Introducción

Cuando un novel estudiante de álgebra abstracta se enfrenta a expresiones como grupo cociente, espacio cociente, cree y con justificada razón, que se enfrentará a conjunto de cocientes, finalmente se resigna a saber que esto no es así, lo cual no significa que sean conceptos difíciles de asimilar. EL objetivo de esta monografía es definir y ejemplificar la idea de grupo factor, también llamado GRUPO COCIENTE debido a la notación empleada, el cual es un conjunto de conjuntos llamados clases laterales que posee una estructura algebraica, la de grupo, es decir, sobre dicho conjunto se ha definido una operación binaria que cumple ciertas condiciones; se enfatiza el hecho que no siempre el conjunto de clases laterales tendrá la estructura de grupo, pequeño inconveniente que fue salvado por Evaristo Galois al introducir la brillante idea de SUBGRUPO NORMAL.

PRELIMINARES

Debemos aclarar que el grupo $(G,*)$ será representado sólo por G, y al elemento $a*b$ se le representará usando la expresión ab. Iniciaremos nuestra exposición con la siguiente ASERCIÓN: Sea H un subgrupo de G, la relación en G definida por $a \equiv b(\text{mod}\, H) \Leftrightarrow ab^{-1} \in H$ es una relación de equivalencia.

Como matemáticos no podemos quedarnos con la duda, en efecto:

i. Reflexividad. $a \equiv a(\text{mod}\, H) \Leftrightarrow aa^{-1} = e \in H$

ii. Simetría. Si $a \equiv b(\text{mod}\, H) \rightarrow ab^{-1} \in H$ luego $\left(ab^{-1}\right)^{-1} \in H$, así $ba^{-1} \in H$. De modo que $b \equiv a(\text{mod}\, H)$.

iii. Transitividad. Sean $a \equiv b(\text{mod}\, H)$ y $b \equiv c(\text{mod}\, H)$ luego $ab^{-1}, bc^{-1} \in H$ multiplicando ambos elementos $\left(ab^{-1}\right)\left(bc^{-1}\right) = aec^{-1} = ac^{-1} \in H$. Se tiene que $a \equiv c(\text{mod}\, H)$.

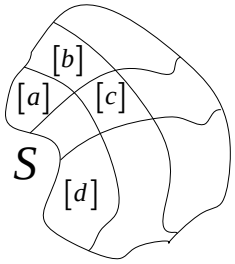
Concluimos que $a \equiv b(\text{mod}\, H)$ es una relación de equivalencia.

Una relación de equivalencia produce una partición del conjunto en subconjuntos o celdas como veremos más adelante.

Nota 01.- La relación también puede ser definida como $a \equiv b(\text{mod}\, H) \Leftrightarrow a^{-1}b \in H$

DEFINICIÓN 01: Si "$\sim$"es una relación de equivalencia en un conjunto $S \neq \Phi$, entonces se define la clase $[a]$ de a, como $[a] = \{b \in S / b \sim a\}$.

De manera que el conjunto S queda particionado en celdas, las cuales son disjuntas, al conjunto $[a]$ también se le denomina **clase de equivalencia**. Donde a es llamado representante de la clase.



Teorema 01.- Si "$\sim$"es una relación de equivalencia en S y $a, b \in S$, entonces las siguientes proposiciones son equivalentes:

1) $[a] = [b]$

2) Si $[a] \neq [b]$, entonces $[a] \cap [b] = \Phi$

3) $S = \cup [a]$

DEFINICIÓN 02: Si H es un subgrupo de G y sea $a \in G$ al conjunto $Ha = \{ha / h \in H\}$ se le denomina **clase lateral izquierda**.
Análogamente se puede definir clase lateral derecha.
Se tiene que:

$$\begin{aligned}[a] &= \{b \in G / \ \ b \sim a\} = \{b \in G / \ \ b \equiv a (\mathrm{mod}\, H)\} \\ &= \{b \in G / \ \ ba^{-1} \in H\} = \{b \in G / \ \exists h \in H,\ ba^{-1} = h\} \\ &= \{b \in G / \ \ b = ha, h \in H\} = \{ha / \ \ h \in H\}\end{aligned}$$

Luego $[a] = Ha$, es decir las clases de equivalencia (congruencia derecha) son las clases laterales derechas.

A continuación veremos un ejemplo de cómo un conjunto es particionado en celdas a partir de una relación de equivalencia. Este ejemplo es importarte y sirve para ejemplificar muchos conceptos que son tratados en álgebra abstracta como el concepto que aquí nos ocupa, el de GRUPO COCIENTE.

