Universidad Tecnológica Nacional
Facultad Regional Buenos Aires

Secretaría de Gestión Académica

GRUPOS Y SEMIGRUPOS

Unidad 5

GRUPOS Y SEMIGRUPOS

En esta unidad estudiaremos algunas de las estructuras algebraicas que se utilizan en Teoría de Codificación y también en el estudio de máquinas de estado finito, como por ejemplo los autómatas que veremos en la última unidad de esta asignatura. Dichas máquinas, reconocedoras de lenguajes, se usan en el diseño de compiladores y por ello es muy importante trabajar con ellas.

Comencemos por retomar el concepto de operación binaria cerrada que hemos estudiado en la unidad 2, y de acuerdo a las propiedades que cumpla le daremos un nombre a la estructura. Es así que podrá tratarse de semigrupo, semigrupo con neutro o grupo, y en algunos casos grupo abeliano.

Recordemos: ¿Qué es una Operación Cerrada?...

Sea $A \neq \emptyset$, $*: A^2 \to A$ es operación binaria cerrada si es función.
O dicho de otra forma:
$*$ es operación binaria cerrada en A si y sólo si: $\forall\, a, b \in A : a * b \in A$

Recordemos también que las operaciones binarias cerradas se pueden denotar con el símbolo $*$ o cualquier otro, como

$\otimes$, $\bullet$, $\blacklozenge$, $\oplus$, Δ, $\square$, etc.

Por ejemplo, para indicar que en el conjunto A se ha definido la operación binaria $*$ se escribe $(A ; *)$

A continuación, daremos los nombres de algunas de las principales estructuras algebraicas que puede alcanzar un conjunto en el que está definida una operación binaria y cerrada.

Sea $A \neq \emptyset$ y $*$ es una operación binaria y cerrada definida en A.

Si además $*$ es asociativa $\Rightarrow (A ; *)$ es SEMIGRUPO

Si además $*$ tiene neutro $\Rightarrow (A ; *)$ es SEMIGRUPO CON NEUTRO

Si además $*$ tiene simétrico

(es decir si TODOS los elementos poseen simétrico respecto de la operación $*$) $\Rightarrow (A ; *)$ es GRUPO

En cualquiera de los casos anteriores, si además es conmutativa entonces a la estructura que posea $(A ; *)$ se le agrega "ABELIANO" (En honor al matemático Niels HenrikAbel (1802-1829), quien entre otras cosas demostró la insolubilidad de la quíntica utilizando la teoría de Grupos)

Si no recuerdas las propiedades mencionadas (asociativa, conmutativa, neutro, simétrico), puedes volver a leer en la unidad 2.

Veamos a continuación varios Ejemplos:

e Ejemplo 1: Indiquemos la estructura de $(R ; \bullet)$.

Sabemos que la multiplicación es cerrada en los reales es asociativa y tiene elemento neutro, que es el 1. Pero no todos los números reales tienen simétrico; en realidad hay sólo uno que no tiene simétrico, que es el cero, lo cual es suficiente para decir que no se cumple la propiedad de simétricos.
Por lo tanto la estructura que alcanza es SEMIGRUPO CON NEUTRO.
Pero la operación multiplicación es conmutativa, entonces la estructura completa será:
SEMIGRUPO ABELIANO CON NEUTRO.

e Ejemplo 2: Indiquemos la estructura de $(Z ; +)$.

Sabemos que la suma es cerrada en los enteros, es asociativa y tiene elemento neutro, que es el 0. También todos los números enteros tienen simétrico, que es el opuesto de cada uno. Por lo tanto la estructura que alcanza es GRUPO, y como la suma es conmutativa, entonces la estructura completa será: GRUPO ABELIANO.

e Ejemplo 3: Indiquemos la estructura de $(Q ; \ast)$ siendo $x \ast y = x + y - 3$

Esta es una operación combinada, no es de las usuales. Ya estuvimos trabajando con este tipo de operaciones en la unidad 2.
Analicemos primero si es operación cerrada y luego las propiedades que cumple:

1) ¿Es $\ast$ cerrada.? Debemos ver si se cumple que $\forall\, a, b \in Q : a \ast b \in Q$

Dem./ como $a \in Q \wedge b \in Q \Rightarrow a + b \in Q$ por ser $+$ cerrada en Q.

Luego como $3 \in Q \Rightarrow (a+b)-3 \in Q \Rightarrow a + b - 3 \in Q \Rightarrow a \ast b \in Q$

2) ¿Es $\ast$ asociativa? Debemos ver si $\forall\, a, b, c \in Q : a \ast (b \ast c) = (a \ast b) \ast c$

Dem./ Desarrollamos cada miembro de nuestra tesis por separado:

(I) $a \ast (b \ast c) = a \ast (b + c - 3) = a + (b + c - 3) - 3 = \mathbf{a + b + c - 6}$

(II) $(a \ast b) \ast c = (a + b - 3) \ast c = (a + b - 3) + c - 3 = \mathbf{a + b + c - 6}$

Las expresiones finales son iguales. Por lo tanto, $\ast$ es asociativa.

3) ¿Es $\ast$ conmutativa? Debemos ver si $\forall\, a, b \in Q: a \ast b = b \ast a$

Dem./ Desarrollamos cada miembro de nuestra tesis por separado:

(I) $a \ast b = \mathbf{a + b - 3}$

(II) $b \ast a = b + a - 3 = \mathbf{a + b - 3}$

Las expresiones finales son iguales. Por lo tanto, $\ast$ es conmutativa.

4) ¿Tiene $\ast$ elemento neutro? Debemos ver si $\exists\, e \in Q : \forall\, a \in Q : e \ast a = a \ast e = a$

Dem./ Como ya sabemos que $\ast$ es conmutativa, podemos buscar el neutro sólo a derecha y el mismo será neutro a izquierda.

$a \ast e = a \Rightarrow a + e - 3 = a \Rightarrow e - 3 = 0 \Rightarrow e = 3$

Por lo tanto $\ast$ tiene neutro que es $e = 3$

5) ¿Tiene $\ast$ elemento simétrico? Debemos ver si $\forall\, a \in Q : \exists\, a' \in Q : a \ast a' = a' \ast a = 3$

Dem./ Como ya sabemos que $\ast$ es conmutativa, podemos buscar el simétrico sólo a derecha y el mismo será simétrico a izquierda.

$a \ast a' = 3 \Rightarrow a + a' - 3 = 3 \Rightarrow a' = 6 - a$

Esto significa, por ejemplo, que el simétrico del 5 es el 1, el simétrico del 2 es el 4, etc.

Como todos los racionales tienen simétrico, con esa operación, se dice que $\ast$ tiene simétrico en ese conjunto.

Por lo tanto la estructura de $(Q ; \ast)$ es GRUPO ABELIANO

e

Ejemplo 4: Sea el conjunto $A = \{ a, b, c \}$ con la operación $\square$ dada por la siguiente tabla:

$\square$	**a**	**b**	**c**
a	c	a	b
b	a	b	c
c	b	c	a

1) ¿Es $\square$ cerrada en A? Eso se comprueba observando la tabla. Como todos los resultados están en el conjunto A, entonces $\square$ es cerrada en A.

2) ¿Es $\square$ conmutativa? Para que lo sea, la tabla debe ser simétrica respecto de su diagonal principal. Como lo es, entonces $\square$ es conmutativa.

$\square$	**a**	**b**	**c**
a	c	a	b
b	a	b	c
c	b	c	a

Aquí podemos ver que los elementos simétricos respecto de la diagonal principal son iguales.

3) ¿Tiene □ elemento neutro? Debemos fijarnos si alguna fila y columna repiten los elementos en el mismo orden en que están dispuestos en la tabla. Vemos que ello ocurre en este caso con la fila y columna del elemento **b**. Por lo tanto **b** es el neutro de □.

□	**a**	**b**	**c**
a	c	a	b
b	a	b	c
c	b	c	a

Aquí podemos ver que la fila y columna del elemento **"b"** repite los elementos dados.

4) ¿Tiene □ elemento simétrico? Debemos buscar el simétrico de cada elemento, buscando en su fila y columna al neutro. Por ejemplo, en la fila y columna de **a,** el elemento **b** (el neutro) se encuentra cuando se opera al elemento **a** con el elemento **c.** Ello significa que **a** y **c** son simétricos. Por lo tanto, **a'=c, c'=a** y **b'=b.** Todos tienen simétrico, por lo tanto la operación □ tiene simétrico.

□	a	b	c
a	c	a	b
b	a	b	c
c	b	c	a

Aquí podemos ver la ubicación del elemento neutro como resultado en cada fila y columna para poder encontrar para cada elemento su simétrico

5) ¿Es □ asociativa? Para analizar esta propiedad no podemos observar la tabla únicamente, sino que debemos verificar todos los casos posibles. Como la definición de la propiedad asociativa nombra a tres elementos genéricos, hay que pensar en todos los casos que existen de valores que pueden tomar dichos elementos. Cada uno de ellos podrá tener cualquier valor de los elementos del conjunto, por lo tanto, en total habrá en este caso $3 \bullet 3 \bullet 3 = 3^3 = 27$ casos posibles. Por ejemplo:

$(a \square b) \square a = a \square (b \square a)$ ya que $(a \square b) \square a = a \square a = c$ y $a \square (b \square a) = a \square a = c$

$(c \square b) \square a = c \square (b \square a)$ ya que $(c \square b) \square a = c \square a = b$ y $c \square (b \square a) = c \square a = b$

$(b \square b) \square a = b \square (b \square a)$ ya que $(b \square b) \square a = b \square a = a$ y $b \square (b \square a) = b \square a = a$

... análogamente con los restantes 24 casos.

En general, si el conjunto tiene **n** elementos, la cantidad total de casos posibles es n^3.

Si en todos los casos se cumple la igualdad, entonces la operación es asociativa.
Por lo tanto la estructura de **(A ; □)** es GRUPO ABELIANO.

Ejemplo 5: Indiquemos la estructura de $(A ; \otimes)$ siendo $A = \{ a, b, c \}$ y la operación $\otimes$ dada en la siguiente tabla:

$\otimes$	**a**	**b**	**c**
a	b	c	a
b	c	b	c
c	a	c	b

1) ¿Es $\otimes$ una operación cerrada en A? Eso se comprueba observando la tabla. Como todos los resultados están en el conjunto A, entonces $\otimes$ es cerrada en A.

2) ¿Es $\otimes$ conmutativa? Para que lo sea, la tabla debe ser simétrica respecto de su diagonal principal. Como lo es, entonces $\otimes$ es conmutativa.

3) ¿Tiene $\otimes$ elemento neutro? Recordemos que debemos fijarnos si alguna fila y columna repiten los elementos en el mismo orden en que están dispuestos en la tabla. Vemos que ello no ocurre en este caso. Por lo tanto no existe elemento neutro de $\otimes$ en A.

4) Como $\otimes$ no tiene neutro, no tiene sentido analizar si hay elementos con simétrico.

5) ¿Es $\otimes$ asociativa? Lamentablemente, como ya dijimos, para analizar esta propiedad no podemos hacerlo a simple vista observando la tabla, sino que debemos verificar todos los casos de elementos tomados de a tres con o sin repetición.

Por ejemplo:

¿$(a \otimes b) \otimes a = a \otimes (b \otimes a)$? Sí, pues $(a \otimes b) \otimes a = c \otimes a = a$ y $a \otimes (b \otimes a) = a \otimes c = a$

Pero...

¿$(a \otimes b) \otimes c = a \otimes (b \otimes c)$? No, pues $(a \otimes b) \otimes c = c \otimes c = b$ y $a \otimes (b \otimes c) = a \otimes c = a$

Entonces no hay necesidad de analizar ningún otro caso, pues al no cumplirse éste no es asociativa.
Por lo tanto la estructura de $(A ; \otimes)$ no llega a ser un semigrupo.

Ejemplo 6: Ahora vamos a analizar la estructura de $(P ; +)$ siendo el conjunto P el siguiente:

$P = \{ x \in Z / x = 2 \bullet k \wedge k \in Z \}$ y la suma habitual.

