Universidad de Jaén

Grado en Ingeniería Informática
ÁLGEBRA

TEMA 2. EL GRUPO SIMÉTRICO

Carmen Ordóñez Cañada

Grado en Ingeniería Informática
TEMA 2. EL GRUPO SIMÉTRICO

Bibliografía básica:

Ruiz J. F., *Métodos computacionales en Álgebra. Matemática discreta: grupos y grafos*. Edición: 2ª ed. revisada. Universidad de Jaén, 2012.

Bujalance, E. y otros. *Elementos de Matemática Discreta*. Edición: 2ª ed., 3ª reimp. Sanz y Torres, 2001.

Dorronsoro, J. Y Hernández, E. *Números, grupos y anillos*. Addison Wesley. Universidad Autónoma de Madrid, 1999.

García Merayo, F. *Matemática Discreta*. Ed. Paraninfo. 2015

Grado en Ingeniería Informática
TEMA 2. EL GRUPO SIMÉTRICO

Bibliografía complementaria (Teoría):

Cohn, *Álgebra*. Volume I, J. WILEY&SONS, 1974.

Dubreil, P. y otros. *Lecciones de álgebra moderna*. Ed. Reverté.

Grimaldi, R.P. *Matemáticas discreta y combinatoria*. Addison Wesley Iberoamericana.

Sigler, L.G. *Álgebra*. Ed. Reverté.

Solman, Busby, Ross. *Estructuras de Matemática Discreta para la computación*. Ed. Prentice Hall. 1997 NUEVO

Vera López, A. y otros. *Álgebra abstracta aplicada*.

Bibliografía complementaria (Problemas):

Anzola, M. y otros. *Problemas de Álgebra: CONJUNTOS Y GRUPOS* (tomo 1). Ed. Autores, 1981/82

Bujalance, E. y otros. *Problemas Elementos de Matemática Discreta*. Sanz Torres, 1993.

García, F. Hernández, G., Nevot, A. *Problemas resueltos de Matemática Discreta*. Ed. Thomson. 2003.

García, C., López, J., Puigjaner, D. *Matemática Discreta. Problemas y ejercicios resueltos*. Ed. Prentice Hall. 2002.

Grado en Ingeniería Informática
TEMA 2. EL GRUPO SIMÉTRICO

ÍNDICE:

Definición. Un *grupo* es un par $(G,*)$ formado por un conjunto $G \neq \emptyset$ y una ley de composición interna $*: G \times G \to G$ verificando las siguientes propiedades:

i. Elemento Neutro: Existe $e \in G$ tal que $e * a = a * e = a$ para cada $a \in G$.

ii. Elemento simétrico: Para cada $a \in G$, existe $a' \in G$ tal que $a * a' = a' * a = e$.

iii. Asociativa: $(a * b) * c = a * (b * c)$ para cada $a, b, c \in G$.

Se dirá que es un grupo abeliano o conmutativo si además verifica:

iv. Conmutativa: $a * b = b * a$ para cada $a, b \in G$.

Ejemplo. *Definimos un grupo* $(G,*)$

$(\mathbb{Z}, +)$

$3 + 4 = 7$

$G = \{2, 3, 4, 5\}$

$+$ dada por:

$3 + 4 = 5$

+	2	3	4	5
2	2	3	4	5
3	3	2	5	4
4	4	5	3	2
5	5	4	2	3

```
In[]:=    G={2,3,4,5};
          operacion={{2,3,4,5},{3,2,5,4},{4,5,3,2},{5,4,2,3}};
```

Demostremos que es grupo:

Un *grupo* es un par $(G,*)$ formado por un conjunto $G \neq \emptyset$ y una ley de composición interna $*: G \times G \to G$ verificando las siguientes propiedades:

i. Elemento Neutro: Existe $e \in G$ tal que $e * a = a * e = a$ para cada $a \in G$.

ii. Elemento simétrico: Para cada $a \in G$, existe $a' \in G$ tal que $a * a' = a' * a = e$.

iii. Asociativa: $(a * b) * c = a * (b * c)$ para cada $a, b, c \in G$.

Se dirá que es un grupo abeliano o conmutativo si además verifica:

iv. Conmutativa: $a * b = b * a$ para cada $a, b \in G$.

Ejemplo.