Nota 02.- Hasta aquí ya es posible demostrar el importantísimo teorema de Lagrange.

Ejemplo: **Congruencia módulo n en el conjunto de los enteros.**
Sean $h, k \in \mathbb{Z}$ definimos la congruencia de h con k módulo n como:

$h \equiv k (\mathrm{mod}\, n) \ \Leftrightarrow \ (h-k)$ es divisible por $n \ \Leftrightarrow \ (h-k) = mn, \ \ m \in \mathbb{Z}$

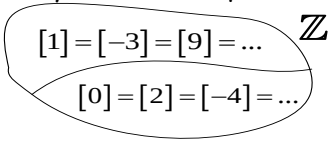
ASERCIÓN: $h \equiv k (\mathrm{mod}\, n)$ es una relación de equivalencia en $\mathbb{Z}$. (Demostración trivial)
Describamos las clases de equivalencia o residuales para $n = 1, 2, 3, \ldots$

- Para $n = 1$, en este caso se tiene $h \equiv k (\mathrm{mod}\, 1) \Leftrightarrow h - k = 1.m = m \in \mathbb{Z}$
  De modo que $[h] = \{k \in \mathbb{Z} / \ \ h - k = m \in \mathbb{Z}\}$, es evidente que $[h] = \mathbb{Z}$.

No existe partición en $\mathbb{Z}$, pues solamente hay una clase, el mismo $\mathbb{Z}$.

- Para $n = 2$, se tiene $h \equiv k (\mathrm{mod}\, 2) \Leftrightarrow h - k = 2m, \ \ m \in \mathbb{Z}$
  Así $[h] = \{2m + k, \ \ m \in \mathbb{Z}\}$,
  *Si $k = 0$ se tiene que $[h] = \{2m, \ \ m \in \mathbb{Z}\}$, o sea que la clase $[h]$ sería la de los números divisibles por 2. Dándole valores a m se obtiene $[h] = \{0, \ \pm 2, \ \pm 4, \ \pm 6, \ldots\}$, como representante de esta clase se puede elegir cualquier valor como; cero, dos, menos cuatro,... etc. $[0] = [2] = [-4] = \{0, \pm 2, \pm 4, \pm 6, \ldots\}$.
  *Si $k = 1$ se tiene que $[h] = \{2m + 1, \ \ m \in \mathbb{Z}\}$, o sea que la clase $[h]$ sería la de los números divisibles por 2 con residuo 1. Dándole valores a m se obtiene $\{\pm 1, \ \pm 3, \ \pm 5, \ \pm 7 \ldots\}$, como representante de esta clase se puede elegir cualquier valor como; uno, menos tres, nueve,...etc. $[1] = [-3] = [9] = \{\pm 1, \pm 3, \pm 5, \pm 7 \ldots\}$.

Es fácil ver que el conjunto de los números enteros se partió o dividió en dos subconjuntos o clases: los enteros divisibles por dos y los enteros que no son divisibles por dos.



- Para $n=3$, se tiene $h\equiv k\left(\operatorname{mod}3\right)\Leftrightarrow h-k=3m,\ \ m\in\mathbb{Z}$

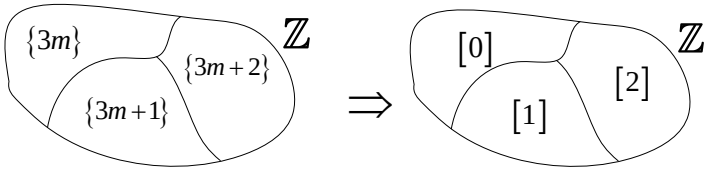
  Así $\left[h\right]=\left\{3m+k,\ \ m\in\mathbb{Z}\right\}$ obviamente se tendrán tres conjuntos diferentes a saber:

  * Si $k=0$ se tiene que $\left[h\right]=\left\{3m,\ \ m\in\mathbb{Z}\right\}$, o sea que la clase $\left[h\right]$ sería la de los números divisibles por 3. Dándole valores a m se obtiene $\left[h\right]=\left\{0,\pm3,\pm6,\pm9,...\right\}$, como representante de esta clase se puede elegir cualquier valor como; cero, tres, menos seis,... etc. $\left[0\right]=\left[3\right]=\left[-6\right]=\left\{0,\pm3,\pm6,\pm9,...\right\}$.