¿Qué conjunto es P? Vemos que el conjunto P es el conjunto de los enteros pares.

1) ¿Es + cerrada en **P**? Debemos probar que $\forall\, a, b \in P : a + b \in P$

Dem./ $\forall\, a, b \in P$: $a = 2 \bullet k_1 \ \wedge \ b = 2 \bullet k_2$ con $k_1, k_2 \in Z$

Sumando miembro a miembro: $a + b = 2 \bullet k_1 + 2 \bullet k_2 \ \Rightarrow \ a + b = 2 \bullet (k_1 + k_2)$

Como k_1 y k_2 son enteros, su suma también lo es $\Rightarrow a + b = 2 \bullet k_3 \wedge k_3 \in Z$

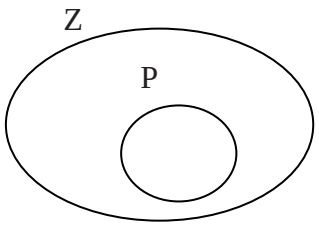
Por lo tanto $a + b \in P$. Y entonces + es cerrada en **P.**

2) ¿Es + asociativa en **P**? Debemos ver si $\forall\, a, b, c \in P: a + (b+ c) = (a+ b) + c$

Dem./ El conjunto **P** está incluido en **Z**. Nosotros sabemos que + es asociativa en **Z**, es decir que

$\forall\, a, b, c \in Z: a + (b+ c) = (a+ b) + c$

Por lo tanto, los elementos de **P** cumplen con esta propiedad.



Se dice que el subconjunto **P** "hereda" la propiedad del conjunto **Z** que lo incluye.

3) ¿Es + conmutativa en **P**? Ocurre lo mismo que con la asociativa. El conjunto **P** "hereda" la propiedad conmutativa de **Z**.

4) ¿Tiene + neutro en **P**? En este caso hay que fijarse, ya que no es algo que pueda heredarse del conjunto mayor. Puede ser que el neutro esté en el subconjunto o no.

En este caso, el neutro de + es el cero. Debemos ver si el cero pertenece a **P**. Si tenemos en cuenta que

$0 = 2 \bullet 0 \ \wedge \ 0 \in Z \Rightarrow 0 \in P \ \Rightarrow$ **P** tiene neutro de **+.**

5) ¿Tiene + simétrico en **P**? Al igual que con el neutro, debemos fijarnos si en este caso todos los elementos de **P** tienen su simétrico en **P**. El simétrico respecto de la suma usual es el opuesto. Entonces debemos ver si $\forall\, a \in P : -a \in P.$

Dem./ $\forall\, a \in P \Rightarrow a = 2 \bullet k \ \wedge k \in Z \ \Rightarrow$ multiplicando ambos miembros por (-1):

$- a = (-1) \bullet 2 \bullet k \ \Rightarrow$ asociando el -1 con k: $\quad - a = 2 \bullet (- k) \ \wedge \ - k \in Z$

Por lo tanto el opuesto de todo número par es par.
Finalmente la estructura de **(P ; +)** es GRUPO ABELIANO.

A continuación veremos otro ejemplo de grupo:

GRUPO DE PERMUTACIONES O GRUPO SIMÉTRICO S_3

Primero definimos el conjunto con el que vamos a trabajar:

Sea $A = \{ f: X \to X / f$ es función biyectiva$\}$ siendo $X = \{ 1, 2, 3 \}$

¿Te animas a dar alguno de los elementos de este conjunto A?

Observá que son las funciones biyectivas definidas en el conjunto $\{1,2,3\}$

Por ejemplo, una función de dicho conjunto podría ser la que asigna:
$f(1) = 3 ; f(2) = 1 ; f(3) = 2$

¿Cuántas hay en total?...

Como la función debe ser biyectiva, los valores 1, 2 y 3 deben aparecer exactamente una vez cada uno como imagen. Por lo tanto, lo que puede cambiar de una función a otra es únicamente el orden en que aparecen. En la función dada en el ejemplo anterior, el orden de las imágenes es: $3,1,2$.
También podría ser de otras formas.

> La cantidad de ordenamientos posibles de una cierta cantidad de elementos distintos, se denomina permutación y se calcula como el factorial de dicho número.

En este caso hay tantas funciones como permutaciones de tres números, es decir $P_3 = 3! = 6$
Vamos a encontrar las seis funciones que llamamos así: $A = \{ f_1, f_2, f_3, f_4, f_5, f_6\}$:

X	f_1	f_2	f_3	f_4	f_5	f_6
1	1	1	2	2	3	3
2	2	3	1	3	1	2
3	3	2	3	1	2	1

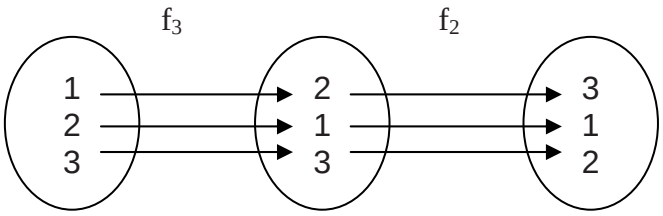
Es decir que la función que habíamos nombrado antes es aquí la f_5, ya que

$f_5(1) = 3$; $f_5(2) = 1$; $f_5(3) = 2$

Sabiendo de qué se trata el conjunto, consideremos la operación $\circ$ que es la composición de funciones, y vamos a analizar si $(A ; \circ)$ es un grupo.

¿Recuerdas cómo componer funciones?

Por ejemplo, para calcular $f_2 \circ f_3$, significa aplicar primero f_3 y a continuación f_2.



Observamos que es lo mismo que aplicar directamente la función f_5 , o sea $f_2 \circ f_3 = f_5$

De la misma manera debemos ir componiendo todas.
Como el conjunto es finito, nos conviene hacer una tabla:

$\circ$	f_1	f_2	f_3	f_4	f_5	f_6
f_1	f_1	f_2	f_3	f_4	f_5	f_6
f_2	f_2	f_1	f_5	f_6	f_3	f_4
f_3	f_3	f_4	f_1	f_2	f_6	f_5
f_4	f_4	f_3	f_6	f_5	f_1	f_2
f_5	f_5	f_6	f_2	f_1	f_4	f_3
f_6	f_6	f_5	f_4	f_3	f_2	f_1

Ya estamos en condiciones de comenzar a estudiar las **propiedades**:

1) Es operación binaria y cerrada, pues todos los resultados de la composición dieron elementos del mismo conjunto.
2) La operación es asociativa, pues lo es la composición de funciones en general. Entonces como este es un subconjunto sigue cumpliendo la propiedad.

Aquí lo demostraremos en general:

$\forall\ x \in \text{Dom}: [f \circ (g \circ h)](x) = f\,[(g \circ h)(x)] = f\,[(g\,(h(x))] = (f \circ g)\,[h(x)] = [(f \circ g) \circ h](x)$

3) La operación no es conmutativa, pues por ejemplo, $f_2 \circ f_3 = f_5$ pero $f_3 \circ f_2 = f_4$

4) El elemento neutro es la función f_1 , que es la función identidad.

5) Los simétricos de los elementos son: $f_1' = f_1$ $f_2' = f_2$ $f_3' = f_3$ $f_4' = f_5$ $f_5' = f_4$ $f_6' = f_6$

Por lo tanto $(A ; \circ)$ es un GRUPO y se lo llama S_3. Es un grupo NO abeliano.

Ahora pensemos...
Si el conjunto X en vez de tener 3 elementos, tuviera otra cantidad n, ¿cuántas funciones biyectivas habría?

En general cualquier Grupo S_n tiene $n!$ elementos.

Volveremos a considerar estos grupos luego de analizar algunas propiedades que nos van a resultar útiles y prácticas para resolver problemas.

PROPIEDADES QUE SE CUMPLEN EN UN GRUPO:

Sea $(A ; \ast)$ un grupo con neutro e. Entonces siempre se cumplen las siguientes propiedades:

1. El elemento neutro e es único.
2. El elemento neutro es su propio simétrico: $e' = e$
3. Propiedad involutiva del simétrico: $\forall a \in A: (a')' = a$
4. El simétrico de un elemento es único.
5. $\forall a, b \in A: (a \ast b)' = b' \ast a'$
6. Las ecuaciones $a \ast x = b$ y $x \ast a = b$ tienen solución única.
7. El único elemento idempotente es el elemento neutro. Es decir, $si\ a \ast a = a \Rightarrow a = e$
8. $\forall a, b \in A: a' = b \Rightarrow b' = a$

Vamos a demostrar aquí las de número impar y te proponemos que intentes demostrar las otras a modo de ejercitación.

Demostración de la propiedad **1**: El elemento neutro e es único.

Para ello, utilizaremos un método válido que se denomina Método de Reducción al absurdo. Consiste en suponer lo contrario a lo que queremos demostrar, y con ello llegar a una contradicción o absurdo, con lo cual queda garantizada nuestra tesis. En este caso, supongamos que en A existen dos elementos neutros distintos e_1 y e_2.

Por ser e_1 elemento neutro cumple: $\forall x \in A: \quad x \ast e_1 = x$

En particular, si tomamos como elemento x a e_2, nos queda: $e_2 \ast e_1 = e_2$ (expresión I)

Por otro lado, como e_2 es elemento neutro se cumple: $\forall x \in A: \quad e_2 \ast x = x$

En particular, si tomamos como elemento x a e_1, nos queda: $e_2 * e_1 = e_1$ (expresión II)

Observa las expresiones I y II. Tienen los primeros miembros iguales, por lo tanto los segundos también lo son. Con lo cual $e_1 = e_2$.

Y por lo tanto queda aprobada **la unicidad del elemento neutro en un grupo.**

Demostración de la propiedad 3: Propiedad involutiva del simétrico: $\forall\, a \in A: \ (a')' = a$

Por ser $(A\ ;\ *)$ un grupo, sabemos que todos los elementos tienen simétrico, es decir:

$\forall\, x \in A: \exists\, x' \in A : \ (x * x' = e \ \wedge \ x' * x = e)$

Entonces el elemento a' como pertenece a A, debe tener un simétrico que se denota $(a')'$.

Lo que debemos hacer es calcular quién es. Por definición se cumple que: $a' * (a')' = e$

Y a partir de esta igualdad vamos a despejar $(a')'$.

Para ello, operamos con a en ambos miembros a izquierda: $a * (a' * (a')') = a * e$

Luego por propiedad asociativa: $(a * a') * (a')' = a * e$

Por definición de los simétricos: $e * (a')' = a * e$

Por definición de elemento neutro: $(a')' = a$ que es lo que queríamos demostrar.

Demostración de la propiedad 5: $\forall\, a, b \in A: \ (a * b)' = b' * a'$

La demostración de esta propiedad es similar a la anterior, ya que como dijimos sabemos que cada elemento tiene simétrico pues estamos en un grupo.
Entonces el elemento $(a * b)$ debe tener un simétrico que se denota $(a * b)'$ y que cumple:

$(a * b) * (a * b)' = e$

Debemos despejar $(a * b)'$. Para ello, lo primero es aplicar la propiedad asociativa:

$a * b * (a * b)' = e$ y ahora operamos con a' en ambos miembros a izquierda

$a' * (a * b * (a * b)') = a' * e$

Nuevamente por propiedad asociativa: $(a' * a) * b * (a * b)' = a' * e$

Y por definición de simétricos: $e * b * (a * b)' = a' * e$

Por definición de elemento neutro: $b * (a * b)' = a'$

Observemos que logramos "pasar" la a que estaba en el primer miembro. Ahora debemos hacer el mismo procedimiento para "pasar" la b:

$$b' * (b * (a * b)') = b' * a' \Rightarrow (b' * b) * (a * b)' = b' * a' \Rightarrow e * (a * b)' = b' * a' \Rightarrow (a * b)' = b' * a'$$

Con lo cual quedó demostrada la propiedad 5.

