Métodos Matemáticos II

Grao en Física.

Tema 2.- Elementos da teoría de grupos.

2.1. Operacións.

2.1.1. Definición.

Dado un conxunto X denomínase **operación interna** en X a unha aplicación:

$$*: X \times X \rightarrow X.$$

Habitualmente a imaxe dun par (x_1, x_2) denótase por $x_1 * x_2$.

2.1.2. Definición.

Sexa $*$ unha operación interna en X. Dise que esta operación interna ten a propiedade:

1) **Conmutativa** se $x_1 * x_2 = x_2 * x_1, \ \forall\, x_1, x_2 \in X$.
2) **Asociativa** se $(x_1 * x_2) * x_3 = x_1 * (x_2 * x_3), \ \forall\, x_1, x_2, x_3 \in X$

2.1.3. Exemplos.

1) $+: \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ é conmutativa e asociativa.
2) En $X = \mathbb{N} \times \mathbb{N}$ as operacións:
   i) $+: X \times X \rightarrow X$, dada por
   $(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2)$
   ii) $\bullet : X \times X \rightarrow X$, dada por
   $(x_1, y_1) \bullet (x_2, y_2) = (x_1 \bullet x_2 + y_1 \bullet y_2, x_1 \bullet y_2 + y_1 \bullet x_2)$
   son conmutativas e asociativas.
3) En $X = \mathbb{Z} \times \mathbb{Z}^*$ ($\mathbb{Z}^* = \mathbb{Z} - \{0\}$) as operacións:

---

i) $+: X \times X \to X$, dada por

$(x_1, y_1) + (x_2, y_2) = (x_1 \bullet y_2 + y_1 \bullet x_2, y_1 \bullet y_2)$

ii) $\bullet : X \times X \to X$, dada por

$(x_1, y_1) \bullet (x_2, y_2) = (x_1 \bullet x_2, y_1 \bullet y_2)$

son conmutativas e asociativas.

2.1.4. Definición.

Sexan $*$ e $\bullet$ dúas operacións internas en X. Dise que $*$ é **distributiva** pola esquerda respecto a $\bullet$ se

$$x_1 * (x_2 \bullet x_3) = (x_1 * x_2) \bullet (x_1 * x_3), \ \forall\, x_1, x_2, x_3 \in X$$

De forma análoga defínese a distributividade pola dereita.

2.1.5. Exemplo.

No apartado 2) e 3) del Exemplo 2.1.3. a operación $\bullet$ é distributiva respecto a +.

2.1.6. Definición.

Sexa $*$ unha operación interna en X. Dise que un elemento $x \in X$ é:

1) o **elemento neutro** para $*$ se

$$x * y = y * x = y, \ \forall\, y \in X.$$

2) un **elemento idempotente** para $*$ se

$$x * x = x.$$

2.1.7. Definición.

Sexa $*$ unha operación interna nun conxunto X e e o elemento neutro. Dise que $x \in X$ é o **simétrico** de $y \in X$ se

$$x * y = y * x = e.$$

Nótese que x é simétrico de y $\Leftrightarrow$ y é simétrico de x.

2.1.8. Exemplos.

1) Consideramos a operación suma, +, en $\mathbb{Z}$. Entonces:

i) 0 é o neutro.

ii) O único elemento idempotente é o 0.

iii)O simétrico de $x \in \mathbb{Z}$ é $-x \in \mathbb{Z}$.

2) Consideramos a operación suma, +, en $\mathbb{N}$. Verifícase: i) e ii) do exemplo anterior.

O único elemento que ten simétrico é o neutro, 0, e o seu simétrico é o propio 0.

3) Consideramos a operación produto, $\bullet$, en $\mathbb{Z}$. Entonces:

i) O 1 é o neutro.

ii) O 0 e o 1 son idempotentes.

iii) Só ten simétrico o 1 e o -1 e cada un é simétrico de si mesmo.

