# UN BREVE PANORAMA DE LA TEORÍA DE GRUPOS

DANIEL LABARDINI-FRAGOSO

Abstract. Estas notas acompañan al curso *Breve panorama de la teoría de grupos*, impartido por quien esto escribe en la *Escuela de Matemáticas de América Latina y el Caribe* (EMALCA) en Arica, Chile. El curso tuvo como propósito principal exponer brevemente los conceptos y resultados que suelen formar parte de los cursos básicos de álgebra de diversos programas de licenciatura y maestría en matemáticas.

Contents



## 1. Teoría de grupos

### 1.1. Definición, ejemplos y propiedades básicas.

**Lema 1.1.** *Sean $G$ un conjunto y $\cdot : G \times G \to G$ cualquier función. A lo más un elemento $e$ de $G$ satisface que $e \cdot g = g = g \cdot e$ para todo $g \in G$.*

*Proof.* Tomemos dos elementos $e_1, e_2 \in G$ y supongamos que $e_1 \cdot g = g = g \cdot e_1$ y $e_2 \cdot g = g = g \cdot e_2$ para todo $g \in G$. Entonces $e_1 = e_1 \cdot e_2 = e_2$. □

**Definición 1.2.** Un **grupo** es una pareja $(G, \cdot)$ consistente de un conjunto $G$ y una función $\cdot : G \times G \to G$ que satisfacen:

(1) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ para cualesquiera $a, b, c \in G$ (es decir, $\cdot$ es *asociativa*);
(2) existe $e \in G$ tal que $e \cdot g = g = g \cdot e$ para todo $g \in G$ (por el lema anterior, un tal $e$ es único);
(3) para todo $g \in G$ existe $h \in G$ tal que $g \cdot h = e = h \cdot g$.

Si $(G, \cdot)$ es un grupo con la propiedad de que $g \cdot h = h \cdot g$ para todo par de elementos $g, h \in G$, diremos que $(G, \cdot)$ es un **grupo abeliano** o **conmutativo**.

*Date*: October 17, 2016.

**Ejemplo 1.3.** Son ejemplos de grupos los siguientes:

(1) $(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{R},+)$, $(\mathbb{C},+)$;
(2) $(\mathbb{Q}\setminus\{0\},\cdot)$, $(\mathbb{R}\setminus\{0\},\cdot)$, $(\mathbb{C}\setminus\{0\},\cdot)$;
(3) $(\mathbb{Z}/n\mathbb{Z},+)$ para cada número entero fijo $n$;
(4) $(\mathbb{U}_n,\cdot)$, donde, para cada número entero $n$ definimos $\mathbb{U}_n=\{X\in\mathbb{Z}/n\mathbb{Z}\mid \text{ existe } Y\in\mathbb{Z}/n\mathbb{Z} \text{ tal que } X\cdot Y=[1]_n\}$;
(5) $(S_n,\circ)$ para cada entero no negativo fijo $n$, donde $S_n=\{f:\{1,\dots,n\}\to\{1,\dots,n\}\mid f \text{ es una función biyectiva}\}$ y $\circ$ es la composición de funciones;
(6) $(\mathrm{GL}_n(K),\cdot)$ para cada entero positivo fijo $n$ y cada campo $K$, donde $\mathrm{GL}_n(K)=\{A\in K^{n\times n}\mid A \text{ es una matriz invertible}\}$ y $\cdot$ es la multiplicación de matrices;
(7) $(\mathrm{SL}_n(K),\cdot)$, donde $\mathrm{SL}_n(K)=\{A\in K^{n\times n}\mid \det(A)=1\}$ y $\cdot$ es la multiplicación de matrices.

**Lema 1.4.** *Sea $(G,\cdot)$ un grupo. Para cada $g\in G$ hay exactamente un elemento $h\in G$ tal que $g\cdot h=e=h\cdot g$.*

*Proof.* Supongamos que $h_1$ y $h_2$ son elementos de $G$ que satisfacen $g\cdot h_1=e=h_1\cdot g$ y $g\cdot h_2=e=h_2\cdot g$. Entonces $h_1=h_1\cdot e=h_1\cdot(g\cdot h_2)=(h_1\cdot g)\cdot h_2=e\cdot h_2=h_2$. □

**Definición 1.5.** Sean $(G,\cdot)$ un grupo y $g\in G$.

(1) El elemento $h\in G$ tal que $g\cdot h=e=h\cdot g$ recibirá el nombre de **inverso de** $g$ (en $G$ con respecto a $\cdot$) y será denotado por $g^{-1}$;
(2) para cada $n\in\mathbb{Z}$ definimos la **$n$-ésima potencia de** $g$ como el elemento $g^n$ de $G$ dado por

$$g^n=\begin{cases}\underbrace{g\cdot\ldots\cdot g}_{n \text{ veces}} & \text{si } n>0;\\ e & \text{si } n=0;\\ \underbrace{g^{-1}\cdot\ldots\cdot g^{-1}}_{-n \text{ veces}} & \text{si } n<0.\end{cases}$$

**Lema 1.6.** *Sean $(G,\cdot)$ un grupo y $g,h\in G$.*

*(1) Las funciones $\lambda_g:G\to G$ y $\rho_g:G\to G$ dadas por las reglas $\lambda_g(x)=gx$ y $\rho_g(x)=xg$ son biyectivas.*
*(2) $(g\cdot h)^{-1}=h^{-1}\cdot g^{-1}$;*
*(3) $g^2=g\implies g=e$.*

*Proof.* EJERCICIO. □

**Nota 1.7.** Siguiendo un abuso notacional y de lenguaje muy común, cuando tengamos un grupo con conjunto subyacente $G$ frecuentemente diremos que $G$ es un grupo, haciendo referencia tácita a la operación que lo hace grupo.

## 1.2. **Subgrupos.**

**Definición 1.8.** Sean $(G,\cdot)$ un grupo y $H$ un subconjunto de $G$. Diremos que $H$ *es un subgrupo de* $G$ (con respecto a la operación $\cdot$), y escribiremos $H\leq G$, si $H$ es grupo bajo (la restricción a $H\times H$ de) la operación $\cdot$, es decir, si las siguientes condiciones son satisfechas simultáneamente:

(1) Para cualesquiera elementos $a,b\in H$, el producto $a\cdot b$ es un elemento de $H$;
(2) existe un elemento $e_H\in H$ tal que $e_H\cdot h=h=h\cdot e_H$ para todo $h\in H$;
(3) para todo $h\in H$ existe $h'\in H$ con la propiedad de que $h\cdot h'=e_H=h'\cdot h$.

**Nota 1.9.** Si $(G,\cdot)$ es un grupo y $H$ es un subconjunto de $G$, la asociatividad de la restricción de $\cdot$ a $H\times H$ es obvia.

**Lema 1.10.** *Si $H$ es un subgrupo de $G$, entonces*

*(1) el elemento neutro de $G$ pertenece a $H$ y coincide con el elemento neutro de $H$;*

*(2) para todo $h \in H$, el inverso de $h$ en $H$ coincide con el inverso de $h$ en $G$.*

*Proof.* (1) Sean $e_H$ el elemento neutro de $H$, $e_G$ el elemento neutro de $G$ y $e_H^{-1}$ el inverso de $e_H$ en $G$. Calculemos: $e_H = e_G e_H = (e_H^{-1} e_H) e_H = e_H^{-1}(e_H e_H) = e_H^{-1} e_H = e_G$,

(2) Sabemos que $e_H = e_G$, lo que implica que el inverso en $H$ de un elemento $h \in H$ cualquiera es necesariamente un inverso de $h$ en $G$, de manera que la afirmación es consecuencia de la unicidad de inversos en $G$.

□

**Lema 1.11.** *Sean $G$ un grupo y $H$ un subconjunto de $G$. Las siguientes afirmaciones son equivalentes:*

*(1) $H$ es un subgrupo de $G$;*

*(2) $H$ posee las siguientes tres propiedades:*

*(a) el producto de cualesquiera dos elementos de $H$ pertenece a $H$;*

*(b) el elemento neutro de $G$ pertenece a $H$;*

*(c) para todo $h \in H$, el inverso de $h$ pertenece a $H$.*

*(3) $H$ satisface que:*

*(a) $H \neq \varnothing$;*

*(b) para todo par de elementos $a, b \in H$, el producto $ab^{-1}$ pertenece a $H$.*

*Proof.* EJERCICIO. □

1.3. **Subgrupo generado por un subconjunto, subgrupos cíclicos.**

**Definición 1.12.** Sean $G$ un grupo, $S$ un subconjunto de $G$ y $H$ un subgrupo de $G$. Diremos que $H$ **es el subgrupo de $G$ generado por** $S$, y escribiremos $H = \langle S \rangle$, si $H$ satisface las siguientes dos condiciones:

(1) $S \subseteq H$;

(2) $\forall K \leq G \ (S \subseteq K \implies H \subseteq K)$.

