

UNIDAD 1: TEORÍA DE GRUPOS

En este capítulo emprenderemos el estudio del objeto algebraico conocido como “*grupo*”, que sirve como uno de los bloques de construcción fundamentales de la gran estructura que hoy se llama *álgebra abstracta*. En capítulos posteriores echaremos una mirada a alguno de los otros, tales como: *anillos, cuerpos y espacios vectoriales*.

Aparte de que ya se ha hecho tradicional comenzar con el estudio de los grupos, hay razones naturales convincentes para esta elección. Para comenzar, los grupos, como sistemas con una sola operación, se prestan a la más simple de las descripciones formales. Sin embargo, a pesar de esta simplicidad de descripción, los conceptos fundamentales del álgebra, tales como *homomorfismo, cociente, etc.*, que juegan un papel tan importante en todas las estructuras algebraicas -en realidad en toda la Matemática- entran aquí en una forma pura y reveladora.

Antes de que los detalles nos abrumen, echemos una ojeada rápida al camino que vamos a recorrer. En el álgebra abstracta tenemos ciertos sistemas básicos que, en la historia y el desarrollo de la Matemática, han alcanzado posiciones de importancia extraordinaria. Éstos son, generalmente, conjuntos con cuyos elementos podemos operar algebraicamente -por lo que entendemos que podemos combinar dos elementos del conjunto, quizás de varias maneras, para obtener un tercer elemento, también del conjunto- y además, suponemos que estas operaciones algebraicas están sujetas a ciertas reglas que se indican explícitamente en los que se llaman *axiomas o postulados definitorios del sistema*. En este marco abstracto, intentaremos probar teoremas acerca de estas mismas estructuras generales, esperando siempre que cuando estos resultados se apliquen a una realización particular y concreta del sistema abstracto, afluirán hechos y conocimientos de la estructura interna del ejemplo que se discuta y que habrían quedado oscurecidos para nosotros por el volumen de información sin importancia que se nos presenta en todo caso particular.

Es importante subrayar que estos sistemas algebraicos y los axiomas que los definen, deben tener cierta naturalidad. Deben surgir de la experiencia que resulta de observar muchos ejemplos; deben ser ricos en resultados significativos. Sentarse, hacer una lista de unos cuantos axiomas y proceder al estudio del sistema así descrito, no resulta un procedimiento adecuado de trabajo en Matemática. Admitimos que esto es lo que hacen algunos, pero la mayor parte de los matemáticos, descartarán estos ensayos como *matemáticas mediocres*. Los sistemas que se estudian, son estudiados porque casos particulares de estas estructuras han aparecido una y otra vez, porque alguien finalmente, notó que estos casos particulares eran realmente concreciones de un fenómeno general, porque alguien nota analogías entre dos objetos matemáticos aparentemente disímiles y ello le dirige hacia una investigación sobre las raíces de estas analogías.

Para citar un ejemplo, hacia finales del siglo XVIII y comienzos del XIX se estaba estudiando caso tras caso de este objeto matemático que hoy conocemos como grupo; pero, sin embargo, no fue sino hasta ya bastante avanzado el siglo XIX que se introdujo la noción de grupo abstracto.

Las únicas estructuras algebraicas hasta ahora encontradas que han resistido el embate del tiempo y han sobrevivido y crecido en importancia, son las basadas en un amplio y alto pilar de casos particulares.

Entre matemáticos, nadie discute ni la belleza ni la importancia de los *grupos*.

Comentarios históricos

Las ideas que contiene la definición de *grupo*, estaban presentes en algunos trabajos de matemáticos realizados durante la segunda mitad del siglo XVIII y todo el siglo XIX. Todas ellas se referían a casos particulares de grupos, principalmente *grupos de permutaciones*.

El estudio de la resolución de ecuaciones algebraicas fue el que aglutinó más trabajos y desde donde más tarde germinarían las ideas que servirían para definir el concepto abstracto de grupo. El matemático que más contribuyó durante el siglo XVIII a este tema fue *Joseph Louis Lagrange* (1736-1813). Fue un matemático francés nacido en Italia, que a los 19 años ya era Profesor en la Escuela Real de Artillería de Turín y acabó trabajando en los grandes centros matemáticos de su época. En 1766 aceptó la invitación de Federico el Grande de Prusia para ocupar la vacante que había dejado **Leonhard Euler** (1707-1783) en la Academia de Ciencias de Berlín y en 1797 fue nombrado Profesor de Matemática de la Escuela Politécnica de París. En un artículo publicado en 1771 en la revista de la Academia de Ciencias de Berlín, trató de sistematizar los resultados conocidos sobre la resolución de las ecuaciones de grado 2, 3 y 4. En el proceso, encontró que las fórmulas para resolver las ecuaciones de estos grados estaban relacionadas con la cantidad de valores distintos que pueden tomar ciertas expresiones de las raíces de la ecuación. Por ejemplo, en la ecuación de grado 4 con raíces x_1, x_2, x_3 y x_4 , la función $y = f(x_1, x_2, x_3, x_4) = x_1x_2 + x_3x_4$ sólo toma tres valores distintos cuando se permutan las raíces de las $4! = 24$ maneras posibles. Esto, encontró Lagrange, estaba ligado con el hecho de que la resolución de la ecuación de cuarto grado pudiera reducirse a encontrar las raíces de una de grado 3.

