Extraordinaria Estructuras Algebraicas

Antonio Cabrera Landín

5 de junio de 2025

Índice

1. Teoremas

Teorema 1 (Propiedad cancelativa)**.** *Para todo grupo $G = \{X, \cdot\}$ se cumple*

$$a \cdot c = b \cdot c \implies a = b \tag{1}$$

$$c \cdot a = c \cdot b \implies a = b \tag{2}$$

Demostración.

$$a \cdot c = b \cdot c \iff a \cdot c \cdot c^{-1} = b \cdot c \cdot c^{-1} \iff a \cdot e = b \cdot e \iff a = b \tag{3}$$

$$c \cdot a = c \cdot b \iff c^{-1} \cdot c \cdot a = c^{-1} \cdot c \cdot b \iff e \cdot a = e \cdot b \iff a = b \tag{4}$$

□

Teorema 2. *En cada grupo solo puede existir un elemento neutro.*

Demostración. Sea el grupo $G = \{X, \cdot\}$ asumamos que tenga dos elementos neutros e_1 y e_2, entonces

$$\begin{cases} x \cdot e_1 = x \\ x \cdot e_2 = x \end{cases} \implies x \cdot e_1 = x \cdot e_2 \iff x^{-1} \cdot x \cdot e_1 = x^{-1} \cdot x \cdot e_2 \iff e \cdot e_1 = e \cdot e_2 \iff e_1 = e_2 \tag{5}$$

□

Teorema 3. *Dado un grupo $G = \{X, \cdot\}$, si para cualquier elemento $a \in G$ se cumple que $a \cdot a = e$, entonces G es abeliano.*

$$\forall a \in G : a \cdot a = e \implies \forall a, b \in G : a \cdot b = b \cdot a \tag{6}$$

Demostración.

$$a \cdot b \in G \implies (ab)^2 = ab \cdot ab = e \tag{7}$$

$$\begin{aligned} &aabb = e \cdot e = e = (ab)^2 \implies a^{-1}(aabb) = a^{-1}(abab) \iff \\ &abb = bab \iff (abb)b^{-1} = (bab)b^{-1} \iff ab = ba \end{aligned} \tag{8}$$

□

Teorema 4. *Dado un grupo $G = \{X, \cdot\}$, si para todo $a, b \in G$ se cumple que $(a \cdot b)^2 = a^2 \cdot b^2$, entonces G es abeliano*

$$\forall a, b \in G : (a \cdot b)^2 = a^2 \cdot b^2 \implies \forall a, b \in G : a \cdot b = b \cdot a \tag{9}$$

Demostración.

$$\begin{aligned} &(a \cdot b)^2 = a^2 \cdot b^2 \implies abab = aabb \iff a^{-1}(abab) = a^{-1}(aabb) \iff \\ &bab = abb \iff (bab)b^{-1} = (abb)b^{-1} \iff ba = ab \end{aligned} \tag{10}$$

□

Teorema 5. *$\mathbb{Z}_n$ tiene $\varphi(n)$ generadores*

Teorema 6. *Dado un grupo $G = \{X, \cdot\}$, para todos sus elementos $a \in G$ el inverso del inverso de a es a.*

$$\forall a \in G : (a^{-1})^{-1} = a \tag{11}$$

Demostración.

$$(a^{-1})^{-1} \cdot a^{-1} = e \iff (a^{-1})^{-1} \cdot a^{-1} \cdot a = e \cdot a \iff (a^{-1})^{-1} = a \tag{12}$$

□

Lema 1. *Dado un grupo $G = \{X, \cdot\}$, para cada pareja $a, b \in G$ se cumple que $(a \cdot b)^{-1} = b^{-1}a^{-1}$*

Demostración.

$$\begin{aligned}&(a\cdot b)^{-1}(a\cdot b)=e \iff (a\cdot b)^{-1}(a\cdot b)\cdot b^{-1}=e\cdot b^{-1} \iff\\ &(a\cdot b)^{-1}a=b^{-1} \iff (a\cdot b)^{-1}a\cdot a^{-1}=b^{-1}a^{-1} \iff\\ &(a\cdot b)^{-1}=b^{-1}a^{-1}\end{aligned} \tag{13}$$

□

Teorema 7. *Dado un grupo $G=\{X,\cdot\}$, para cada pareja $a,b\in G$ el orden de ab es el mismo que el de ba*

$$\forall a,b\in G:(a\cdot b)^k=e \iff (b\cdot a)^k=e \tag{14}$$

Demostración.