Resulta obvio que para cada subconjunto $S$ de $G$ hay a lo más un subgrupo de $G$ que satisface las condiciones de la Definición 1.12.

**Lema 1.13.** *Sean $G$ un grupo y $\mathcal{F}$ una colección no vacía de subgrupos de $G$. La intersección $\bigcap \mathcal{F} = \bigcap_{H \in \mathcal{F}} H$ es un subgrupo de $G$.*

*Proof.* EJERCICIO. □

**Corolario 1.14.** *Si $G$ es un grupo y $S$ es un subconjunto de $G$, entonces el subgrupo de $G$ generado por $S$ existe.*

*Proof.* Para un subconjunto $S \subseteq G$ definamos $\mathcal{F}_S = \{H \mid H \text{ es subgrupo de } G \text{ y } S \subseteq H\}$. Resulta obvio que $\mathcal{F}_S$ es una colección no vacía de subgrupos de $G$, y que $\bigcap \mathcal{F}_S$ es el subgrupo de $G$ generado por $S$. □

**Lema 1.15.** *Sea $G$ un grupo. Para cada subconjunto $S$ de $G$ se tiene la igualdad*

$$\langle S \rangle = \{x_1 \cdots x_m \mid m \in \mathbb{Z}_{>0} \text{ y } x_1, \ldots, x_m \in S'\},$$

*donde $S' = S \cup \{s^{-1} \mid s \in S\} \cup \{e\}$.*

*Proof.* EJERCICIO. □

En particular, si $S$ tiene exactamente un elemento, digamos que $S = \{a\}$, entonces $\langle S \rangle = \{a^m \mid m \in \mathbb{Z}\}$, subgrupo al que también denotaremos $\langle a \rangle$.

**Definición 1.16.** Un grupo $G$ es **cíclico** si existe un elemento $a \in G$ tal que $G = \langle \{a\} \rangle$.

**Definición 1.17.** Sea $G$ un grupo. El **orden de** $G$ es la cardinalidad de $G$. El **orden de un elemento** $g \in G$ es el orden del subgrupo de $G$ generado por $g$.

**Lema 1.18.** *(1) Para cada $n \in \mathbb{Z}_{>0}$ existe un grupo de orden $n$;*

*(2) todo subgrupo de un grupo cíclico es cíclico.*

*Proof.* EJERCICIO. □

**Lema 1.19.** *Sean $G$ un grupo, $g$ un elemento de $G$ y $n$ un entero positivo. Las siguientes afirmaciones son equivalentes:*

*(1) $n$ es el orden de $g$;*
*(2) $n = \min\{m \in \mathbb{Z}_{>0} \mid g^m = e\}$;*
*(3) $g^n = e$ y $n$ divide a todo entero $m$ que tenga la propiedad de que $g^m = e$.*

*Proof.* Supongamos que $n$ es el orden de $g$. Por definición, esto significa que $|\langle g\rangle| = n \in \mathbb{Z}_{>0}$, lo que en particular nos dice que $\langle g\rangle$ es un grupo finito. Así, el conjunto $\{g^m \mid m \in \mathbb{Z}_{>0}\}$ es necesariamente finito. Por lo tanto, existen enteros positivos distintos $m_1$ y $m_2$ tales que $g^{m_1} = gm_2$, de donde deducimos que existe un entero positivo $s$ tal que $g^s = e$. Sea $s_0$ el elemento mínimo del conjunto $\{s \in \mathbb{Z}_{>0} \mid g^s = e\}$. Para cualquier $m \in \mathbb{Z}$ existen $q, r \in \mathbb{Z}$ tales que $0 \leq r < s_0$ y $m = qs_0 + r$, y así, $g^m = g^{qs_0+r} = (g^s)^q g^r = g^r$. Esto significa que $\langle g\rangle = \{g^r \mid 0 \leq r < s_0\}$, lo que implica que $n \leq s_0$. Pero si $r_1, r_2 \in \{0, \ldots, s_0 - 1\}$ satisfacen $g^{r_1} = g^{r_2}$, entonces $|r_1 - r_2|$ es un entero no negativo menor que $s_0$ y satisface $g^{|r_1-r_2|} = e$, y la minimalidad de $s_0$ implica entonces que $|r_1 - r_2| = 0$. Por lo tanto, $n = s_0$.

Supongamos ahora que $n = \min\{m \in \mathbb{Z}_{>0} \mid g^m = e\}$. Es obvio que entonces $g^n = e$. Sea $m$ cualquier entero que satisfaga $g^m = e$, y tomemos enteros $q$ y $r$ tales que $0 \leq r < n$ y $m = nq + r$. Entonces $e = g^m = g^r$, lo que implica que $r = 0$ dada la hípotesis sobre $n$.

Finalmente, supongamos que $g^n = e$ y que $n$ divide a todo entero $m$ que tenga la propiedad de que $g^m = e$. Entonces $|\{g^r \mid 0 \leq r < n\}| = n$, pues ningún elemento de $\{1, \ldots, n-1\}$ es divisible entre $n$. Dado que $g^n = e$, es claro que $\{g^r \mid 0 \leq r < n\}$ es un subgrupo de $G$. Así, $\{g^r \mid 0 \leq r < n\} = \langle g\rangle$. □

## 1.4. **Clases laterales izquierdas y derechas.**

**Definición 1.20.** Sean $G$ un grupo, $H$ un subgrupo de $G$ y $a, b \in G$.

(1) Diremos que $a$ **es congruente con** $b$ **por la izquierda módulo** $H$, y escribiremos $a \equiv^i_H b$, si $a^{-1}b \in H$;
(2) diremos que $a$ **es congruente con** $b$ **por la derecha módulo** $H$, y escribiremos $a \equiv^d_H$, si $ab^{-1} \in H$.

**Lema 1.21.** *Sean $G$ un grupo y $H$ un subgrupo de $G$.*

*(1) $\equiv^i_H$ y $\equiv^d_H$ son relaciones de equivalencia para $G$;*
*(2) para cada $g \in G$ se tiene $[g]^i_H = gH$ y $[g]^d_H = Hg$.*
*(3) para cada $g \in G$ hay biyecciones $H \to [g]^i_H$ y $H \to [g]^d_H$.*

*Proof.* EJERCICIO. □

**Corolario 1.22** (Teorema de Lagrange)**.** *Sea $G$ un grupo finito.*

*(1) Si $H$ es un subgrupo de $G$, entonces $|H|$ divide a $|G|$;*
*(2) todo $g \in G$ satisface $g^{|G|} = e$.*

## 1.5. **Subgrupos normales.**

**Pregunta 1.23.** *¿Cuándo sucede que $\equiv^i_H = \equiv^d_H$?*

Es un sencillo ejercicio verificar que para $g \in G$ se cumple que $gH = Hg$ si y sólo si $gHg^{-1} = H$. Puesto que $gH = [g]^i_H$ y $Hg = [g]^d_H$, vemos que $\equiv^i_H = \equiv^d_H$ si y sólo si para todo $g \in G$ se satisface que $gHg^{-1} = H$.

**Definición 1.24.** Sean $G$ un grupo y $H$ un subgrupo de $G$. Diremos que $H$ es un **subgrupo normal** de $G$, y escribiremos $H \trianglelefteq G$, si todo elemento $g \in G$ tiene la propiedad de que $gHg^{-1} = H$.

Por el ejercicio **??**, un subgrupo $H$ de un grupo $G$ es normal en $G$ si y sólo si para todo $g \in G$ y todo $h \in H$ se tiene $ghg^{-1} \in H$.

Supongamos que $H$ es un subgrupo normal de un grupo $G$. Entonces la congruencia izquierda módulo $H$ y la congruencia derecha módulo $H$ son la misma relación de equivalencia para $G$. Escribiremos $\equiv_H = \equiv^i_H = \equiv^d_H$, y denotaremos por $G/H$ la partición de $G$ inducida por esta relación. Así, los elementos de $G/H$ son las clases de equivalencia de la relación de equivalencia $\equiv_H$. Para $X, Y \in G/H$ y $x_1, x_2 \in X$, $y_1, y_2 \in Y$, siempre se tiene $x_1^{-1}x_2, y_1^{-1}y_2 \in H$, y la normalidad de $H$ implica que $y_1^{-1}x_1^{-1}x_2y_1 \in H$. Así,

$$(x_1y_1)^{-1}(x_2y_2) = y_1^{-1}x_1^{-1}x_2y_2 = (y_1^{-1}x_1^{-1}x_2y_1)(y_1^{-1}y_2) \in H,$$

es decir, $x_1y_1 \equiv_H x_2y_2$. Con la ayuda del axioma de elección, esto significa que tenemos una función bien definida $G/H \times G/H \to G/H$ dada por la regla $(X, Y) \mapsto Z_{XY}$, donde $Z_{XY} = [xy]_H$ para cualesquiera elementos $x \in X$, $y \in Y$. ¿Será $G/H$ grupo bajo esta operación?

