Estructuras algebraicas

26 de abril de 2007

Grupos

Un **grupo** es un caso particular de una estructura algebraica. Veremos que esta noción rescata ampliamente las propiedades de estructuras tales como $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$ y $(\mathbb{R}, +)$.

Dedicaremos una sección especial a grupos, debido a que las particularidades que poseen nos permiten conocer muy bien sus propiedades, las cuales son bastantes.

Grupo

Sea $(G, *)$ una estructura algebraica. Diremos que es un **grupo** si

- $*$ es asociativa.
- $(G, *)$ posee neutro $e \in G$.
- Todo elemento $x \in G$ posee inverso $x^{-1} \in G$.

Además, si $*$ es conmutativa, llamaremos a $(G, *)$ **grupo abeliano**.

A modo de ejemplo, notemos que $(\mathbb{R}, \cdot)$ no es un grupo pues 0 no posee inverso. Sin embargo, $(\mathbb{R} \setminus \{0\}, \cdot)$ sí es un grupo.

Si $(G, *)$ es un grupo, entonces cumple las siguientes propiedades (las cuales ya vimos):

1. El inverso de cada elemento es único
2. $(\forall x \in G)\ (x^{-1})^{-1} = x$
3. $(\forall x, y \in G)\ (x * y)^{-1} = y^{-1} * x^{-1}$
4. Todo elemento $x \in G$ es cancelable.

Grupos: Propiedades

Si $(G, *)$ es un grupo, las siguientes propiedades se agregan a las mencionadas:

Propiedades

Dado $(G, *)$ grupo, entonces:

1. Para todo $a, b \in G$, las ecuaciones

$$a * x_1 = b$$
$$x_2 * a = b$$

tienen solución única. Ellas son $x_1 = a^{-1} * b$ y $x_2 = b * a^{-1}$

2. El único elemento idempotente de G es su neutro.

Demostración.

1. Consideremos sólo el caso de la primera ecuación. Como G es grupo, a posee neutro a^{-1}. Luego tendremos:

$$\begin{aligned} a^{-1} * (a * x_1) = a^{-1} * b &\Leftrightarrow (a^{-1} * a) * x_1 = a^{-1} * b \quad \text{Por asociativida.} \\ &\Leftrightarrow e * x_1 = a^{-1} * b \quad \text{Por definición de inverso.} \\ &\Leftrightarrow x_1 = a^{-1} * b \quad \text{Por definición de neutro.} \end{aligned}$$

Y esta última expresión es única, pues a^{-1} es único.

2. Si a es un elemento idempotente, satisface: $a * a = a$.
Pero esto es precisamente una ecuación como la anterior (con $b = a$ y a nuestra incógnita). Luego sabemos que la solución es única y es:

$$a = a^{-1} * a = e.$$

Subgrupos

Subgrupo

Sea $(G, *)$ un grupo, y sea $H \subseteq G$, $H \neq \emptyset$. Diremos que H es **subgrupo** de G si $(H, *)$ también es grupo.

Si consideramos el grupo $(\mathbb{R}, +)$, entonces un posible subgrupo es $(\mathbb{Q}, +)$. También tenemos a $(\{-1, 1\}, \cdot)$ como subgrupo de $(\mathbb{R} \setminus \{0\}, \cdot)$.

Todo grupo $(G, *)$ tiene dos subgrupos a los cuales llamaremos **triviales**:

$$(G, *) \quad \text{y} \quad (\{e\}, *)$$

donde e es el neutro de $(G, *)$.

Propiedades

Sea $(G, *)$ un grupo, y $(H, *)$ un subgrupo de él. Un par de propiedades básicas que salen de ver los elementos de H como elementos de G:

1. Si $e \in G$ es el neutro de G y $e_H \in H$ es el neutro de H, entonces $e = e_H$.
2. Además, sea $x \in H$. Si $x^{-1} \in G$ es el inverso de x en $(G, *)$ y $\tilde{x} \in H$ es el inverso de x en $(H, *)$, entonces $x^{-1} = \tilde{x}$.

Estas propiedades quedan propuestas como ejercicios.