Demostración de la propiedad 7: El único elemento idempotente es el elemento neutro.

$$a * a = a \Rightarrow a = e$$

Esta demostración es muy sencilla, partimos del antecedente o hipótesis: $a * a = a$

Y operamos en ambos miembros con a': $(a * a) * a' = a * a'$

Luego por propiedad asociativa: $a * (a * a') = a * a'$

Por definición de simétricos: $a * e = e$

Y finalmente por definición de elemento neutro: $a = e$

Queda demostrada la propiedad 7.

Te proponemos que intentes demostrar las restantes propiedades. Si tienes dificultades consulta a tu tutor, para que te oriente o revise tus demostraciones. Buena suerte!

ELEMENTOS REGULARES

Reconocer los elementos regulares de un semigrupo nos permite trabajar de una manera más rápida y agilizar los cálculos ya que podremos ahorrar pasos. Así denominaremos a los elementos de un semigrupo que cumplan con una cierta particularidad. Veamos la definición:

Sea $(A ; *)$ un semigrupo con neutro.

El elemento $a \in A$ es regular a izquierda $\Leftrightarrow a * x = a * y$ entonces $x = y$

El elemento $a \in A$ es regular a derecha $\Leftrightarrow x * a = y * a$ entonces $x = y$

El elemento $a \in A$ es regular si es regular a izquierda y a derecha.

Es decir:

Los elementos regulares son los cancelables, o sea los que se pueden suprimir al estar operados en ambos miembros de una igualdad.

- En la adición de enteros, todos los elementos son regulares.
- En la multiplicación de reales, todos excepto el cero son regulares.
- Consideremos la operación triangulito en Q: $x \Delta y = 3 \bullet (x + y)$

Veamos si todos sus elementos son regulares. Como es conmutativa, lo hacemos solo a derecha, arrancando del antecedente:

$x \Delta a = y \Delta a \Rightarrow 3 \bullet (x + a) = 3 \bullet (y + a) \Rightarrow x + a = y + a \Rightarrow x = y$

Por lo tanto, son todos regulares.

Propiedad: en un grupo todos los elementos son regulares.
Como en un grupo, todos los elementos tienen simétrico:

$a*x=a*y \Rightarrow a'*a*x=a'*a*y \Rightarrow (a'*a)*x=(a'*a)*y \Rightarrow e*x=e*y \Rightarrow x=y$

Análogamente se prueba a derecha.

Por ello, cuando trabajemos en un grupo, directamente vamos a poder usar la propiedad cancelativa, sin necesidad de hacer todos los pasos involucrados (operar ambos miembros con el simétrico del elemento, asociar, obtener el neutro, y por propiedad del neutro llegar la igualdad en la que ya no figura dicho elemento).
Pero si estamos trabajando en un semigrupo que no llega a ser grupo, podremos cancelar sólo aquellos elemento que tiene simétrico.
Por ejemplo, si cursaste Álgebra, recordarás que no todas las matrices son regulares respecto de la multiplicación. Solamente aquellas que tienen inversa.

INVERSIBLES DE UN SEMIGRUPO

Sea $(A ; *)$ un semigrupo con neutro. El conjunto de inversibles de A es:

$INV(A) = \{ a \in A / a' \in A \}$

O sea, es el conjunto de todos los elementos que tienen simétrico en el conjunto A respecto de la operación $*$

Veamos algunos ejemplos:

1) En $(Z ; \bullet)$, los inversibles son solamente el 1 y el -1, pues los demás enteros no tienen inverso entero.

2) En $(R ; \bullet)$, los inversibles son todos excepto el cero.

3) En el conjunto de matrices cuadradas de nxn con elementos reales y la multiplicación $(R^{nxn} ; \bullet)$, los elementos inversibles son las llamadas matrices inversibles o regulares, es decir aquellas cuyo determinante es distinto de cero.

4) En $(N_0 ; +)$, el único elemento inversible es el cero, ya que los demás no tienen su opuesto en este conjunto.

5) En $(Z_5 ; \bar{+})$, los inversibles son todos $\bar{0}, \bar{1}, \bar{2}, \bar{3}$ y $\bar{4}$, o sea todos.

6) En $(Z_6 ; \bar{\bullet})$, los inversibles son únicamente $\bar{1}$ y $\bar{5}$

En general: $INV(Z_n ; \bar{\bullet}) = \{ \bar{k} / m.c.d.\{k, n\} = 1 \wedge 1 \leq k \leq n-1 \}$

Propiedad:

Sea $(A ; \ast)$ un semigrupo con neutro. Entonces $(INV (A) ; \ast)$ es grupo y se lo llama Grupo de Inversibles del semigrupo
$(A; \ast)$.

Con referencia al ejemplo 6 anterior, el conjunto $\{ \bar{1} , \bar{5} \}$ es grupo multiplicativo.
Veamos su tabla:

$\bar{\bullet}$	$\bar{1}$	$\bar{5}$
$\bar{1}$	$\bar{1}$	$\bar{5}$
$\bar{5}$	$\bar{5}$	$\bar{1}$

PRODUCTO CARTESIANO DE GRUPOS

Sean $(G_1 ; \ast_1)$ y $(G_2 ; \ast_2)$ dos grupos con neutros e_1 y e_2 respectivamente.
En el conjunto $G_1 \times G_2$ se define la siguiente operación $\ast$ tal que:
$(a ; b) \ast (c ; d) = (a \ast_1 c ; b \ast_2 d)$
Entonces $(G_1 \times G_2 ; \ast)$ es grupo y se denomina grupo producto.

A modo de ejercitación, te proponemos que intentes demostrar lo enunciado anteriormente, es decir, que el producto cartesiano de dos grupos es también un grupo. Recuerda que si tienes dudas, puedes consultar al tutor.

Observación: Si $\ast_1$ y $\ast_2$ son conmutativas entonces $\ast$ también es conmutativa.

Te proponemos que demuestres la propiedad anterior.

Analicemos ahora algunos ejemplos:
Sean los grupos finitos $(G_1 ; \ast_1)$ y $(G_2 ; \ast_2)$ dados por las siguientes tablas:

$*_1$	**0**	**1**	**2**
0	0	1	2
1	1	2	0
2	2	0	1

$*_2$	**a**	**b**
a	a	b
b	b	a

Vamos a hallar el producto $G_1 \times G_2$ y definir la operación $*$ de modo que $(G_1 \times G_2 ; *)$ sea grupo.

$G_1 \times G_2 = \{ (0 ; a) , (0 ; b) , (1 ; a) , (1 ; b) , (2 ; a) , (2 ; b) \}$

La operación $*$ la indicamos en la siguiente tabla teniendo en cuenta que:

$(x ; y) * (z ; t) = (x *_1 z ; y *_2 t)$

Por ejemplo, para saber cuanto es $(1 ; a) * (2 ; b)$ hay que resolver: $(1 *_1 2 ; a *_2 b) = (0 ; b)$

y así con todos completamos la tabla:

$*$	(0 ; a)	(0 ; b)	(1 ; a)	(1 ; b)	(2 ; a)	(2 ; b)
(0 ; a)	(0 ; a)	(0 ; b)	(1 ; a)	(1 ; b)	(2 ; a)	(2 ; b)
(0 ; b)	(0 ; b)	(0 ; a)	(1 ; b)	(1 ; a)	(2 ; b)	(2 ; a)
(1 ; a)	(1 ; a)	(1 ; b)	(2 ; a)	(2 ; b)	(0 ; a)	(0 ; b)
(1 ; b)	(1 ; b)	(1 ; a)	(2 ; b)	(2 ; a)	(0 ; b)	(0 ; a)
(2 ; a)	(2 ; a)	(2 ; b)	(0 ; a)	(0 ; b)	(1 ; a)	(1 ; b)
(2 ; b)	(2 ; b)	(2 ; a)	(0 ; b)	(0 ; a)	(1 ; b)	(1 ; a)

Antes de continuar, sinteticemos lo que hemos desarrollado hasta aquí:

- *Presentamos las definiciones de semigrupo y de grupo, que son estructuras algebraicas que puede alcanzar un conjunto con una operación binaria y cerrada definida en él.*
- *Estudiamos varios ejemplos, de grupos y semigrupos finitos o infinitos.*
- *En particular, nos detuvimos en un grupo no conmutativo llamado grupo de permutaciones o grupo simétrico S_3 y un grupo producto de dos grupos dados.*
- *También presentamos algunas propiedades importantes de los grupos, los elementos regulares y los inversibles de un semigrupo.*

SUBGRUPOS

¿Qué te sugiere este nombre?...
Si lo relacionas con otros similares, como subconjunto, subespacio, subgrafo, etc. en lo que también se aplica el prefijo "sub" que indica que "está incluido", nos sugiere que se trata de una estructura dentro de otra.
En Álgebra para los Espacios Vectoriales, si dentro de un espacio está incluido otro, se lo llama subespacio. Lo mismo pasa con los grafos, y también con los grupos.
Básicamente, un subgrupo será "un grupo dentro de otro grupo". Veamos la definición formal:

Sea $(G ; *)$ un grupo y sea $H \neq \varnothing$ $H \subseteq G$.

Si $(H ; *)$ es grupo entonces H es subgrupo de G.

Dicho con palabras, un subgrupo es un conjunto no vacío, que está incluido en un grupo, y que en sí mismo es también grupo con la misma operación.

e Por ejemplo…

1) $(Z ; +)$ es un subgrupo del grupo $(R ; +)$, ya que cumple con la definición de subgrupo.

2) Consideremos el conjunto $P = \{ x \in Z / x = 2k$ con $k \in Z \}$

Observamos que el conjunto P es el de los enteros pares. Entonces: $(P ; +)$ es subgrupo del grupo $(Z ; +)$, pues cumple las condiciones:

a) No es vacío ;
b) Está incluido en Z ; y
c) Al sumar números pares, obtenemos siempre un número par, la suma es asociativa, el elemento neutro de la suma es el cero que es par, y el opuesto de un número par también es par, o sea que $(P ; +)$ es un grupo en sí mismo.

3) Si $(G ; *)$ es un grupo con neutro e , entonces $(\{e\} ; *)$ es el subgrupo más pequeño que puede tener y se denomina **subgrupo trivial** de $(G ; *)$

4) $(G ; *)$ es el subgrupo más grande de $(G ; *)$ y se denomina **subgrupo impropio** de $(G ; *)$

Todos los subgrupos de un grupo que no sean ni el trivial ni el impropio, se llaman subgrupos propios.

A continuación, veremos un teorema que nos va a resultar muy útil cuando tengamos que analizar si un determinado conjunto es subgrupo de un grupo dado.

TEOREMA: CONDICIÓN NECESARIA Y SUFICIENTE para SUBGRUPOS

Sea $(G ; *)$ un grupo.

H es subgrupo de $G \Leftrightarrow$
1) $H \neq \varnothing$
2) $H \subseteq G$
3) $\forall a,b \in H \Rightarrow a * b' \in H$

La demostración puedes encontrarla en el libro de la cátedra, capítulo18. Te invitamos a consultarlo.

¿Cómo usar la condición suficiente?

Dado un conjunto H y un grupo $(G ; *)$, si probamos que H cumple las tres condiciones numeradas 1,2 y 3, por este teorema ya podremos afirmar que H es un subgrupo del grupo dado.

¿Cómo usar la condición necesaria?

Dado un conjunto H y un grupo $(G ; *)$, si H no cumple con alguna de las 3 condiciones, podremos afirmar que H NO es subgrupo del grupo dado.

Para los subgrupos finitos, existe una propiedad que nos ahorra más esfuerzo aún:

Propiedad:

Si $(G ; *)$ es un grupo y H es un subconjunto finito no vacío, entonces H es subgrupo de G si y sólo si $*$ es cerrada en H.

Ejemplo 1:

Demostremos que $(nZ ; +)$ es subgrupo de $(Z ; +)$ siendo $nZ = \{ x \in Z / x = n k \text{ con } k \in Z \}$
Es decir, nZ es el conjunto de todos los múltiplos de n.