Obsérvese que, por definición, para $x, y \in G$ se tiene $[x]_H[y]_H = [xy]_H$, de manera que

(1) La operación $G/H \times G/H \to G/H$ que hemos definido es trivialmente asociativa;
(2) hay un neutro, a saber, la clase $[e]_H$;
(3) para cada $g \in G$ se tiene $[g]_H[g^{-1}]_H = [e]_H$.

Así, vemos que $G/H$ es, en efecto, un grupo, en el que el producto de dos clases de equivalencia es, por definición, la clase de equivalencia del producto de cualesquiera representantes de las clases de equivalencia dadas.

### 1.6. **Homomorfismos.**

**Definición 1.25.** Sean $G$ y $H$ grupos. Un **homomorfismo de grupos de $G$ a $H$** es una función $\varphi : G \to H$ que satisface $\varphi(xy) = \varphi(x)\varphi(y)$ para todo par de elementos $x, y \in G$.

**Ejemplo 1.26.**
(1) Si $G$ es un grupo y $H$ es un subgrupo normal de $G$, entonces la función $[\bullet]_H : G \to G/H$ dada por $g \mapsto [g]_H$ es un homomorfismo de grupos de $G$ a $G/H$.
(2) Si $H$ es un subgrupo de un grupo $G$, entonces la función inclusión $\iota : H \to G$ es un homomorfismo de grupos.
(3) Para cada número entero fijo $n$, la función $\mu_n : \mathbb{Z} \to \mathbb{Z}$ dada por $\mu_n(m) = nm$, es un homomorfismo de grupos.
(4) Dado cualquier elemento $g$ de un grupo $G$, la función $\mathbb{Z} \to G$ dada por $m \mapsto g^m$ es un homomorfismo de grupos.
(5) La función $\mathbb{R} \to \mathbb{R}_{>0}$ dada por $x \mapsto e^x$ es un homomorfismo de grupos.
(6) La función $\mathbb{R}_{>0} \to \mathbb{R}$ dada por $x \mapsto \log(x)$ es un homomorfismo de grupos.

**Lema 1.27.** *Supongamos que $\varphi : G \to H$ es un homomorfismo de grupos. Entonces:*
*(1) $\varphi(e_G) = e_H$;*
*(2) $\varphi(g^{-1}) = (\varphi(g))^{-1}$ para todo $g \in G$.*

**Definición 1.28.** Si $\varphi : G \to H$ es un homomorfismo de grupos,
(1) se define el **núcleo** o **kernel** de $\varphi$ como el conjunto $\mathrm{Nuc}(\varphi) = \{g \in G \mid \varphi(g) = e\} \subseteq G$;
(2) se define la **imagen** de $\varphi$ como el conjunto $\mathrm{Im}(\varphi) = \{\varphi(g) \mid g \in G\} = \{h \in H \mid \exists g \in G \text{ tal que } \varphi(g) = h\} \subseteq H$.

**Lema 1.29.** *Si $\varphi : G \to H$ es un homomorfismo de grupos, entonces*
*(1) $\mathrm{Nuc}(\varphi)$ es un subgrupo normal de $G$;*
*(2) $\mathrm{Im}(\varphi)$ es un subgrupo de $H$;*
*(3) $\varphi$ es una función inyectiva si y sólo si $\mathrm{Nuc}(\varphi) = \{e\}$.*

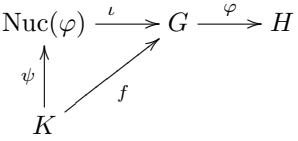
**Teorema 1.30.** *Supongamos que $\varphi : G \to H$ es un homomorfismo de grupos. Entonces para todo $g \in G$ se tiene $g\,\mathrm{Nuc}(\varphi) = \varphi^{-1}(\varphi(g))$. Consecuentemente, la función $\overline{\varphi} : G/\mathrm{Nuc}(\varphi) \to H$ dada por $\overline{\varphi}([g]_{\mathrm{Nuc}(\varphi)}) =$*

*$\varphi(g)$ está bien definida y es inyectiva. Correstringiendo el dominio de $\overline{\varphi}$ obtenemos un homomorfismo biyectivo de grupos $G/\operatorname{Nuc}(\varphi) \to \operatorname{Im}(\varphi)$.*

*Proof.* □

**Teorema 1.31.** *El núcleo de un homomorfismo de grupos $\varphi : G \to H$ posee la siguiente **propiedad universal**: Sea $\iota : \operatorname{Nuc}(\varphi) \to G$ la función inclusión. Entonces:*

1. *$\varphi \circ \iota$ es la función constante con valor $e_H$;*
2. *para cada homomorfismo de grupos $f : K \to G$ tal que la composición $\varphi \circ f : K \to G$ es la función constante con valor $e_H$, existe un único homomorfismo de grupos $\psi : K \to \operatorname{Nuc}(\varphi)$ tal que $f = \iota \circ \psi$.*




*Proof.* □

**Definición 1.32.** Sea $\varphi : G \to H$ un homomorfismo de grupos. Diremos que:

1. $\varphi$ es un **isomorfismo** si existe un homomorfismo de grupos $\psi : H \to G$ tal que $\psi \circ \varphi = \mathbf{1}_G$ y $\varphi \circ \psi = \mathbf{1}_H$;
2. $\varphi$ es un **monomorfismo** si para todo par de homomorfismos de grupos $f, g : K \to G$ se cumple la implicación $\varphi \circ f = \varphi \circ g \implies f = g$;
3. $\varphi$ es un **epimorfismo** si para todo par de homomorfismos de grupos $f, g : K \to G$ se cumple la implicación $f \circ \varphi = g \circ \varphi \implies f = g$;
4. $\varphi$ es un **endomorfismo** de $G$ si $G = H$;
5. $\varphi$ es un **automorfismo** de $G$ si $G = H$ y $\varphi$ es un isomorfismo.

## 1.7. **Acciones de grupos.**

**Definición 1.33.** Sean $G$ un grupo y $X$ un conjunto. Una **acción** de $G$ en $X$ es una función $\cdot : G \times X \to X$ que satisface:

1. $e \cdot x = x$ para todo $x \in X$;
2. $(gh) \cdot x = g \cdot (h \cdot x)$ para todo $x \in X$ y todo par de elementos $g, h \in G$.

**Lema 1.34.** *Denotemos $\operatorname{Acc}_G(X) = \{\bullet \mid \bullet \text{ es una acción de } G \text{ en } X\}$. Las asignaciones*

$$\varphi \mapsto \begin{bmatrix} (g,x) \\ \downarrow \\ (\varphi(g))(x) \end{bmatrix} \quad y \quad \bullet \mapsto \begin{bmatrix} g \\ \downarrow \\ [x \mapsto g \bullet x] \end{bmatrix}$$

*son biyecciones mutuamente inversas $\operatorname{Hom}(G, S_X) \rightleftarrows \operatorname{Acc}_G(X)$.*

**Ejemplo 1.35.** La función $\cdot : \mathrm{GL}_2(\mathbb{C}) \times \overline{\mathbb{C}} \to \overline{\mathbb{C}}$ dada por $A \cdot z = m_A(z)$ es una acción de $\mathrm{GL}_2(\mathbb{C})$ en $\overline{\mathbb{C}}$ (**EJERCICIO**). Así, $\mathrm{GL}_2(\mathbb{C})$ actúa en $\overline{\mathbb{C}}$ por **transformaciones de Mbius**.

**Definición 1.36.** Supongamos que $\cdot : G \times X \to X$ es una acción del grupo $G$ en el conjunto $X$.

1. Para cada $x \in X$ definimos la **órbita** de $x$ bajo $\cdot$ (o bajo $G$) como $G \cdot x = \{g \cdot x \mid g \in G\} = \{y \in X \mid \exists g \in G \text{ tal que } g \cdot x = y\}$;
2. para cada $x \in X$ definimos el **estabilizador** de $x$ como $G_x = \{g \in G \mid g \cdot x = x\}$;
3. para cada $g \in G$ definimos el **conjunto fijo** de $g$ como $\operatorname{Fij}_X(g) = \{x \in X \mid g \cdot x = x\}$;
4. definimos el **conjunto fijo de la acción** como $\operatorname{Fij}_X(G) = \bigcap_{g \in G} \operatorname{Fij}_X(g)$.

