{\sigma(i)}^{m_{\sigma(i)}}$

ii) Existen $d_1, d_2, \cdots, d_t$ números naturales tales que d_i/d_{i+1}

$$G \simeq \mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \cdots \times \mathbb{Z}_{d_t}$$

Ejemplo 71 *¿Cuántos grupos abeliano de orden 15 existen?*

Solución: Salvo isomorfismo existe solamente uno y es

$$\mathbb{Z}_3 \times \mathbb{Z}_5 \simeq \mathbb{Z}_{15}$$

□

Ejemplo 72 *¿Cuántos grupos abeliano de orden 16 existen?*

Solución: Salvo isomorfismo solamente hay 5 grupos

1. $\mathbb{Z}_{2^4}$
2. $\mathbb{Z}_{2^3} \times \mathbb{Z}_2$
3. $\mathbb{Z}_{2^2} \times \mathbb{Z}_2 \times \mathbb{Z}_2$
4. $\mathbb{Z}_{2^2} \times \mathbb{Z}_{2^2}$
5. $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$

□

Definición 22 *Si $k \in \mathbb{N}$ una partición de k es una $m-$upla, $(k_1, k_2, ..., k_m)$ de números naturales tales que*

$$k = \sum_{i=1}^{m} k_i, \qquad con\ 0 < k_i \leq k_{i+1}$$

Propiedad 98 *Sea $n \in \mathbb{N}$, tal que $n = p_1^{n_1} p_2^{n_2} \cdot \cdots p_r^{n_r}$, con p_i primos distintos y $p(n_i)$ es igual al número de particiones de n_i, entonces la cantidad de grupos abelianos de orden n es igual a*

$$\prod_{i=1}^{r} p(n_i)$$

1.17.1. Problemas Propuestos

Problema 73.

Determinar la cantidad de grupos abelianos salvo isomorfismo de orden $2^7 3^4 5^2$

Problema 74.

¿Cuántos grupos abelianos no isomorfos existen de orden $2^2 5^5 6^4$?

1.18. Teorema de Sylow

Definición 23 *Un grupo finito G, se dice un* ***p-grupo*** *si*

$$|G| = p^n \quad \forall n \in \mathbb{N},$$

con p un número primo.

Ejemplo 73 *Sea p un numero primo, los grupos $\mathbb{Z}_{p^n}$, $\mathbb{Z}_p^n$ son p-grupo.*
El grupo de simetrías del cuadrado es un 2-grupo de orden 8.

Definición 24 *Sea X un G-espacio.*
Se define el conjunto de ***puntos fijos***

$$Fix_G(X) = \{x \in X \mid (\forall g \in G)(\ g \cdot x = x)\ \}$$

Lema 99 *Sea G un p-grupo y X un G-espacio con $|X| < \infty$, entonces*

$$|X| \equiv |Fix_G(X)| \quad (p)$$

Demostración: Sea X un G-espacio, luego tenemos que

$$\begin{aligned} X &= \dot{\bigcup_{i\in I}} O_i \\ |X| &= \sum_{i\in I} |O_i| \\ |X| &= \sum_{i\in I,\ |O_i|=1} |O_i| + \sum_{i\in I,\ |O_i|>1} |O_i| \end{aligned}$$

Pero $|O_i| = 1$ si y sólo si $O_i = \{x_i\}$ es decir,

$$\{x_i\} = \{g \cdot x_i \mid g \in G\}$$

Así obtenemos que

$$\begin{aligned} \dot{\bigcup_{i\in I,\ |O_i|=1}} O_i &= \dot{\bigcup_{i\in I,\ |O_i|=1}} \{g \cdot x_i \mid g \in G\} \\ &= \{x \in X \mid (\forall g \in G)(\ g \cdot x = x)\ \} \\ &= Fix_G(X) \end{aligned}$$

