Elementos de Teoría de la Computación
Clase: Grupos Isomórficos

Depart. de Teoría de la Computación - Facultad de Informática
Universidad Nacional del Comahue
2021

Pablo Kogan
pablo.kogan@fi.uncoma.edu.ar

Contenido

¿Qué vimos?

- Función
  - Dominio - Pre-Imagen
  - Imagen - Codominio -Rango
  - Sobreyectiva
  - Inyectiva o Uno a uno
  - Biyectiva
- Composición de Funciones
- Inversa

¿Qué vimos?

- Grafos
- Digrafos
- Nodo
  - Grado
  - Aislado
  - Simple (en la definición de árbol)
- Simple - Completo - Conectado - Subgrafo
- Camino - Longitud - Ciclo o Circuito
- **Camino** de Euler (tratable) y **Ciclo** de Hamilton(hard)
- Grafos Isomórficos
- Representación Computacional: matriz y lista de adyacencia

¿Qué vimos?

- Árboles
- Nodos internos - Hojas
- Profundidad
- Árboles Binarios
- Recorridos
  - Pre-orden
  - Inorden
  - Pos-orden
- Representación Computacional: matriz y lista de adyacencia

¿Qué vimos?

- Sistemas Algebraicos
- Semigrupo
- Monoide
- Grupo
- Subgrupo

HOY: Grupos Isomórficos

Grupos Isomórficos

Importante

Cuando tenemos dos grupos isomórficos, toda computación realizada en uno de ellos puede ser *simulada* en el otro.

Grupos Isomórficos

¿Qué significa que dos grupos $[S, \bullet]$ y $[T, \circ]$ sean isomórficos?

- Que las estructuras son idénticas, excepto por el etiquetado.
- Debe existir una biyección desde S a T.
- Esta biyección debe preservar los efectos de la operación binaria.
  - *Operar (en el primer conjunto) y mapear* debe producir el mismo resultado que *mapear y operar (en el segundo conjunto)*.

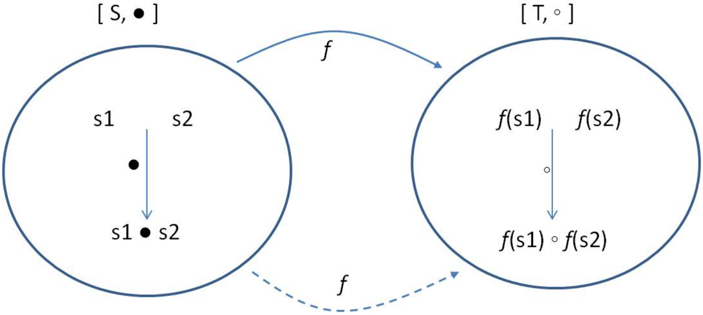
Homomorfismos - Isomorfismos

Definición

Sean $[S, \bullet]$ y $[T, \circ]$ dos grupos. Una función $f : S \rightarrow T$ es un homomorfismo de $[S, \bullet]$ a $[T, \circ]$ si:

- para todo par $s_1, s_2 \in S$, $f(s_1 \bullet s_2) = f(s_1) \circ f(s_2)$.

Si f es biyectiva, entonces f es un isomorfismo.



Isomorfismos

EJEMPLO: $[\mathbb{R}^+, *]$ y $[\mathbb{R}, +]$ son dos grupos. Sea b un número real positivo, $b \neq 1$, y sea la función $f : \mathbb{R}^+ \to \mathbb{R}$ tal que

$$f(x) = \log_b x$$

¿Cuál es la definición de logaritmo?

Back to ... Logaritmo

$$b^{exp} = x$$

¿Cuál es la operación inversa? La radicación, si dejamos fijo el exponente:

$$\sqrt[exp]{x} = b$$

¿Qué pasa si dejamos fija la base?

¿Cuál es la operación inversa?

$$log_b x = exp$$

¿Cuál es el $log_b 1$? 0
Sin importar la base, dado que $b^0 = 1$

Back to Isomorfismos en ETC :)

15 de Octubre del año 2020.

Isomorfismos

EJEMPLO: $[\mathbb{R}^+, *]$ y $[\mathbb{R}, +]$ son dos grupos. Sea b un número real positivo, $b \neq 1$, y sea la función $f : \mathbb{R}^+ \to \mathbb{R}$ tal que

$$f(x) = \log_b x$$

f es un isomorfismo de $[\mathbb{R}^+, *]$ a $[\mathbb{R}, +]$.

¿Cómo se prueba y cuál es la utilidad de este ejemplo ?

Isomorfismos. Ejemplo

EJEMPLO: $[\mathbb{R}^+, *]$ y $[\mathbb{R}, +]$ son dos grupos. Sea b un número real positivo, $b \neq 1$, y sea la función $f : \mathbb{R}^+ \to \mathbb{R}$ tal que $f(x) = \log_b x$. Entonces, f es un isomorfismo de $[\mathbb{R}^+, *]$ a $[\mathbb{R}, +]$.

Debemos probar que f es biyectiva (*inyectiva* y *sobreyectiva*) y que f es un *homomorfismo*.

f es *sobreyectiva*: para cada $r \in \mathbb{R}$, $b^r \in \mathbb{R}^+$ y $f(b^r) = log_b\, b^r = r$.

También, f es *inyectiva*:

si $f(x_1) = f(x_2)$, entonces $log_b\, x_1 = log_b\, x_2$.
Sea $p = log_b\, x_1 = log_b\, x_2$. Entonces $b^p = x_1$ y $b^p = x_2$, por lo tanto $x_1 = x_2$.