Para probar que es subgrupo, utilizaremos la condición suficiente del Teorema visto.

1) Como sabemos, el 1 es elemento neutro de la multiplicación, entonces : $n = n \bullet 1$ y $1 \in Z$,
por lo tanto, $n \in nZ$. Entonces $nZ \neq \varnothing$ ya que por lo menos tiene un elemento.

En realidad hay infinitos elementos, pero para garantizar que el conjunto no es vacío, mostrando uno solo - cualquiera sea - alcanza. A veces es cómodo utilizar al elemento neutro, pero no es necesario para probar que el conjunto no es vacío.

2) $nZ \subseteq Z$ por la definición de nZ (específicamente donde dice que está formado por $x \in Z$)

3) Sean $a, b \in nZ$. Entonces $a = n \bullet k \ \wedge \ b = n \bullet t$ con $k,t \in Z$

Primero obtenemos el opuesto de b: $-b = - n \bullet t$

Y ahora sumamos miembro a miembro: $a + (- b) = n \bullet k + (- n \bullet t)$

$\Rightarrow \quad a + (- b) = n \bullet (k +(- t)) \ \wedge \ \ k + (- t) \in Z$ ya que la suma de enteros es cerrada.

Por lo tanto $a + (- b) \in nZ$

Finalmente, como se cumplieron las tres condiciones suficientes de subgrupos, podemos afirmar que $(nZ ; +)$ es subgrupo de $(Z ; +)$

e Ejemplo 2:

Dado el grupo finito $(A ; \otimes)$ dado por la siguiente tabla:

$\otimes$	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**
a	a	b	c	d	e	f	g	h
b	b	c	d	a	h	g	e	f
c	c	d	a	b	f	e	h	g
d	d	a	b	c	g	h	f	e
e	e	g	f	h	a	c	b	d
f	f	h	e	g	c	a	d	b
g	g	f	h	e	d	b	a	c
h	h	e	g	f	b	d	c	a

¿Cuáles de los siguientes conjuntos son subgrupos?

$H = \{a, b\}$ $K = \{a, b, c, d\}$ $F = \{a, e\}$ $M = \{a, e, f \}$

Para responderlo, tengamos en cuenta la propiedad de los subgrupos finitos, que dice que es suficiente que el subconjunto no sea vacío, y que la operación sea cerrada.

Con ese criterio, $H = \{a, b\}$ no es subgrupo, pues $b \ast b = c \notin H$
$K = \{a, b, c, d\}$ es subgrupo de A pues como podemos observar en la tabla,
la operación $\ast$ es cerrada en K
Lo mismo ocurre con $F = \{a, e\}$ en el que $\ast$ es cerrada, por lo tanto es otro subgrupo.
Pero $M = \{a, e, f \}$ no lo es, pues $e \ast f = c \notin M$

Ejemplo 3:

Dados dos subgrupos $(H_1 ; *)$ y $(H_2 ; *)$ de un mismo grupo $(G ; *)$, nos preguntamos si la intersección de los subgrupos $H = H_1 \cap H_2$ es también otro subgrupo del mismo grupo $(G ; *)$.

Para responderlo, utilizaremos también la condición suficiente del teorema.

1) Hay que demostrar que H no es vacío. Para ello, por hipótesis sabemos que H_1 y H_2 son subgrupos, por lo tanto en cada uno está el elemento neutro del grupo:
$e \in H_1 \wedge e \in H_2 \Rightarrow$ por definición de intersección: $e \in H_1 \cap H_2 \Rightarrow e \in H \Rightarrow H \neq \varnothing$

2) $\forall x \in H : x \in H_1 \cap H_2 \Rightarrow x \in H_1 \wedge x \in H_2 \Rightarrow$ por hipótesis $(H_1 \subseteq G \wedge H_2 \subseteq G)$:
$x \in G \wedge x \in G \Rightarrow x \in G$ con lo cual queda probado que $H \subseteq G$

3) $\forall x, y \in H : x \in (H_1 \cap H_2) \wedge y \in (H_1 \cap H_2) \Rightarrow (x \in H_1 \wedge x \in H_2) \wedge (y \in H_1 \wedge y \in H_2) \Rightarrow$
por conmutatividad y asociatividad de la conjunción:

$\Rightarrow (x \in H_1 \wedge y \in H_1) \wedge (x \in H_2 \wedge y \in H_2) \Rightarrow$ por condición necesaria de subgrupos:

$\Rightarrow (x * y' \in H_1) \wedge (x * y' \in H_2) \Rightarrow$ por definición de intersección:

$\Rightarrow x * y' \in H_1 \cap H_2 \Rightarrow x * y' \in H$

Por lo tanto, por haberse cumplido las tres condiciones suficientes de subgrupos,
podemos decir que $(H_1 \cap H_2 ; *)$ es subgrupo de $(G ; *)$

El ejemplo anterior se puede generalizar para una familia de subgrupos $H_1, ..., H_n$ de un grupo G, tal que la intersección de todos ellos es también un subgrupo.

Esta demostración generalizada la puedes encontrar en el libro de la cátedra, capítulo 18.

Ejemplo 4:

Dados dos subgrupos $(H_1 ; *)$ y $(H_2 ; *)$ de un mismo grupo $(G ; *)$, nos preguntamos si la unión de los subgrupos $H = H_1 \cup H_2$ es también otro subgrupo del mismo grupo $(G ; *)$.
Piénsalo un poco...

Si no pudiste responderlo, aquí va la solución:

La respuesta es NO, no siempre la unión de subgrupos es subgrupo.
Por ejemplo, consideremos los subgrupos $3Z$ y $5Z$ de $(Z ; +)$, que ya sabemos que son subgrupos pues lo demostramos antes.
Sea $H = 3Z \cup 5Z$

Tomando los siguientes elementos: $9 \in 3Z \Rightarrow 9 \in 3Z \cup 5Z \Rightarrow 9 \in H$

$$20 \in 5Z \Rightarrow 20 \in 3Z \cup 5Z \Rightarrow 9 \in H$$

O sea que $9 \in H \wedge 20 \in H$, pero $9+20 = 29 \notin H$ pues $29 \notin 3Z \wedge 29 \notin 5Z$

Por lo tanto, al no ser cerrada la suma, no es subgrupo.

A continuación, veremos un tema que vincula a los grupos con las relaciones de equivalencia.
Seguramente recordarás que las relaciones de equivalencia cumplen con las propiedades reflexiva, simétrica y transitiva. Lo fundamental de este tipo de relaciones es que particionan al conjunto en distintas "celdas" llamadas clases de equivalencia.

Definiremos un tipo de relaciones de equivalencia llamadas **relaciones de congruencia**, que generalizan la congruencia módulo n.

RELACIONES DE CONGRUENCIA

Sea $(G ; \ast)$ un semigrupo con neutro e. Sea $\sim$ una relación de equivalencia en G.

$\sim$ es compatible a izquierda con $\ast \Leftrightarrow \forall a, b, x \in G : a \sim b \Rightarrow x \ast a \sim x \ast b$

$\sim$ es compatible a derecha con $\ast \Leftrightarrow \forall a, b, x \in G : a \sim b \Rightarrow a \ast x \sim b \ast x$

La relación $\sim$ es compatible con $\ast$ (o es de congruencia) $\Leftrightarrow$ es compatible a derecha y a izquierda.

Veamos un ejemplo:

Consideremos el grupo $(Q-\{0\} ; \bullet)$

y la relación de equivalencia $\sim$ tal que: $a \sim b \Leftrightarrow a^2 = b^2$

Analicemos si la relación dada es compatible con la operación del grupo $\bullet$.

Para ello, vamos a demostrar sólo a derecha, ya que la operación es conmutativa:
$\forall a, b, x \in Q-\{0\} : a \sim b \Rightarrow a^2 = b^2 \Rightarrow a^2 x^2 = b^2 x^2 \Rightarrow (ax)^2 = (bx)^2 \Rightarrow ax \sim bx$

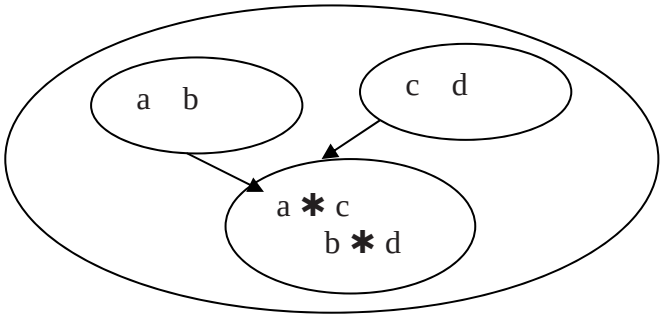
Por lo tanto, la relación $\sim$ es compatible con la multiplicación, o es de congruencia en el grupo.

Observaciones:

1. Las relaciones de congruencia generalizan las propiedades de la congruencia módulo n y pueden recibir otros nombres como "compatible" respecto de la operación de grupo o "estable".

2. Una forma equivalente de definir la compatibilidad es:
La relación $\sim$ es compatible con $\ast \Leftrightarrow \forall a, b, c, d \in G : a \sim b \wedge c \sim d \Rightarrow a \ast c \sim b \ast d$

Lo cual muestra que el resultado es independiente del representante de clase.



Observa la belleza de este grupo, donde se ven en diferentes tonos las clases de equivalencia

D[4] x * y

x \ y	g1	g2	g3	g4	g5	g6	g7	g8
g1	g1	g2	g3	g4	g5	g6	g7	g8
g2	g2	g1	g4	g3	g6	g5	g8	g7
g3	g3	g4	g2	g1	g7	g8	g6	g5
g4	g4	g3	g1	g2	g8	g7	g5	g6
g5	g5	g6	g8	g7	g1	g2	g4	g3
g6	g6	g5	g7	g8	g2	g1	g3	g4
g7	g7	g8	g5	g6	g3	g4	g1	g2
g8	g8	g7	g6	g5	g4	g3	g2	g1

TEOREMA FUNDAMENTAL DE COMPATIBILIDAD

Sea $(G\ ;\ *)$ un semigrupo con neutro e y $\sim$ una relación de equivalencia compatible con $*$

Entonces el conjunto cociente $(G/\sim\ ;\ \bar{*})$ es un semigrupo con neutro, siendo la operación $\bar{*}$ la siguiente: $\bar{a}\ \bar{*}\ \bar{b} = \overline{a * b}$

Si $(G\ ;\ *)$ es grupo entonces $(G/\sim\ ;\ \bar{*})$ también es grupo.

Si $(G\ ;\ *)$ es abeliano entonces $(G/\sim\ ;\ \bar{*})$ también es abeliano.

La demostración de este teorema puedes encontrarla en el libro de la cátedra, capítulo 18.
Es importante tener en cuenta que no se trata de poder reproducir de memoria el Teorema; apuntamos a que comprendas su enunciado, las hipótesis y su aplicación.

Observación:

Este Teorema nos garantiza que si la relación de equivalencia es compatible, la estructura del conjunto cociente es la misma que la del conjunto original. Se "traspasa" la estructura y las propiedades estructurales y por lo tanto resulta una herramienta muy útil en el momento de modelizar situaciones reales a resolver.

Por ejemplo:
Consideremos el grupo $(Z\ ;\ +)$ y la relación de equivalencia congruencia módulo n.

1) Primero demostremos que la relación es compatible con la $+$.

$\forall\ a, b, c, d \in Z : a \equiv b\ (n) \wedge c \equiv d\ (n) \Rightarrow n \mid a - b \ \wedge\ n \mid c - d \ \Rightarrow\ a - b = n \bullet k \ \wedge\ c - d = n \bullet t$

con $k, t \in Z \Rightarrow\ a - b + c - d = n \bullet k + n \bullet t \ \Rightarrow\ (a + c) - (b + d) = n \bullet (k + t)$

siendo $k+t \in Z$ por ser la suma cerrada en Z.