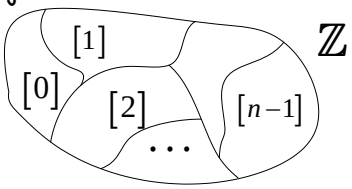
  * Si $k=1$ se tiene que $\left[h\right]=\left\{3m+1,\ \ m\in\mathbb{Z}\right\}$, o sea que la clase $\left[h\right]$ sería la de los números divisibles por 3 con residuo 1. Dándole valores a m se obtiene $\left\{1,4,7,10,13...,-2,-5,-8,-11,...\right\}$, como representante de esta clase se puede elegir cualquier valor. Se suele elegir a 1.

  * Si $k=2$ se tiene que $\left[h\right]=\left\{3m+2,\ \ m\in\mathbb{Z}\right\}$, o sea que la clase $\left[h\right]$ sería la de los números divisibles por 3 con residuo 2. Dándole valores a m se obtiene $\left\{2,5,8,11,14...,-1,-4,-7,-10,...\right\}$, como representante de esta clase se puede elegir cualquier valor. Se suele elegir a 2.

Es fácil ver que el conjunto de los números enteros se divide en tres subconjuntos o clases:



Podemos inferir inductivamente que para la congruencia módulo n el conjunto de los números enteros se particiona en n subconjuntos:



Nota 03.- El número de elementos de las clases de equivalencia o clases laterales es el mismo, como se demuestra rápidamente empleando la transformación $\lambda_a : H\to Ha$ definida mediante $\lambda_a\left(h\right)=ha$, la cual por definición es una sobreyección, además es uno a uno.

DEFINICIÓN 03: Un subgrupo N de un grupo G se denomina subgrupo normal de G, si $g^{-1}Ng=N,\ \ \forall g\in G$, y se denota $N\lhd G$.

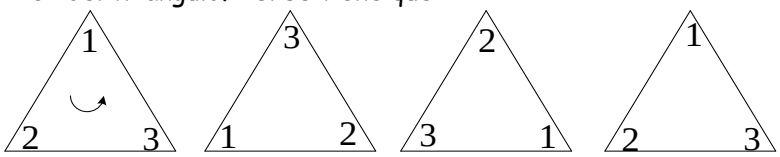
La expresión $g^{-1}Ng=N$ debe entenderse en el siguiente sentido: si g y n son elementos cualesquiera de G y N respectivamente el producto $g^{-1}ng$ siempre es un elemento de N. A veces se escribe en la definición $g^{-1}Ng\subset N$, no obstante es posible demostrar $N\subset g^{-1}Ng$ (¡Hágalo!) de modo que la igualdad es válida.

Los subgrupos normales son los subgrupos resaltantes de un grupo ya que tienen la propiedad de mantenerse invariantes bajo un **automorfismo interno** $\varphi_g : G\to G/\ \varphi_g\left(h\right)=g^{-1}hg$, podemos decir que bajo este automorfismo dos elementos de N permutan respecto a un

elemento de G entiéndase $n_1 g = g n_2$, es decir, pueden cambiar de nombre pero no dejan N. Por otro lado, las clases laterales izquierdas obtenidas a partir de N coinciden con las clases derechas lo cual permite una de las construcciones más simples en la teoría de grupos.

Nota 04.- Un isomorfismo es una sobreyección entre dos grupos, $\varphi : G \to G'$, que cumple la condición $\varphi(ab) = (\varphi a)(\varphi b)$, cuando $G' = G$ se le denomina automorfismo.

Ejemplo: Consideremos el grupo simétrico de grado tres S_3. Recordemos que **el grupo simétrico de grado n** denotado S_n ó $A(S)$ es el grupo de todas las aplicaciones inyecticas del conjunto S sobre si mismo, con $card(S) = n$, cuyos elementos son denominados permutaciones. En el caso S_3 tomaremos $S = \{1,2,3\}$, ya que es posible hacer una comparación maravillosa entre los elementos de S_3 y las permutaciones de los vértices de un triángulo equilátero.
Si consideramos un triángulo equilátero de vértices $1, 2$ y 3, llamaremos ρ_i a las rotaciones de 120° del triángulo. Así se tiene que:

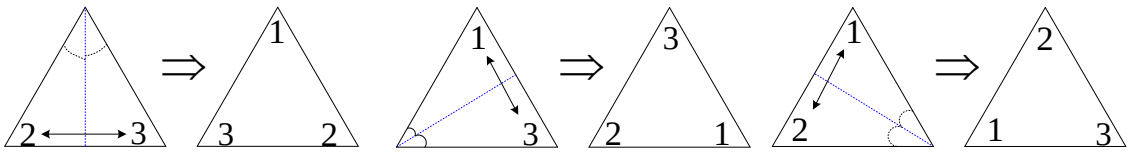


Posición inicial rota 120° rota 240° rota 360°

Obteniéndose las rotaciones sucesivas $\rho_i : S \to S$ dadas por:

$$\rho_1 := \begin{cases} 1 \to 2 \\ 2 \to 3 \\ 3 \to 1 \end{cases} \quad \rho_2 := \begin{cases} 1 \to 3 \\ 2 \to 1 \\ 3 \to 2 \end{cases} \quad \rho_0 := \begin{cases} 1 \to 1 \\ 2 \to 2 \\ 3 \to 3 \end{cases}$$

A las reflexiones de dos vértices respecto de la bisectriz del tercer vértice del triángulo las llamaremos μ_i de modo que:



Se han generado las aplicaciones

$$\mu_1 := \begin{cases} 1 \to 1 \\ 2 \to 3 \\ 3 \to 2 \end{cases} \quad \mu_2 := \begin{cases} 1 \to 3 \\ 2 \to 2 \\ 3 \to 1 \end{cases} \quad \mu_3 := \begin{cases} 1 \to 2 \\ 2 \to 1 \\ 3 \to 3 \end{cases}$$

El poder identificar los elementos de S_3 con las aplicaciones definidas anteriormente se debe a la poderosa idea de isomorfismo, a través del cual dos conjuntos son indistinguibles desde el punto de vista algebraico.
La tabla obtenida al realizar todas las posibles "multiplicaciones" entre los elementos de S_3 se muestra más abajo. Debe aclararse que la operación de grupo adecuada es la composición de aplicaciones la cual se define como $\sigma\tau = \tau \circ \sigma$, $\forall \sigma, \tau \in S_3$.

Por ejemplo:

Sean $\mu_1, \rho_2 \in S_3$ entonces $\mu_1\rho_2 = \rho_2 \circ \mu_1$, así se tendrá que:

$(\rho_2 \circ \mu_1)(1) = \rho_2(\mu_1(1)) = \rho_2(1) = 3$, de modo que $1 \to 3$

$(\rho_2 \circ \mu_1)(2) = \rho_2(\mu_1(2)) = \rho_2(3) = 2$, de modo que $2 \to 2$

$(\rho_2 \circ \mu_1)(3) = \rho_2(\mu_1(3)) = \rho_2(2) = 1$, de modo que $3 \to 1$

Podemos ver que se ha generado la aplicación μ_2.

La tabla para el grupo será:

	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_0	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_1	ρ_1	ρ_2	ρ_0	μ_2	μ_3	μ_1
ρ_2	ρ_2	ρ_0	ρ_1	μ_3	μ_1	μ_2
μ_1	μ_1	μ_3	μ_2	ρ_0	ρ_2	ρ_1
μ_2	μ_2	μ_1	μ_3	ρ_1	ρ_0	ρ_2
μ_3	μ_3	μ_2	μ_1	ρ_2	ρ_1	ρ_0

De la tabla se puede deducir que:
El elemento identidad es ρ_0 y la inversa de una rotación es otra rotación de 360° en sentido horario, además las inversas de las reflexiones son las misma reflexiones $\mu_i^{-1} = \mu_i$.

* Consideremos el subgrupo $N_1 = \{\rho_0, \mu_1\}$, ¿será $N_1 \lhd S_3$?

Debemos verificar que se cumple la condición $g^{-1}ng \in N_1$

Tomemos $\mu_2 \in S_3 \to \mu_2^{-1}(\mu_1)\mu_2 = \mu_2(\mu_1)\mu_2 = \mu_2(\mu_1\mu_2) = \mu_2(\rho_2) = \mu_3 \notin N_1$, por lo tanto N_1 no es subgrupo normal de S_3. La condición $g^{-1}ng \in N_1$ se debe cumplir $\forall g \in S_3$.

* Ahora sea el subgrupo $N_2 = \{\rho_0, \rho_1, \rho_2\}$, ¿será $N_2 \lhd S_3$?