**Lema 1.37.** *Supongamos que $\cdot : G \times X \to X$ es una acción del grupo $G$ en el conjunto $X$.*

1. *El conjunto $\{G \cdot x \mid x \in X\}$ es una partición de $X$;*

*(2) para cada $x \in X$, el estabilizador $G_x$ es un subgrupo de $G$.*

**Definición 1.38.** Supongamos que $\cdot : G \times X \to X$ es una acción del grupo $G$ en el conjunto $X$. Diremos que la acción $\cdot$ es:

(1) **libre de puntos fijos** si $\mathrm{Fij}_X(g) = \varnothing$ para todo $g \in G \setminus \{e\}$; equivalentemente, si $G_x = \{e\}$ para todo $x \in X$;
(2) **fiel** si $\bigcap_{x \in X} G_x = \{e\}$; esto es, si sólo el elemento neutro $e$ tiene la propiedad de simultáneamente dejar fijos a todos los elementos de $X$;
(3) **transitiva** si existe $x \in X$ tal que $G \cdot x = X$.

**Proposición 1.39.** *Supongamos que $\cdot : G \times X \to X$ es una acción del grupo $G$ en el conjunto $X$. Sean $x$ y $y$ elementos de $X$ que yacen en la misma órbita de la acción. Los elementos de $G$ que llevan $x$ en $y$ son precisamente los elementos de alguna clase lateral izquierda de $G_x$ en $G$. Consecuentemente, $|G \cdot x| = [G : G_x]$.*

*Proof.* Consideremos la función $f : G \to G \cdot x$ dada por $f(g) = g \cdot x$. Resulta claro que $f^{-1}(y)$, la imagen inversa de $y$ bajo $f$, es el conjunto cuyos elementos son precisamente los elementos de $G$ que llevan $x$ en $y$. Fijemos un elemento $g_0 \in G$ tal que $g_0 \cdot x = y$ (elemento que existe, pues las órbitas de $x$ y de $y$ coinciden). Es obvio que $g_0 G_x \subseteq f^{-1}(y)$. Si $g \in f^{-1}(y)$, entonces $g \cdot x = g_0 \cdot x$, es decir, $g_0^{-1} g \in G_x$, lo que significa que $g \in g_0 G_x$. Así, $f^{-1}(y) = g_0 G_x$.

Vemos que para cualesquiera dos elementos $y_1, y_2 \in G.x$ se cumple que $|f^{-1}(y_1)| = |G_x| = |f^{-1}(y_2)|$, de donde se deduce fácilmente que $|G \cdot x| = [G : G_x]$. □

**Ejemplo 1.40** (Conjugación)**.** Sea $G$ un grupo. Definamos una función $\star : G \times G \to G$ mediante la regla $g \star x = gxg^{-1}$. Es un **EJERCICIO** verificar que $\star$ es una acción de $G$ en el conjunto $G$. La órbita de un elemento $x \in G$ bajo esta acción recibe el nombre de **clase de conjugación** de $x$, mientras que el estabilizador $C_G(x) := G_x$ de $x$ es usualmente llamado **centralizador** de $x$. Obérvese que $C_G(x)$ consiste de todos los elementos de $G$ que conmutan con $x$.

Supongamos que $X$ es un $G$-conjunto finito, que $\mathcal{O}_1, \ldots, \mathcal{O}_r$ son las órbitas que tienen más de un elemento, y que $x_1 \in \mathcal{O}_1, \ldots, x_r \in \mathcal{O}_r$. Entonces

$$|X| = |\,\mathrm{Fij}_X(G)| + \sum_{i=1}^{r} |\mathcal{O}_i| = |\,\mathrm{Fij}_X(G)| + \sum_{i=1}^{r} [G : G_{x_i}]. \tag{1.1}$$

Aplicando esta ecuación a la situación en la que $X = G$ y $G$ actúa por conjugación, obtenemos:

**Teorema 1.41** (Ecuación de clase)**.** *Sea $\Delta$ el conjunto de clases de conjugación de $G$ (es decir, la partición de $G$ cuyos elementos son las órbitas de la acción $\star$ del Ejemplo 1.40), y sea $\Delta' = \{D \in \Delta \mid |D| > 1\}$ el conjunto consistente de las clases de conjugación que tienen más de un elemento. Para cada elemento $D$ de $\Delta$ fijemos un elemento $g_D \in D$. Si $G$ es finito, entonces*

$$|G| = \sum_{D \in \Delta} [G : C_G(g_D)] = |Z(G)| + \sum_{D \in \Delta'} [G : C_G(g_D)],$$

*donde $Z(G) = \{g \in G \mid gh = hg \ \forall h \in G\}$ es el **centro** de $G$.*

*Proof.* EJERCICIO. □

**Corolario 1.42.** *Sea $p$ un número primo positivo y $n$ un entero positivo. Si $G$ es un grupo de orden $p^n$, entonces $|Z(G)| > 1$.*

*Proof.* EJERCICIO. □

**Corolario 1.43.** *Si $p$ es un número primo positivo, entonces todo grupo de orden $p^2$ es abeliano.*

*Proof.* Supongamos que $p$ es un número primo positivo y que $G$ es un grupo de orden $p^2$. Por el corolario anterior, la cardinalidad del centro de $G$ es $p$ o $p^2$. En búsqueda de una contradicción, supongamos que $|Z(G)| = p$ y tomemos $a \in G \setminus Z(G)$. Entonces $Z(G) \cup \{a\} \subseteq C_G(a)$, lo que implica que $C_G(a) = G$. Así, $a \in Z(G)$ y hemos arribado a una contradicción. Por lo tanto, $|Z(G)| = p^2$, es decir $G$ es abeliano. □

**Teorema 1.44** (Burnside)**.** *Sean $G$ un grupo finito y $X$ un $G$-conjunto finito. Si $r$ es el número de órbitas de la acción de $G$ en $X$, entonces $r|G| = \sum_{g\in G} |\operatorname{Fij}_X(g)|$.*

*Proof.* Consideremos el conjunto $Y = \{(g, x) \in G \times X \mid g \cdot x = x\}$. Para cada $g \in G$ hay $|\operatorname{Fij}_X(g)|$ elementos de $Y$ que tienen a $g$ como primer miembro. Por lo tanto, $|Y| = \sum_{g\in G} |\operatorname{Fij}_X(g)|$.

Por otro lado, para cada $x \in X$ hay $|G_x|$ elementos de $Y$ que tienen a $x$ como segundo miembro. Por lo tanto, $|Y| = \sum_{x\in X} |G_x| = \sum_{x\in X} \frac{|G|}{|G\cdot x|} = |G| \sum_{x\in X} \frac{1}{|G\cdot x|} = |G| \sum_{\mathcal{O}\in X/G} \sum_{x\in\mathcal{O}} \frac{1}{|\mathcal{O}|} = |G| \sum_{\mathcal{O}\in X/G} 1 = |G|r$. □

1.8. **Teoremas de Cauchy y Sylow.**

**Proposición 1.45.** *Sean $p$ un número primo positivo y $G$ un grupo de $p^n$. Si $X$ es un $G$-conjunto finito, entonces $|X| \equiv_p |\operatorname{Fij}_X(G)|$.*

*Proof.* Esto es consecuencia directa de la ecuación (1.1). En efecto, si $\mathcal{O}_1, \ldots, \mathcal{O}_r$ son las órbitas que tienen más de un elemento, y si $x_1 \in \mathcal{O}_1, \ldots, x_r \in \mathcal{O}_r$, entonces

$$|X| = |\operatorname{Fij}_X(G)| + \sum_{i=1}^{r} [G : G_{x_i}]$$

y $p$ divide a $[G : G_{x_i}]$ para toda $i \in \{1, \ldots, r\}$. □

**Teorema 1.46** (Cauchy)**.** *Sean $G$ un grupo y $p$ un número primo positivo. Si $p$ divide al orden de $G$, entonces $G$ tiene un subgrupo de orden $p$.*

*Proof.* Hagamos que el grupo $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$ actue en $G^p$ mediante la regla

$$[n]_p \cdot (g_{[1]_p}, \ldots, g_{[p]_p}) := (g_{[n+1]_p}, \ldots, g_{[n+p]_p})$$