2.1.9. Proposición.

Nunha operación interna, o neutro, se existe, é único.

Demostración. Se $*$ é unha operación interna en X y e_1 e e_2 dous neutros, entonces:

$e_1 * e_2 = e_1$ por ser e_2 neutro

$e_1 * e_2 = e_2$ por ser e_1 neutro

En consecuencia $e_1 = e_1 * e_2 = e_2$.

2.1.10. Proposición.

Se $*$ é unha operación interna asociativa no conxunto X, entonces o simétrico de $x \in X$, se existe, é único.

Demostración. Sexa e o elemento neutro e supoñamos que x ten dous simétricos x' e x''. Entonces $x' = x' * e = x' * (x * x'') = (x'' * x) * x'' = e * x'' = x''$.

4

2.2. Elementos da teoría de grupos.

2.2.1.- Definición.

Sexa G un conxunto non baleiro e $*$ unha operación interna en G. Dise que (G, $*$) é un grupo se se verifica:

i) $*$ é unha operación asociativa.

ii) Existe elemento neutro para a operación interna $*$.

É dicir: $\exists\, e \in G \,/\, e * x = x * e = x, \ \forall\, x \in G$.

iii) Todos os elementos de G teñen simétrico.

É dicir: $\forall\, x \in G, \ \exists\, y \in G \,/\, x * y = y * x = e$.

iv) Se a operación $*$ ten a propiedade conmutativa, diremos que o grupo é abeliano ou conmutativo.

2.2.2.- Nota.

Tendo en conta os resultados do apartado anterior, dado que a operación interna dun grupo é asociativa, temos que:

i) O elemento neutro dun grupo é único (Proposición **2.1.**9.)

ii) Cada elemento $x \in G$ ten un único simétrico que denotaremos x^{-1} e o simétrico de x é único (Proposición **2.1.**10.). Se utilizamos o símbolo + para denotar a operación do grupo, o simétrico de x denotarémolo por -x.

2.2.3.- Exemplos.

1) ($\mathbb{Z}$, +), ($\mathbb{Q}$, +), ($\mathbb{R}$, +) y ($\mathbb{C}$, +) son grupos abelianos.

2) ($\mathbb{Z}$, $\bullet$) non é grupo.

3) ($\mathbb{Q}$, $\bullet$), ($\mathbb{R}$, $\bullet$) y ($\mathbb{C}$, $\bullet$) non son grupos.

4) Se denotamos por $\mathbb{Q}^*$ o conxunto dos números racionais sen o cero ($\mathbb{Q}^* = \mathbb{Q}-\{0\}$) e, analogamente, $\mathbb{R}^*$ e $\mathbb{C}^*$ os respectivos conxuntos dos números reais e complexos sen o cero, entonces ($\mathbb{Q}^*$, $\bullet$), ($\mathbb{R}^*$, $\bullet$) e ($\mathbb{C}^*$, $\bullet$) son grupos abelianos.

5) $G = \mathbb{Q} \times \mathbb{Q}$ coa operación

$(x_1, y_1) * (x_2, y_2) = (x_1+x_2, y_1+y_2)$

é un grupo abeliano.

6) $G = \mathbb{Q}\times\mathbb{Q}-\{(0, 0)\}$. É dicir $G = \{(x, y)\in\mathbb{Q}\times\mathbb{Q} / (x, y) \neq (0, 0)\}$ coa operación

$(x_1, y_1)*(x_2, y_2) = (x_1x_2+3y_1y_2, x_1y_2+y_1x_2)$

é un grupo abeliano.

2.2.4.- Proposición.