Entonces $n \mid \ (a + c) - (b + d) \ \Rightarrow\ (a + c) \equiv (b + d)\ (n)$

2) Consideremos $n = 5$ y verifiquemos que $(Z_5\ ;\ \overline{+})$ es grupo abeliano (la misma estructura que el conjunto original).

$\overline{+}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$

De la tabla se desprende que es cerrada, conmutativa (ya que es simétrica respecto de su diagonal principal) , tiene elemento neutro: $\overline{0}$, cada uno tiene simétrico: $\overline{0}' = \overline{0}$, $\overline{1}' = \overline{4}$, $\overline{2}' = \overline{3}$, $\overline{3}' = \overline{2}$ y $\overline{4}' = \overline{1}$

En el punto 1 del ejemplo demostramos que la congruencia módulo n es compatible con la adición en los enteros. Por lo tanto, podemos garantizar, en virtud del Teorema Fundamental de Compatibilidad que $(Z_5\ ;\ \overline{+})$ es grupo abeliano., ya que $(Z_5\ ;\ \overline{+})$ es un grupo abeliano.

GENERADORES. GRUPOS CÍCLICOS

Sea $(G ; \ast)$ un grupo y $a \in G$. Llamamos **Subgrupo cíclico de G generado por a** al siguiente conjunto:

$< a > = \{ a^n / n \in Z \}$

Aclaraciones:

a^n significa $a \ast a \ast a \ast .... \ast a$ (n veces)

a^{-n} significa $a^{-1} \ast a^{-1} \ast a^{-1} ... \ast a^{-1}$ (n veces, siendo a^{-1} el simétrico de a)

$a^0 = e$ (elemento neutro)

Es decir el conjunto $< a >$ tiene a todos los elementos que se pueden obtener operando al elemento con sí mismo o con su simétrico.

Vayamos a los ejemplos:

Ejemplo 1:

Consideremos el grupo $(Z ; +)$ y calculemos el subgrupo cíclico generado por el 2, en este caso son todos los números que se obtienen sumando el 2 con sí mismo cualquier cantidad de veces, o el -2. Es decir son todos los números pares:

$< 2 > = \{ x \in Z / x = 2 \bullet k \text{ con } k \in Z \}$

Ejemplo 2:

Consideremos el grupo finito $(A ; \otimes)$ dado por la siguiente tabla:

⊗	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**
a	a	b	c	d	e	f	g	h
b	b	c	d	a	h	g	e	f
c	c	d	a	b	f	e	h	g
d	d	a	b	c	g	h	f	e
e	e	g	f	h	a	c	b	d
f	f	h	e	g	c	a	d	b
g	g	f	h	e	d	b	a	c
h	h	e	g	f	b	d	c	a

y calculemos el subgrupo cíclico generado por el elemento "d"

Supongamos ahora que existe un elemento de un grupo **(G ; ✱)** que al operarlo con sí mismo el subgrupo que genera es el impropio.

Calculamos $d \otimes d = c$; $d \otimes d \otimes d = c \otimes d = b$; $d \otimes d \otimes d \otimes d = b \otimes d = a$

$d \otimes d \otimes d \otimes d \otimes d = a \otimes d = d$

Además, **"a"** es el elemento neutro del grupo, y el simétrico de **"d"** es **"b"** , que ya lo operamos.

Por lo tanto, no se pueden obtener más elementos distintos. Entonces:

$< d > = \{ a, b, c, d \}$

Concretando, podemos decir:

Si **(G ; ✱)** un grupo, $a \in G$ y $< a > = G$ entonces **a** es generador del grupo **G** y el grupo **(G ; ✱)** es cíclico porque tiene al menos un elemento generador.

e Analicemos cuales de los siguientes grupos son cíclicos, y en caso afirmativo indiquemos los generadores:

1) El grupo **(Z ; +) es** cíclico pues todos los enteros se pueden obtener sumando al **1** con sí mismo o con el **-1** la cantidad necesaria de veces. O sea, que el **1** y el **-1** son generadores de **(Z ; +)**

2) Consideremos el grupo **({1,-1, i, -i } ; •)** siendo **i** la unidad imaginaria **($i^2 = -1$) .** Si construimos la tabla:

•	1	-1	i	-i
1	1	-1	i	-i
-1	-1	1	-i	i
i	i	-i	-1	-1
-i	-i	i	-1	i

Veamos...

El **1** no puede ser generador pues multiplicado por sí mismo siempre da **1.**

El **-1** tampoco es generador pues multiplicado por sí mismo siempre da **1** o **-1.**

En cambio veamos que pasa con la **i:**

$i \bullet i = -1$; $i \bullet i \bullet i = -i$; $i \bullet i \bullet i \bullet i = 1$; $i \bullet i \bullet i \bullet i \bullet i = i$

O sea que i es generador del grupo **({1,-1, i, -i } ; •)**

Y lo mismo ocurre con su simétrico **-i.**

3) Recordemos el grupo simétrico $(S_3 ; o)$, formado por las seis funciones biyectivas con dominio y codominio en un conjunto de 3 elementos.

La tabla que habíamos armado es:

$\circ$	f_1	f_2	f_3	f_4	f_5	f_6
f_1	f_1	f_2	f_3	f_4	f_5	f_6
f_2	f_2	f_1	f_5	f_6	f_3	f_4
f_3	f_3	f_4	f_1	f_2	f_6	f_5
f_4	f_4	f_3	f_6	f_5	f_1	f_2
f_5	f_5	f_6	f_2	f_1	f_4	f_3
f_6	f_6	f_5	f_4	f_3	f_2	f_1

Analicemos si es cíclico. Para ello vamos a calcular los subgrupos generados por cada uno de los elementos:

$< f_1 > = \{ f_1 \}$

$< f_2 > = \{ f_2 , f_1 \}$

$< f_3 > = \{ f_3 , f_1 \}$

$< f_4 > = \{ f_4 , f_5 , f_1 \}$

$< f_5 > = \{ f_5 , f_4 , f_1 \}$

$< f_6 > = \{ f_6 , f_1 \}$

Vemos que ninguna generó al grupo completo, sino que han generado subgrupos. Entonces el grupo $(S_3 ; o)$ NO ES CICLICO.

4) Tomemos el grupo $(Z_5 ; \bar{+})$, cuya tabla es:

$\bar{+}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$

Este grupo es CICLICO ya que $< \overline{1} > = \{ \overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4} \}$

y lo mismo ocurre con su simétrico $\overline{5}$

Por lo visto en los ejemplos, y pensando un poco más, podemos arribar a las siguientes conclusiones:

- Todo grupo cíclico es abeliano
- Todo subgrupo de **(Z ;+)** es cíclico
- Todo subgrupo de un grupo cíclico es cíclico

Te proponemos que trates de demostrarlas. Recuerda que puedes solicitar orientación a tu tutor.

Orden de un elemento y de un subgrupo

Sea $(G ; *)$ un grupo y $a \in G$.

El orden de un elemento es el cardinal del subgrupo que genera.
El Orden de un subgrupo es el orden de su generador, o bien el cardinal del subgrupo.

Si $< a > = n$ entonces se dice que **a** tiene orden finito **n.**

Si $< a > = \infty$ entonces se dice que **a** tiene orden infinito.

Retículo o Red de subgrupos

Dado un grupo $(G ; *)$ con neutro **e**, entonces el conjunto de todos los subgrupos puede ser ordenado por la inclusión.

Si G es finito, entonces: (subgrupos de $G ; \subseteq$) es una Red con primer elemento ,el subgrupo trivial, y con último elemento, el subgrupo impropio.

Por ejemplo:

Armemos la red de los subgrupos del grupo $(S_3 ; o)$

Los subgrupos son:

$H_1 = \{ f_1 \}$

$H_2 = \{ f_2, f_1 \}$

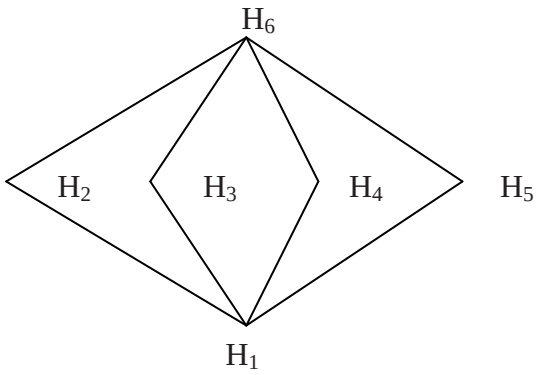
$H_3 = \{ f_3, f_1 \}$

$H_4 = \{ f_4, f_5, f_1 \}$

$H_5 = \{ f_6, f_1 \}$

$H_6 = \{ f_1, f_2, f_3, f_4, f_5, f_6 \}$

Armemos el diagrama de Hasse considerando la relación de inclusión:



Para tener en cuenta: Si el grupo no es cíclico, además de los subgrupos generados por los elementos, hay que considerar al propio grupo y buscar si existen otros subgrupos no cíclicos.

Propiedades del grupo **$(Zn ; +)$**

- El grupo $(Z_n ; +)$ es cíclico
- Sus generadores son: $\{ \overline{k} / mcd(k,n) = 1, 1 \leq k \leq n - 1 \}$
- La cantidad de subgrupos de Z_n es: $|D_n|$ y la red de subgrupos es isomorfa a $(D_n ; |)$

e Hallemos todos los generadores de $(Z_{18} ; +)$, los subgrupos y armemos la Red de Subgrupos.

$Z_{18} = \{ \overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}, \overline{7}, \overline{8}, \overline{9}, \overline{10}, \overline{11}, \overline{12}, \overline{13}, \overline{14}, \overline{15}, \overline{16}, \overline{17} \}$

De acuerdo a la propiedad enunciada, los generadores son todas las clases coprimas con 18 - es decir aquellas cuyo máximo común divisor con el 18 es 1.

Gen Z_{18} : $\{ \overline{1}, \overline{5}, \overline{7}, \overline{11}, \overline{13}, \overline{17} \}$

Es decir que el subgrupo generado por cada una de ellas es el grupo completo.

Ahora debemos hallar los demás subgrupos. Primero hallemos cuántos debe haber en total. Para ello, calculamos:

Cantidad de Subgrupos = $| D_{18} | = | \{ 1, 2, 3, 6, 9, 18 \} | = 6$

y además, existe al menos un subgrupo cuyo orden o cardinal es cada uno de los divisores de 18.

El subgrupo de orden 1 es el trivial: $H_1 = < \overline{0} > = \{ \overline{0} \}$

El subgrupo de orden 2 es: $H_2 = < \overline{9} > = \{ \overline{0}, \overline{9} \}$

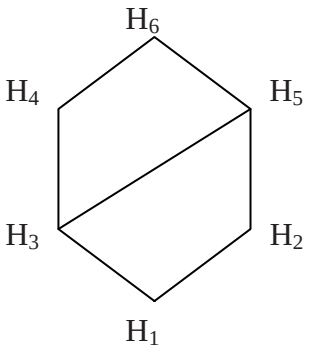
El subgrupo de orden 3 es: $H_3 = < \overline{6} > = \{ \overline{0}, \overline{6}, \overline{12} \}$

El subgrupo de orden 6 es: $H_4 = < \overline{3} > = \{ \overline{0}, \overline{3}, \overline{6}, \overline{9}, \overline{12}, \overline{15} \}$

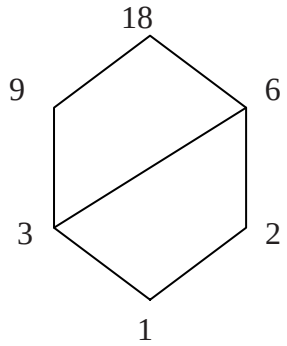
El subgrupo de orden 9 es: $H_5 = < \overline{2} > = \{ \overline{0}, \overline{2}, \overline{4}, \overline{6}, \overline{8}, \overline{10}, \overline{12}, \overline{14}, \overline{16} \}$

El subgrupo de orden 18 es el subgrupo impropio: $H_6 = Z_{18}$

Ahora podemos armar la red de subgrupos:



y es isomorfa a la red (D_{18}, |)



Antes de continuar, repasemos y sinteticemos:

- *Definimos los subgrupos y vimos diferentes ejemplos, tanto de grupos finitos como infinitos.*
- *El teorema de condición necesaria y suficiente de subgrupos nos resultó útil para investigar y demostrar si un determinado subconjunto es subgrupo de un grupo dado.*
- *Observamos que algunos subgrupos son cíclicos, pues se generan a partir de un elemento. Pero hay grupos y subgrupos que no tienen generadores, y por lo tanto no son cíclicos.*
- *Consideramos que si se toman todos los subgrupos de un grupo finito dado y se los ordena con la inclusión, se tiene una red de subgrupos.*
- *En particular estudiamos los grupos cíclicos* $(Zn ; +)$
- *Analizamos las relaciones de congruencia, que son relaciones de equivalencia compatibles con la estructura de grupo o semigrupo.*
- *Nos detuvimos en un Teorema muy importante que nos demuestra que si se tiene una relación de congruencia, la estructura del conjunto cociente era la misma que la del conjunto original dado.*

A continuación, vamos a seguir considerando relaciones de congruencia, pero en este caso congruencia módulo un subgrupo.
Concéntrate bien, ya que se trata de conceptos abstractos, aunque si los analizas cuidadosamente no resultarán complicados.