$$\begin{aligned}&(ab)^k=ab\cdot ab\cdots ab=a\cdot(ba\cdots ba)\cdot b=a\cdot(ba)^{k-1}\cdot b=e \iff\\ &a^{-1}\cdot a\cdot(ba)^{k-1}\cdot b=a^{-1} \iff (ba)^{k-1}\cdot b=a^{-1} \iff\\ &(ba)^{k-1}\cdot b\cdot b^{-1}=a^{-1}b^{-1} \iff (ba)^{k-1}=a^{-1}b^{-1}\overset{\text{lema 1}}{\overset{\downarrow}{=}}(ba)^{-1} \iff\\ &(ba)^{k-1}(ba)=(ba)^{-1}(ba) \iff (ba)^k=e\end{aligned} \tag{15}$$

□

Teorema 8 (Teorema de Caley)**.** *Todo grupo G es isomorfo a un subgrupo de las biyecciones de G, $B(G)$, que es el grupo simétrico.*

Teorema 9. *El centro de un grupo es un subgrupo y es normal.*

Demostración. El centro $Z(G)$ es un subgrupo de G

1. El centro $Z(G)$, al mantener la operación de G, seguirá cumpliendo la propiedad asociativa.
2. El centro mantiene el neutro:

$$\forall x\in G:e\cdot x=x\cdot e \implies e\in Z(G) \tag{16}$$

3. Si x está en el centro entonces su inverso x^{-1} también:

$$\begin{aligned}&x\in Z(G) \implies \forall g\in G:g\cdot x^{-1}=x\cdot x^{-1}\cdot g\cdot x^{-1}=\\ &x^{-1}\cdot g\cdot x\cdot x^{-1}=x^{-1} \implies x^{-1}\in Z(G)\end{aligned} \tag{17}$$

□

Demostración. El centro $Z(G)$ es un subgrupo normal

$$\begin{aligned}&\forall h\in Z(G),g\in G:g\cdot h\cdot g^{-1}=g\cdot g^{-1}\cdot h=h \implies\\ &gHg^{-1}=H \implies Z(G)\text{ subgrupo normal}\end{aligned} \tag{18}$$

□

Teorema 10. *Todos los subgrupos de índice 2 son normales*

Demostración. Si un subgrupo tiene índice 2, significa que solo tiene dos clases laterales izquierdas y 2 clases laterales derechas.
Tendremos dos clases laterales izquierdas, aH y bH. Como e estará en una de las dos, podemos hablar de H y xH. Lo mismo ocurre con las clases laterales derechas, tendremos H y Hx

$$\begin{cases}H\cup xH=G\\ H\cup Hx=G\end{cases} \implies xH=Hx \implies H\text{ es normal} \tag{19}$$

□

Lema 2. *Si $a \in xH$ entonces $xH = aH$*

Demostración.

$$a \in xH \implies \exists h \in H : a = xh \iff aH = xhH \implies aH = xH \tag{20}$$

□

Teorema 11. *Las clases laterales izquierdas o coinciden o no tienen intersección.*

Demostración. Dado un grupo $G = \{X, \cdot\}$ con un subgrupo $H \subseteq G$. Supongamos que $\exists a \in xH$ que además $a \in yH$, entonces:

$$\begin{gathered} \begin{cases} a \in xH \implies \exists h_1 \in H : a = xh_1 \\ a \in yH \implies \exists h_2 \in H : a = yh_2 \end{cases} \implies xh_1 = yh_2 \iff \\ xh_1 \cdot h_1^{-1} = yh_2h_1^{-1} \iff x = yh_2h_1^{-1} = yh_3,\ h_3 \in H \implies x \in yH \end{gathered} \tag{21}$$

Utilizando el lema 1, sabemos que $x \in yH \implies xH = yH$. □

Teorema 12 (Teorema de Lagrange)**.** *El orden del grupo es múltipo del orden del subgrupo*

$$H \subseteq G \implies |G| = |H| \cdot n \quad n \in \mathbb{N} \tag{22}$$

Demostración. Dado un grupo G con un subgrupo H y con clases laterales x_iH, por el teorema 11 sabemos que las clases laterales no tienen intersección. Como tienen que abarcar a todo el grupo G y no tienen intersección, entonces necesariamente el orden de G será múltiplo del orden de las clases laterales.

$$\sum_{i=1}^{\text{índice}} |x_iH| = |G| \implies |G| = |x_iH| \cdot n \quad n \in \mathbb{N} \tag{23}$$

Las clases laterales x_iH tienen el mismo orden que H, ya que se construyen operando x_i con los elementos de H, entonces el orden de G es múltiplo del orden de H.

