Grupos

Operaciones

Cerrada

Una operación $*$ es cerrada en un conjuto si el resultado de operar dos elemntos es siempre un elemento del mismo conjunto.

$\forall x, y \in A : x * y \in A$

A las operaciones cerradas tambien se las llama leyes de composición interna.

La tabla debe contener solo elementos del conjunto.

Asociativa

Se dice que una operacion $*$ es asociativa si:

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

Se pueden cambiar los parentesis de lugar sin que ello afecte al resultado.

No se puede hacer a simple vista viendo la tabla de operación

Elemento neutro

Se dice que una operación $*$ tiene elemento neutro o identidad si:

$\exists e \in A : \forall a \in A : e * a = a * e = a$

O sea que el elemento neutro de una operación cerrada es aquel que al estar operado con cualquier otro no afecta el resultado.

La tabla debe contener una fila y una columna que repita los elementos en el mismo orden que están dispuestos en la tabla.

Elementos simetricos

Dado un elementro neutro e el simetrico de un elemento a se define:

$$a' \in A : a * a' = a' * a = e$$

Si todos los elementos tienen simetrico se dice que $*$ tiene simetrico.

En la tabla se busca el simetrico de un elemento buscando en su fila y columna al elemento neutro.

Conmutativa

Se dice que una operación $*$ es conmutatica si:

$$\forall a, b \in A : a * b = b * a$$

La tabla debe ser simetrica respecto de su diagonal principal.

Elementos idempotentes

Dado un elemento a se dice que es idempotente si:

$$a * a = a$$

Si se cumple para todos los elementos del conjunto se dice que $*$ es idempotente.

En la tabla la diagonal principal debe contener los mismos elementos dispuestos en el mismo orden de la tabla.

Elemento absorbente

Dado un elementro b se dice que b es absorbente si:

$$\forall a \in A : b * a = a * b = b$$

Es decir que si existe un elemento absorbente, cuando se opera cualquier elemento a el resultado siempre es b.

En la tabla, la fila y columna de dicho elemento tiene a ese elemento en todos los lugares.

Distributividad de dos operaciones binarias

Sean $*$ y $\bullet$ dos operaciones cerradas definidas en el mismo conjunto A.

Se dice que $\bullet$ es distributiva respecto de $*$ si y solo si:

$$\forall a, b, c \in A : a \bullet (b * c) = (a \bullet b) * (a \bullet c) \quad \text{(Distributiva a izquierda)}$$
$$\forall a, b, c \in A : (b * c) \bullet a = (b \bullet a) * (c \bullet a) \quad \text{(Distributiva a derecha)}$$

Grupos y semigrupos

Sea $\mathbf{A} \neq \varnothing$ y $\ast$ es una operación binaria y cerrada definida en $\mathbf{A}$.

Si además $\ast$ es asociativa $\Rightarrow (\mathbf{A} ; \ast)$ es SEMIGRUPO

Si además $\ast$ tiene neutro $\Rightarrow (\mathbf{A} ; \ast)$ es SEMIGRUPO CON NEUTRO

Si además $\ast$ tiene simétrico

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

En cualquiera de los casos anteriores, si además es conmutativa entonces a la estructura que posea $(\mathbf{A} ; \ast)$ 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)

Propiedades de un grupo

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

Elementos regulares

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 $x = y$

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

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 $*$.

Subgrupos

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

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

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

Sea $(G; *)$ un grupo. H es subgrupo de $G \Leftrightarrow$

1) $H \neq \emptyset$

2) $H \subseteq G$

3) $\forall a, b \in H \Rightarrow a * b' \in H$

Si afirmamos que H cumple las tres condiciones ya podremos afirmar que H es subgrupo de G.

Si H no cumple alguna de las tres condiciones ya podremos afirmar que H NO es subgrupo de G.

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.

Relaciones de congruencia

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

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

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

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

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 $* \Leftrightarrow \forall a, b, c, d \in G : a \sim b \wedge c \sim d \Rightarrow a * c \sim b * d$

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:

$\bar{a} \bar{*} \bar{b} = a \bar{*} b$

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

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

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.

Generadores, grupos cíclicos

Sea $(G; *)$ un grupo y $a \in G$. Llamamos Subgrupo cíclico de G generado por a al siguiente conjunto: $< a >= \{a^n \ / \ n \in \mathbb{Z}\}$

Aclaraciones:

a^n significa $a * a * a * \ldots * a$ (n veces)

a^{-n} significa $a^{-1} * a^{-1} * a^{-1} \ldots * a^{-1}$ (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.

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.

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.

Reticulo o Red de subgrupos

Dado un grupo $(G; *)$ con neutro $e4, entonces el conjunto de todos los subgrupos puede ser ordenado por la inclusión.

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

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.

Congruencia modulo un subgrupo

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

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

Lo indicamos así: $a \equiv_d b(H)$

Análogamente, definimos la relación:

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

Lo indicamos así: $a \equiv_i b(H)$

Propiedades:

Si $(G; *)$ es un grupo abeliano, entonces la congruencia a derecha coincide con la congruencia a izquierda

La relación de congruencia módulo n en $\mathbb{Z}$ (estudiada anteriormente) es un caso particular de la congruencia módulo H, considerando $H = nZ = \{x \in \mathbb{Z} / x = nk, k \in \mathbb{Z}\}$

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:

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

$\bar{a_i} = a * H$ (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.

Indice 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: $[G : H]$

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.

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.

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 $\forall a, b \in G_1 : f(a *_1 b) = f(a) *_2 f(b)$

Clasificación de homomorfismos

Sea $f : G_1 \to G_2$ 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

Imagen de un homomorfismo

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

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.

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 $G_1 \approx G_2$