Podemos verificar fácilmente que

$\mu_i^{-1}(\rho_1)\mu_i = \mu_i(\rho_1)\mu_i = \mu_i(\rho_1\mu_i) = \mu_i(\mu_j) = \rho_2 \in N_2$, para $i \neq j$

$\mu_i^{-1}(\rho_2)\mu_i = \mu_i(\rho_2)\mu_i = \mu_i(\rho_2\mu_i) = \mu_i(\mu_j) = \rho_1 \in N_2$, para $i \neq j$

$\mu_i^{-1}(\rho_0)\mu_i = \mu_i(\rho_0)\mu_i = \mu_i(\rho_0\mu_i) = \mu_i(\mu_i) = \rho_0 \in N_2$

Evidentemente $\rho_i^{-1}(\rho_j)\rho_i \in N_2$ luego $N_2 \lhd S_3$.

Teorema 02.- $N \lhd G$ si y sólo si toda clase lateral derecha de N es una clase lateral izquierda.

Demostración:

$(\Rightarrow)$ Si $N \lhd G$ entonces $g^{-1}Ng = N, \quad \forall g \in G$, sean $n_1, n_2 \in N$ cualesquiera. Así $g^{-1}n_1g = n_2$ luego $g(g^{-1}n_1g) = gn_2 \Rightarrow (gg^{-1})n_1g = gn_2 \Rightarrow n_1g = gn_2$ así $Ng = gN, \quad \forall g \in G$.

$(\Leftarrow)$ Si $g \in G$, además $gN = N\overline{g}$ para alguna clase $N\overline{g}$

Ahora si $g = ge \to g \in gN \to g \in N\overline{g}$, también $g = eg \to g \in Ng$ pero según el teorema 01 las clases son disjuntas, así $N\overline{g} = Ng$. Por lo tanto $Ng = gN$ evidentemente se tiene que $g^{-1}Ng = N$ ■

Hasta aquí hemos visto que un grupo puede ser dividido en celdas, ¿será posible operar con estas celdas?

DEFINICIÓN 04: Sea $N \lhd G$ y sean Na y Nb clases laterales de N definimos el producto de clases laterales (derechas) como $(Na)(Nb) = Nab$.

Veamos si este producto está bien definido, es decir, que si elegimos cualquier par de representantes de ambas clases el producto siempre está en la misma clase lateral (derecha en este caso).

Sean $a', a'' \in Na$ y $b', b'' \in Nb$ se debe probar que $a'b' \in Nab$ y $a''b'' \in Nab$ ó lo que es lo mismo $a'b' \equiv a''b'' (\mathrm{mod}\, N)$. Se tiene que, si $a' \in Na \to a' = n_1 a''$, $b' \in Na \to b' = n_2 b''$ luego $a'b' = (n_1 a'')(n_2 b'') = n_1 (a'' n_2) b''$, pero por el teorema 02 $Na = aN$, así $n_1 (a'' n_2) b'' = n_1 (n_3 a'') b'' = (n_1 n_3) a''b'' \to (a'b')(a''b'')^{-1} = n_1 n_3 \in N$ ■

Nota 05.- En el caso de emplear la notación aditiva, que es reservada para grupos abelianos, $G = (G, +)$, la operación de clases se escribiría $(N + a) + (N + b) = N + a + b$.

Ya tenemos los elementos necesarios construir nuestro grupo, pues hablar de grupo implica tener un conjunto (como el conjunto de clases laterales derechas o bien izquierdas), ¡ya lo tenemos! y una operación binaria ¡ya la definimos! , ¿Podemos formar un grupo? veamos:

GRUPO COCIENTE

Teorema 03.- Si $N \lhd G$ y sea el conjunto $G/N = \{[g] / g \in G\} = \{Ng / g \in G\}$, entonces G/N es un grupo bajo la operación $(Na)(Nb) = Nab$.

Demostración:
Ya se probó que la operación inducida está bien definida. La asociatividad es inmediata, si Na, Nb y Nc son elementos de G/N de ahí que $(Na)(NbNc) = Na(Nbc) = Na(bc)$, y por otro lado $(NaNb)(Nc) = Nab(Nc) = N(ab)c$, pero por la asociatividad en G tenemos que $a(bc) = (ab)c$, de modo que se cumple la ley asociativa para clases.
Por otro lado afirmamos que $Ne = N$ es el elemento identidad del grupo, pues es fácil verificar que $NaNe = Nae = Na$ y $NeNa = Nea = Na$. Esto debe entenderse como si en la clase $Ne = N$ todos los elementos de N se convierten en "e". Finalmente el inverso para cada elemento de G/N viene dado por $(Na)^{-1} = Na^{-1}$. Por lo tanto G/N es un grupo llamado **grupo factor de G módulo N ó grupo cociente de G por N.**

Nótese que la definición de G/N se hace para clases derechas, igualmente resulta si se hace para clases izquierdas.