(es un EJERCICIO verificar que esta regla define, en efecto, una acción de $\mathbb{Z}_p$ en $G^p$). El conjunto $X = \{(g_{[1]_p}, \ldots, g_{[p]_p}) \mid g_{[1]_p} \ldots g_{[p]_p} = e\}$, cuya cardinalidad es claramente $|G|^{p-1}$ (EJERCICIO), es estable bajo esta acción (EJERCICIO), de manera que la misma regla define una acción de $\mathbb{Z}_p$ en $X$. Por la Proposición 1.45, $|G|^{p-1} = X \equiv_p |\operatorname{Fij}_{\mathbb{Z}_p}(X)|$, de manera que el número entero no negativo $|\operatorname{Fij}_{\mathbb{Z}_p}(X)|$ es un múltiplo de $p$. Como $(e, \ldots, e) \in \operatorname{Fij}_{\mathbb{Z}_p}(X)$, el conjunto $\operatorname{Fij}_{\mathbb{Z}_p}(X)$ es no vacío. Así, $|\operatorname{Fij}_{\mathbb{Z}_p}(X)|$ es un múltiplo positivo de $p$, de donde deducimos que $\operatorname{Fij}_{\mathbb{Z}_p}(X)$ tiene al menos un elemento $(g_{[1]_p}, \ldots, g_{[p]_p})$ que es diferente de $(e, \ldots, e)$. Este elemento satisface $g_{[1]_p} = g_{[2]_p} = \ldots = g_{[p]_p}$ y $g_{[1]_p} \ldots g_{[p]_p} = e$, hechos de los que deducimos que $g_{[1]_p}$ es un elemento de $G$ que tiene orden $p$. □

**Corolario 1.47.** *Sean $G$ un grupo finito y $p$ un número primo positivo. Si todos los elementos de $G$ tienen por orden alguna potencia de $p$, entonces el orden de $G$ es una potencia de $p$.*

*Proof.* EJERCICIO. □

**Definición 1.48.** Sea $p$ un número primo positivo. Si todos los elementos de un grupo $G$ tienen por orden algúna potencia de $p$, diremos que G es un **$p$-grupo**.

**Lema 1.49.** *Si $G$ es un grupo finito, $p$ es un número primo positivo y $H$ es un $p$-subgrupo de $G$, entonces:*

*(1) $[G : H] \equiv_p [N_G(H) : H]$;*
*(2) si $p|[G : H]$, entonces $H \neq N_G(H)$.*

*Proof.* Sea $L$ el conjunto cuyos elementos son las clases laterales izquierdas de $H$ en $G$. Por definición de índice se cumple que $|L| = [G : H]$. Consideremos la acción de $H$ en $L$ dada por la regla $h \cdot (xH) := (hx)H$, de manera que tenemos $|L| \equiv_p |\operatorname{Fij}_H(L)|$. Ahora bien, una clase lateral izquierda $xH$ pertenece a $\operatorname{Fij}_H(L)$

si y sólo si $hxH = xH$ para toda $h \in H$, es decir, si y sólo si $x^{-1}Hx = H$. En otras palabras, los elementos de $\mathrm{Fij}_H(L)$ son precisamente las clases laterales izquierdas contenidas en $N_G(H)$. El número de éstas es $[N_G(H) : H]$. Deducimos que $[G : H] \equiv_p [N_G(H) : H]$.

La segunda afirmación es consecuencia obvia de la primera, ya que $[N_G(H) : H]$ es un entero positivo. □

**Teorema 1.50** (Sylow)**.** *Sean $G$ un grupo finito y $p$ un número primo positivo. Escribamos $|G| = p^n m$ con $n, m \in \mathbb{Z}_{\geq 0}$ y $\mathrm{mcd}(p, m) = 1$*

*(1) Para cada $j \in \{0, \ldots, n\}$ existe un subgrupo de $G$ que tiene orden $p^j$;*
*(2) para cada subgrupo $H$ de $G$ que tenga orden $p^j$ con $0 \leq j < n$ existe un subgrupo $K$ de $G$ tal que $H \subseteq K$ y $|K| = p^{j+1}$;*
*(3) cualesquiera dos subgrupos de $G$ que tengan orden $p^n$ son conjugados;*
*(4) el número de subgrupos de $G$ que tienen orden $p^n$ es congruente con 1 módulo $p$ y divide a $|G|$.*

*Proof.* Claramente, la primera afirmación es consecuencia de la segunda. Probaremos la segunda afirmación por inducción sobre $j \in \{0, \ldots, n-1\}$. Si $0 < n$, entonces $p$ divide a $G$ y el teorema de Cauchy nos permite deducir que $G$ tiene un subgrupo de orden $p$, de donde vemos que el único subgrupo de $G$ que tiene orden $p^0$ está, en efecto, contenido en un subgrupo de orden $p^{0+1}$. Supongamos, pues, que $j \in \{0, \ldots, n-1\}$, y que $H$ es un subgrupo de $G$ que tiene orden $p^j$. Entonces $p|[G : H]$, por lo que $H$ está contenido propiamente en su normalizador $N_G(H)$ por el Lema 1.49. Por el mismo lema, $p$ divide al orden del grupo cociente $N_G(H)/H$, por lo que el teorema de Cauchy implica que $N_G(H)/H$ tiene un subgrupo de orden $p$. Dicho subgrupo es de la forma $K/H$ para algún subgrupo $K$ de $N_G(H)$ que contiene a $H$. Como $K/H$ tiene orden $p$, el orden de $K$ es necesariamente $p^{j+1}$.

Para probar la tercera afirmación, tomemos dos subgrupos $H$ y $K$ de $G$ y supongamos que $|H| = p^n = |K|$. Definamos $X$ como el conjunto cuyos elementos son precisamente los subgrupos de $G$ que son conjugados de $K$ en $G$. Consideremos la acción de $H$ en $X$ por conjugación, que satisface

$$|X| \equiv_p |\mathrm{Fij}_H(X)|.$$

De la igualdad $|X| = [G : N_G(K)]$ deducimos que $p$ no divide a $|X|$, de manera que $p$ tampoco divide a $|\mathrm{Fij}_H(X)|$, de donde deducimos que $\mathrm{Fij}_H(X) \neq \varnothing$. Tomemos un elemento de $\mathrm{Fij}_H(X)$, digamos $T$. Entonces existe $g \in G$ tal que $T = gKg^{-1}$, y todo $h \in H$ satisface $hTh^{-1} = T$. Así, para todo $h \in H$ se cumple que $hgKg^{-1}h^{-1} = gKg^{-1}$, es decir, que $g^{-1}hgKg^{-1}h^{-1}g = K$. Deducimos que $g^{-1}Hg \subseteq N_G(K)$. Como $p$ no divide a $[G : K]$, vemos que $p$ no divide a $[N_G(K) : K]$, de donde deducimos que $g^{-1}Hg \subseteq K$. El hecho de que $g^{-1}Hg$ y $K$ son conjuntos finitos con el mismo número de elementos implica ahora que $g^{-1}Hg = K$.

Definamos $\mathcal{P} := \{K \mid K \text{ es subgrupo de } G \text{ y } |K| = p^n\}$ y tomemos un elemento $H \in \mathcal{P}$. Haciendo actuar $H$ en $\mathcal{P}$ por conjugación obtenemos $|\mathcal{P}| \equiv_p |\mathrm{Fij}_{\mathcal{P}}(H)|$. Ahora bien, un elemento $K$ de $\mathcal{P}$ pertenece a $\mathrm{Fij}_{\mathcal{P}}(H)$ si y sólo si $hKh^{-1} = K$ para toda $h \in H$, es decir, si y sólo si $H \subseteq N_G(K)$, lo que sucede si y sólo si $H = K$. Esto prueba que $|\mathrm{Fij}_{\mathcal{P}}(H)| = 1$. Así, $|\mathcal{P}| \equiv_p 1$. Por otro lado, como gracias al párrafo previo la acción de $G$ en $\mathcal{P}$ por conjugación es transitiva, $|\mathcal{P}|$ es igual al índice $[G : N_G(H)]$ y por lo tanto divide a $|G|$. □

## 1.9. **Estructura de los grupos abelianos finitamente generados.**

**Teorema 1.51.** *Si $G$ es un grupo abeliano finitamente generado, entonces existen enteros no negativos $r, s_1, \ldots, s_m$ tales que $G$ es isomorfo al grupo $\mathbb{Z}^r \oplus \mathbb{Z}_{s_1} \oplus \ldots \oplus \mathbb{Z}_{s_m}$.*

## 1.10. **Ejercicios.**

(1) Sea $X$ un conjunto finito. ¿Cuántas funciones hay de $X \times X$ a $X$?
(2) Da un ejemplo de un conjunto $G$ y una función $\cdot : G \times G \to G$ que satisfagan las siguientes propiedades de manera simulánea:
   (a) $\cdot$ es asociativa;
   (b) existe $e \in G$ tal que $e \cdot g = g$ para todo $g \in G$;

(c) para todo $g \in G$ existen $e \in G$ y $h \in G$ tales que $e \cdot x = x$ para todo $x \in G$ y $h \cdot g = e$ (en símbolos: $\forall g \in G\ [\exists (e, h) \in G \times G\ (\forall x \in G\ (e \cdot x = x))\ \wedge\ (h \cdot g = e)]$);
(d) $G$ no es grupo bajo $\cdot$.

