Matemática Discreta

Vaira, Stella - Fedonczuk, Miguel
Colliard, David - Cottonaro, Mariana

Lic en Sistemas de Información - FCyT - UADER

2022

Grupos y teoría de codificación.

Definiciones, ejemplos y propiedades elementales.

Grupo

Si G es un conjunto no vacío y $\circ$ es una operación binaria en G, entonces $(G, \circ)$ es un grupo si cumple las siguientes condiciones:

1. $\forall a, b \in G$,$a \circ b \in G$. (ley de cierre)
2. $\forall a, b, c \in G,\ a \circ (b \circ c) = (a \circ) b \circ c$. (asociativa)
3. Existe $e \in G$ tal que $a \circ e = e \circ a = a$, para todo $a \in G$. (neutro)
4. Para todo $a \in G$ existe un elemento $b \in G$ tal que $a \circ b = b \circ a = e$. (inversos)

Si además se verifica para todo $a, b \in G$ que $a \circ b = b \circ a$, entonces el grupo es *abeliano o conmutativo*.

Con la suma ordinaria, $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ y $\mathbb{C}$ con cada uno grupo abeliano.

Sin el cero, $\mathbb{Q}^*, \mathbb{R}^*$ y $\mathbb{C}^*$ son grupos abelianos multiplicativos.

En general: Si $(R, +, .)$ es un anillo, entonces $(R, +)$ es un grupo abeliano. Los elementos distintos de cero de un *cuerpo* forman un grupo abeliano multiplicativo.

Orden de un grupo

Para cualquier grupo G, el número de elementos de G es el *orden* de G, y se denota con $|G|$. Cuando el número de elementos de un grupo no es finito, su orden es infinito.

Ejemplos
Para $c \in Z^+$, $n > 1$, $(\mathbb{Z}_n, +)$ es un grupo abeliano. $|(\mathbb{Z}_n, +)| = n$
Si p es primo, $(\mathbb{Z}_p^*, .)$ es un grupo abeliano. $|(\mathbb{Z}_p^*, .)| = p - 1$
Veamos el ejemplo de $(\mathbb{Z}_5, +)$ y $(\mathbb{Z}_7^*, .)$

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

·	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

Ejemplo
Sea $(\mathbb{Z}_n, +, .)$ un anillo, el conjunto formado por las unidades de dicho anillo forman un grupo multiplicativo $(U_n, .)$. Además $|(U_n, .)| = \varphi(n)$
Veamos el ejemplo de U_9

·	1	2	4	5	7	8
1	1	2	4	5	7	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	4	2
8	8	7	5	4	2	1

Teorema

Sean $(G, \circ)$ y $(H, *)$ grupos. Definimos la operación binaria $\cdot$ en $G \times H$ como $(g_1, h_1) \cdot (g_2, h_2) = (g_1 \circ g_2, h_1 * h_2)$. Entonces $(G \times H, \cdot)$ es un grupo llamado *producto directo* de G y H.

Ejemplo

Sea $(\mathbb{Z}_2, +)$ y $(\mathbb{Z}_3, +)$. Entonces $(\mathbb{Z}_2 \times \mathbb{Z}_3, .)$ es un anillo donde el neutro es $(0, 0)$ y, por ejemplo, $(1, 2)$ y $(1, 1)$ son inversos.

Teorema

Para cualquier grupo G,

- el neutro de G es único.
- el inverso de cada elemento de G es único.
- $\forall a, b, c \in G$ y $ab = ac$, entonces $b = c$. (cancelativa por izquierda)
- $\forall a, b, c \in G$ y $ba = ca$, entonces $b = c$. (cancelativa por derecha)

Subgrupo

Sea G un grupo y H un subconjunto no vacío de G. Si H es un grupo mediante la operación binaria de G, entonces H es un subgrupo de G.

Teorema

Si H es un subconjunto no vacío de un grupo G, entonces H es subgrupo de G si y sólo si $\forall a, b \in H$: (a) $ab \in H$ y (b) $a^{-1} \in H$.

Teorema

Si H es un subconjunto finito no vacío de un grupo G, entonces H es subgrupo de G si y sólo si $\forall a, b \in H$ se verifica que $ab \in H$.

Ejemplos de subgrupo

- Todo grupo G tiene como subgrupos a G y e. (subgrupos triviales).
- $H = \{0, 2, 4\}$ y $K = \{0, 3\}$ son subgrupos de $(\mathbb{Z}_6, +)$.
- $H = \{1, 8\}$ y $K = \{1, 4, 7\}$ son subgrupos de $(U_9, .)$.
- El grupo $(\mathbb{Z}, +)$ es un subgrupo de $(\mathbb{Q}, +)$ que a su vez en subgrupo de $(\mathbb{R}, +)$

Grupos y teoría de codificación.