$$|x_iH| = |H| \implies |G| = |H| \cdot n \quad n \in \mathbb{N} \tag{24}$$

□

Colorario 13. *El orden del grupo es múltiplo del orden de un elemento*

$$x \in G : x^k = e \implies |G| = k \cdot n \quad n \in \mathbb{N} \tag{25}$$

Teorema 14. *Cualquier grupo de orden primo es cíclico*

$$|G| = p \text{ primo} \implies \exists x \in G : x^p = e \tag{26}$$

Demostración. Por el colorario 13 sabemos que el orden del grupo tiene que ser múltiplo del orden de los elementos. Como el orden del grupo es primo, los elementos solo pueden tener orden 1 u orden p. Por el teorema 2, el único elemento de orden 1 es el neutro, entonces el resto de elementos del grupo tienen orden p. Como existe al menos un elemento de orden p, el grupo es cíclico. □

Teorema 15. *Si $H \subset G$ es un subgrupo, entonces gHg^{-1}, con $g \in G$, también lo es.*

$$H \subset G \implies gHg^{-1} \subset G \quad g \in G \tag{27}$$

Demostración. gHg^{-1} cumple con las tres propiedades del los subgrupos:

1. gHg^{-1} seguirá manteniendo la propiedad asociativa ya que solo hemos operado los elementos de H con elementos de G.

2. El elemento neutro $e \in G$ está en gHg^{-1}:

$$e \in H \implies g \cdot e \cdot g^{-1} = g \cdot g^{-1} = e \implies e \in gHg^{-1} \tag{28}$$

3. Cada elemento $x = ghg^{-1} \in gHg^{-1}$ tiene inverso x^{-1}:

$$ghg^{-1} \cdot g(h^{-1})g^{-1} = gh(h^{-1})g^{-1} \cdot g^{-1} = gg^{-1} = e \implies g(h^{-1})g = x^{-1} \in gHg^{-1} \tag{29}$$

□

Teorema 16. *Para todo grupo $G = \{X, \cdot\}$ con un subgrupo $H \subset G$:*

$$gHg^{-1} = H \quad g \in G \iff xH = Hx \tag{30}$$

Demostración. $\implies$

$$gHg^{-1} = H \iff gHg^{-1} \cdot g = Hg \iff gH = Hg \quad h \in G \tag{31}$$

□

Demostración. $\impliedby$

$$xH = Hx \implies xH \cdot x^{-1} = Hx \cdot x^{-1} \iff xHx^{-1} = H \quad x \in G \tag{32}$$

□

Teorema 17. *Las clases laterales izquierdas x_iH de un subgrupo H normal, forman un grupo.*

Demostración. Las clases laterales izquierdas de un subgrupo H cumplen con las tres propiedades de los grupos:

1. La operación no se sale del conjunto y por tanto conserva la propiedad asociativa:

$$xH = Hx \implies \forall a \in xH : xH \cdot yH = xyHH = xyH \implies ab \in xyH \tag{33}$$

2. El neutro pertenece a la clase lateral izquierda eH.
3. Todo elemento $a \in xH$ tiene inverso $a^{-1} \in (x^{-1})H$:

$$\forall a = xh_1 \in xH \; \exists a^{-1} = (x^{-1})h_2 \in (x^{-1})H : h_1x \cdot (x^{-1})h_2 = h_1h_2 \in eH \quad h_1, h_2 \in H \tag{34}$$

□

Teorema 18. *El conmutador es un subgrupo y es normal*

Demostración. El conmutador $G' = \{< [a, b] >: a, b \in G\}$ es un subgrupo.

1. Como estamos operando elementos de G con la misma operación, se seguirá conservando la propiedad asociativa.
2. El elemento neutro $[a, e] = e$ pertenece a C:

$$[a, e] = a \cdot e \cdot a^{-1} \cdot e^{-1} = a \cdot e \cdot a^{-1} \cdot e = a \cdot a^{-1} = e \implies e \in C \quad a, b \in G \tag{35}$$

3. Todo elemento $x = [a, b]$ tiene inverso $x^{-1} = [b, a]$

$$\begin{aligned} &\forall x = [a, b] = aba^{-1}b^{-1} \in C \exists x^{-1} = [b, a] = bab^{-1}a^{-1} \in C : x \cdot x^{-1} = \\ &aba^{-1}b^{-1} \cdot bab^{-1}a^{-1} = aba^{-1}ab^{-1}a^{-1} = abb^{-1}a^{-1} = aa^{-1} = e \end{aligned} \tag{36}$$

□

Demostración. El conmutador $C =< [a, b] >$ es un subgrupo normal.

$$\forall h \in G' : aha^{-1} = aha^{-1}h^{-1}h = [a, h] \cdot h \in G' \implies g(G')g = G' \tag{37}$$

□