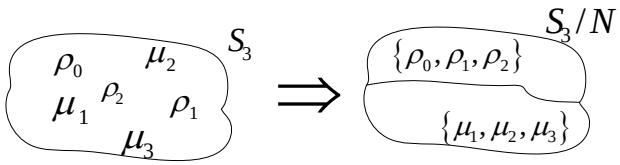
Debe quedar claro que la idea de subgrupo normal es aquí primordial, puesto que para cualquier subgrupo H de G el conjunto de clases laterales derechas o izquierdas no siempre será un grupo con la operación inducida como podemos ver en el:

Ejemplo: Sea $H=\{\rho_0,\mu_1\}$, como vimos anteriormente no es subgrupo normal, si hallamos las clases laterales derechas de H obtenemos tres: $H\rho_1=\{\rho_1,\mu_3\}$, $H\rho_2=\{\rho_2,\mu_2\}$ y el mismo $H=\{\rho_0,\mu_1\}$ ¿el conjunto $\{H\rho_1,H\rho_2,H\rho_0\}$ será grupo?... No. Ya que la operación no es cerrada como se ve fácilmente: $H\rho_1 H\rho_2=H\rho_1\rho_2=H\rho_0=H$, o sea, si tomamos elementos de clases diferentes de H su producto debe estar en H, pero $\mu_3\mu_2=\rho_1\notin H$.

Podemos resumir que: si un grupo es dividido en celdas, o mediante las clases laterales generadas a partir de determinado subgrupo o mediante una relación de equivalencia congruente con determinado subgrupo, no obstante estas celdas se operan empleando la operación heredada del grupo; entonces este nuevo conjunto será un grupo siempre y cuando el subgrupo empleado sea normal o invariante.

¿Quién es G/N?...no es más que un reagrupamiento de los elementos de G de modo que es posible pensar en una relación entre ambos grupos…un homomorfismo (lo tratamos brevemente más adelante y conlleva a una idea capital: la de isomorfismo).
De ser G finito se tiene que el número de elementos de G/N es $|G|/|N|$ como es fácil demostrar.

Ejemplo: Si volvemos al grupo simétrico S_3 y consideramos el subgrupo normal $N=\{\rho_0,\rho_1,\rho_2\}$, ¿quién será S_3/N?, ¿cómo se divide S_3 a partir de este subgrupo?, ¿Cuáles son las clases laterales de N?, vemos que las clases laterales son:
$N\rho_1=N\rho_2=N\rho_0=N$, por otro lado $N\mu_1=N\mu_2=N\mu_3=\{\mu_1,\mu_2,\mu_3\}$ así S_3 se divide en dos clases la clase de las rotaciones ρ_i y la clase de las reflexiones μ_i.



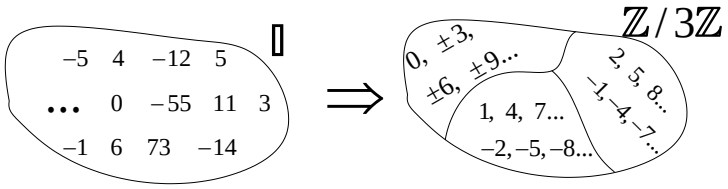
Se observa a simple vista que $|S_3|=6$, $|N|=3$ luego $|S_3/N|=|S_3|/|N|=6/3=2$.

Ejemplo: Si consideramos el grupo infinito $(\mathbb{Z},+)$, recordemos que en un ejemplo anterior vimos que la congruencia módulo 3 en $\mathbb{Z}$ a divide a $\mathbb{Z}$ en tres subconjuntos.
Tomemos el subgrupo normal $(3\mathbb{Z},+)$ (el grupo formado por los múltiplos de 3) entonces las clases laterales, con la notación aditiva, que se obtienen a partir de este subgrupo serán solo tres:

$$3\mathbb{Z}+0=\{3m+0=3m\ /\ m\in\mathbb{Z}\}=[0]$$
$$3\mathbb{Z}+1=\{3m+1\ /\ m\in\mathbb{Z}\}=[1]$$
$$3\mathbb{Z}+2=\{3m+2\ /\ m\in\mathbb{Z}\}=[2]$$

De modo que las clases laterales son exactamente las clases de equivalencia que obtuvimos anteriormente.

