Tema 1.-. Grupos. Subgrupos. Teorema de Lagrange. Operaciones.

1.1. Primeras definiciones

DEFINICIÓN 1.1.1.– Una *operación binaria* en un conjunto A es una aplicación $\alpha : A \times A \to A$.

En un lenguaje más coloquial, una operación binaria en A es una regla que asocia a cada par ordenado (a, b) de elementos de A otro elemento de A, $\alpha(a, b)$.

Normalmente, si $\alpha : A \times A \to A$ es una operación binaria, es costumbre elegir algún símbolo $\star$ para notar $\alpha(a, b) \overset{not.}{=} a \star b$. En el caso en que necesitemos considerar simultáneamente varias operaciones binarias, nos veremos obligados a elegir un símbolo distinto para cada una de ellas.

A veces, y con ánimo de simplificar la escritura, no es necesario elegir ningún símbolo (o si se quiere, elegimos el símbolo "vacío") y escribiremos una simple yuxtaposición $\alpha(a, b) \overset{not.}{=} ab$.

Tabla de una operación: Para estudiar un conjunto A con "pocos"elementos dotado de una operación binaria $\star$, podemos trabajar con la *tabla de la operación*. Esta tabla es un cuadro de doble entrada en el que se colocan los elementos de A en la línea horizontal de arriba y vertical de la izquierda. En cada casilla libre correspondiente al par ordenado $(a, b) \in A \times A$ se coloca el elemento $a \star b$. Por ejemplo, si $A = \{a, b\}$ y la operación viene determinada por $a \star a = a, a \star b = b, b \star a = b, b \star b = a$, la tabla será:

$\star$	a	b
a	a	b
b	b	a

EJEMPLO 1.1.2.–

1. Si a_0 es un elemento fijo de A, la aplicación $(a, b) \in A \times A \mapsto a_0$ es una operación binaria (constante).

2. La suma y el producto usuales son operaciones binarias en el conjunto de los números naturales $\mathbb{N}$, de los números enteros $\mathbb{Z}$, de los números racionales $\mathbb{Q}$, de los números reales $\mathbb{R}$ o de los números complejos $\mathbb{C}$.

3. La suma es una operación binaria en el conjunto de los vectores $\mathbb{R}^n$ o de las matrices $m \times n$ de números reales o complejos.

4. Cualquier función de dos variables reales $f : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ define una operación binaria en $\mathbb{R}$.

5. Dado un natural $n \geq 1$ consideremos el conjunto $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ y en él la operación binaria cuya tabla es:

	0	1	2	...	$n-2$	$n-1$
0	0	1	2	...	$n-2$	$n-1$
1	1	2	3	...	$n-1$	0
2	2	3	4	...	0	1
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$n-2$	$n-2$	$n-1$	0	...	$n-3$	$n-2$
$n-1$	$n-1$	0	1	...	$n-3$	$n-2$

(Para $n = 12$, la tabla anterior indica la "aritmética del reloj").

6. Dado un conjunto B, notemos A al conjunto de las aplicaciones de B en sí mismo. La composición de aplicaciones es una operación binaria en A.

DEFINICIÓN 1.1.3.– Dado un conjunto A y una operación binaria $\star$ en él, diremos que un subconjunto $H \subset A$ es *estable* por la operación si $x \star y \in H$ para cualesquiera $x, y \in H$.

Se deja al lector encontrar subconjuntos estables en cada uno de los ejemplos anteriores.

DEFINICIÓN 1.1.4.– Dada una operación binaria $(a, b) \in A \times A \mapsto a \star b \in A$, diremos que:

1. Es *conmutativa* si $a \star b = b \star a$ para todos los elementos $a, b \in A$.
2. Es *asociativa* si $a \star (b \star c) = (a \star b) \star c$ para todos los elementos $a, b, c \in A$.
3. El elemento $e \in A$ es *elemento neutro a la izquierda* si $e \star a = a$ para todo $a \in A$.
4. El elemento $e \in A$ es *elemento neutro a la derecha* si $a \star e = a$ para todo $a \in A$.
5. El elemento $e \in A$ es *elemento neutro* si $a \star e = a = e \star a$ para todo $a \in A$.

PROPOSICIÓN 1.1.5.– Si una operación binaria en un conjunto tiene un elemento neutro a la izquierda y un elemento neutro a la derecha, ambos han de ser iguales. En particular, si una operación binaria posee elemento neutro, éste es único.

DEFINICIÓN 1.1.6.– Dado un conjunto A dotado de una operación binaria $\star$ con elemento neutro e, y dado un elemento $x \in A$, diremos que un $x' \in A$ es *simétrico a la izquierda* de x (resp. *simétrico a la derecha*) si $x' \star x = e$ (resp. $x \star x' = e$). Asimismo diremos que x' es *simétrico* de x si lo es a la izquierda y a la derecha.

PROPOSICIÓN 1.1.7.– En las condiciones de la definición anterior, se tiene lo siguiente:

1. x' es simétrico a la izquierda de x si y sólo si x es simétrico a la derecha de x'.
2. Si x' es simétrico de x e y' es simétrico de y, entonces $y' \star x'$ es simétrico de $x \star y$.