$(\mathbb{Z},+)$

- $\mathbb{Z} \neq \emptyset$
- $+$ operación interna:

$\forall a,b \in \mathbb{Z} \quad \Rightarrow a+b \in \mathbb{Z}$

$G = \{2, 3, 4, 5\}$

- $G \neq \emptyset$
- $+$ operación interna:

$\forall a,b \in G \quad \Rightarrow a+b \in G$

+	2	3	4	5
2	2	3	4	5
3	3	2	5	4
4	4	5	3	2
5	5	4	2	3

```
In[]:=    G={2,3,4,5};
          operacion={{2,3,4,5},{3,2,5,4},{4,5,3,2},{5,4,2,3}};
In[]:=    INTERNA
Out[]=    True
```

Demostremos que es grupo:

Un *grupo* es un par $(G,*)$ formado por un conjunto $G \neq \emptyset$ y una ley de composición interna $*: G \times G \to G$ verificando las siguientes propiedades:

i. Elemento Neutro: Existe $e \in G$ tal que $e * a = a * e = a$ para cada $a \in G$.

ii. Elemento simétrico: Para cada $a \in G$, existe $a' \in G$ tal que $a * a' = a' * a = e$.

iii. Asociativa: $(a * b) * c = a * (b * c)$ para cada $a, b, c \in G$.

Se dirá que es un grupo abeliano o conmutativo si además verifica:

iv. Conmutativa: $a * b = b * a$ para cada $a, b \in G$.

Ejemplo.

$(\mathbb{Z},+)$

Elemento neutro: 0

$0 \in \mathbb{Z}$ y verifica

$a+0 = 0+a=a \quad \forall a \in \mathbb{Z}$

$G = \{2, 3, 4, 5\}$

Elemento neutro: 2

2+2=2=2+2
2+3=3=3+2
2+4=4=4+2
2+5=5=5+2

+	2	3	4	5
2	2	3	4	5
3	3	2	5	4
4	4	5	3	2
5	5	4	2	3

```
In[]:=    G={2,3,4,5};
          operacion={{2,3,4,5},{3,2,5,4},{4,5,3,2},{5,4,2,3}};
          ELEMENTONEUTRO[G,operacion]
Out[]=    2
```

Demostremos que es grupo:

Un *grupo* es un par $(G,*)$ formado por un conjunto $G \neq \emptyset$ y una ley de composición interna $*: G \times G \to G$ verificando las siguientes propiedades:

i. Elemento Neutro: Existe $e \in G$ tal que $e * a = a * e = a$ para cada $a \in G$.

ii. Elemento simétrico: Para cada $a \in G$, existe $a' \in G$ tal que $a * a' = a' * a = e$.

iii. Asociativa: $(a * b) * c = a * (b * c)$ para cada $a, b, c \in G$.

Se dirá que es un grupo abeliano o conmutativo si además verifica:

iv. Conmutativa: $a * b = b * a$ para cada $a, b \in G$.

Ejemplo.

$(\mathbb{Z},+)$

Elemento neutro: 0

Para cada $a \in \mathbb{Z}$, $\exists -a \in \mathbb{Z}$ tal que $a -a = -a + a = 0$

G = {2, 3, 4, 5}
Elemento neutro 2
Elemento simétrico:
a+_=2
2+2=2; -2=2
3+3=2; -3=3
4+5=2; -4=5
5+4=5; -5=4

+	2	3	4	5
2	2	3	4	5
3	3	2	5	4
4	4	5	3	2
5	5	4	2	3

In[]:= G={2,3,4,5};
operacion={{2,3,4,5},{3,2,5,4},{4,5,3,2},{5,4,2,3}};
ELEMENTOSIMÉTRICO[G,operacion]

Out[]=
2 3 4 5
2 3 5 4

Demostremos que es grupo:

Un *grupo* es un par $(G,*)$ formado por un conjunto $G \neq \emptyset$ y una ley de composición interna $*: G \times G \to G$ verificando las siguientes propiedades:

i. Elemento Neutro: Existe $e \in G$ tal que $e * a = a * e = a$ para cada $a \in G$.

ii. Elemento simétrico: Para cada $a \in G$, existe $a' \in G$ tal que $a * a' = a' * a = e$.

iii. Asociativa: $(a * b) * c = a * (b * c)$ para cada $a, b, c \in G$.

Se dirá que es un grupo abeliano o conmutativo si además verifica:

iv. Conmutativa: $a * b = b * a$ para cada $a, b \in G$.

Ejemplo.