Subgrupos: Caracterización

En principio, si uno quisiera demostrar que un conjunto $H \subseteq G$, $H \neq \emptyset$, forma un subgrupo de $(G, *)$, tendría que demostrar que $(H, *)$ cumple todas las propiedades de la definición de grupo, además de mostrar (el cual es el punto de partida) que

$$(\forall x, y \in H)\ x * y \in H$$

A esta propiedad se le conoce como **cerradura**, y es lo que nos permite decir que $*$ es una ley de composición interna también en H.

La siguiente es una forma compacta para determinar si $(H, *)$ es subgrupo de $(G, *)$.

Teorema

Sea $H \neq \emptyset$. Entonces

$$(H, *) \text{ es subgrupo de } (G, *) \iff (\forall x, y \in H)\ x * y^{-1} \in H$$

Demostración.

La implicancia $\Rightarrow$ se verifica directamente. Sin embargo, la propiedad fuerte es la implicancia $\Leftarrow$.
Para demostrarla, supongamos que $\forall x, y \in H,\ x * y^{-1} \in H$. Debemos probar que $(H, *)$ es grupo.
Notemos que la asociatividad se hereda automáticamente del hecho que $(G, *)$ sea grupo.Nos basta entonces probar que:

- $(H, *)$ es una estructura algebraica (cerradura de $*$ en H).
- $(H, *)$ admite un neutro (que por las propiedades anteriores, sabemos que debe ser el neutro de G).
- Todo elemento en H tiene inverso **en** H.

Continúa...

Subgrupos: Caracterización

Continuación demostración.

Probaremos estas afirmaciones en un orden distinto:

- Veamos primero que, si $e \in G$ es el neutro de $(G, *)$, entonces $e \in H$. Con esto e será el neutro de H.
  En efecto, como $H \neq \emptyset$, tomando $h \in H$, por hipótesis se tiene que
  $$h * h^{-1} = e \in H.$$
- Ahora probemos que dado $h \in H$, éste admite un inverso en H.
  Sabemos que h^{-1} es inverso de h, pero sólo para $(G, *)$. O sea, no sabemos si pertenece a H.
  Pero usando la hipótesis con $x = e$ e $y = h$, tenemos que:
  $$e * h^{-1} \in H \Leftrightarrow h^{-1} \in H.$$
- Finalmente, probamos la cerradura de $*$ en H.
  Dados $x, y \in H$. Por lo que vimos antes, $y^{-1} \in H$. Así que aplicando la hipótesis para x e y^{-1}, tenemos que:
  $$x * (y^{-1})^{-1} \in H \Leftrightarrow x * y \in H.$$

Concluímos de esta manera que $(H, *)$ es subgrupo de $(G, *)$. □

Ejemplo: $\mathbb{Z}_n$ como grupo

Propiedad

Sea $n \geq 2$. Entonces $(\mathbb{Z}_n, +_n)$ es un grupo.

Demostración.

Demostraremos que $+_n$ es asociativa, y que posee neutro. Las otras propiedades necesarias quedan de ejercicio para el lector.

Asociatividad: Sean $[x]_n, [y]_n, [z]_n \in \mathbb{Z}_n$. Se tiene que

$$\begin{aligned} ([x]_n +_n [y]_n) +_n [z]_n &= [x+y]_n +_n [z]_n \\ &= [(x+y)+z]_n \end{aligned}$$

Como $+$ es asociativa en $\mathbb{Z}$ y $x, y, z \in \mathbb{Z}$ entonces

$$(x+y)+z = x+(y+z)$$

Entonces

$$\begin{aligned} ([x]_n +_n [y]_n) +_n [z]_n &= [x+(y+z)]_n \\ &= [x]_n +_n [y+z]_n \\ &= [x]_n +_n ([y]_n +_n [z]_n) \end{aligned}$$

Continúa...

□

Ejemplo: $\mathbb{Z}_n$ como grupo

Continuación demostración.

Neutro: Demostraremos que $[0]_n \in \mathbb{Z}_n$ es neutro para $+_n$.
En efecto, si $[x]_n \in \mathbb{Z}_n$

$$[x]_n +_n [0]_n = [x+0]_n = [x]_n$$
$$[0]_n +_n [x]_n = [0+x]_n = [x]_n$$

□

Teorema de Lagrange

Sea $(G, *)$ un grupo. Diremos que es un grupo **finito** si G es un conjunto finito. A $|G|$ se le llama **orden** del grupo. Por ejemplo, $\mathbb{Z}_3$ es un grupo finito de orden 3.