Siendo así, el grupo cociente $\mathbb{Z}/3\mathbb{Z}$ tiene sólo tres elementos: $\{[0],[1],[2]\}$



HOMOMORFISMOS

La relación existente entre el grupo inicial G y el grupo resultante G/N viene dada matemáticamente a través de una transformación llamada homomorfismo, idea que analizamos a continuación:

Sea una transformación, digamos φ, entre dos grupos G y G' con sus respectivas operaciones, es decir, un $g \in G$ es transformado en $g' = \varphi(g) \in G'$ vía φ. Ahora, si $a, b \in G$ es posible hablar de $ab \in G$ del mismo modo que se debe tener $\varphi(a)\varphi(b) \in G'$. Si exigimos para cualquier par se cumpla $\varphi(ab) = \varphi(a)\varphi(b)$ (la transformación φ preserva la operatividad de a y b para sus imágenes), entonces a φ se le llama homomorfismo. Una definición formal será:

DEFINICIÓN 05: Sean los grupos $(G,*)$ y $(G',\otimes)$ se llama homomorfismo a la transformación $\varphi: G \to G'$ que satisface $\varphi(a*b) = \varphi(a) \otimes \varphi(b)$, para cualquier $a, b \in G$.

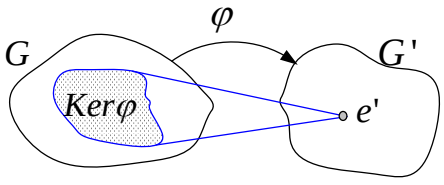
Ejemplo: Sean $(\mathbb{Z},+)$ y $(5\mathbb{Z},+)$ grupos bajo la suma usual, la transformación $\varphi: \mathbb{Z} \to 5\mathbb{Z}$ dada por $\varphi(n) = 5n$ es un homomorfismo, ya que $\varphi(n+m) = 5(n+m) = 5n + 5m = \varphi(n) + \varphi(m)$

Teorema 04.-Si $N \lhd G$ entonces existe un homomorfismo Ψ de G sobre G/N.

Para la demostración del teorema se necesita definir la transformación Ψ, la cual existe naturalmente como se ve en los dos últimos ejemplos de grupo cociente. Así $\Psi: G \to G/N$ dado por $\Psi(a) = [a]$.
Luego $\Psi(ab) = [ab] = [a][b] = \Psi(a)\Psi(b)$.

DEFINICIÓN 06: Se llama kernel de un homorfismo $\varphi: G \to G'$, denotado $Ker\varphi$, a todos los elementos de G cuya imagen bajo φ sea el elemento identidad e' de G', así:

$$Ker\varphi = \{g \in G / \ \varphi(g) = e'\}$$



Ejemplo: De acuerdo con el teorema 04 podemos definir $\varphi:\mathbb{Z}\to\mathbb{Z}/3\mathbb{Z}$, digamos $\varphi(n)=[n]$, ¿quién será $Ker\varphi$?

Por definición $Ker\varphi=\{k\in\mathbb{Z}/\ \varphi(k)=[0]\}$, ya que el elemento identidad de $\mathbb{Z}/3\mathbb{Z}$ es $[0]$, luego $\varphi(k)=[0]=\{3m/m\in\mathbb{Z}\}=[3m]$, entonces $k=3m\to Ker\varphi=\{3m/m\in\mathbb{Z}\}=3\mathbb{Z}$ que maravilla, el kernel del homomorfismo es el subgrupo normal que "genera" al grupo cociente. Esto queda justificado en los siguientes teoremas:

Teorema 05.- Si $\varphi:G\to G'$ es un homomorfismo y H es un subgrupo de G, entonces $\varphi(H)=\{\varphi(h),\ \ \forall h\in H\}$ es subgrupo de G'.

Nota 06.- Se demuestra fácilmente que $\varphi(e)=e'$ y $\varphi(g^{-1})=(\varphi(g))^{-1}$, en este sentido los homomorfismos son las transformaciones que preservan la estructura algebraica de grupo.

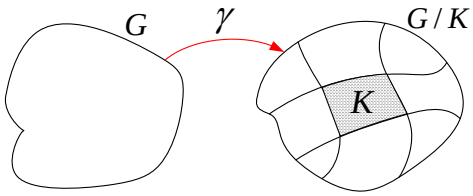
Teorema 06.- Si $\varphi:G\to G'$ es homomorfismo, entonces $Ker\varphi\lhd G$.