La exposición anterior tiene relación con los grupos tal como lo entendemos actualmente. En el ejemplo anterior, el conjunto de las permutaciones que producen el mismo valor de f constituyen un *subgrupo* del *grupo de todas las permutaciones*. Precisamente, hay tantos subgrupos distintos de este tipo como valores distintos toma f : en nuestro ejemplo 3. Lagrange, denominó a este tipo de razonamientos “*teoría de las sustituciones*” y todos sus trabajos están escritos en el lenguaje de los valores que puede tomar una función de las raíces de una ecuación. Así, por ejemplo, logró probar que el número de valores diferentes que puede tomar una función de las raíces, es un divisor del total de sustituciones que pueden hacerse, lo que es una formulación particular del que nosotros hemos denominado *Teorema de Lagrange*. La “*teoría de las sustituciones*” de Lagrange, influyó en los trabajos del matemático italiano *Paolo Ruffini* (1765-1822), quien creyó haber demostrado que las ecuaciones de quinto grado no pueden resolverse mediante radicales, y en los del matemático noruego *Niels Herik Abel* (1802-1829), a quien se le reconoce la primera demostración correcta del resultado que creyó haber demostrado Ruffini. Todos estos trabajos fueron superados por los de *Evariste Galois* (1811-1832) quien en su juventud sentó las bases de la resolución de las ecuaciones algebraicas, enlazando la solución de éstas con las propiedades de los grupos de las sustituciones. Mientras tanto, usó por primera vez las palabras “*grupo*”, “*normal*”, “*isomorfismo*” y “*simple*”, siempre referidas a permutaciones.

Evariste Galois nació en un pueblo cercano a París y tuvo una corta, pero azarosa, vida. A la muerte de su padre, ocurrida en 1829, se sumó el rechazo para entrar en la Escuela Politécnica de París, con lo que tuvo que conformarse con ingresar en la Escuela Normal Superior. Sus ideas revolucionarias le valieron la prisión en dos ocasiones, lo que aprovechó para continuar trabajando en sus ideas acerca de la resolución de ecuaciones algebraicas. Poco después de salir de su segundo período en la cárcel, Galois se vio envuelto en un duelo, no se sabe si por razones políticas o amorosas. Temiendo no sobrevivir al duelo, dedicó los últimos días de su vida a escribir los principales resultados de sus investigaciones matemáticas. El manuscrito, que envió a su amigo *Auguste Chevalier*, contenía las ideas principales para resolver el problema de solubilidad mediante radicales de las ecuaciones de quinto grado o superior. Permaneció olvidado hasta que *Joseph Liouville* (1809-1882) lo presentó en 1843 a la Academia de Ciencias de París y fue aceptado para publicarlo.

Mientras tanto el matemático francés *Augustin-Louis Cauchy* (1789-1857) continuó trabajando en la teoría de los valores que puede tomar una función de las raíces de una ecuación, como había sido descrita por Lagrange. Sus artículos sobre este tema comenzaron en 1815, pero fue en 1846 cuando apareció el resultado que hoy lleva su nombre: *todo grupo de permutaciones cuyo orden es divisible por un primo p tiene al menos un subgrupo de orden p* .

También en el contexto de las permutaciones, el matemático noruego, *Mejdell Ludwig Sylow* (1832-1918) publicó en 1873 uno de los trabajos que supuso el mayor avance en esta teoría desde los resultados de Cauchy. Sylow logró demostrar, escrito en lenguaje moderno, que *no sólo todo grupo de orden n tiene un subgrupo de orden p si p es primo y divide a n , sino que los tiene de todos los órdenes p^s siempre que p^s divida a n y para el mayor s para el que esto suceda solamente hay uno de ellos*. Estos resultados se conocen con el nombre de *Teoremas de Sylow*.