Además tenemos que $1 < |O_i| = [G : G_{x_i}] = p^{n_i}$, es decir $1 < |O_i| \equiv 0\,(\text{mód } p)$, con lo cual

$$\begin{aligned} |X| &= \sum_{i\in I,\ |O_i|=1} |O_i| + \sum_{i\in I,\ |O_i|>1} |O_i| \\ |X| &= |Fix_G(X)| + \sum_{i\in I,\ |O_i|>1} |O_i| \qquad (\text{mód } p) \\ |X| &\equiv |Fix_G(X)| \qquad (\text{mód } p) \end{aligned}$$

□

Propiedad 100 (Teorema de Cauchy) *Sea p un número primo tal que p divide a $|G|$, entonces en G hay un elemento de orden p.*

Demostración: Sea p un número primo tal que $p \not| |G|$, entonces definimos

$$X = \{(g_1, \ldots, g_p) \in G^p \mid g_1 \cdots g_p = e\}$$

Primera Parte. $|X| = |G|^{p-1}$, para demostrar esta afirmación veremos que

$$\begin{aligned} (g_1, \ldots, g_p) \in X &\Leftrightarrow\ g_1 \cdots g_p = e \\ &\Leftrightarrow\ g_p = (g_1 \cdots g_{p-1})^{-1} \end{aligned}$$

Con lo cual, se construye la siguiente biyección

$$\begin{array}{rccc} \varphi & G^{p-1} & \longrightarrow & X \\ & (g_1, \ldots, g_{p-1}) & \longmapsto & (g_1, \ldots, g_{p-1}, (g_1 \cdots g_{p-1})^{-1}) \end{array}$$

Segunda Parte. Sea $H =< (1\ 2\ \ldots\ p) > \leq S_p$, sabemos que $|H| = p$ y además

$$\begin{aligned} (g_1, \ldots, g_p) \in X &\Leftrightarrow\ g_1 \cdots g_p = e \\ &\Leftrightarrow\ (g_1)^{-1} g_1 \cdots g_p g_1 = e \\ &\Leftrightarrow\ g_2 \cdots g_p g_1 = e \\ &\Leftrightarrow\ (g_2, \ldots, g_p, g_1) \in X \end{aligned}$$

De lo cual se tiene que H actúa en X en los subíndices

$$\begin{array}{rccc} \cdot : & H \times X & \longrightarrow & X \\ & (\sigma, (g_1, \ldots, g_p)) & \longmapsto & (g_{\sigma(1)}, \ldots, g_{\sigma(p)}) \end{array}$$

Tercera Parte. Sabemos por Lema 99 que

$$\begin{aligned} |X| &\equiv |Fix_H(X)| \quad (p) \\ 0 &\equiv |Fix_H(X)| \quad (p) \\ |Fix_H(X)| &= \dot{p} \end{aligned}$$

Pero $(e, \cdots, e) \in Fix_H(X)$, luego existe al menos otro elemento. Sea $(e, \cdots, e) \neq (g_1, \ldots, g_p) \in Fix_H(X)$, así tenemos que

$$(g_1, \ldots, g_p) = (g_2, \ldots, g_{p-1}, g_1)$$

de donde obtenemos que

$$g_1 = g_2 = g_3 = \cdots = g_p \neq e$$

y es distinto de neutro luego tiene orden p. □

Corolario 101 *Sea G un grupo finito.*

G es un p-grupo si y sólo si todo elemento tiene como orden una potencia de p.

Demostración: Sea G un p grupo finito, luego $|g|$ divide a G, luego $|g|$ es una potencia de p.

En el otro sentido, si G es un grupo finito y todos los elementos tine orden una potencia de p, se q un número primo que divide al $|G|$, luego teorema de Cauchy existe un elemento de orden $q = p$. luego el único primo que divide a $|G|$ es p, por lo tanto $|G| = p^n$. □

Definición 25 *Se dice que G es un* `grupo simple` *si y sólo si G no tiene subgrupos normales no triviales, es decir, los únicos subgrupos normales son los triviales.*

Ejemplo 74 *Sea p un número primo Todos grupos de orden p son simple, ya que, es cíclico y todo elemento no nulo lo genera, por lo tanto los únicos subgrupos, son os triviales.*

Todos grupos G de orden p^2 no son simple, sabemos por teorema de Cauchy, que existe $g \in G$ de orden p, luego $[G :< g >] = p$, y es el menor primo que divide a orden del grupo, luego $< g > \trianglelefteq G$.