(3) Sean $G$ un conjunto y $\cdot : G \times G \to G$ una función que satisfacen:
(a) $\cdot$ es asociativa;
(b) existe $e \in G$ tal que $e \cdot g = g$ para todo $g \in G$;
(c) para todo $g \in G$ y todo $e \in G$ tal que $e \cdot x = x$ para todo $x \in G$, existe $h \in G$ con la propiedad de que $h \cdot g = e$ (en símbolos: $\forall g \in G\ \forall e \in G\ [\forall x \in G\ (e \cdot x = x)\ \implies \exists h \in G\ (h \cdot g = e)]$).
Demuestra que $(G, \cdot)$ es un grupo.

(4) Sean $G$ un grupo y $H$ un subconjunto finito de $G$. Demuestra que las siguientes afirmaciones son equivalentes:
(a) $H$ es subgrupo de $G$;
(b) $H \neq \varnothing$ y $H$ es cerrado bajo la operación de $G$;
(c) $e \in H$ y $H$ es cerrado bajo la operación de $G$.

(5) Da un ejemplo de un grupo $G$ y un subconjunto finito $H$ de $G$ que tengan las siguientes propiedades de forma simultánea:
(a) $H \neq \varnothing$;
(b) $H$ es cerrado bajo tomar inversos, es decir, $\forall g \in G\ (g \in H\ \implies g^{-1} \in H$;
(c) $H$ no es subgrupo de $G$.

(6) Da un ejemplo de un grupo $G$ y un subconjunto no vacío $H$ de $G$ que, sin ser subgrupo de $G$, sea cerrado bajo la operación de $G$.

(7) Sean $G$ un grupo, $H$ un subgrupo de $G$ y $g \in G$. Demuestra que $gH = Hg$ si y sólo si $gHg^{-1} = H$.

(8) Sean $G$ un grupo y $H$ un subgrupo de $G$. Demuestra que si $H$ satisface que $gHg^{-1} \subseteq H$ para todo elemento $g$ de $G$, entonces necesariamente satisface $aHa^{-1} = H$ para todo $a \in G$.

(9) Definamos $XY = \{xy \mid x \in X, y \in Y\} \subseteq G$. Hemos probado que si $H$ es un subgrupo normal de $G$ y $X$ y $Y$ son clases de equivalencia de $\equiv_H$, entonces $XY \subseteq Z_{XY}$, donde $Z_{XY} = [xy]_H$ para cualesquiera elementos $x \in X$, $y \in Y$. Demuestra que, de hecho, se tiene la igualdad $XY = Z_{XY}$.

(10) Sean $G$ un grupo y $\mathcal{P}$ una partición de $G$. Supongamos que $\mathcal{P}$ es grupo bajo una operación $\bullet : \mathcal{P} \times \mathcal{P} \to \mathcal{P}$ que satisface $[x] \bullet [y] = [xy]$ para cualesquiera $x, y \in G$, donde, para $z \in G$, $[z]$ denota el elemento de $\mathcal{P}$ del que $z$ es elemento.
(a) Demuestra que $[e]$ es un subgrupo normal de $G$;
(b) demuestra que, como conjunto, $\mathcal{P}$ es precisamente el conjunto de clases laterales de $[e]$;
(c) demuestra que, como grupo, $\mathcal{P} = G/[e]$.

(11) Da ejemplos de:
(a) un subgrupo normal de $S_3$;
(b) un subgrupo de $S_3$ que no sea normal en $S_3$.

(12) Sean $G$ un grupo y $\mathcal{F}$ un conjunto no vacío de subgrupos normales de $G$.
(a) Demuestra que la intersección $\bigcap \mathcal{F}$ es un subgrupo normal de $G$;
(b) deduce que para cada subconjunto $S$ de $G$ existe un subgrupo normal de $G$ que contiene a $S$ y que está contenido en cualquier subgrupo normal de $G$ que contenga a $S$;
(c) demuestra que el subgrupo del inciso anterior es igual al conjunto

$$\{x_1 \dots x_m \mid m \in \mathbb{Z}_{>0}, x_1, \dots, x_m \in \bigcup_{g \in G} gS'g^{-1}\},$$

donde $S' = \{e\} \cup S \cup \{s^{-1} \mid s \in S\}$ y $gS'g^{-1} = \{gsg^{-1} \mid s \in S'\}$.

(13) Definamos $\overline{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$ y $S_{\overline{\mathbb{C}}} = \{f : \overline{\mathbb{C}} \to \overline{\mathbb{C}} \mid f \text{ es una función biyectiva}\}$. Para cada matriz $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{GL}_2(\mathbb{C})$, definamos una función $m_A : \overline{\mathbb{C}} \to \overline{\mathbb{C}}$ mediante la regla

$$m_A(z) = \begin{cases} \frac{az+b}{cz+d} & \text{si } z \in \mathbb{C} \text{ y } cz + d \neq 0; \\ \infty & \text{si } z \in \mathbb{C} \text{ y } cz + d = 0; \\ \frac{a}{c} & \text{si } z = \infty \text{ y } c \neq 0; \\ \infty & \text{si } z = \infty \text{ y } c = 0. \end{cases}$$

(a) Demuestra que $m_A \in S_{\overline{\mathbb{C}}}$ para toda $A \in \mathrm{GL}_2(\mathbb{C})$;
(b) demuestra que la función $m : \mathrm{GL}_2(\mathbb{C}) \to S_{\overline{\mathbb{C}}}$ dada por $A \mapsto m_A$ es un homomorfismo de grupos;
(c) demuestra que para cada $A \in \mathrm{GL}_2(\mathbb{C})$ se tiene $m^{-1}(m_A) = \{\lambda A \mid \lambda \in \mathbb{C} \setminus \{0\}\} = m^{-1}(\mathbf{1}_{\overline{\mathbb{C}}})A$.

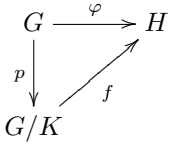
(14) Da un ejemplo de un homomorfismo de grupos $\varphi : G \to H$ cuya imagen no sea un subgrupo normal de $H$.

(15) Sean $G$ un grupo y $K$ un subgrupo de $G$. Demuestra que $K$ es normal en $G$ si y sólo si existen un grupo $H$ y un homomorfismo de grupos $\varphi : G \to H$ tales que $\mathrm{Nuc}(\varphi) = K$. Esto es, los subgrupos normales de $G$ son precisamente los núcleos de los homomorfismos que salen de $G$.

(16) Sea $\varphi : G \to H$ un homomorfismo de grupos. Demuestra que:
(a) $\varphi$ es un isomorfismo si y sólo si es una función biyectiva;
(b) $\varphi$ es un monomorfismo si y sólo si es una función inyectiva;
(c) $\varphi$ es un epimorfimos si y sólo si es una función suprayectiva.

(17) Sea $G$ un grupo. Demuestra que el conjunto $\mathrm{Aut}(G) = \{\varphi : G \to G \mid \varphi \text{ es un automorfismo de } G\}$ es un grupo bajo la composicion de funciones.

(18) Demuestra la siguiente generalización del Teorema 1.30: Si $\varphi : G \to H$ es un homomorfismo de grupos y $K$ es un subgrupo normal de $G$, entonces $K \subseteq \mathrm{Nuc}(\varphi)$ si y sólo si existe un homomorfismo de grupos $f : G/K \to H$ tal que $\varphi = f \circ p$, es decir, tal que el diagrama




conmuta, donde $p : G \to G/K$ es la **proyección canónica** (esto es, la función definida mediante la regla $g \mapsto [g]_K$). Más aun, si $K \subseteq \mathrm{Nuc}(\varphi)$, entonces $f$ es una función inyectiva si y sólo si $K = \mathrm{Nuc}(\varphi)$.

(19) Consideremos la acción $\cdot : \mathrm{GL}_2(\mathbb{C}) \times \overline{\mathbb{C}} \to \overline{\mathbb{C}}$ dada por $A \cdot z = m_A(z)$. Demuestra que:
(a) $\cdot$ es transitiva;
(b) para cada $A \in \mathrm{GL}_2(C)$, la cardinalidad del conjunto $\mathrm{Fij}_X(G)$ es 1 o 2;
(c) para cada $z \in \overline{\mathbb{C}}$, el estabilizador $G_z$ es infinito no numerable;
(d) $\cdot$ no es fiel.

(20) Demuestra que si $G$ es un $p$-grupo finito y $H$ es un subgrupo propio de $G$, entonces $H$ está contenido propiamente en su normalizador.

(21) Sean $p$ y $q$ números primos positivos con $p > q$, y sea $k$ un entero positivo. Demuestra que si $G$ es un grupo de orden $p^k q$, entonces los únicos subgrupos normales de $G$ son $\{e\}$ y $G$ mismo.