En el proceso de gestación de la definición abstracta de grupo hay que mencionar al matemático británico *Arthur Cayley* (1821-1895) quien en 1854 propuso una definición abstracta de estructuras que satisficieran algunas propiedades que se asemejaban a la definición de grupo. Ni sus contemporáneos están preparados para manejar una definición tan abstracta, ni Cayley estaba convencido de que fuera necesaria, puesto que él continuó trabajando con las permutaciones y además sabía que sus estructuras abstractas podían considerarse grupos de permutaciones.

A principios del siglo XX las ideas ya estaban maduras para que una definición abstracta de grupo no ofreciera problemas. Varios matemáticos publicaron artículos durante la primera década de este siglo en donde, con ligeras modificaciones, aparecería el concepto abstracto de grupo tal como nosotros lo definimos. A partir de aquí los matemáticos empezaron a trasladar a este contexto más general las definiciones y los resultados de sus antepasados sobre grupos de permutaciones. El *Teorema de Lagrange*, el de *Cauchy* y los de *Sylow* fueron generalizados. En lugar de buscar propiedades de algún grupo concreto y después tratar de demostrarlas en la estructura más general, se definieron conceptos directamente para esta estructura y se obtuvieron resultados con ellos. Los *conmutadores de dos elementos de un grupo* y los *automorfismos de un grupo*, son ejemplos de ello.

El siglo XX ha vivido una gran actividad en torno a la teoría de grupos. La clasificación de todos los grupos finitos, ha ocupado gran parte de los trabajos de muchos de los matemáticos que se han dedicado a esta rama. Muchos de los conceptos y de las teorías aparecidas han podido parafrasearse en el lenguaje de los grupos y se han encontrado aplicaciones en *crystalografía*. Siendo, quizás, demasiado optimista, el matemático francés *Jules Henri Poincaré* (1854-1912) afirmaba que la teoría de grupos permitiría reducir toda la Matemática a su forma más pura.

Definición

Sea G un conjunto no vacío. Una **operación binaria** en G , es una aplicación $G \times G \rightarrow G$.

Hay varias notaciones de uso común para la imagen de $(a, b) \in G \times G$ bajo una operación binaria: ab (notación multiplicativa), $a + b$ (notación aditiva), $a \bullet b$, $a * b$, etc.

Ejemplo

La adición y la multiplicación son ejemplos de operaciones binarias en $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ y \mathbb{C} .

Definición

Un **semigrupo** es un conjunto no vacío G junto con una operación binaria en G que es

i) *asociativa*: $a(bc) = (ab)c \forall a, b, c \in G$

Un **monoide** es un semigrupo G que contiene un

ii) *elemento identidad* $e \in G$ tal que $ae = ea = a \forall a \in G$

Un **grupo** es un monoide G tal que

iii) $\forall a \in G, \exists a^{-1} \in G$ (*elemento inverso*) tal que $a^{-1}a = aa^{-1} = e$

Un semigrupo G se dice **abeliano** o **conmutativo** si su operación binaria es

iv) *conmutativa*: $ab = ba \forall a, b \in G$

Cuando G es conmutativo, la operación binaria se suele denotar como *suma* (+), el elemento identidad se llama *neutro* y el inverso de un elemento se dice *opuesto*.

El **orden** de un grupo G es el número cardinal $|G|$.

G se dice **finito** (respectivamente **infinito**) si $|G|$ es finito (respectivamente infinito).

Teorema

1. Si G es un *monoide*, entonces el elemento identidad es único (y se denota e)
Si G es un *grupo*, entonces:
2. $\forall a \in G, \exists! a^{-1} : aa^{-1} = a^{-1}a = e$ (por lo tanto, el inverso de cada elemento es único)
3. $\forall a, b, c \in G : ab = ac \Rightarrow b = c$ y $ba = ca \Rightarrow b = c$ (*leyes de cancelación a izquierda y a derecha*)
4. $\forall a \in G : (a^{-1})^{-1} = a$
5. $\forall a, b \in G : (ab)^{-1} = b^{-1}a^{-1}$
6. $\forall a, b \in G$, las ecuaciones $ax = b$ e $ya = b$ tienen soluciones únicas en G : $x = a^{-1}b$ e $y = ba^{-1}$

Dem.: (Ejercicio)