Propiedad 102 *Si H es un p-grupo de un grupo finito G, entonces*

$$[N_G(H) : H] \equiv [G : H] \pmod{p}.$$

Demostración: Considerar la acción $H \times G/H \longrightarrow G/H$, dada por $a \cdot bH = (ab)H$, por Lema 99. tenemos que

$$|G/H| \equiv |Fix_H(G/H)| \pmod{p}$$

pero

$$\begin{aligned} Fix_H(G/H) =& \{\ bH \in G/H \ \mid\ (\forall h \in H)(h \cdot bH = bH)\ \} \\ =& \{bH \in G/H \ \mid\ (\forall h \in H)((hb)H = bH) \ \} \\ =& \{bH \in G/H \ \mid\ (\forall h \in H)(b^{-1}(hb) \in H)\ \} \\ =& \{bH \in G/H \ \mid\ b^{-1}Hb \subseteq H\ \} \\ =& \ N_G(H)/H \end{aligned}$$

con lo cual obtenemos

$$|Fix_H(X)| \equiv [N_G(H) : H] \pmod{p}$$

□

Ejemplo 75 *Sea G un grupo de orden 33. Demostrar que todos p-subgrupos de G son normales.*

Solución: *Sean H un 3-subgrupo y K un 11-subgrupo de G.*

Notemos que

$$[G : K] = 3$$

donde 3 es el menor primo que divide al orden de G, entonces $K \trianglelefteq G$.

Ahora utilicemos la proposición anterior para probar que $N_G(H) = G$, es decir H es normal en G. Tenemos:

$$\begin{aligned} [N_G(H) : H] &\equiv [G : H] \quad (\text{mód } 3) \\ [N_G(H) : H] &\equiv 11 \quad (\text{mód } 3) \\ [N_G(H) : H] &\equiv 2 \quad (\text{mód } 3) \end{aligned}$$

luego

$$|N_G(H)| = |H|(3q + 2) = 9q + 6, \qquad q \in \mathbb{N}_0$$

Así tenemos las posibilidades

$$|N_G(H)| = 6, 15, 24, 33$$

pero las primeras tres las descartamos ya que no son divisores de 33 (por teorema de Lagrange). Luego $|N_G(H)| = 33$ y por lo tanto

$$N_G(H) = G$$

□

Ejercicio 76 *Demostrar que los grupos de orden 21 no son simples.*

Corolario 103 *Sea H un p-subgrupo del grupo finito G y p divide a $[G : H]$, entonces*

$$N_G(H) \neq H.$$

Demostración: Usando la proposición anterior tenemos

$$\begin{aligned} [N_G(H) : H] &\equiv [G : H] \quad (p) \\ [N_G(H) : H] &\equiv 0 \quad (p) \end{aligned}$$

Luego tenemos

$$[N_G(H) : H] \geq p$$

es decir, $N_G(H) \neq H$.

□

Teorema 104 (Primer Teorema de Sylow) *Si G es un grupo de orden $p^r m$, con p, m primos relativos. Entonces G contiene un subgrupo de orden p^i, para cada $1 \leq i \leq r$. Además cada subgrupo de orden p^i es normal en el subgrupo de orden p^{i+1}, es decir existen H_i tales que*

$$H_1 \trianglelefteq H_2 \trianglelefteq H_3 \trianglelefteq \cdots \trianglelefteq H_r \leq G$$

y $|H_i| = p^i$.

Demostración: Por Teorema de Cauchy existe $H \leq G$ tal que $|H| = p$.