Teorema de Lagrange

Sea $(G, *)$ un grupo finito y $(H, *)$ un subgrupo cualquiera de él. Entonces $|H|$ divide a $|G|$.

Demostración.

Definamos primero, dado $g \in G$, la **traslación izquierda** de H como el conjunto $g * H = \{g * h \mid h \in H\}$. Notemos que dado que g es cancelable, $|H| = |g * H|$.

Además, definimos las siguiente relación $\mathcal{R}$ sobre G por:

$$g_1 \mathcal{R} g_2 \Leftrightarrow (\forall g_1, g_2 \in G)\ g_2 \in g_1 * H.$$

Lo cual equivale a $(\exists h \in H)\ g_2 = g_1 * h$ y también a $g_1^{-1} * g_2 \in H$ (Verifíquelo).
Se tiene que $\mathcal{R}$ es una relación de equivalencia. En efecto:

- **Refleja.** Sea $g \in G$. Como H es subgrupo, $e \in H$ y $g = g * e$, pero esto es exactamente que $g \mathcal{R} g$.
- **Simétrica.** Sean $g_1, g_2 \in G$ tales que $g_1 \mathcal{R} g_2 \Leftrightarrow g_1^{-1} * g_2 \in H$.
  Pero como H es subgrupo, el inverso de este último término también pertence a H. Es decir:

$$(g_1^{-1} * g_2)^{-1} = g_2 - 1 * g_1 \in H.$$

Así, $g_2 \mathcal{R} g_1$.
Continúa...

□

Teorema de Lagrange

Continuación demostración.

- **Transitiva.** Supongamos que $g_1 \mathcal{R} g_2$ y $g_2 \mathcal{R} g_3$. Esto se traduce en que

$$g_1^{-1} * g_2,\ g_2^{-1} * g_3 \in H.$$

Y como H es cerrado para $*$, se deduce que:

$$(g_1^{-1} * g_2) * (g_2^{-1} * g_3) = g_1^{-1} * g_3 \in H.$$

De donde se conlcluye que $g_1 \mathcal{R} g_3$.

Ahora, dado que $\mathcal{R}$ es de equivalencia podemos calcular, para $g \in G$:

$$\begin{aligned}[g]_{\mathcal{R}} &= \{g' \in G \mid g \mathcal{R} g'\} \\ &= \{g' \in G \mid (\exists h \in H)\ g' = g * h\} \\ &= g * H.\end{aligned}$$

Luego, $|[g]_{\mathcal{R}}| = |H|$.
Sean entonces $[g_1]_{\mathcal{R}},\ [g_2]_{\mathcal{R}}, \ldots, [g_s]_{\mathcal{R}}$ las clases de equivalencia de $\mathcal{R}$.
Sabemos que estas clases conforman una partición de G, es decir: $G = [g_1]_{\mathcal{R}} \cup [g_2]_{\mathcal{R}} \cup \cdots \cup [g_s]_{\mathcal{R}}$.Luego:

$$\begin{aligned}|G| &= \sum_{i=1}^{s} |[g_i]_{\mathcal{R}}| \\ &= \sum_{i=1}^{s} |H| = s|H|.\end{aligned}$$

De donde se concluye el resultado. □

Ejemplo: diferencia simétrica

Antes de seguir:

Observación

Como implicancia de este teorema, tenemos por ejemplo que $(\mathbb{Z}_3, +_3)$ sólo puede tener subgrupos de orden 1 ó 3. Si $(H, +_3)$ es un subgrupo de orden 1, entonces debe tenerse que $H = \{[0]_3\}$, y si $(H, +_3)$ es un subgrupo de orden 3, entonces necesariamente $H = \mathbb{Z}_3$ (ejercicio para el lector). Es decir, los únicos subgrupos que tiene $(\mathbb{Z}_3, +_3)$ son los triviales. Este resultado es también válido para $(\mathbb{Z}_p, +_p)$ con p primo.