Ejemplos

1. $G = \{e\}$ es el *grupo trivial*
2. $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +)$ son grupos abelianos
3. $(\mathbb{Z}, \cdot), (\mathbb{Q}, \cdot), (\mathbb{R}, \cdot), (\mathbb{C}, \cdot)$ son monoides
4. $(\mathbb{Q} - \{0\}, \cdot), (\mathbb{R} - \{0\}, \cdot)$ son grupos abelianos
5. $GL(n, \mathbb{R})$ el conjunto de las matrices $n \times n$ sobre \mathbb{R} inversibles (*determinante* $\neq 0$) es un grupo con el producto usual de matrices
6. $SL(n, \mathbb{R})$ el conjunto de las matrices $n \times n$ sobre \mathbb{R} de determinante 1, es un grupo con el producto usual de matrices

Otros ejemplos (¡¡¡muy importantes!!!)*** Grupo simétrico (o de permutaciones) en n letras**

Consideremos un conjunto $S \neq \emptyset$. Sea $A(S)$ el conjunto de biyecciones de S . $A(S)$ es un grupo con la composición de funciones (Ejercicio).

Supongamos que $S = \{1, 2, \dots, n\}$. El conjunto $A(S)$, en este caso, se denota S_n y se llama el *grupo simétrico (o de permutaciones) en n letras*.

Los elementos de S_n se denotan de la siguiente manera:

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}$$

Por ejemplo, S_3 está formado por:

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

En general, $|S_n| = n!$ (Ejercicio)

*** El producto directo de grupos**

Sean G, H grupos.

$$G \times H = \{(g, h) : g \in G \wedge h \in H\}$$

es un grupo con la operación

$$(g_1, h_1) \cdot (g_2, h_2) = (g_1 \cdot g_2, h_1 \cdot h_2)$$

Además, $|G \times H| = |G| \cdot |H|$

(Ejercicio)

* Consideremos \mathbb{Z} grupo.

Sea $k \in \mathbb{N}$ fijo. Definimos la relación *congruencia módulo k* de la siguiente manera: $x_1, x_2 \in \mathbb{Z}$,

$$x_1 \propto x_2 \Leftrightarrow x_2 - x_1 = kp \quad (p \in \mathbb{Z})$$

Esta *relación* es de *equivalencia*. (Ejercicio)

Por el *algoritmo de la división*,

$$\begin{aligned} x_1 &= kp_1 + r_1 & 0 \leq r_1 < k \\ x_2 &= kp_2 + r_2 & 0 \leq r_2 < k \\ \Rightarrow x_1 \propto r_1 \wedge x_2 \propto r_2 & \text{ (Ejercicio)} \end{aligned}$$

Más aún, $x_1 \propto x_2 \Leftrightarrow r_1 \propto r_2$ (Ejercicio)

Podemos entonces, *partir* a \mathbb{Z} , en *clases de equivalencia*, por la relación \propto .

Así, $\mathbb{Z}/\propto = \{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{k-1}\}$ (tiene k elementos).

Además, tenemos que:

$$\begin{aligned} x_1 \propto x_2 &\Rightarrow x_2 - x_1 = kp_1 \\ y_1 \propto y_2 &\Rightarrow y_2 - y_1 = kp_2 \end{aligned}$$

de donde $(x_2 + y_2) - (x_1 + y_1) = k(p_1 + p_2) \Rightarrow (x_2 + y_2) \propto (x_1 + y_1)$

Por lo tanto, la relación dada, es una *relación de congruencia*.

Luego, en \mathbb{Z}/\propto se define la siguiente operación:

$$\bar{x} + \bar{y} = \overline{x + y}$$

y \mathbb{Z}/α se denota \mathbb{Z}_k .

Por ejemplo, en $\mathbb{Z}_3 = \{\bar{0}, \bar{1}, \bar{2}\}$ tenemos:

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

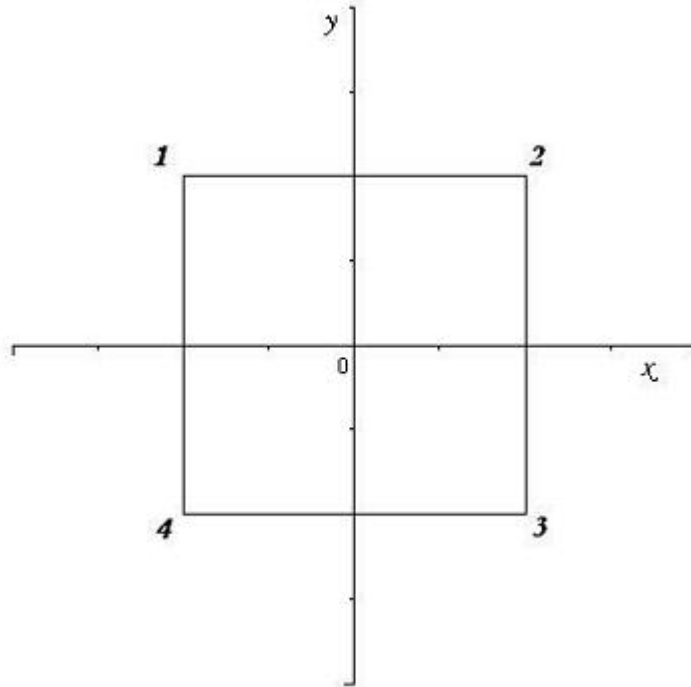
Se puede probar que el producto de \mathbb{Z} se puede inducir a \mathbb{Z}_k , mostrando que:

$$x_1 \alpha x_2 \wedge y_1 \alpha y_2 \Rightarrow x_1 \cdot y_1 \alpha x_2 \cdot y_2$$

Luego, en \mathbb{Z}/α se define también la operación:

$$\bar{x} \cdot \bar{y} = \overline{x \cdot y}$$

* Consideremos ahora, el cuadrado con vértices consecutivamente numerados 1, 2, 3, 4, centrado en el origen del plano $x - y$, y de lados paralelos a los ejes.



Sea D_4^* el conjunto de las siguientes transformaciones en el plano:

- Id : transformación identidad.
- R : rotación en $\frac{\pi}{2}$, con centro en el origen, en el sentido de las agujas del reloj.
- $R^2 = R \circ R$: rotación en π , con centro en el origen, en el sentido de las agujas del reloj.
- $R^3 = R^2 \circ R$: rotación en $\frac{3\pi}{2}$, con centro en el origen, en el sentido de las agujas del reloj.
- S_{13} : simetría axial respecto de la recta que pasa por los vértices 1 y 3.
- S_{24} : simetría axial respecto de la recta que pasa por los vértices 2 y 4.
- S_x : simetría axial respecto del eje x .

- S_y : simetría axial respecto del eje y .

$D_4^* = \{Id, R, R^2, R^3, S_{13}, S_{24}, S_x, S_y\}$ es un grupo no abeliano, con la composición (Ejercicio).

\circ	Id	R	R^2	R^3	S_{13}	S_{24}	S_x	S_y
Id								
R					S_y			
R^2								
R^3								
S_{13}								
S_{24}								
S_x								
S_y								

Ejercicio: completar la tabla.

Análogamente, se define D_n^* , el grupo de las *transformaciones rígidas del plano* que dejan invariante un polígono regular de n lados, centrado en el origen.

Definición

Si $n \in \mathbb{N}$, $a^n = \prod_{i=1}^n a_i$ con $a_i = a$

$$a^0 = e$$

Teorema

Si G es grupo (respectivamente, semigrupo y monoide) y $a \in G$, entonces, $\forall m, n \in \mathbb{Z}$:

1. $a^m a^n = a^{m+n}$ (notación aditiva: $ma + na = (m+n)a$)
2. $(a^m)^n = a^{mn}$ (notación aditiva: $n(ma) = nma$)

Dem.: no la haremos.

Definición

Sean G, H semigrupos. La función $f : G \rightarrow H$ es un **homomorfismo de semigrupos** si:

$$f(ab) = f(a)f(b), \forall a, b \in G$$

- Si f es inyectiva, f se dice **monomorfismo**.
- Si f es suryectiva, f se dice **epimorfismo**.
- Si f es biyectiva, f se dice **isomorfismo**.
- Si $H = G$, un homomorfismo f , se llama **endomorfismo**.
- Si $H = G$ y f es un isomorfismo, f se llama **automorfismo**.

Observación 1

Si $f : G \rightarrow H$ y $g : H \rightarrow K$ son homomorfismos de semigrupos, entonces $g \circ f : G \rightarrow K$ es homomorfismo.

Dem.: Ejercicio

Observación 2

Si G, H grupos y $f : G \rightarrow H$ homomorfismo, entonces:

1. $f(e_G) = e_H$
2. $f(a)^{-1} = f(a^{-1})$

Dem.:

1. $e_G = e_G e_G$ Luego, como f es homomorfismo, $f(e_G) = f(e_G) f(e_G)$ (*)
 Ahora bien, $e_H = f(e_G)^{-1} f(e_G) \underbrace{=}_{(*)} f(e_G)^{-1} f(e_G) f(e_G) = e_H f(e_G) = f(e_G)$, como queríamos probar.
2. (Ejercicio. Sug.: utilizar el resultado probado en 1.)