(22) Sean $G$ un grupo finito y $p$ un número primo positivo. Demuestra que si $p$ divide al orden de $G$, entonces $G$ tiene un subgrupo de orden $p$.

(23) Da un ejemplo de un grupo finito $G$ y un divisor positivo $m$ de $|G|$ con la propiedad de que $G$ no tiene subgrupos de orden $m$.

(24) Sean $G$ un grupo finito y $H$ un subgrupo propio de $G$. Demuestra que $\bigcup_{g \in G} gHg^{-1}$ es un subconjunto propio de $G$.

(25) Supongamos que $G$ es un grupo finito y que $N$ es un subgrupo normal de $G$ de índice 4.
   (a) Demuestra que $G$ tiene un subgrupo de índice 2, necesariamente normal.
   (b) Demuestra que si $G/N$ no es cíclico, entonces $G$ es la unión de tres subgrupos propios.

(26) Demuestra que si $G$ es un grupo finito sin subgrupos normales no triviales y $H$ es un subgrupo de $G$, entonces existe un homomorfismo inyectivo de grupos de $G$ en el grupo simétrico $S_H$.

(27) Sean $G$ un grupo y $H$ un subgrupo de $G$ de índice 2. Demuestra que si $H$ es simple, entonces $H$ es el único subgrupo normal no trivial de $G$ o $G$ tiene un subgrupo normal $K$ de orden 2 tal que la función $\varphi : K \times H \to G$ dada por $\varphi(k, h) = kh$ es un isomorfismo.

(28) Enuncia y demuestra el teorema de Lagrange.

(29) Enuncia y demuestra el teorema principal de Sylow.

(30) Demuestra que si $G$ es un grupo simple infinito, entonces $G$ no tiene subgrupos de índice finito.

(31) Sean $H$ y $K$ subgrupos de un grupo finito $G$. Recuerda que se define $HK = \{hk \mid h \in H, k \in K\}$. Demuestra que:
   (a) $|HK| = \frac{|H||K|}{|H \cap K|}$;
   (b) si $H$ es un subgrupo normal de $G$, entonces $HK$ es un subgrupo de $G$ y $[HK : H]$ es un divisor común de $|K|$ y $[G : H]$;
   (c) si $H$ es normal en $G$ y $\text{mcd}(|K|, [G : H]) = 1$, entonces $K \subseteq H$.

(32) Sea $G$ un $p$-grupo finito. Demuestra que:
   (a) $|Z(G)| > 1$;
   (b) si $|G| = p^2$, entonces $G$ es abeliano;
   (c) si $|G| = p^3$, entonces $Z(G)$ coincide con el subgrupo conmutador de $G$.

(33) Da un ejemplo de un primo positivo $p$, un número entero $n > 2$ y un grupo de orden $p^n$ que no sea abeliano.

(34) Sean $K$ un campo, $V$ un espacio vectorial sobre $K$, y $\mathcal{B}$ una base de $V$ sobre $K$. Demuestra que:
   (a) toda función $b : \mathcal{B} \times \mathcal{B} \to V$ puede extenderse de manera única a una función $K$-bilineal $\beta : V \times V \to V$;
   (b) si $b(\mathcal{B} \times \mathcal{B}) \subseteq \mathcal{B}$ y $b(b(u, v), w) = b(u, b(v, w))$ para toda terna de elementos $u, v, w \in \mathcal{B}$, entonces la correspondiente función $K$-bilineal $\beta$ es asociativa, es decir, $\beta(\beta(u, v), w) = \beta(u, \beta(v, w))$ para toda terna de elementos $u, v, w \in V$.

## 2. Elementos de la teoría de representaciones de grupos finitos

2.1. **El álgebra de grupo de un grupo finito.** Sean $G$ un grupo finito y $K$ un campo. Denotemos por $K[G]$ al $K$-espacio vectorial que tiene a $G$ por base. Definamos una función $\cdot : K[G] \times K[G] \to K[G]$ mediante la regla

$$\left(\sum_{g\in G} \alpha_g g\right) \cdot \left(\sum_{g\in G} \beta_g g\right) := \sum_{g\in G} \left(\sum_{\substack{h_1,h_2\in G\\ h_1h_2=g}} \alpha_{h_1}\beta_{h_2}\right) g. \tag{2.1}$$

Un sencillo EJERCICIO muestra que $K[G]$ es un anillo asociativo unitario bajo esta función, y que para todo $\alpha \in K$ y todo par de elementos $u, v \in K[G]$ son satisfechas las igualdades $\alpha(u \cdot v) = (\alpha u) \cdot v = u \cdot (\alpha v)$, hechos que justifican la siguiente definición:

**Definición 2.1.** El **álgebra de grupo** de $G$ sobre $K$ es $K[G]$ con la multiplicación dada por (2.1).

2.2. **Definición, ejemplos y propiedades básicas.**

**Definición 2.2.** Una **representación** de un grupo $G$ sobre un campo $K$ es una pareja $(V, \cdot)$ consistente de un $K$-espacio vectorial $V$ y una acción $\cdot : G \times V \to V$ que satisface

$$g \cdot (v + w) = (g \cdot v) + (g \cdot w) \qquad \text{y} \qquad g \cdot (\alpha v) = \alpha(g \cdot v) \tag{2.2}$$

para todo $g \in G$, todo $\alpha \in K$ y todo par de vectores $v, w \in V$.

De acuerdo al Lema 1.34, a cualquier acción $\cdot$ de $G$ en $V$ corresponde un homomorfismo de grupos $\rho : G \to S_V$. Es un sencillo EJERCICIO verificar que la acción $\cdot$ satisface las dos condiciones de (2.2) si y sólo si la imagen de $\rho$ está contenida en $\mathrm{GL}(V)$, de manera que hay una biyección entre el conjunto cuyos elementos son las acciones de $G$ en $V$ bajo las que $V$ es una representación de $G$ y el conjunto cuyos elementos son los homomorfismos de grupos $G \to \mathrm{GL}(V)$. Si $(V, \cdot)$ es una representación de $G$ y $\rho : G \to \mathrm{GL}(V)$ es el homomorfismo de grupos que corresponde a $\cdot$, a veces será conveniente que digamos también que $(V, \rho)$ es una representación de $G$.

A lo largo de estas notas trabajaremos siempre con **representaciones de dimensión finita** sobre el campo base $K$.

Un sencillo EJERCICIO muestra que si $(V, \cdot)$ es una representación del grupo $G$ sobre el campo $K$, entonces es posible hacer de $V$ un módulo sobre el anillo $K[G]$. En efecto, la regla

$$\left(\sum_{g\in G} \alpha_g g\right) \star v := \sum_{g\in G} \alpha_g (g \cdot v)$$

provee a $V$ de una estructura de $K[G]$-módulo izquierdo. Recíprocamente, si $M$ es un $K[G]$-módulo izquierdo, podemos ver a $M$ como representación de $G$ sobre $K$ si restringimos nuestra atención a la forma en la que $G \subseteq K[G]$ actúa en $M$.

2.3. **La categoría de representaciones de un grupo.**

**Definición 2.3.** Supongamos que $(V, \cdot)$ y $(W, \bullet)$ son representaciones de un grupo $G$ sobre un campo $K$. Un **homomorfismo de representaciones** de $(V, \cdot)$ a $(W, \bullet)$ es una función $K$-lineal $f : V \to W$ tal que $f(g \cdot v) = g \bullet f(v)$ para todo $g \in G$ y todo $v \in V$. Denotaremos por $\mathrm{Hom}_{K[G]}(V, W)$ al conjunto cuyos elemetos son precisamente los homomorfismos de representaciones de $(V, \cdot)$ a $(W, \bullet)$.

Un sencillo EJERCICIO muestra que si vemos a $(V, \cdot)$ y $(W, \bullet)$ como $K[G]$-módulos izquierdos como en el último párrafo de la subsección anterior, entonces una función $f : V \to W$ es un homomorfismo de representaciones si y sólo si es un homomorfismo de $K[G]$-módulos izquierdos.