Se $(G, *)$ é un grupo, (definimos en 2.1.6. 2) que un elemento $a\in G$ é idempotente se $a*a = a$). Nun grupo o único elemento idempotente é o neutro

(é dicir $a\in G$, $a*a = a \Rightarrow a = e$)

Demostración:

Por ser $(G, *)$ un grupo, temos que existe o simétrico de a, que denotamos por a^{-1}, e a operación * ten a propiedade asociativa. Entón,

$a*a = a \Rightarrow e = a^{-1}*a = a^{-1}*(a*a) = a^{-1}*(a*a) = (a^{-1}*a)*a = e*a = a$

2.2.5.- Outras propiedades básicas.

i) $\forall\, x, y\in G$, existe un único $z\in G / x*z = y$.

ii) $\forall\, x, y\in G$, existe un único $z\in G / z*x = y$.

Demostración.

$x * z = y \Rightarrow x^{-1}*(x*z) = x^{-1}*y \Rightarrow z = x^{-1}*y$.

Analogamente para $z*x = y$.

2.2.6.- Definición.

Sexa $(G, *)$ un grupo e $H\subseteq G$, $H\neq\phi$. Decimos que H é un **subgrupo** de G se * é unha operación interna en H e $(H, *)$ é un grupo.

Exemplos: Véxase o caso de

$\mathbb{Z}\subseteq\mathbb{Q}\subseteq\mathbb{R}\subseteq\mathbb{C}$ coa operación suma ou

$\mathbb{Q}^*\subseteq\mathbb{R}^*\subseteq\mathbb{C}^*$ coa operación produto

2.2.7.- Definición

Se $(G, *)$ e $(G', \circ)$ son grupos unha aplicación $f : \mathbf{G} \longrightarrow \mathbf{G'}$ é un **homomorfismo de grupos** de G en G' se verifica,

$$f(x*y) = f(x)\circ f(y)$$

2.2.8.- Proposición (Propiedades básicas).

Se (G, *) e (G', $\circ$) son grupos e f : **G** $\longrightarrow$ **G'** é un homomorfismo de grupos, entón:

i) $f(e_G) = e_{G'}$.

ii) $f(x^{-1}) = f(x)^{-1}$, $\forall\, x \in G$.

Demostración:

i) $f(e_G) \circ f(e_G) = f(e_G * e_G) = f(e_G)$. Logo $f(e_G)$ é idempotente e polo tanto é o neutro de G', $f(e_G) = e_{G'}$.

ii) $f(x^{-1}) \circ f(x) = f(x^{-1} * x) = f(e_G) = e_{G'}$. Analogamente $f(x) \circ f(x^{-1}) = e_{G'}$.

En consecuencia $f(x^{-1})$ é o inverso de f(x)

2.2.9.- Definición

Sexan (G, *) e (G', $\circ$) grupos e f : **G** $\longrightarrow$ **G'** é un homomorfismo de grupos, entón denomínase núcleo de f e denótase Ker(f) ou Nuc(f) ó conxunto:

$$Ker(f) = \{x \in \mathbf{G} \,/\, f(x) = e_{G'}\}$$

2.2.10.- Proposición

f : **G** $\longrightarrow$ **G'** é un homomorfismo de grupos, entón

i) Ker(f) é subgrupo de G.

ii) Se H é subgrupo de G, f(H) é subgrupo de G'.

iii) Se T é subgrupo de G', $f^{-1}(T)$ é subgrupo de G.

iv) Im(f) é subgrupo de G'.

Demostración:

i)

Se x, $y \in$ Ker(f), entón $f(x * y) = f(x) \circ f(y) = e_{G'} \circ e_{G'} = e_{G'}$, polo que $(x * y) \in$ Ker(f).

A propiedade asociativa verifícana todos os elementos de G e polo tanto os de Ker(f)

$f(e_G) = e_{G'}$ e polo tanto $e_G \in Ker(f)$.

Se $x \in Ker(f)$, entón $f(x) = e_{G'} \Rightarrow f(x^{-1}) = f(x)^{-1} = (e_{G'})^{-1} = e_{G'} \Rightarrow x^{-1} \in Ker(f)$

ii) É un exercicio sinxelo.

iii) É un exercicio sinxelo.

iv) Basta ter en conta o apartado ii) para o caso de H = G.