Ejemplos

1. G grupos abeliano
 $i : G \rightarrow G/x \mapsto x^{-1}$ es un *automorfismo*.
 (Ejercicio: Verificarlo)
2. G, H grupos y $f : G \rightarrow H$ homomorfismo

$$f \text{ isomorfismo} \Leftrightarrow f^{-1} : H \rightarrow G \text{ homomorfismo tal que } f \circ f^{-1} = id_H \text{ y } f^{-1} \circ f = id_G$$

Dem.: Ejercicio

Sug.: Como $f : G \rightarrow H$ es una función biyectiva, existe su función inversa $f^{-1} : H \rightarrow G$ que también es biyectiva (*¿Por qué?*)

Dados $h_1, h_2 \in H, \exists! g_1, g_2 \in G$ tales que $f(g_1) = h_1 \wedge f(g_2) = h_2$ (*¿Por qué?*)

Luego, $g_1 = f^{-1}(h_1) \wedge g_2 = f^{-1}(h_2)$

Utilizando las hipótesis dadas, probar que f^{-1} es un homomorfismo.

3. G, H grupos, la proyección $\pi_1 : G \times H \rightarrow G/(g, h) \mapsto g$ es un epimorfismo.
 (Ejercicio: Probarlo)
4. G, H grupos, la inyección/inclusión $i_2 : H \rightarrow G \times H/h \mapsto (e_G, h)$ es un monomorfismo.
 (Ejercicio: Probarlo)

Definición

Sean G, H grupos y $f : G \rightarrow H$ homomorfismo, al conjunto

$$\ker f = \{g \in G : f(g) = e_H\}$$

se le llama **núcleo de f** .

Proposición

Sean G, H grupos y $f : G \rightarrow H$ homomorfismo de grupos, entonces:

$$f \text{ inyectivo} \Leftrightarrow \ker f = \{e_G\}$$

Dem.:

\Rightarrow Sea $g \in \ker f \Rightarrow f(g) = e_H$. Además, $e_G \in \ker f$ pues $f(e_G) = e_H$. Como f inyectivo, resulta que $g = e_G$.

$$\text{Luego, } \ker f = \{e_G\}$$

⇐) Ejercicio.

Definición

Sea G grupo y $\emptyset \neq H \subset G$. Se dice que H es **cerrado** por el producto (o por la operación binaria) si $\forall a, b \in H : ab \in H$.

Si H con esa operación binaria es un grupo, entonces se llama **subgrupo** de G y se denota $H < G$.

Observación

Si G es un grupo, $\{e_G\}$ es un subgrupo de G , y si $H < G$ y $H \neq \{e_G\}$, H se dice **subgrupo propio** de G .

Ejemplos

1. Si $G \neq \{e_G\}$ es grupo, G contiene al menos los subgrupos G y $\{e_G\}$ (**subgrupos triviales**).
2. En \mathbb{Z} , el conjunto $m\mathbb{Z} = \{mk : k \in \mathbb{Z}\}$ es un subgrupo de \mathbb{Z} .
Más aún, $m\mathbb{Z} \cong \mathbb{Z}$ si $m \neq 0$ y el isomorfismo viene dado por $\phi : \mathbb{Z} \rightarrow m\mathbb{Z}/k \mapsto \phi(k) = mk$
(Ejercicio: Verificarlo)
3. En $\mathbb{Z}_6 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$ son subgrupos $\{\bar{0}, \bar{3}\}$ y $\{\bar{0}, \bar{2}, \bar{4}\}$
4. Si G es grupo, $Aut(G) = \{f : G \rightarrow G : f \text{ homomorfismo biyectivo}\}$ es grupo con la composición.
(Ejercicio: Verificarlo).

Teorema

Sea G grupo y $\emptyset \neq H \subset G$, entonces:

$$H \text{ es subgrupo de } G \Leftrightarrow ab^{-1} \in H, \forall a, b \in H$$

Dem.:

⇒) Ejercicio

⇐) Como $H \neq \emptyset, \exists a \in H$. Luego, por hipótesis, $aa^{-1} \in H$

$$\therefore e \in H$$

Para $e, a \in H$, por hipótesis, $ea^{-1} \in H$

$$\therefore a^{-1} \in H, \forall a \in H$$

Si $a, b \in H \Rightarrow a, b^{-1} \in H \Rightarrow a(b^{-1})^{-1} \in H$

$$\therefore ab \in H$$

La asociatividad vale en H , pues ella vale en G y H es cerrado por el producto.