Si $r = 1$, está demostrado

$$\{e\} < H < G$$

Si $r > 1$, por corolario anterior $N_G(H) \neq H$, además tenemos p divide a $[N_G(H) : H]$ y $H \trianglelefteq N_G(H)$, luego por Cauchy existe $\overline{H_1}$ subgrupo de orden p de $N_G(H)/H$, por teorema de la correspondencia.

$$\overline{H_1} = H_1/H.$$

Sea

$$H_1 = \{\ a \in G \ \mid \ aH \in \overline{H_1}\ \}$$

con lo cual tenemos que

$$\{e\} \trianglelefteq H \trianglelefteq H_1 \leq G.$$

Proceso que podemos repetir inductivamente hasta que p no divida a $[N_G(H) : H]$, lo cual se obtiene cuando se alcanza la potencia máxima, propiedad 102. □

Definición 26 *Si $|G| = p^r m$, con p, m primos relativos,*

Los subgrupos del teorema anterior de orden p^r se llaman `p-subgrupos de Sylow`

Observación: El teorema anterior asegura que si p divide a $|G|$, entonces

i) G contiene un p-subgrupo de Sylow.

ii) Un p-subgrupo de Sylow H de G es un p-grupo de orden maximal de G.

Corolario 105 *Sea p un número primo*

Todos grupos de orden p^r, con $r \geq 2$ no son simple.

Teorema 106 (Segundo Teorema de Sylow) *Si H es un p-grupo y P un p-subgrupo de Sylow de G, entonces existe $x \in G$ tal que $H \leq xPx^{-1}$.*

En particular, si H es un p-subgrupo de Sylow se tiene $H = xPx^{-1}$.

Demostración: Considerar la acción

$$\begin{array}{rccc} \cdot : & H \times G/P & \longrightarrow & G/P \\ & (g, bP) & \longmapsto & gaP \end{array}$$

luego por el lema 99 tenemos

$$|Fix_H(G/P)| \equiv [G : P] \quad (p)$$

Pero p no divide a $[G : P]$, luego

$$|Fix_H(G/P)| \not\equiv 0 \quad (p)$$

es decir, existe $xP \in G/P$, tal que

$$\begin{aligned} hxP = xP, &\quad \forall h \in H \\ x^{-1}hxP = P, &\quad \forall h \in H \\ x^{-1}hx \in P, &\quad \forall h \in H \\ x^{-1}Hx \subseteq P & \end{aligned}$$

con lo cual tenemos

$$H \leq xPx^{-1}.$$

La segunda parte se obtiene por cardinalidad maximal. □

Corolario 107 *Sean G un grupo finito, p un primo que divide a $|G|$ y P un p subgrupo de Sylow.*

P es un subgrupo normal si y sólo si P es único subgrupo de Sylow de G

Teorema 108 (Tercer Teorema de Sylow) *El número de p-subgrupo de Sylow n_p de un grupo G satisface n_p divide a $|G|$ y $n_p \equiv 1\ (p)$.*

Demostración: Sea

$$X = \{P \mid P \text{ p-subgrupo de Sylow de } G\},$$

luego se tiene que $|X| = n_p$.

Veamos la acción

$$\begin{array}{rccc} \cdot : & G \times X & \longrightarrow & X \\ & (g, P) & \longmapsto & gPg^{-1} \end{array}$$

es transitivo, por el teorema anterior, luego n_p divide a $|G|$.

Para la segunda parte, redefinimos la acción, del siguiente modo

$$\begin{array}{rccc} \cdot : & P \times X & \longrightarrow & X \\ & (g, Q) & \longmapsto & gQg^{-1} \end{array}$$

Y los puntos fijos, están dados por

$$Fix_P(X) = \{Q \in X \ \mid \ (\forall g \in P)(gQg^{-1} \subseteq Q)\}$$

Por lema se tiene que

$$\begin{aligned} |X| &\equiv |Fix_P(X)| \pmod{p} \\ n_p &\equiv |Fix_P(X)| \pmod{p} \end{aligned}$$

Ahora sea $Q \in Fix_P(X)$, luego tenemos que

$$\begin{aligned} gQg^{-1} = Q, &\quad \forall g \in P \\ P \subseteq N_G(Q) & \end{aligned}$$

Pero P, Q son dos p-subgrupos de Sylow de $N_G(Q)$, por el segundo teorema de Sylow los subgrupos son conjugados

$$P = xQx^{-1}, \quad x \in N_G(Q)$$

por lo tanto $P = Q$, y con ello tenemos $Fix_P(X) = \{P\}$.

$$n_p \equiv |Fix_P(X)| \equiv |\{P\}| \equiv 1 \pmod{p}$$

□

Ejemplo 77 *Clasificar los grupos de orden* 33.