Congruencia módulo un subgrupo

Sea $(G ; \ast)$ un grupo y H un subgrupo de G. Definimos la siguiente relación en G:

a es **congruente a derecha** con b **módulo** $H \Leftrightarrow a \ast b' \in H$

Lo indicamos así: $a \equiv_d b\ (H)$

Análogamente, definimos la relación:
a es **congruente a izquierda** con b **módulo** $H \Leftrightarrow a' \ast b \in H$

Lo indicamos así: $a \equiv_i b\ (H)$

Observaciones:

- Si $(G ; \ast)$ es un grupo abeliano, entonces la congruencia a derecha coincide con la congruencia a izquierda.
- La relación de congruencia módulo n en Z (estudiada anteriormente) es un caso particular de la congruencia módulo H, considerando $H = nZ = \{ x \in Z / x = nk , k \in Z\}$

Demostración:

$a \equiv b \ (H) \Leftrightarrow a * b' \in H \Leftrightarrow a + (-b) \in H \Leftrightarrow a - b = nk \Leftrightarrow n \mid a - b \Leftrightarrow a \equiv b \ (n)$

- La congruencia módulo H , tanto a derecha como a izquierda, es una relación de equivalencia
- La clase de equivalencia de cualquier elemento a de G es:

  $\overline{a_d} = H * a$ (en la relación de congruencia a derecha)

  $\overline{a_i} = a * H$ (en la relación de congruencia a izquierda)
- $|H| = |a * H| = |H * a|$

  Es decir, todas las clases de equivalencia producidas por la congruencia módulo H (ya sea a derecha o izquierda) tienen la misma cantidad de elementos.

  Se las llama clases laterales o co-clases a derecha y a izquierda.

La relación de congruencia módulo H (tanto a derecha como a izquierda), como hemos demostrado que es de equivalencia, produce una partición en el conjunto.

Puedes consultar la demostración de algunas de estas observaciones en el libro de la cátedra, capítulo 18

Veamos algunos ejemplos:

¿Recuerdas el grupo de permutaciones $S_3 = \{ f_1, f_2, f_3, f_4, f_5, f_6 \}$?

Considera $H = < f_3 > = \{ f_1 , f_3 \}$

Como hemos visto, podemos aplicar la relación de congruencia módulo H a derecha y obtener una partición del conjunto:

Para ello calculemos las clases de equivalencia:

$\overline{f_{1d}} = H * f_1 = \{ f_1 , f_3 \} \circ f_1 = \{ f_1 \circ f_1 , f_3 \circ f_1 \} = \{ f_1 , f_3 \}$

Vemos que es el mismo subgrupo. Esto siempre va a ocurrir al calcular la clase de un elemento del subgrupo, pues por ser H un subgrupo, la operación es cerrada en H.

Es decir, los elementos de H siempre forman una clase de equivalencia.

Ahora hallemos otra clase:

$\overline{f_{2d}} = H * f_2 = \{f_1 , f_3\} \circ f_2 = \{f_1 \circ f_2 , f_3 \circ f_2 \} = \{ f_2 , f_4 \}$

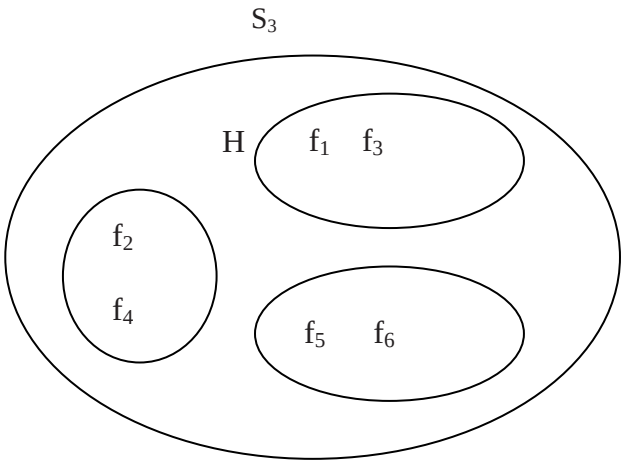
Nos preguntamos... ¿Hay necesidad de calcular alguna otra clase? ¿Por qué?

Como ya hemos visto, en este tipo de relación de equivalencia (la congruencia módulo un subgrupo), todas las clases de equivalencia tienen la misma cantidad de elementos; y teniendo en cuenta la definición de partición, no queda otra posibilidad más que las dos funciones que nos faltan $(f_5 \text{ y } f_6)$ conformen una clase de equivalencia,
Por lo tanto, no hay necesidad de calcularla, pues ya sabemos quienes la forman:
$\overline{f_{5d}} = \{ f_5 , f_6 \}$

Por lo tanto la Partición de S_3 a derecha es:

$P_d = \{ \{ f_1 , f_3 \} , \{ f_2 , f_4 \} , \{ f_5 , f_6 \} \}$

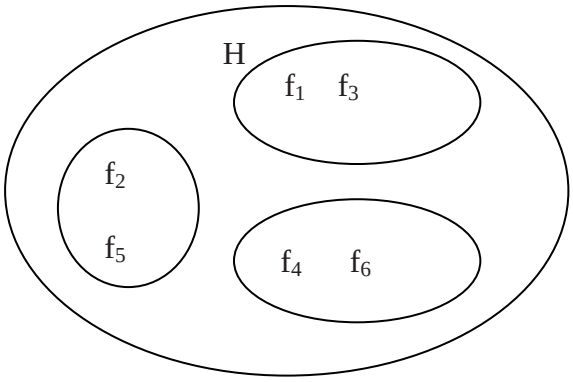
Gráficamente:



Ahora calculemos la partición a izquierda, para lo cual solamente es necesario calcular una clase, por ejemplo la de $\mathbf{f_2}$:

$\overline{f_{2i}} = f_2 * H = f_2 \circ \{ f_1 , f_3 \} = \{ f_2 \circ f_1 , f_2 \circ f_3 \} = \{ f_2 , f_5 \}$

Y haciendo el mismo razonamiento anterior, ya podemos indicar las otras clases:
$P_i = \{ \{ f_1 , f_3 \} , \{ f_2 , f_5 \} , \{ f_4 , f_6 \} \}$



Miremos los gráficos anteriores y observemos que, las particiones a derecha - en el primer gráfico - y a izquierda – en el segundo gráfico - son distintas. Más adelante veremos una definición que tiene en cuenta cuándo coinciden las particiones a ambos lados.

e

Ejemplo 2:

Consideremos el grupo finito $(A ; \otimes)$ dado por la siguiente tabla:

$\otimes$	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**
a	a	b	c	d	e	f	g	h
b	b	c	d	a	h	g	e	F
c	c	d	a	b	f	e	h	g
d	d	a	b	c	g	h	f	e
e	e	g	f	h	a	c	b	d
f	f	h	e	g	c	a	d	b
g	g	f	h	e	d	b	a	c
h	h	e	g	f	b	d	c	a

y el subgrupo $H = \{ a, e \}$

Partición a derecha:

Como este subgrupo es de orden 2, significa que la partición tendrá cuatro clases de equivalencia.

Ya sabemos que $\overline{a}_d = \{ a, e \}$, entonces calculamos: $\overline{b}_d = \{ a, e \} \otimes b = \{ b, g \}$

$\overline{c}_d = \{ a, e \} \otimes c = \{ c, f \}$ y ya está, pues seguro que la clase que falta está formada por $\{ d, h \}$

Por lo tanto:

$P_d = \{ \{ a, e \} , \{ b, g \} , \{ c, f \} , \{ d, h \} \}$

Partición a izquierda:

Ya sabemos que $\overline{a}_i = \{ a, e \}$, entonces calculamos: $\overline{b}_i = b \otimes \{ a, e \} = \{ b, h \}$

$\overline{c}_i = c \otimes \{ a, e \} = \{ c, f \}$ y ya está, pues seguro que la clase que falta está formada por $\{ d, g \}$

Por lo tanto:

$P_d = \{ \{ a, e \} , \{ b, h \} , \{ c, f \} , \{ d, g \} \}$

En este caso tampoco son iguales ambas particiones.

Índice de un subgrupo

Sea $(G ; *)$ un grupo y H un subgrupo de G.

El índice de H en G es la cantidad de clases de equivalencia módulo H.

Se indica: $[G : H]$

Ejemplos:

Tomemos los dos ejemplos anteriores en los que calculamos las particiones:

1. En el grupo S_3 con $H = \{ f_1, f_3 \}$ se cumple $[S_3 : H] = 3$
2. En el grupo $(A ; \otimes)$ con $H = \{ a, e \}$ se cumple : $[A : H] = 4$

Te proponemos que pienses las siguientes cuestiones y completes en las líneas punteadas. Ante cualquier duda o dificultad, consulta a tu tutor.

- $[G : G]$ = ...
- $[G : \{e\}]$ = ...
- Si G y H son finitos entonces $[G : H]$ es .....
- Si G y H no son finitos, $[G : H]$ es necesariamente infinito?

Considera este ejemplo para responder:
$G = (Z,+)$ $H = 3Z$ (múltiplos de 3) $[G : H]$ = ...

Pasemos ahora al siguiente teorema, que constituye una herramienta muy útil a la hora de buscar los subgrupos de un grupo finito ya que nos indica el orden que tales subgrupos pueden tener:

Teorema de Lagrange

Sea $(G ; *)$ un grupo de orden finito n y H un subgrupo de G.

Entonces, el orden de H divide al orden de G.

Demostración:

Si el orden de H es m, como todas las clases de equivalencia tienen el mismo cardinal, significa que $n = k\ m$ siendo k la cantidad de clases. Por lo tanto, m divide a n.

De acuerdo a este importante teorema, responde:

1) Un grupo de 20 elementos, ¿puede tener un subgrupo de orden 6? .....

2) ¿Cuáles son los órdenes posibles de los subgrupos de un grupo de 20 elementos? .....

3) Si $|G| = p$ siendo p un número primo. ¿Cuáles son los únicos subgrupos que tiene? .....

Como siempre si tienes dudas, consulta a tus tutores.

Subgrupo Normal

Sea $(G\ ;\ *)$ un grupo con neutro e y H un subgrupo de G.

H es subgrupo normal $\Leftrightarrow$ las clases a derecha coinciden con las clases a izquierda.

Ejemplos:

1) El subgrupo $H = \{ f_1, f_3 \}$ NO es subgrupo normal de S_3 pues cuando anteriormente calculamos las particiones, vimos que no eran iguales.

2) El subgrupo $H = < f_4 > = \{ f_1, f_4, f_5 \}$ es subgrupo normal de S_3 ya que aunque no hayamos calculado las co-clases de equivalencia, como el cardinal de este subgrupo es exactamente la mitad del cardinal del grupo, tendremos dos clases de equivalencia, siendo una de ellas el subgrupo. Por lo tanto, la otra la forman las restantes tres funciones $\{ f_2, f_3, f_6 \}$. Es decir, que tanto a derecha como a izquierda resultan iguales.