2.2.11.- Proposición

Se f : **G** $\longrightarrow$ **G'** é un homomorfismo de grupos, entón:

1) f é inxectivo se, e só se, Ker f = {e}
2) f é sobrexectivo se, e só se, Im f = G'.

Demostración:

1) "$\Rightarrow$" é evidente.

"$\Leftarrow$" $x_1, x_2 \in G$, $f(x_1) = f(x_2) \Rightarrow f(x_1 * x_2^{-1}) = f(x_1) * f(x_2^{-1}) = e_{G'} \Rightarrow$

$\Rightarrow (x_1 * x_2^{-1}) \in Ker(f) = \{e_G\} \Rightarrow x_1 * x_2^{-1} = e_G \Rightarrow x_1 = x_2$.

2) É conscuencia directa da definición de sobrexectivo.

2.2.12.- Definición.

Sexa A un conxunto con dúas operacións internas: $*$ e $\bullet$.

Dise que $(A, *, \bullet)$ é un anel se se verifica:

1) $(A, *)$ é un grupo conmutativo.
2) $\bullet$ é unha operación asociativa.
3) $\bullet$ é distributiva respecto a $*$ por ambos lados.

Se a operación $\bullet$ é conmutativa dise que é un anel conmutativo ou abeliano.

2.2.13.- Definición.

Un anel $(A, *, \bullet)$ dise anel unitario se existe neutro para a operación $\bullet$.

2.2.14.- Definición.

Un corpo é un anel unitario $(K, *, \bullet)$ no que todo elemento non nulo ten simétrico respecto á segunda operación.

(Suporemos sempre que a segunda operación $\bullet$ é conmutativa).

2.2.15.- Exemplos.

1) $(\mathbb{N}, +)$ non é grupo.

$(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ e $(\mathbb{C}, +)$ son grupos abelianos.

$(\{f(x) \in \mathbb{R}[x] / \partial f(x) \leq n\}, +)$ é un grupo abeliano, para calquera $n \in \mathbb{N}$.

2) $(\mathbb{Z}, \bullet)$ non é grupo.

3) $(\mathbb{Q}, \bullet)$, $(\mathbb{R}, \bullet)$ e $(\mathbb{C}, \bullet)$ non son grupos.

4) Se denotamos por $\mathbb{Q}^*$ o conxunto dos números racionais sen o cero (ou sexa $\mathbb{Q}^* = \mathbb{Q}-\{0\}$) e, da mesma forma, $\mathbb{R}^*$ e $\mathbb{C}^*$ os respectivos conxuntos dos números reais e complexos sen o cero, entón $(\mathbb{Q}^*, \bullet)$, $(\mathbb{R}^*, \bullet)$ e $(\mathbb{C}^*, \bullet)$ son grupos abelianos.

5) $(\mathbb{Z}, +, \bullet)$ e $(\mathbb{R}[x], +, \bullet)$ son aneis pero non son corpos.

$(\{f(x) \in \mathbb{R}[x] / \partial f(x) \leq n\}, +, \bullet)$, $n \in \mathbb{N}$, non é un anel.

6) $(\mathbb{Q}, +, \bullet)$, $(\mathbb{R}, +, \bullet)$ e $(\mathbb{C}, +, \bullet)$ son corpos

7) $G = \mathbb{Q} \times \mathbb{Q}$ coa operación $(x_1, y_1) * (x_2, y_2) = (x_1+x_2, y_1+y_2)$

é un grupo abeliano.

8) $G = \mathbb{Q} \times \mathbb{Q}-\{(0, 0)\}$. É dicir $G = \{(x, y) \in \mathbb{Q} \times \mathbb{Q} / (x, y) \neq (0, 0)\}$ coa operación

$(x_1, y_1) * (x_2, y_2) = (x_1x_2+3y_1y_2, x_1y_2+y_1x_2)$

é un grupo abeliano.