Demostración:

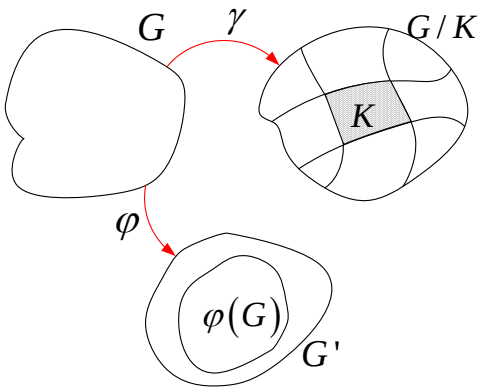
Si $k_1,k_2\in Ker\varphi\to\varphi(k_1)=\varphi(k_2)=e'$. Así $\varphi(k_1k_2)=\varphi(k_1)\varphi(k_2)=e'e'=e'$, $\therefore(k_1k_2)\in Ker\varphi$

Hemos probado la cerradura en $Ker\varphi$, ahora empleando un conocido teorema, sean $k_1,k_2\in Ker\varphi$, luego $\varphi(k_1k_2^{-1})=\varphi(k_1)\varphi(k_2^{-1})=e'(\varphi(k_2))^{-1}=e'(e')^{-1}=e'$. Por tanto $Ker\varphi$ es subgrupo, nos falta demostrar la invarianza, ie, si $g\in G\to g^{-1}kg\in Ker\varphi,\ \forall k\in Ker\varphi$, veamos $\varphi(g^{-1}kg)=\varphi(g^{-1})\varphi(k)\varphi(g)=(\varphi(g))^{-1}e'\varphi(g)=e'$. Se concluye que $Ker\varphi\lhd G$ ■

Finalmente, hemos visto que G y G/N están relacionados (teorema 04). Además puesto que el núcleo (kernel) de cualquier homomorfismo es un subgrupo normal (teorema 06) podemos construir el grupo cociente G/K donde K representa el kernel. Así existe un homomorfismo $\gamma:G\to G/K$, $K=Ker\gamma$.

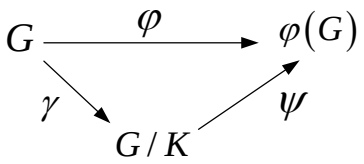


Por otro lado, el kernel de un homomorfismo $\varphi:G\to G'$ por definición está relacionado con G', precisamente con $e'=\varphi(e)\in\varphi(G)$



Nos preguntamos ¿existirá alguna relación entre G/K y $\varphi(G)$?...Por supuesto, la relación viene dada por el teorema siguiente, donde empleamos la idea de isomorfismo (un homomorfismo que además es una biyección) que nos indica que dos estructuras algebraicas (grupos) son idénticas salvo por el nombre de sus elementos y la forma de operar a sus elementos.
En el gráfico anterior vale preguntar cómo son $\varphi(G)$ y G', ¿serán iguales?

Teorema Fundamental del homomorfismo.- Si $\varphi: G \to G'$ es un homomorfismo y $K = Ker\varphi$, entonces existe un isomorfismo canónico del grupo $\varphi(G)$ sobre G/K.
Aquí la palabra canónico debe entenderse como natural, existencia evidente.
Para la demostración se define naturalmente la transformación $\psi: G/K \to \varphi(G)$ como $\psi(Ka) = \varphi(a)$, generando



Del diagrama se obtiene la factorización $\varphi = \gamma\psi$.

Esperamos haber cumplido con nuestro objetivo, rogamos a los estudiantes en quienes caiga esta monografía no dejar de maravillarse con las matemáticas puras.

Referencias:

- Herstein I. N. — "Álgebra Abstracta" Grupo Editorial Iberoamericana, México 1988
- Fraleigh Jhon B. — "Álgebra Abstracta" Addison-Wesley Iberoamerica, México 1988
- Adilson Goncalves — "Introducao à álgebra" IMPA, Brasil 1999.

Algunos enlaces en la Web:

http://docentes.uacj.mx/gtapia/Moderna/Contenido/Unidad%20III/NORMALES%20Y%20COCIENTE.htm

http://www.monografias.com/trabajos57/grupo-sobre-conjunto/grupo-sobre-conjunto2.shtml