Solución: Sea G un grupo de orden 33.

Con las notaciones del tercer teorema de Sylow, tenemos que $n_3 = 1$ y $n_{11} = 1$. Luego, existen únicos 3-subgrupo de Sylow y 11-subgrupos de Sylow, por lo tanto son normales en G.

Sean H y K los respectivos 3 y 11 subgrupos de Sylow de G, entonces nótese que:

$H \cap K = \{e\}$, ya que el orden de cualquier elemento en la intersección debe dividir al orden de H y al orden de K, es decir, debe dividir a 3 y a 11, luego no queda otra opción que el orden de ese elemento sea 1.

Por segundo teorema del isomorfismo tenemos que

$$HK/H \simeq K/H \cap K$$

lo cual implica que

$$|HK| = \frac{|H||K|}{|H \cap K|} = 33$$

Luego, como $HK \leq G$ y además poseen el mismo orden, se tiene que $HK = G$.

Para cada $a \in H$ y $b \in K$ tenemos

$$a(ba^{-1}b^{-1}) = (aba^{-1})b^{-1} \in H \cap K$$

ya que $H, K \trianglelefteq G$. Entonces

$$aba^{-1}b^{-1} = e \Leftrightarrow ab = ba$$

Por lo tanto G es abeliano, ya que $G \simeq H \times K$.

Por proposición 46, tenemos que el único grupo salvo isomorfismo de orden 33 es

$$G \simeq H \times K \simeq \mathbb{Z}_3 \times \mathbb{Z}_{11} \simeq \mathbb{Z}_{33}$$

□

Ejemplo 78 *Demuestre que los grupos de orden* $28, 80$ *y* 200 *no son simple.*

Solución: Vamos a analizar cada caso.

1. Sea G un grupo de orden $28 = 2^2 7$. Entonces por tercer teorema de Sylow tenemos:

$$n_2 = 1, 7 \quad \wedge \quad n_7 = 1$$

Como existe un único 7-subgrupo de Sylow, éste es normal en G, lo cual demuestra que G no es simple.

2. Sea G un grupo de orden $80 = 2^4 5$. Entonces por tercer teorema de Sylow tenemos:

$$n_2 = 1, 5 \quad \wedge \quad n_5 = 1, 16$$

En los casos; $n_5 = 1$, se tiene que existe un único 5-subgrupo de Sylow de G, lo cual implica que G no es simple.

Ahora, veamos el caso en que $n_5 = 16$.

Recordemos el hecho que todo grupo de orden p está generado por cada elemento perteneciente a él, salvo la identidad, es decir, en dos subgrupo de orden p el único elemento en común es el neutro.

Como existen 16 5-subgrupos de Sylow de orden 5, entonces G tiene $16(5-1) = 64$ elementos de orden 5. Además hay sólo 16 elementos no considerados, entonces sólo podemos formar un único 2-subgrupo de Sylow, lo cual implica que $n_2 = 1$, es decir, existe un único 2-subgrupo de Sylow, lo cual implica que G no es simple.

3. Sea G un grupo de orden $200 = 2^3 5^2$. Entonces por tercer teorema de Sylow tenemos:

$n_5 \equiv 1$ (mód 5) y además $n_5 \in \{1, 2, 4, 8\}$ (basta ver estos divisores ya que estamos seguros que los otros son múltiplos de 5 y por tanto son congruentes a 0 módulo 5). Luego de esta observación tenemos que $n_5 = 1$, lo cual nos dice que existe un único 5-subgrupo de Sylow, y es por tanto un subgrupo normal de G. Así tenemos que G no es simple.

□

1.18.1. Problemas Propuestos

Problema 75.

Demostrar que un grupo de orden 45 tiene un subgrupo normal de orden 9

Problema 76.