3) El subgrupo $H = < \overline{2} >$ es subgrupo normal de $(Z_{12}\ ;\ \overline{+})$ ya que la $\overline{+}$ es conmutativa, por lo tanto, a derecha y a izquierda se obtiene la misma partición.

Te proponemos que teniendo en cuenta los ejemplos analizados intentes completar estas generalizaciones:

1. Si $(G ; *)$ es un grupo abeliano, entonces todos los subgrupos son .....

2. ¿$H = \{e\}$ es subgrupo normal de G?.....

3. ¿G es subgrupo normal de G? .....

4. Si $|G| = 2\ |H|$ entonces H es subgrupo .....

A continuación presentamos un teorema que nos va a garantizar la estructura del grupo cociente.

Teorema:

Sea $(G ; *)$ un grupo y H un subgrupo normal de G.

Entonces $(G/H, \bar{*})$ es grupo siendo $\bar{a}\ \bar{*}\ \bar{b} = \overline{a * b}$ y el cardinal de G/H es $[G : H]$

La importancia de este teorema es que da la estructura del conjunto cociente del grupo G módulo del subgrupo normal H y muestra que es un subgrupo con la operación $\bar{*}$. Este grupo se llama GRUPO COCIENTE de G MÓDULO H y tiene $[G : H]$ elementos.

Para consultar la demostración de este teorema podés recurrir al libro de la cátedra, capítulo 18.

Veamos algunos ejemplos:

Volviendo al grupo $(A ; \otimes)$ dado por la siguiente tabla:

$\otimes$	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**
a	a	b	c	d	e	f	g	h
b	b	c	d	a	h	g	e	f
c	c	d	a	b	f	e	h	g
d	d	a	b	c	g	h	f	e
e	e	g	f	h	a	c	b	d
f	f	h	e	g	c	a	d	b
g	g	f	h	e	d	b	a	c
h	h	e	g	f	b	d	c	a

Consideremos el subgrupo normal $H = \{ a, b, c, d \}$

El conjunto cociente es: $\{ A = \{ a, b, c, d\} , E = \{e, f, g, h\} \}$

Justamente lo que nos garantizó el teorema es que este conjunto con la operación inducida de las clases es también un grupo. Su tabla es:

$\bar{\otimes}$	A	E
A	A	E
E	E	A

Y esto sucede pues, en primer lugar, la relación de congruencia módulo el subgrupo H es compatible con la operación $\otimes$ del grupo (esto significa que el resultado es independiente del representante de clase. En este caso podemos ver que cualquier elemento de la clase de a llamada **A,** operado con cualquier elemento de la clase de **e** llamada **E,** da por resultado un elemento de la clase de **e).** Si la relación no fuese compatible, entonces no se podría haber armado esta tabla del cociente.
Además, como el subgrupo H es normal, esta partición es la misma a derecha y a izquierda, por eso directamente lo llamamos el grupo cociente sin especificar lateralidad.

Sintetizando:

- *Definimos la congruencia módulo un subgrupo que es una relación de equivalencia que generaliza la congruencia módulo* n *que ya habíamos estudiado, definida en el conjunto de los números enteros.*
- *Buscamos las clases de equivalencia y analizamos algunas propiedades que resultaron muy útiles para resolver ejercicios.*
- *Nos detuvimos en algunos ejemplos donde pudimos verificar las propiedades enunciadas.*
- *Definimos índice de un subgrupo en un grupo.*
- *Demostramos el Teorema de Lagrange que resulta muy práctico para encontrar los subgrupos de un grupo finito.*
- *Nos detuvimos en la definición de subgrupo normal que luego utilizamos para construir el grupo cociente de un grupo generado por un subgrupo normal.*

El tema que sigue es el último, dentro de la unidad de Grupos, y se refiere a funciones que podemos definir entre dos grupos dados. Nuestro mayor interés se centra en aquellas funciones que sean biyectivas ya que en esos casos, los grupos dados se comportarán de la misma manera.
Si ya cursaste Álgebra, y estudiaste Transformaciones Lineales, que eran homomorfismos entre espacios vectoriales, muchas definiciones y propiedades que veremos a continuación te van a resultar conocidas, ya que se trata de lo mismo, pero ahora entre distintos grupos.

Tengamos en cuenta que el conjunto de los vectores de un espacio vectorial, con la suma de vectores, es un grupo abeliano, o sea que las propiedades que estamos estudiando ahora no pueden ser distintas, sólo se trata de que cambiamos de conjunto.

Homomorfismos de Grupos

Sean $(G_1 \; ; *_1)$ y $(G_2 \; ; *_2)$ dos grupos con neutros e_1 y e_2 respectivamente

$f: G_1 \to G_2$ es homomorfismo $\Leftrightarrow$ f es función y $\forall a, b \in G_1: f(a *_1 b) = f(a) *_2 f(b)$

Veamos algunos ejemplos:

1) Sea la función $f: (Z \; ; +) \to (3Z \; ; +) \; / \; f(x) = 3x$

Vamos a demostrar que f es homomorfismo de grupos:

$\forall \; a, b \in Z: \; f(a + b) = 3 \; (a+b) = 3 \; a + 3 \; b = f(a) + f(b)$

Con lo cual queda demostrado.

2) Sea la función $g: (R^+ \; ; \bullet) \to (R \; ; +) \; / \; g(x) = \log x$

Vamos a demostrar que g es homomorfismo de grupos:

$\forall \; a, b \in R^+: \; g(a \bullet b) = \log (a \bullet b) = \log(a) + \log(b) = g(a) + g(b)$

Con lo cual queda demostrado.

A continuación, enunciaremos algunas propiedades que se cumplen en todo homomorfismo de grupos:

Sea $f : (G_1 \; ; *_1) \to (G_2 \; ; *_2)$ un homomorfismo de grupos.

Entonces:

1) $f(e_1) = e_2$

Por ser e_1 el elemento neutro de G_1, se cumple: $\forall \; x \in G_1 : x *_1 e_1 = x \; \wedge \; e_1 *_1 x = x$

Aplicamos la función en ambos miembros:

$f(x *_1 e_1) = f(x) \; \wedge \; f(e_1 *_1 x) = f(x)$

Por ser f un homomorfismo, en los primeros miembros:

$f(x) *_2 f(e_1) = f(x) \quad \wedge \quad f(e_1) *_2 f(x) = f(x)$

Por ser G_2 también un grupo, cada elemento tiene simétrico, en particular el simétrico de $f(x)$ será $[\ f(x)\ ]'$. Lo operamos a izquierda en la primera igualdad:

$[\ f(x)\ ]' *_2 f(x) *_2 f(e_1) = [\ f(x)\ ]' *_2 f(x)$

Asociando: $\{\ [\ f(x)\ ]' *_2 f(x)\ \} *_2 f(e_1) = [\ f(x)\ ]' *_2 f(x)$

Por definición de simétrico: $e_2 *_2 f(e_1) = e_2$

Y por ser e_2 elemento neutro: $f(e_1) = e_2$

Con lo que quedó demostrado.

2) $\forall\ a \in G_1$: $f(a') = [\ f(a)\ ]'$

Por ser G_1 un grupo sabemos que: $\forall\ a \in G_1 : \exists\ a' \in G_1$: $a *_1 a' = e_1$

Aplicamos la función f en ambos miembros: $f(\ a *_1 a'\ ) = f(e_1)$

Por ser f un homomorfismo, en el primer miembro; y por la propiedad anterior en el segundo:
$f(a) *_2 f(a') = e_2$

Por ser G_2 también un grupo, cada elemento tiene simétrico, en particular el simétrico de $f(a)$ será $[\ f(a)\ ]'$. Lo operamos a izquierda:

$[\ f(a)\ ]' *_2 f(a) *_2 f(a') = [\ f(a)\ ]' *_2 e_2$

Asociamos y utilizamos la propiedad de los simétricos: $e_2 *_2 f(a') = [\ f(a)\ ]' *_2 e_2$

Por propiedad del elemento neutro: $f(a') = [\ f(a)\ ]'$

Con lo que quedó demostrado.

Clasificación de homomorfismos:

Sea $f : G_1 \rightarrow G_2$ un homomorfismo de grupos:

- Si f es inyectiva, f se llama **monomorfismo**
- Si f es sobreyectiva, f se llama **epimorfismo**
- Si f es biyectiva, f se llama **isomorfismo**

- Si $G_1 = G_2$, f se llama **endomorfismo**
- Si $G_1 = G_2$ y f es biyectiva, f se llama **automorfismo**

Ejemplos:

1) Sea $(G ; *)$ un grupo abeliano. Demostraremos que la función $f: G \to G \ / \ f(x) = x'$ es un isomorfismo.

Primero hay que averiguar que sea homomorfismo:

$\forall\ a, b \in G:\ f(a * b) = (a * b)' = b' * a'$
pero por ser G abeliano: $= a' * b' = f(a) * f(b)$

Ahora vamos a clasificarlo:

La función f es inyectiva, ya que $\forall\ a, b \in G : f(a) = f(b) \Rightarrow a' = b' \Rightarrow (a')' = (b')' \Rightarrow a = b$

También la función f es sobreyectiva, pues: $\forall\ b \in G : \exists\ a \in G : b = f(a)$ para esto alcanza con tomar $a = b'$

Por lo tanto, como f es biyectiva, resulta ser un ISOMORFISMO.

2) La función $g: (Z ; +) \to (Z_5 ; \bar{+})$ es un EPIMORFISMO.

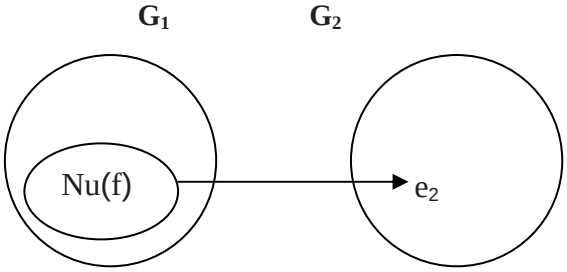
Primero averiguamos si es homomorfismo:

$\forall\ a, b \in Z:\ g(a + b) = \overline{a + b} = \bar{a} \ \bar{+} \ \bar{b} = g(a) \ \bar{+} \ g(b)$

No es inyectiva, pues existen infinitos enteros que pertenecen a una misma clase. Pero sí es sobreyectiva, ya que las clases de equivalencia no son vacías.

Núcleo de un homomorfismo

Sea $f: G_1 \to G_2$ un homomorfismo de grupos. Se define: $Nu(f) = \{ x \in G_1 / f(x) = e_2 \}$



Es decir el núcleo está formado por todos aquellos elementos del primer grupo cuya imagen es el elemento neutro del segundo grupo.

Ejemplo:

Si consideramos la función del ejemplo anterior $g: (Z ; +) \rightarrow (Z_5 ; \overline{+})$
El núcleo es el conjunto formado por todos los múltiplos de **5**, ya que todos ellos tienen como imagen a la clase del cero, que es el neutro de Z_5.

Propiedad del Núcleo: $Nu(f)$ es subgrupo de G_1

Te proponemos que intentes demostrarlo. Para ello, recuerda las condiciones necesarias y suficientes de subgrupos.
Si necesitas ayuda puedes consultar el capítulo 18 del libro de la cátedra, donde se presenta esta demostración, o bien consultar a tu tutor.