**Teorema 2.4** (Maschke)**.** *Si la característica del campo $K$ no divide al orden del grupo $G$, entonces para toda representación $V$ de $G$ cuya dimensión sobre $K$ sea finita, y para toda subrepresentación $U$ de $V$, existe una subrepresentación $W$ de $V$ tal que $V$ y $U \oplus W$ son isomorfas como representaciones de $G$.*

*Proof.* Sean $V$ y $U$ como en el enunciado del teorema, y que la acción de $G$ en $V$ corresponde al homomorfismo de grupos $\rho : G \to \mathrm{GL}(V)$. Como $U$ es $K$-subespacio vectorial de $V$, existe un $K$-subespacio vectorial $\overline{W}$ de $V$ tal que, como $K$-espacio vectorial, $V$ es la suma directa interna de $U$ y $\overline{W}$. Denotemos por $p_{U,\overline{W}} : V \to V$ la función $K$-lineal que tiene a $\overline{W}$ por núcleo y que satisface $p_{U,\overline{W}}(u) = u$ para todo $u \in U$, y definamos una nueva función $\pi_{U,\overline{W}} : V \to V$ como sigue:

$$\pi_{U,\overline{W}} = \frac{1}{|G|} \sum_{g \in G} \rho(g^{-1}) \circ p_{U,\overline{W}} \circ \rho(g).$$

Esta función $\pi_{U,\overline{W}}$, cuya $K$-linealinad resulta obvia, es un homomorfismo de representaciones; en efecto, para cualquier $h \in G$ y cualquier $v \in V$ se tiene

$$\begin{aligned}
\pi_{U,\overline{W}}(h \cdot v) &= \frac{1}{|G|} \sum_{g \in G} \rho(g^{-1}) \circ p_{U,\overline{W}} \circ \rho(g)(h \cdot v) \\
&= \frac{1}{|G|} \sum_{g \in G} g^{-1} \cdot p_{U,\overline{W}}(g \cdot (h \cdot v)) \\
&= \frac{1}{|G|} \sum_{g \in G} g^{-1} \cdot p_{U,\overline{W}}((gh) \cdot v) \\
&= \frac{1}{|G|} \sum_{k \in G} (hk^{-1}) \cdot p_{U,\overline{W}}(k \cdot v) \\
&= \frac{1}{|G|} \sum_{k \in G} h \cdot (k^{-1} \cdot p_{U,\overline{W}}(k \cdot v)) \\
&= h \cdot \left( \frac{1}{|G|} \sum_{k \in G} k^{-1} \cdot p_{U,\overline{W}}(k \cdot v) \right).
\end{aligned}$$

Ahora bien, cualquier $u \in U$ satisface

$$\begin{aligned}
\pi_{U,\overline{W}}(u) &= \frac{1}{|G|} \sum_{g \in G} g^{-1} \cdot p_{U,\overline{W}}(g \cdot u) \\
&= \frac{1}{|G|} \sum_{g \in G} g^{-1} \cdot (g \cdot u) \\
&= \frac{1}{|G|} \sum_{g \in G} u \\
&= u,
\end{aligned}$$

pues para todo $g \in G$ se tiene $g \cdot u \in U$. En particular, $U \subseteq \mathrm{im}(\pi_{U,\overline{W}})$. Pero si $w \in \mathrm{im}(\pi_{U,\overline{W}})$, entonces existe $v \in V$ tal que

$$w = \frac{1}{|G|} \sum_{g \in G} g^{-1} \cdot p_{U,\overline{W}}(g \cdot v),$$

expresión de la que se deduce que $w \in U$, pues $U$ es subrepresentación de $V$. Así, $U = \mathrm{im}(\pi_{U,\overline{W}})$.

Como $\pi_{U,\overline{W}}$ es homomorfismo de representaciones, su núcleo $\mathrm{Nuc}(\pi_{U,\overline{W}})$ es una subrepresentación de $V$. Un resultado de álgebra lineal básica nos dice que $V$ es la suma directa interna de $U = \mathrm{im}(\pi_{U,\overline{W}})$ y $\mathrm{Nuc}(\pi_{U,\overline{W}})$. Un momento de reflexión muestra que esta expresión de $V$ como suma directa interna se da, de hecho, al nivel de representaciones. □

**Corolario 2.5.** *Si la característica del campo $K$ no divide al orden del grupo $G$, entonces toda representación de $G$ cuya dimensión sobre $K$ sea finita es isomorfa, como representación de $G$, a una suma directa de representaciones irreducibles de $G$.*

*Proof.* EJERCICIO. □

A partir de este momento supondremos que nuestro campo base es $\mathbb{C}$, el campo de los números complejos.

**Teorema 2.6** (Lema de Schur)**.** *Si $V$ y $W$ son representaciones irreducibles del grupo $G$ sobre el campo complejo $\mathbb{C}$, entonces*

$$\mathrm{Hom}_{\mathbb{C}[G]}(V,W) \cong \begin{cases} \mathbb{C} & \text{si } V \cong W; \\ 0 & \text{si } V \ncong W. \end{cases}$$

*Proof.* Supongamos que $V$ y $W$ son representaciones irreducibles de $G$. Si $\varphi : V \to W$ es un homomorfismo de representaciones, entonces $\mathrm{Nuc}(\varphi)$ es una subrepresentación de $V$ e $\mathrm{Im}(\varphi)$ es una subrepresentación de $W$. La irreducibilidad de $V$ implica que $\mathrm{Nuc}(\varphi) = V$ o $\mathrm{Nuc}(\varphi) = 0$; es decir, que si $\varphi \neq 0$, entonces $\varphi$ es inyectivo. Por otro lado, la irreducibilidad de $W$ implica que $\mathrm{Im}(\varphi) = 0$ o $\mathrm{Im}(\varphi) = W$; es decir, que si $\varphi \neq 0$, entonces $\varphi$ es suprayectivo. Por lo tanto, si $\mathrm{Hom}_{\mathbb{C}[G]}(V,W) \neq 0$, entonces $V \cong W$; es decir, si $V \ncong W$, entonces $\mathrm{Hom}_{\mathbb{C}[G]}(V,W) = 0$.

Verifiquemos que $\mathrm{Hom}_{\mathbb{C}[G]}(V,V) \cong \mathbb{C}$. La función $\iota : \mathbb{C} \to \mathrm{Hom}_{\mathbb{C}[G]}(V,V)$ dada por $\iota(\alpha) = \alpha \mathbf{1}_V$ es obviamente $\mathbb{C}$-lineal e inyectiva. Tomemos $\varphi \in \mathrm{Hom}_{\mathbb{C}[G]}(V,V)$. Por ser una transformación $\mathbb{C}$-lineal de un $\mathbb{C}$-espacio vectorial de dimensión finita en sí mismo, $\varphi$ tiene al menos un eigenvalor $\lambda \in \mathbb{C}$ y un eigenvector $v \in V \in \{0\}$ tal que $\varphi(v) = \lambda v$. Por ser $V$ una representación irreducible, todo elemento suyo puede ser escrito como combinación $\mathbb{C}$-lineal del conjunto $\{g \cdot v \mid g \in G\}$ es todo $V$. Tomemos un elemento arbitrario de $V$, digamos $\sum_g \beta_g (g \cdot v)$. Entonces $\varphi\left(\sum_g \beta_g (g \cdot v)\right) = \sum_g \beta_g (g \cdot \varphi(v)) = \lambda \sum_g \beta_g (g \cdot v)$. Vemos que $\varphi = \lambda \mathbf{1}_V = \iota(\lambda)$. Por lo tanto, $\iota$ es biyectiva.

Hemos mostrado ya que $\mathrm{Hom}_{\mathbb{C}[G]}(V,V) \cong \mathbb{C}$. Queda como EJERCICIO probar que si $V \cong W$ como representaciones, entonces $\mathrm{Hom}_{\mathbb{C}[G]}(V,W) \cong \mathbb{C}$. □

**Corolario 2.7.** *Si $G$ es un grupo abeliano, entonces toda representación compleja irreducible de $G$ tiene dimensión 1 sobre $\mathbb{C}$.*

*Proof.* Supongamos que $G$ es abeliano, que $V$ es una representación compleja irreducible de $G$, y que $\rho : G \to \mathrm{GL}_(V))$ es la función dada por $\rho(g)(v) = gv$. Como $G$ es abeliano, para todo $h \in G$ la función $\rho(h) : V \to V$ es un homomorfismo de representaciones, por lo que, gracias al Teorema 2.6, existe $\lambda_h \in \mathbb{C}$ tal que $hv = \lambda_h v$ para todo $v \in V$. Esto implica que si $v_0$ es cualquier elemento no cero de $V$, entonces el subespacio $\mathbb{C}v_0$, cuya dimensión sobre $\mathbb{C}$ es claramente igual a 1, es una subrepresentación de $V$. La irreducibilidad de $V$ implica entonces que $V = \mathbb{C}v_0$. □

## References


[1] Garrett Birkhoff, Saunders Mac Lane. *Algebra*, tercera edición. AMS Chelsea Publishing, 1988.

[2] David S. Dummit, Richard M. Foote. *Abstract Algebra*, tercera edición. John Wiley & Sons, Inc., 2004.

[3] John Fraleigh. *Álgebra Abstracta, primer curso*. Addison-Wesley Iberoamericana, 1988.

[4] I. N. Hernstein. *Álgebra Moderna*.

[5] Charles Thomas. *Representations of finite and Lie groups*. Imperial College Press, 2004.



Instituto de Matemáticas, Universidad Nacional Autónoma de México

*E-mail address*: labardini@matem.unam.mx