Clasificar los grupos de orden $1, 2, 3, 4, 5, 6, 7, 9, 10, 11$ salvo isomorfismo.

Problema 77.

Sea $|G| = pn$ con $p > n$, $\quad p$ primo y H un subgrupo de orden p entonces H es normal en G

Problema 78.

Sea $|G| = p^n q$ con $p > q, \quad p, q$ primos entonces G contiene un único subgrupo normal de índice q

Problema 79.

Clasificar todos lo grupos de orden 18 y 75

Problema 80.

Sea P un p-subgrupo de Sylow normal de G y $f \in End(G)$ entonces $f(P) \leq P$

Problema 81.

Demuestre que todo grupo G tal que $a^2 = 1$ para todo $a \in G$, entonces G es abeliano

Problema 82.

Clasificar todos los grupos de orden 8.

Problema 83.

Clasificar todos los grupos de orden 12.

1.19. Problemas Misceláneos

Problema 84.

Sea G el grupo de las simetrías del cubo.

Sean $V_4 = V_4^+$ la rotación en 120 grados que no mueve el vértice 4, $V_6 = V_6^+$ la rotación en 120 grados que no mueve el vértice 6 y $C = C_{1256}^+$ es la rotación en 90 grado que no mueve la cara $\{1, 2, 5, 6\}$.

Resolver explícitamente las siguiente ecuación:

$$C \circ X \circ V_4 = V_6$$

Problema 85.

Sea G el grupo de las simetrías del cubo.

Sean $A = A_{14}$ la rotación que no mueve la arista $\{1, 4\}$, $V = V_6^+$ la rotación en 120 grados que no mueve el vértice 6 y $C = C_{5876}^+$ es la rotación en 90 grado que no mueve la cara $\{5, 8, 7, 6\}$.

Resolver explícitamente las siguiente ecuación:

$$C \circ X \circ V = A$$

Problema 86.

Sean H un subgrupo del grupo G y

$$H^g = \{x \in G \mid (\exists h \in H)(\ x = ghg^{-1}\ )\}.$$

Demostrar que, para todo $g \in G$, H^g es un subgrupo de G.

Problema 87.

Sea V un $\mathbb{R}$-espacio vectorial,

$$End(V) = \{f \in F(V,V) \mid f \text{ es una transformación lineal sobre } \mathbb{R}\}$$

y

$$\mathcal{H} = \{h_t \in F(V,V) \mid h_t(v) = tv,\ t \in \mathbb{R}^*\}$$

Demostrar que

$$\mathcal{H} \trianglelefteq End(V)$$

Problema 88.

Sean $n, m \in \mathbb{N}^*$ primos relativos entonces

$$\mathbb{Z}/ < nm > \simeq (\mathbb{Z}/ < n >) \times (\mathbb{Z}/ < m >)\,.$$

Problema 89.

Sean $n, m \in \mathbb{N}^*$ y $d = MCD\{n, m\}$.
Demuestre

$$\mathbb{Z}/d\mathbb{Z} \simeq Hom(\mathbb{Z}_n, \mathbb{Z}_m)$$

Problema 90.

Sean $n, r \in \mathbb{N}^*$ naturales no nulos entonces

$$\mathbb{Z}_{nr}/ < n > \simeq \mathbb{Z}_n.$$

Problema 91.

Dada la acción definida por

$$\begin{array}{rccc} \cdot : & \mathbb{R} \times \mathbb{R}^2 & \to & \mathbb{R}^2 \\ & (a,(x,y)) & \to & (e^a x, y + a) \end{array}$$

Determinar la cantidad o el número de órbitas, es decir, un sistema de representante de las clases de equivalencia.

Problema 92.

Dada la función

$$\begin{array}{rccc} \cdot: & \mathbb{R}^* \times \mathbb{R}^2 & \to & \mathbb{R}^2 \\ & (a,(x,y)) & \to & (ax, a^2y) \end{array}$$

Demostrar que $\cdot$ es una acción y determinar todas sus órbitas.

Problema 93.