Isomorfismos. Ejemplo (cont.)

EJEMPLO: $[\mathbb{R}^+, *]$ y $[\mathbb{R}, +]$ son dos grupos. Sea b un número real positivo, $b \neq 1$, y sea la función $f : \mathbb{R}^+ \to \mathbb{R}$ tal que $f(x) = \log_b x$. Entonces, f es un isomorfismo de $[\mathbb{R}^+, *]$ a $[\mathbb{R}, +]$.

Debemos probar que f es biyectiva (*inyectiva* y *sobreyectiva*) y que f es un *homomorfismo*.

Finalmente, f es un *homomorfismo*:

para $x_1, x_2 \in \mathbb{R}^+$, $f(x_1 * x_2) = log_b\,(x_1 * x_2) = log_b\, x_1 + log_b\, x_2 = f(x_1) + f(x_2)$.

Además, notemos que:

$$log_b\, 1 = 0$$

$$log_b\, 1/x = log_b\, 1 - log_b\, x = 0 - log_b\, x = -log_b\, x = -f(x)$$

Isomorfismos. Ejemplo (cont.)

EJEMPLO: $[\mathbb{R}^+, *]$ y $[\mathbb{R}, +]$ son dos grupos. Sea b un número real positivo, $b \neq 1$, y sea la función $f : \mathbb{R}^+ \to \mathbb{R}$ tal que $f(x) = \log_b x$. Tal como vimos, f es un isomorfismo de $[\mathbb{R}^+, *]$ a $[\mathbb{R}, +]$.

Supongamos que $b = 2$. Luego, $[\mathbb{R}, +]$ puede ser usado para simular la computación de $64 * 512$ en $[\mathbb{R}^+, *]$. Primero, mapeamos desde $\mathbb{R}^+$ a $\mathbb{R}$:

$$\begin{array}{rcccc} f(64) & = & log_2\, 64 & = & 6 \\ f(512) & = & log_2\, 512 & = & 9 \end{array}$$

Ahora, ya en $[\mathbb{R}, +]$ realizamos la computación

$$6 + 9 = 15$$

Finalmente, usamos f^{-1} (como f es una biyección, sabemos que existe f^{-1} también biyectiva) para *regresar* a $\mathbb{R}^+$ y obtener el resultado buscado:

$$f^{-1}(15) = 2^{15} = 32.768$$

Isomorfismos. Ejemplo (final)

- Tal como vimos en este ejemplo, dados dos grupos isomórficos, cualquiera de ellos puede ser empleado para simular computaciones en el otro.

- En la época AC, antes de las calculadoras, el producto de números grandes era resuelto por medio de tablas de logaritmos en base 10. Un problema de multiplicación se convertía en un problema de suma.

- Hoy en día, los logaritmos en base 2 (y sus propiedades) son aún empleados para el diseño y optimización de circuitos digitales.

Núcleo de un Homomorfismo

Definición

Sean $[S, \bullet]$ y $[T, \circ]$ dos grupos. Sea i_t la identidad en $[T, \circ]$ y sea f un homomorfismo de $[S, \bullet]$ a $[T, \circ]$.

El núcleo de f, denotado $Nuc(f)$, se define como

$$Nuc(f) = \{s \in S : f(s) = i_t\}$$

Núcleo de un Homomorfismo - Ejemplo

EJEMPLO: $[\mathbb{R}^+, *]$ y $[\mathbb{R}, +]$ son dos grupos. Sea b un número real positivo, $b \neq 1$, y sea la función $f : \mathbb{R}^+ \to \mathbb{R}$ tal que $f(x) = \log_b x$. Tal como vimos, f es un homomorfismo (isomorfismo) de $[\mathbb{R}^+, *]$ a $[\mathbb{R}, +]$.

¿Cuál es el núcleo de f?

$$Nuc(f) = \{r \in \mathbb{R}^+ : f(r) = 0\} = \{r \in \mathbb{R}^+ : \log_b r = 0\} = \{1\}$$

Imagen Homomórfica

Definición

Sean $[S, \bullet]$ y $[T, \circ]$ dos grupos. Sea f un homomorfismo de $[S, \bullet]$ a $[T, \circ]$.

La imagen homomórfica de f, denotada $f(S)$, se define como

$$f(S) = \{t \in T : \text{ existe } s \in S \text{ y } f(s) = t\}$$

Imagen Homomórfica - Ejemplo

EJEMPLO: $[\mathbb{R}^+, *]$ y $[\mathbb{R}, +]$ son dos grupos. Sea b un número real positivo, $b \neq 1$, y sea la función $f : \mathbb{R}^+ \to \mathbb{R}$ tal que $f(x) = \log_b x$. Tal como vimos, f es un homomorfismo (isomorfismo) de $[\mathbb{R}^+, *]$ a $[\mathbb{R}, +]$.

¿Cuál es la imagen homomórfica de f?

Como f es sobreyectiva..

$$f(\mathbb{R}^+) = \{t \in \mathbb{R} : \text{ existe } s \in \mathbb{R}^+ \text{ y } f(s) = t\} = \mathbb{R}$$

Bibliografía

Mathematical Structures for Computer Science. Capítulo 8.
J. Gersting
Sixth edition
2007

Estructuras de Matemáticas Discretas para la Computación. Capítulo 9.
B. Kolman, A. Busby and S. Ross
3ra. Edición
1997

¿Preguntas?