Ejemplos

1. Si $f : G \rightarrow H$ es un homomorfismo de grupos, entonces:

- $\ker f < G$
- $f(G) < H$

Además,

- $\tilde{G} < G \Rightarrow f(\tilde{G}) < H$
- $\tilde{H} < H \Rightarrow f^{-1}(\tilde{H}) < G$

(Ejercicio: Probarlo)

2. Sea $\{H_i\}$ una familia de subgrupos de un grupo G , entonces $\bigcap_{i \in I} H_i$ es un subgrupo de G pues:

$$\text{Sean } a, b \in \bigcap_{i \in I} H_i \Rightarrow a, b \in H_i, \forall i \in I \Rightarrow ab^{-1} \in H_i, \forall i \in I \Rightarrow ab^{-1} \in \bigcap_{i \in I} H_i$$

Ahora, si H_1 y H_2 son subgrupos de un grupo G , ¿qué sucede con $H_1 \cup H_2$? (Ejercicio)

Definición/Teorema

Sea G un grupo y $\emptyset \neq X \subset G$, entonces el **subgrupo generado** por X , que denotaremos $\langle X \rangle$, consiste en elementos de la forma $a_1^{n_1} a_2^{n_2} \dots a_t^{n_t}$ con $a_i \in X \wedge n_i \in \mathbb{Z}, \forall i = 1, 2, \dots, t$.

Los elementos de X se dicen los **generadores** de $\langle X \rangle$.

Si $X = \{a_1, a_2, \dots, a_n\}$, escribimos $\langle X \rangle = \langle a_1, a_2, \dots, a_n \rangle$ y este se dice **finitamente generado**.

Dem.: No la haremos.

(Ejercicio: pensar qué forma tienen los elementos de $\langle X \rangle$ cuando usamos la notación aditiva)

Observación

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

Definición

Un subgrupo H de un grupo G se dice **cíclico** si $H = \langle a \rangle = \{a^k : k \in \mathbb{Z}\}$

Ejemplos

1. $\mathbb{Z} = \langle 1 \rangle$ cíclico infinito.
2. $\mathbb{Z}_k = \langle \bar{1} \rangle$ cíclico finito.
3. $\langle R \rangle < D_4^*$ con $|\langle R \rangle| = 4$.

Definición

Sea G un grupo y $a \in G$. El **orden de a** es el orden del subgrupo cíclico $\langle a \rangle$ y se denota $|a|$.

Ejemplo

En D_4^* , $|R| = 4$ y $|S_x| = 2$

Este ejemplo nos permite intuir la siguiente:

Proposición

Si G es un grupo finito y $a \in G$, el orden de a es un divisor del número de elementos de G .

Dem.: No la haremos.

Los siguientes ejemplos muestran que el resultado de la proposición puede ser también cierto para todos los subgrupos de G .

Ejemplos

Los subgrupos de S_3 tienen órdenes 1,2,3 ó 6, mientras que los subgrupos de D_4^* tienen órdenes 1,2,4 u 8.

(Ejercicio: buscar ejemplos de tales subgrupos).

Se infiere que la afirmación de que “el número de elementos de un subgrupo H de G divide al número de elementos de G ” puede ser cierta siempre. Este resultado se conoce con el nombre de **Teorema de Lagrange**, pero no lo probaremos en este curso por carecer de las herramientas para hacerlo.

Definición

Un grupo en el cual cualquier elemento tiene orden una potencia (≥ 0) de un primo fijo p , se llama **p -grupo**. Si $H < G$ y H es un p -grupo, entonces H se dice **p -subgrupo** de G . En particular, $\langle e \rangle$ es un p -grupo (p -subgrupo).

Resultados importantes (Sin demostración)

- G es un p -grupo $\Leftrightarrow |G|$ es una potencia de p
- Sea G un p -grupo, entonces: $H < G \Rightarrow H$ es un p -grupo

Definición

Sea p primo. Un subgrupo P de un grupo G se dice **p -subgrupo Sylow** si P es un subgrupo maximal de G (es decir, $P < H < G \wedge H$ p -subgrupo $\Rightarrow H = P$).

Ejemplo

En \mathbb{Z}_{12} , $\langle 3 \rangle$ es un 2-subgrupo Sylow y $\langle 4 \rangle$ es un 3-subgrupo Sylow.

FIN

Bibliografía

- DORRONSORO, J. y HERNÁNDEZ, E. *Números, grupos y anillos*. Madrid, España: Ed. Addison-Wesley Iberoamericana España, S.A., 1996.
- HERSTEIN, I.N. *Álgebra moderna*. México: Editorial F. Trillas, 1970.
- HUNGERFORD, T. W. *Algebra*. New York: Springer-Verlag, 1974.
- ROJO, A. *Álgebra*. Buenos Aires: Ed. El Ateneo, 1987.