Sea $\mathbb{R}^+$ grupo con el producto y la acción

$$\begin{array}{rccc} \cdot: & \mathbb{R}^+ \times \mathbb{R}^2 & \to & \mathbb{R}^2 \\ & (a,(x,y)) & \to & (ax, a^4y) \end{array}$$

Determinar un sistema de representante de las clases de equivalencia u órbitas.

Problema 94.

Sea $J_n = \{1, 2, ..., n\}$ y $\mathbb{P}(J_n)$ el conjunto potencia de J_n

Demostrar que

$$\begin{array}{rccc} \cdot: & S_n \times \mathbb{P}(J_n) & \to & \mathbb{P}(J_n) \\ & (\sigma, A) & \to & \sigma(A) = \{\sigma(a) \mid a \in A\} \end{array}$$

es una acción.

Problema 95.

Dada la función

$$\begin{array}{rccc} \cdot : & S_n \times \mathbb{R}^n & \to & \mathbb{R}^n \\ & (\sigma, (x_i)) & \to & (x_{\sigma(i)}) \end{array}$$

1. Demostrar que $\cdot$ es una acción.
2. Si $n = 6$, determinar el estabilizador de $(1, -1, 1, -1, 1, -1)$

Problema 96.

Sea $B(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid a, c \in \mathbb{R}^*,\ b \in \mathbb{R} \right\}$ el grupo de Borel de $GL_2(\mathbb{R})$.

$$\begin{array}{rccc} \cdot : & B(\mathbb{R}) \times \mathbb{R}^2 & \longrightarrow & \mathbb{R}^2 \\ & (g, (x, y)) & \rightsquigarrow & g \cdot (x, y) \end{array}, \text{ donde } \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \cdot (x, y) = (ax + by, cy)$$

Demostrar que $\cdot$ es una acción y determinar todas sus órbitas

Problema 97.

Dado el grupo afín, es decir

$$\mathcal{A} = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{R}) \;\middle|\; c = 0, d = 1 \right\}$$

y la acción dada por

$$\begin{array}{rccc} \cdot : & \mathcal{A} \times \mathbb{R}^2 & \to & \mathbb{R}^2 \\ & \left(\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}, (x, y) \right) & \to & (ax + b, ay + b) \end{array}$$

Determinar la cantidad o el número de órbitas, es decir, un sistema de representante de las clases de equivalencia.

Problema 98.

Sea $Y = \{\{1, 2\}, \{2, 3\}, \{3, 4\}, \{4, 1\}\}$ las aristas del cuadrado, G el grupo de simetrías del cuadrado.

Describa órbitas y estabilizadores de la acción natural de G sobre los aristas.

Problema 99.

Sea $G = D_3$ el grupo de simetría del triángulo equilátero

$$X = \{(x, y, z) \in \mathbb{N}^* \times \mathbb{N}^* \times \mathbb{N}^* \quad : \quad x \leq 3 \wedge y \leq 3 \wedge z \leq 3\}$$

y la acción

$$\cdot : G \times X \to X,\ g \cdot (x, y, z) = (g(x), g(y), g(z))$$

Determinar el número de órbitas y su cardinal

Problema 100.

Sea $G = Aut(\mathbb{Z}_{12})$ el grupo de automorfismo de $\mathbb{Z}_{12}$ con la composición y la acción

$$\cdot : G \times \mathbb{Z}_{12} \to \mathbb{Z}_{12},\ g \cdot x = g(x)$$

Determinar el número de órbitas y su cardinal.

Problema 101.

Sea $G = Aut(\mathbb{Z}_{15})$ el grupo de automorfismo de $\mathbb{Z}_{15}$ con la composición y la acción

$$\cdot : G \times \mathbb{Z}_{15} \to \mathbb{Z}_{15},\ g \cdot x = g(x)$$

Determinar el número de órbitas y su cardinal.

Problema 102.

Sea $G = Aut(\mathbb{Z}_8 \times \mathbb{Z}_3)$ el grupo de automorfismo de $\mathbb{Z}_8 \times \mathbb{Z}_3$ con la composición y la acción

$$\cdot : G \times \mathbb{Z}_8 \times \mathbb{Z}_3 \to \mathbb{Z}_8 \times \mathbb{Z}_3,\ g \cdot (x, y) = (g(x), g(y))$$

Determinar el número de órbitas y su cardinal.