Sea A un conjunto no vacío. Veamos que $(\mathcal{P}(A), \Delta)$ es un grupo abeliano, donde Δ denota la diferencia simétrica

$$X \Delta Y = (X \setminus Y) \cup (Y \setminus X) = (X \cup Y) \setminus (X \cap Y)$$

Demostración.

Es claro que Δ es una ley de composición interna en $\mathcal{P}(A)$. De nuestro estudio de teoría de conjuntos, sabemos que Δ es asociativa y conmutativa.

Si $X \subseteq A$, entonces $X \Delta \emptyset = (X \cup \emptyset) \setminus (X \cap \emptyset) = X \setminus \emptyset = X$. Concluimos así que $\emptyset$ es el neutro de Δ.

Además, notando que $X \Delta X = (X \setminus X) \cup (X \setminus X) = \emptyset \cup \emptyset = \emptyset$, obtenemos que todo $X \in \mathcal{P}(A)$ es invertible, y que $X^{-1} = X$ (es decir, cada elemento es su propio inverso).

□

Morfismos

Sean $(A, *)$ y $(B, \triangle)$ dos estructuras algebraicas, y sea $f : A \to B$ una función. Sabemos que si $x, y \in A$ entonces $f(x), f(y) \in B$. Como sobre A tenemos definida una operación $*$, podemos hacernos la pregunta: ¿cuánto vale $f(x * y)$?

Los morfismos serán las funciones de A en B tales que $f(x * y)$ se construye operando $f(x)$ y $f(y)$, es decir tales que $f(x * y) = f(x) \triangle f(y)$ (recordemos que como $f(x), f(y) \in B$, entonces la operación que podemos aplicarles no es $*$, sino $\triangle$).

Morfismo

Una función $f : A \to B$ es un **homomorfismo**, o simplemente un **morfismo**, si

$$(\forall x, y \in A)\, f(x * y) = f(x) \triangle f(y)$$

Isomorfismo

Si $f : A \to B$ es un morfismo, y además es una función biyectiva, entonces le llamaremos **isomorfismo**.

Si existe un isomorfismo $f : A \to B$, diremos que $(A, *)$ y $(B, \triangle)$ son **estructuras isomorfas**, lo cual denotaremos $(A, *) \cong (B, \triangle)$. $\cong$ resulta ser una relación de equivalencia entre estructuras algebraicas con una operación.

Morfismos

Propiedad

$$(\mathbb{R}_+, \cdot) \cong (\mathbb{R}, +)$$

Demostración.

Consideremos la función

$$\begin{array}{rccc} \log: & \mathbb{R}_+ & \to & \mathbb{R} \\ & x & \to & \log(x) \end{array}$$

log es una función biyectiva, y cumple $\log(x \cdot y) = \log(x) + \log(y)$ para $x, y \in \mathbb{R}_+$.

□

Morfismos sobreyectivos

Propiedades

Sean $(A, *)$ y $(B, \triangle)$ estructuras algebraicas, y sea $f : A \to B$ un morfismo sobreyectivo. Se tiene que:

1. Si $*$ es asociativa, entonces $\triangle$ también.
2. Si $*$ es conmutativa, entonces $\triangle$ también.
3. Si $(A, *)$ tiene neutro $e \in A$, entonces $(B, \triangle)$ también tiene neutro, el cual es $f(e)$.
4. Sea $(A, *)$ es asociativa con neutro e, y sea $a \in A$. Si a posee inverso a^{-1}, entonces $f(a)$ también posee inverso, y más aún, $(f(a))^{-1} = f(a^{-1})$.

Demostración.

Demostraremos lo segundo.
Sean $b_1, b_2 \in B$. Como f es sobreyectiva, entonces existen $a_1, a_2 \in A$ tales que

$$f(a_1) = b_1 \quad \wedge \quad f(a_2) = b_2$$

Entonces

$$\begin{aligned} & b_1 \triangle b_2 \\ = \; & f(a_1) \triangle f(a_2) \\ = \; & f(a_1 * a_2) && (f \text{ es morfismo}) \\ = \; & f(a_2 * a_1) && (* \text{ es conmutativa}) \\ = \; & f(a_2) \triangle f(a_1) && (f \text{ es morfismo}) \\ = \; & b_2 \triangle b_1 \end{aligned}$$

□