$(\mathbb{Z},+)$

$(3+4)+4 = 7+4=11$

$3+(4+4) = 3+8=11$

Demostrarlo en general

$G = \{2, 3, 4, 5\}$

$(3+4)+4 = 5+4=2$

$3+(4+4) = 3+3=2$

Hacer todas las combinaciones

+	2	3	4	5
2	2	3	4	5
3	3	2	5	4
4	4	5	3	2
5	5	4	2	3

In[]:= G={2,3,4,5};
operacion={{2,3,4,5},{3,2,5,4},{4,5,3,2},{5,4,2,3}};
ASOCIATIVA
Out[]= True

Demostremos que es grupo:

Un *grupo* es un par $(G,*)$ formado por un conjunto $G \neq \emptyset$ y una ley de composición interna $*: G \times G \to G$ verificando las siguientes propiedades:

i. Elemento Neutro: Existe $e \in G$ tal que $e * a = a * e = a$ para cada $a \in G$.

ii. Elemento simétrico: Para cada $a \in G$, existe $a' \in G$ tal que $a * a' = a' * a = e$.

iii. Asociativa: $(a * b) * c = a * (b * c)$ para cada $a, b, c \in G$.

Se dirá que es un grupo abeliano o conmutativo si además verifica:

iv. Conmutativa: $a * b = b * a$ para cada $a, b \in G$.

Ejemplo.

$(\mathbb{Z},+)$

$a+b = b+a \quad \forall a, b \in \mathbb{Z}$

Demostrarlo en general

$G = \{2, 3, 4, 5\}$

$2+3=3=3+2$

$2+4=4=4+2$

$2+5=5=5+2$

Análogamente el resto

Simetría

+	2	3	4	5
2	2	3	4	5
3	3	2	5	4
4	4	5	3	2
5	5	4	2	3

In[]:= G={2,3,4,5};
operacion={{2,3,4,5},{3,2,5,4},{4,5,3,2},{5,4,2,3}};
CONMUTATIVA

Out[]= True

Otros ejemplos:

1. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ son grupos aditivos abelianos
2. $\mathbb{Q}^*$, $\mathbb{R}^*$ y $\mathbb{C}^*$, son grupos multiplicativos abelianos
3. $(\mathbb{Z}_n , +)$ y $(\mathbb{Z}_p -\{0\}, \cdot)$ son grupos conmutativos
4. Sea S conjunto no vacío, las transformaciones de S es un grupo no conmutativo, con la composición.

Notación:

- Si (G,+) grupo, entonces e= O y a'=-a
- Si $(G,\cdot)$ grupo, entonces e= 1 y $a'=a^{-1}$

Proposición. Sea $(G,*)$ grupo. Entonces el elemento neutro y el elemento simétrico son únicos.

Proposición. Sea $(G,*)$ grupo. Entonces se verifican:

1. $a*b=e \Rightarrow a=b'$ y $a'=b$
2. $a*b=a*c \Rightarrow b=c$ y $b*a=c*a \Rightarrow b=c$
3. $a*b=b \Rightarrow a=e$ y $b*a=b \Rightarrow a=e$
4. $(a*b)'=b' * a'$
5. $(a')'=a$

Definición. Sea $(G,*)$ grupo. Llamaremos *subgrupo de G* a todo subconjunto de G, $H \neq \emptyset$, verificando las siguientes propiedades:

i. $e_G \in H$

ii. Para cada $a \in H \Rightarrow a' \in H$

iii. Para todo $a, b \in H \Rightarrow a * b \in H$

Proposición. Sea $(G,*)$ grupo, $H \subseteq G$, $H \neq \emptyset$. Entonces

$$H \text{ es subgrupo de } G \text{ si y sólo si } \forall a, b \in H \Rightarrow a * b' \in H$$

Ejemplos:

1. $\{e\}$ y G son los subgrupos impropios

2. G = {2, 3, 4, 5}

+	2	3	4	5
2	2	3	4	5
3	3	2	5	4
4	4	5	3	2
5	5	4	2	3

- $H_1=\{2,3\}$ es subgrupo
- $H_2=\{2,4\}$ no es subgrupo
- $H_3=\{4,5\}$ no es subgrupo

3. ***Teorema.*** Todos los subgrupos de $\mathbb{Z}$ son de la forma $n\mathbb{Z}$, para algún $n \geq 0$

CÁLCULO DE SUBGRUPOS:

Definición. Llamamos *orden* de un grupo G, finito, |G|, al número de elementos del mismo.

Teorema de Lagrange. Sea G un grupo finito.
Si H subgrupo de G entonces |H| divide a |G|.