Otra propiedad relativa al núcleo de un homomorfismo, que resulta bastante útil para clasificarlo es la siguiente:

Propiedad:

Sea $f: G_1 \rightarrow G_2$ un homomorfismo de grupos. Entonces se cumple: $Nu(f) = \{ e_1 \} \Leftrightarrow f$ es inyectiva

Como la propiedad es un bicondicional, demostraremos cada parte por separado:

1) $Nu(f) = \{ e_1 \} \Rightarrow f$ es inyectiva

Dem) $\forall a, b \in G_1$: $f(a) = f(b) \Rightarrow f(a) *_2 f(b)' = f(b) *_2 f(b)'$

$\Rightarrow f(a) *_2 f(b') = e_2 \Rightarrow f(a *_1 b') = e_2$

Pero por hipótesis, el único elemento del núcleo es e_1, o sea el único cuya imagen es e_2, por lo tanto debe ser:

$a *_1 b' = e_1 \Rightarrow a *_1 b' *_1 b = e_1 *_1 b \Rightarrow a *_1 e_1 = b \Rightarrow a = b$

Con lo cual queda demostrado que f es INYECTIVA

2) f es inyectiva $\Rightarrow Nu(f) = \{ e_1 \}$

Por método del absurdo. Supongamos que en el núcleo, además de e_1 existiera otro elemento x, entonces $f(x) = e_2$. Pero como f es inyectiva, si $f(e_1) = e_2 \wedge f(x) = e_2$, deben ser iguales $e_1 = x$

Con lo cual queda demostrado.

Imagen de un homomorfismo

Sea $f: G_1 \to G_2$ un homomorfismo. Se define: $Im(f) = \{ y \in G_2 / \exists x \in G_1 \wedge f(x) = y \}$

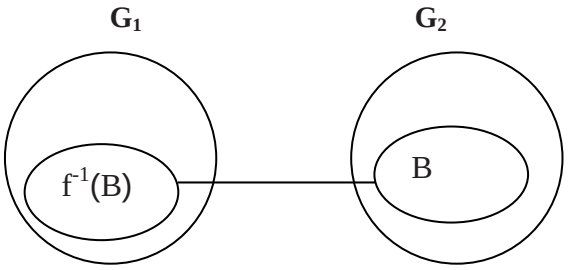
Observa que es la misma definición de Imagen de una función cualquiera.

Propiedad de la Imagen: $Im(f)$ es subgrupo de G_2

Como en el caso anterior, te proponemos que intentes demostrarlo. También para esta propiedad recuerda las condiciones necesarias y suficientes de subgrupos.
Si necesitas ayuda puedes consultar el capítulo 18 del libro de la cátedra, donde se presenta esta demostración, o bien consultar a tu tutor.

Preimagen o Imagen Recíproca

Sea $f : G_1 \to G_2$ un homomorfismo y sea $B \subseteq G_2$. Se define:
$f^{-1}(B) = \{ x \in G_1 / f(x) \in B \}$



Es decir son todos los elementos de G_1 que tienen como imagen algún elemento de B.

Para pensar...

De acuerdo a esta última definición, y teniendo en cuenta todo lo visto anteriormente ¿puedes decir qué nombre recibe la preimagen de $B = \{ e_2 \}$*?*

Si quieres asegurarte, consulta a tu tutor.

Grupos isomorfos

Muchas de las definiciones dadas apuntan a poder definir este concepto de isomorfismo de grupos ya que dados dos grupos nos va a interesar saber si son o no isomorfos. Ello es importante pues los grupos isomorfos comparten las mismas propiedades estructurales, es decir tienen las mismas características. Por ejemplo ambos son cíclicos; en ese caso tienen el mismo número de generadores, ambos son conmutativos o no , y si son finitos y hacemos la red de subgrupos , vemos que excepto el nombre de los elementos es la misma red. Si son isomorfos podemos usar cualquiera de ellos para resolver algún problema puntual. A medida que avancemos podremos aclarar más estas ideas.

Comencemos por definir **grupos isomorfos:**

> Sean $(G_1 ; *_1)$ y $(G_2 ; *_2)$ dos grupos. Diremos que son isomorfos si y solo si existe al menos un isomorfismo entre ellos.
> En es caso indicamos $\mathbf{G_1 \approx G_2}$

Es decir, para garantizar que dos grupos son isomorfos, debemos encontrar al menos una función biyectiva entre ambos que sea homomorfismo.

Los grupos isomorfos tienen las **mismas propiedades estructurales**, como ya dijimos deben compartir la conmutatividad, cardinalidad de los conjuntos subyacentes, cantidad de generadores, ser o no cíclico, etc.

e

Por ejemplo, un grupo de 6 elementos no puede ser isomorfo a un grupo de 8 elementos.
Un grupo abeliano no puede ser isomorfo a un grupo no abeliano.
Un grupo cíclico no puede ser isomorfo a un grupo no cíclico.

Consideremos el grupo $(A = \{1,-1, i, -i \} ; \bullet)$ siendo i la unidad imaginaria $(i^2 = -1)$ cuya tabla es:

•	1	-1	i	-i
1	1	-1	i	-i
-1	-1	1	-i	i
i	i	-i	-1	1
-i	-i	i	1	-1

Y el grupo $(B = \{ a, b, c, d \} ; *)$ dado por la siguiente tabla:

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

Nos preguntamos si alguno de ellos es isomorfo a algún grupo $(Z_n ; \bar{+})$

Para empezar, si alguno de ellos lo fuera, el valor de n debería ser 4, ya que para poder establecer una función biyectiva, los cardinales de los conjuntos subyacentes deben ser iguales.
Hagamos entonces la tabla de $(Z_4 ; \bar{+})$:

$\bar{+}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$

Debemos ir analizando, entonces, cuál de los dos grupos anteriores comparte las mismas propiedades estructurales que éste, ya que si encontramos alguna no compartida, descartamos la posibilidad de isomorfismo.

Por ejemplo, este grupo es abeliano. ¿Y los anteriores? Si observas que la tabla sea simétrica respecto de la diagonal principal, verás que también lo son. Por lo tanto seguimos analizando sin descartar a ninguno.
Otra propiedad estructural es ser o no cíclicos. El grupo Z_4 es cíclico. Veamos que pasa con los dos grupos dados.

El primero es cíclico pues por ejemplo un generador del mismo es i, ya que:

$$i \bullet i = -1 \quad \wedge \quad i \bullet i \bullet i = -i \quad \wedge \quad i \bullet i \bullet i \bullet i = 1$$

En cambio, el segundo grupo no es cíclico ya que:
$< a > = \{ a \}$; $< b > = \{ b , a \}$; $< c > = \{ c , a \}$; $< d > = \{ d , a \}$

Es decir no tiene generadores, por lo tanto no es cíclico. Y como Z_4 sí lo es, es imposible que sean isomorfos.

Otra forma de justificar que no son isomorfos, puede ser diciendo que este grupo B tiene 3 subgrupos de orden 2 (los calculados arriba), y en cambio Z_4 tiene uno solo de orden 2.

Habiendo descartado la posibilidad de isomorfismo entre B y Z_4, sigamos analizando qué pasa con el grupo A.

En este caso, si tenemos en cuenta todos los subgrupos (que por ser el grupo cíclico, solamente tiene subgrupos cíclicos) :
$< 1 > = \{ 1 \}$; $< -1 > = \{ -1 , 1 \}$; $< i > = \{ 1, -1, i, -i \} = < -i >$

Vemos que la cantidad y orden de los subgrupos coincide con los de Z_4.

Hasta acá todo va coincidiendo. Es hora de establecer la correspondencia biunívoca para poder estar seguros que son isomorfos. Para ello tengamos en cuenta que si un elemento es de un cierto orden en uno de los grupos, le tenemos que hacer corresponder un elemento del mismo orden en el otro grupo.
Por lo tanto, una posible función a definir es:

$$f: Z_4 \rightarrow A \,/\, f(\bar{0}) = 1 \,;\, f(\bar{1}) = i \,;\, f(\bar{2}) = -1 \,;\, f(\bar{3}) = -i$$

Si se quisiera dar por comprensión podría ser: $f(\bar{x}) = i^x$

Para estar seguros que es homomorfismo, tenemos dos opciones:

1ra opción: demostrarlo por la definición $f(\bar{a} \mathbin{\bar{+}} \bar{b}) = f(\bar{a}) \bullet f(\bar{b})$

Esto se puede hacer caso por caso (será necesario cuando no se tenga una fórmula), o bien en éste se puede hacer genéricamente: $f(\bar{a} \mathbin{\bar{+}} \bar{b}) = i^{a+b} = i^a \bullet i^b = f(\bar{a}) \bullet f(\bar{b})$

2da opción: solamente válida para grupos finitos: construir las tablas de ambos grupos con el mismo ordenamiento dado por la función definida y ver que se trata de la misma tabla pero con distinto nombre, es decir si se reemplazara cada uno de los elementos de la primer tabla por su imagen, se debería obtener la otra tabla.

En este caso:

$\bar{+}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$

•	1	i	-1	-i
1	1	i	-1	-i
i	i	-1	-i	1
-1	-1	-i	1	i
-i	-i	1	i	-1

Si observamos se nota que si hacemos abstracción de los nombres de los elementos las dos tablas son estructuralmente la misma. Incluso podemos armar una tabla isomorfa a estas dos utilizando otros nombres, siempre que respetemos la estructura, por ejemplo:

$\otimes$	x	y	z	t
x	x	y	z	t
y	y	z	t	x
z	z	t	x	y
t	t	x	y	z

y así de muchas maneras más...

En cambio, por más que intentáramos todas las permutaciones posibles de los elementos del otro grupo ($B = \{ a, b, c, d \}$; $\ast$) nunca nos iba a coincidir con estos, pues no es isomorfo.

De hecho, este grupo no cíclico de 4 elementos se llama 4-grupo de Klein.

Felix Klein (1849-1925) es un matemático estudioso de la geometría que introduce, en esa disciplina, el concepto de grupo ya que considera que esa disciplina es el estudio de las transformaciones y sus invariantes (propiedades que no cambian, por ejemplo las transformaciones geométricas formado por traslaciones, rotaciones y reflexiones que no

alteran las distancias entre los puntos de un conjunto). Justamente los invariantes, forma n grupo con la composición de funciones.

Nuestro ejemplo es interesante porque es abeliano y no cíclico.
Su tabla era:

✱	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

También existe el 8-grupo de Klein con características similares (abeliano y no cíclico) y es isomorfo a Z_2 X Z_4 pero no es isomorfo a Z_8.

En general, Z_m x Z_n es isomorfo a $Z_{nm} \Leftrightarrow$ m.c.d.(m,n) =1

El 8-grupo de Klein es el siguiente: (G = { 1, 2, 3, 4, 5, 6, 7, 8 } , ✱)

✱	1	2	3	4	5	6	7	8
1	3	4	1	2	7	8	5	6
2	4	1	2	3	8	5	6	7
3	1	2	3	4	5	6	7	8
4	2	3	4	1	6	7	8	5
5	7	8	5	6	3	4	1	2
6	8	5	6	7	4	1	2	3
7	5	6	7	8	1	2	3	4
8	6	7	8	5	2	3	4	1

Sinteticemos lo que vimos en esta última parte de esta unidad:

- *Definimos homomorfismos de grupos como funciones de correspondencia entre ellos.*
- *Vimos algunas propiedades de los homomorfismos y analizamos ejemplos.*
- *Definimos núcleo e imagen y sus propiedades.*
- *Clasificamos en: monomorfismos, epimorfismos e isomorfismos dándole mayor importancia a estos últimos.*

Finalizamos aquí el desarrollo de esta unidad. Te proponemos que para ejercitar, consideres este grupo (G ; ✱) y respondas las siguientes preguntas:

1) ¿Es $*$ conmutativa?
2) ¿Cuál es el elemento neutro y los simétricos de cada elemento?
3) ¿Es $H = \{ 1, 3, 5, 7 \}$ un subgrupo de G? ¿Es subgrupo normal? ¿Por qué?
4) ¿Cuál es la partición que produce H en el grupo?
5) ¿Cuáles son los subgrupos? .Grafica la red de subgrupos.
6) Dicha red ¿alcanza la estructura de Álgebra de Boole? ¿Por qué?
7) ¿Es $(G ; *)$ isomorfo a $(Z_8 ; +)$? ¿Por qué?

Las respuestas serán dadas por los tutores para que compares si has resuelto correctamente las consignas correctamente. Buena suerte!