PRÁCTICA 1: Teoría de grupos

1. Completar los ejercicios de la teoría
2. Se define $\otimes : \mathbb{Q} \times \mathbb{Q} \rightarrow \mathbb{Q}$ mediante $a \otimes b = a + b + a \cdot b$. Analizar las propiedades de asociatividad, conmutatividad, cancelación, existencia de elemento identidad y elementos inversos.
3. Determinar si G es un grupo, semigrupo o monoide, justificando en cada caso:
 - (a) $G = \mathbb{Q}$ con la operación $a \cdot b = \frac{a+b}{5}$ donde $+$ es la suma usual en \mathbb{Q}
 - (b) (G, \cdot) , donde $G = \mathbb{Z} \times \mathbb{Z}$ con $(a, b) \cdot (c, d) = (ad + bc, bd)$
4. En el conjunto \mathbb{C} de los números complejos, se considera \bullet definida por

$$m \bullet n = m + n - i$$

Probar que (\mathbb{C}, \bullet) es un grupo abeliano.

5. El grupo de los cuaterniones

Definimos en el conjunto $G = \{1, -1, i, -i, j, -j, k, -k\}$ un operación que verifica:

- $1 \cdot x = x \cdot 1 = x, \forall x \in G$
- $(-1) \cdot x = x \cdot (-1) = -x, \forall x \in G$
- $i \cdot j = k$
- $j \cdot k = i$
- $k \cdot i = j$
- $x \cdot y = -y \cdot x, \forall x, y \in G$
- $i \cdot i = j \cdot j = k \cdot k = -1$

Realizar una tabla de operaciones para G y mostrar que G es grupo.

6. Mediante una tabla de operaciones para la suma y el producto, analizar la estructura de \mathbb{Z}_6
7. Encuentre los inversos y el orden de los siguientes elementos:
 - (a) $\tau_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \in S_3$
 - (b) $\tau_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix} \in S_4$
8. Sean $(\mathbb{R}, +)$ y (\mathbb{R}^+, \cdot) . Verificar que $f : \mathbb{R} \rightarrow \mathbb{R}^+ / x \mapsto f(x) = 2^x$ es un homomorfismo. ¿Qué sucede con $g : \mathbb{R}^+ \rightarrow \mathbb{R} / x \mapsto g(x) = \log_2 x$?
9. Analizar si $f : \mathbb{R}^3 \rightarrow M(2, \mathbb{R}) / (x_1, x_2, x_3) \mapsto \begin{pmatrix} x_1 & 0 \\ x_2 & x_3 \end{pmatrix}$ es un homomorfismo de grupos. En caso afirmativo, clasificarlo.
10. Verificar que $f : \mathbb{R} \rightarrow \mathbb{R} / x \mapsto f(x) = -3x$ es un automorfismo de \mathbb{R} en sí mismo. ¿Qué sucede con $g : \mathbb{R} \rightarrow \mathbb{R} / x \mapsto g(x) = x + 1$?
11. Determinar si $f : \mathbb{R}^3 \rightarrow \mathbb{R}^2 / (a, b, c) \mapsto (a - c, b - c)$ es un homomorfismo de grupos. En caso afirmativo, hallar su núcleo.
12. Sean $(M(n, \mathbb{R}), +)$ y $(\mathbb{R}, +)$ grupos aditivos. Verificar que $f : M(n, \mathbb{R}) \rightarrow \mathbb{R}$ dada por $f \left(\begin{bmatrix} a & b \\ c & d \end{bmatrix} \right) = a + d$ es un homomorfismo y hallar su núcleo.

13. Analizar si $f : \mathbb{Z} \rightarrow \mathbb{C}/n \mapsto i^n$ es un homomorfismo de grupos. En caso afirmativo, determinar núcleo e imagen.
14. Analizar si $S = \{(x, y) \in \mathbb{R}^2 / y = 2x\}$ es subgrupo de \mathbb{R}^2 .
15. Verificar que $G = \{1, -1, i, -i\}$ es un grupo cíclico y determinar sus generadores.
16. Encontrar los generadores de $(\mathbb{Z}_6, +)$ y de $(\mathbb{Z}_5 - \{\bar{0}\})$.
17. Indicar el orden de todos los elementos de $(\mathbb{Z}_6, +)$ y de $(\mathbb{Z}_5 - \{\bar{0}\})$.