Problema 103.

Determinar el orden de $G = Aut(\mathbb{Z}_{15} \times \mathbb{Z}_3)$ el grupo de automorfismo de $\mathbb{Z}_{15} \times \mathbb{Z}_3$.

Problema 104.

Sea G un grupo finito que actúa en X conjunto finito.
Se define el conjunto $L = \{(x, g) \in X \times G \quad | \quad g \cdot x = x\}$.

1. Demostrar que si $(x, g) \in L, h \in G$ entonces $(h \cdot x, g(h^{-1})) \in L$
2. Demostrar que $\cdot : G \times L \to L, h \cdot (x, g) = (h \cdot x, g(h^{-1}))$ es una acción
3. Demostrar $G_{(x,e)} = \{e\}$,para todo $x \in X$ (e es el neutro de G)

Problema 105.

Determinar el normalizador de $\{(2\ 1), (3\ 2)\}$ en S_4.

$$N_{S_4}(\{(2\ 1), (3\ 2)\})$$

Problema 106.

Determinar el normalizador $\{(1\ 2\ 3), (2\ 3\ 4)\}$ en S_6.

$$N_{S_6}(\{(1\ 2\ 3), (2\ 3\ 4)\})$$

Problema 107.

Sea $n \geq 3$. Demostrar que el centro de S_n es el neutro

$$Z(S_n) = \{e\}$$

Problema 108.

Sea $n \geq 3$, $H \trianglelefteq S_n$ y H contiene un 3-ciclo entonces $A_n \subset H$.

Problema 109.

Sea $n \geq 4$. Demostrar que
A_n esta generado por los 3-ciclos

Problema 110.

Sean $n \geq 5$, $H \trianglelefteq S_n$ y $(12)(34) \in H$.
Demuestre que

$$A_n \subseteq H.$$

Problema 111.

Determinar la cantidad de grupos abelianos salvo isomorfismo de orden $2^2 3^4 4^2 5^3$.

Problema 112.

Determinar el valor de verdad de las siguientes proposiciones. JUSTIFIQUE

1. Todos los grupos son cíclicos.
2. Si dos grupos tiene el mismo cardinal entonces son isomorfos.
3. Si $H \leq G$ y H es abeliano entonces H es normal de G.
4. Si X, G son finitos y G actúa en X entonces $|X|$ divide $|G|$.
5. $F : \mathbb{Q}^+ \times \mathbb{R}^+ \to \mathbb{R}^+$; con $F(a, x) = x^a$ es una acción.
6. Sea $T : \{t_b \in F(\mathbb{R}, \mathbb{R}) \mid t_b \text{ es una traslación, con } b \in \mathbb{R}\}$ y
   $L : \mathbb{R} \times T \to T$. tal que $L(a, t_b) = t_{a+b}$ es una acción.
7. Sea V un $\mathbb{R}$-espacio vectorial, $End(V) = \{f \in F(V, V) \mid f \text{ es una transformación lineal de } V \text{ en } V\}$ y $R : End(V) \times V \to V$ donde $R(f, x) = f(x)$ es una acción.

8. Dada la función $F : GL_2(\mathbb{R}) \times Biy(M_2(\mathbb{R})) \to Biy(M_2(\mathbb{R}))$, definida por

$$F(A, h)(X) = h(XA)$$

entonces F es una acción.

9. Sea $A \in M_2(\mathbb{R})$ y la función $T_A : \mathbb{R} \times M_2(\mathbb{R}) \to M_2(\mathbb{R})$, definida por

$$T_A(t, B) = B - tA$$

entonces T es una acción.

10. $S_n/A_n \simeq \mathbb{Z}_2$
11. La permutación $\sigma = (1\ 2\ 3 \cdots n)^2$ es par, para todo $n \in \mathbb{N}^*$
12. El número de grupos abeliano no isomorfo de orden 15 es 2

Índice alfabético