Homomorfismos, isomorfismos y grupos cíclicos

Homomorfismo e isomorfismo

Si $(G, \circ)$ y $(H, *)$ son grupos y $f : G \to H$, entonces f es un *homomorfismo de grupos* si $\forall a, b \in G$ se verifica que $f(a \circ b) = f(a) * f(b)$.
Si además f es biyectiva, f es un *isomorfismo de grupos*. En tal caso, se dice que H y G son isomorfos.

Teorema

Sean $(G, \circ)$ y $(H, *)$ grupos con neutros respectivos e_G y e_H. Si $f : G \to H$ es un homomorfismo, entonces

- $f(e_G) = e_H$.
- $f(a^{-1}) = [f(a)]^{-1}$, para todo a en G.
- $f(a^n) = [f(a)]^n$ para todo a en G, con n entero.
- $f(S)$ es un subgrupo de H para cada subgrupo S de G.

Ejemplos

- Sean $(\mathbb{Z}, +)$ y $(\mathbb{Z}_4, +)$, con $f(x) = [x]$ es homomorfismo de grupo porque: $f(x+y) = [x+y] = [x] + [y] = f(x) + f(y)$ para todo x e y en G.
- $f : (\mathbb{R}^+, .) \to (\mathbb{R}, +)$, con $f(x) = log(x)$ es isomorfismo de grupo porque f es biyectiva, y $f(xy) = log(ab) = log(a) + log(b) = f(x) + f(y)$ para todo x e y en G.
- También es isomorfismo de grupo $f : (\{1, -1, i, -i\}, .) \to (\mathbb{Z}_4, +)$, con f definida por

$$f(1) = [0] \qquad f(-1) = [2] \qquad f(i) = [1] \qquad f(-i) = [3]$$

$\cdot$	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

Como se puede observar $i^1 = i, \quad i^2 = -1, \quad i^3 = -i, \quad i^4 = 1$, tenemos que todo elemento de G es una potencia de i, y decimos, i genera a G. Se denota $G = < i >$.

Grupos cíclicos

Un grupo G es *cíclico* si existe un elemento $x \in G$ tal que para todo $a \in G$,$a = x^n$ para algún n entero.

Ejemplos

- Sean $(\mathbb{Z}_4, +)$ es cíclico porque [1] y [3] lo generan. Para el caso de [3]: 1.[3] = [3], 2.[3] = [2], 3.[3] = [1] y 4.[3] = [0]. Escibimos $H =< [3] >=< [1] >$.
- U_9 es cíclico porque 2 lo genera. Verificar.

Si un elemento no genera a todo el grupo, generará un subgrupo distinto al grupo.

Orden de un generador

Si G es un grupo y $a \in G$, el *orden de* a, que denotamos con $o(a)$, $| < a > |$.

Así por ejemplo, para U_9, $< 4 >= \{1, 4, 7\}$ por lo que $o(7) = 3$.

Teorema

Sea $a \in G$ con $o(a) = n$. Si $k \in \mathbb{Z}$ y $a^k = e$, entonces $n|k$.

Teorema

Sea G un grupo cíclico:

- Si $|G|$ es infinito, entonces G es isomorfo a $(\mathbb{Z}, +)$.
- Si $|G| = n$, con $n > 1$, entonces G es isomorfo a $(\mathbb{Z}_n, +)$.

Teorema

Cualquier subgrupo de un grupo cíclico es cíclico.

Ejemplo

Verificar que $f : U_9 \to (\mathbb{Z}_6, +)$ son isomorfos.

Grupos y teoría de codificación.

Clases laterales y el teorema de Lagrange

Clase lateral

Si H es un subgrupo de G, entonces para cualquier $a \in G$, el conjunto $aH = \{ah/h \in H\}$ es una *clase lateral izquierda* de H en G. El conjunto $Ha = \{ha/h \in H\}$ es una *clase lateral derecha* de H en G. Si la operación en G es suma, escribimos $a + H$ en vez de aH.

Lema

Si H es un subgrupo de un grupo finito G, entonces para cualquier $a, b \in G$:

(a) $|aH| = |H|$ (b) $aH = bH$ o $aH \cap bH = \emptyset$.

Ejemplo

Verificar el lema para $G = (\mathbb{Z}_{12}, +)$ y $H = \{0, 4, 8\}$.

Teorema de Lagrange

Si G es un grupo finito de orden n y H es un subgrupo de orden m, entonces $m|n$.

Corolario 1

Si G es un grupo finito de orden n y $a \in G$, entonces $o(a)|n$.

Corolario 1

Cualquier grupo de orden primo es cíclico.