Observación: En el caso de un grupo finito, el teorema descarta aquellos subconjuntos que no pueden ser subgrupos (atendiendo al orden)

Definición. Sea $S=\{1, 2,\dots,n\}$. Llamamos $S_n=(B(S), \circ)$ el *grupo simétrico o de las permutaciones de n elementos*. A sus elementos los notaremos

$$\sigma=\begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}$$

y los llamaremos *permutaciones*.

Teorema. S_n es un grupo, no abeliano ($\forall n\geq 3$) y $|S_n|=n!$

Definición. Llamamos *ciclo de longitud r*, a todo $\tau\in S_n$ para el que existe $\{i_1,\dots, i_r\}\subseteq\{1, 2,\dots,n\}$ tal que:

$$\tau(i_1)= i_2\,;\ \tau(i_2)= i_3\,;\dots;\ \tau(i_{r-1})= i_r\,;\ \tau(i_r)= i_1$$

y $\forall j\in\{1, 2,\dots,n\}-\{i_1,\dots, i_r\}$ entonces $\tau(j)=j$. Lo notaremos $\tau=(i_1\dots i_r)$.

Llamaremos *trasposición* a todo ciclo de longitud 2.

Proposición. Si τ es un ciclo de longitud r de S_n, entonces $\tau^r=I$

Definición. Dos *ciclos* se dicen *disjuntos* si los elementos que mueve cada uno quedan fijos por el otro.

Proposición. Ciclos disjuntos conmutan.

Teorema de estructura. Toda permutación de S_n, distinta de la identidad, descompone de forma única, salvo el orden, como composición de ciclos disjuntos.

Corolario. Toda permutación de S_n descompone como composición de trasposiciones

4. DESCOMPOSICIÓN DE UNA PERMUTACIÓN

Proposición. Si τ es un ciclo de longitud r de S_n, entonces $\tau^r=I$

Definición. Dos *ciclos* se dicen *disjuntos* si los elementos que mueve cada uno quedan fijos por el otro.

Proposición. Ciclos disjuntos conmutan.

Teorema de estructura. Toda permutación de S_n, distinta de la identidad, descompone de forma única, salvo el orden, como composición de ciclos disjuntos.

Corolario. Toda permutación de S_n descompone como composición de trasposiciones

Definiciones. Sea $\sigma \in S_n$. Diremos que i, j $\in \{1, 2,\ldots,n\}$ dan una *inversión* en σ si

$$i<j \Rightarrow \sigma(i)>\sigma(j)$$

Notaremos $I(\sigma)$ al número de inversiones de σ.

Llamaremos *signatura de* σ, $\text{sign}(\sigma)=(-1)^{I(\sigma)}$

Una permutación $\sigma \in S_n$ se dice *par* $\Leftrightarrow$ $I(\sigma)$es par $\Leftrightarrow$ $\text{sign}(\sigma)=1$

Una permutación $\sigma \in S_n$ se dice *impar* $\Leftrightarrow$ $I(\sigma)$es impar $\Leftrightarrow$ $\text{sign}(\sigma)=-1$

Proposición. Toda trasposición de S_n es impar

Lema 1. Si τ es una trasposición de S_n, entonces , $\mathrm{sign}(\tau\sigma)=-\mathrm{sign}(\sigma)$.

Proposición 1. Si $\sigma\in S_n$ y $\sigma=\tau_1\ldots\ \tau_p$ donde τ_i son trasposiciones, entonces $\mathrm{sign}(\sigma)=(-1)^p$

Lema 2. Si $\sigma\in S_n$ y $\sigma=\tau_1\ldots\ \tau_p=\tau'_1\ldots\ \tau'_q$ donde τ_i y τ'_j son trasposiciones, entonces p y q tienen la misma paridad

Proposición 2. Si $\sigma,\beta\in S_n$, entonces

$$\mathrm{sign}(\sigma\beta)=\mathrm{sign}(\sigma)\mathrm{sign}(\beta)$$

Definición. Consideremos S_n el grupo simétrico.

Notaremos $A_n=\{\sigma\in S_n : \text{sign}(\sigma)=1\}$

Proposición. A_n es un subgrupo de S_n y $|A_n|=\frac{n!}{2}$

A_n se llama el *subgrupo alternado* de S_n

Universidad de Jaén

Grado en Ingeniería Informática
ÁLGEBRA

TEMA 2. EL GRUPO SIMÉTRICO

Carmen Ordóñez Cañada