3. Si la operación $\star$ es asociativa, entonces el simétrico de un elemento, si existe, es único.

Se deja al lector practicar con las nociones de elemento neutro y de elemento simétrico en los ejemplos anteriores.

DEFINICIÓN 1.1.8.– Un grupo es un par $(G, *)$, donde G es un conjunto y $*$ una operación binaria sobre G verificando las siguientes propiedades:

1. La operación es asociativa.
2. La operación tiene elemento neutro.
3. Cada elemento de G posee un elemento simétrico.

Si además la operación es conmutativa, diremos que el grupo es *abeliano* o conmutativo.

En los grupos se tiene la propiedad cancelativa: $x \star y = x \star z \Rightarrow y = z$.

EJEMPLO 1.1.9.–

1. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ son grupos con la adición.
2. $\mathbb{Q}^* = \mathbb{Q} - \{0\}$, $\mathbb{R}^* = \mathbb{R} - \{0\}$, $\mathbb{C}^* = \mathbb{C} - \{0\}$ son grupos abelianos con la multiplicación.
3. El conjunto S_A de las biyecciones de A en A es un grupo con la composición. Si A tiene más de 2 elementos, S_A no es abeliano. Si $A = \{1, \ldots, n\}$, se nota $S_n \overset{not.}{=} S_A$.
4. El conjunto de los automorfismos de un espacio vectorial con la composición es un grupo no abeliano en general.
5. El conjunto de las afinidades de un espacio afín con la composición es un grupo no abeliano en general (Grupo afín).
6. El conjunto de los movimientos del plano con la composición es un grupo no abeliano.
7. El conjunto de las homografías de un espacio proyectivo con la composición es un grupo no abeliano en general.
8. El conjunto de las funciones (continuas, diferenciables, ...) definidas en un abierto de $\mathbb{R}^n$ con valores reales, con la suma "punto a punto", es un grupo abeliano.
9. El conjunto de las matrices $n \times n$ con elementos en k, k cuerpo, y determinante distinto de cero, $\mathrm{GL}(n, k)$, es un grupo (no abeliano si $n \geq 2$) con la multiplicación de matrices.

NOTACIÓN 1.1.10.– Normalmente usaremos la "aditiva" para los grupos abelianos y la "multiplicativa" o yuxtaposición para los grupos en general. Para cada una de estas notaciones, el elemento neutro y el simétrico de x serán notados de la siguiente forma:

	elemento neutro	elemento simétrico de x
$+$	0	$-x$ (opuesto de x)
$\cdot$	1	x^{-1} (inverso de x)

1.2. Subgrupos

DEFINICIÓN 1.2.1.– Sea $(G, \cdot)$ un grupo. Un subconjunto H de G se dice que es un *subgrupo* de $(G, \cdot)$ si se verifican las siguientes condiciones:

1. H es no vacío.
2. H es estable para la operación binaria $\cdot$, i.e. $x \cdot y \in H$ para todos $x, y \in H$ (ver def. 1.1.3).
3. $x^{-1} \in H$ para cada $x \in H$.

Nótese que si H es un subgrupo de $(G, \cdot)$, entonces $(H, \cdot)$ es de nuevo un grupo, donde hemos notado por el mismo símbolo $\cdot$ la operación binaria en G y su restricción a H. Nótese también que, en la definición de subgrupo, podemos sustituir la propiedad "H es no vacío"por "$1 \in H$".

PROPOSICIÓN 1.2.2.– Sea $(G, \cdot)$ un grupo y $H \subset G$ un subconjunto no vacío. Las condiciones siguientes son equivalentes:

1. H es un subgrupo de $(G, \cdot)$.
2. $\forall\, x, y \in H$, $x \cdot y^{-1} \in H$.

De ahora en adelante escribiremos el "grupo G"en lugar de el "grupo $(G, \cdot)$", sobrentendiendo que la operación binaria la notaremos con el símbolo $\cdot$ o simplemente con la yuxtaposición de elementos de G.

EJEMPLO 1.2.3.–

1. Para todo grupo G, $\{1\}$ y G son subgrupos de G y se denominan *subgrupos triviales* de G.
2. **Subgrupos de** $(\mathbb{Z}, +)$**:** Dado $n \in \mathbb{Z}, n \geq 0$ sea $\mathbb{Z}n = \{k \cdot n : \ k \in \mathbb{Z}\}$. Se tiene:
   a) $\mathbb{Z}n$ es un subgrupo de $\mathbb{Z}$.
   b) Todo subgrupo de $\mathbb{Z}$ es de la forma $\mathbb{Z}n$ para algún $n \geq 0$.
3. Raíces n-ésimas de la unidad dentro de $\mathbb{C}^*$.

4. Si $C \subset A$, el conjunto $\{f \in S_A \mid f(a) = a, \forall a \in C\}$ es un subgrupo de S_A.
5. Traslaciones dentro del grupo de los movimientos o de las afinidades.
6. Movimientos que dejan invariante una figura.
7. Dilataciones dentro del grupo afín.
8. Homologías de eje y centro dado dentro del grupo de las homografías.
9. Algún subgrupo finito de GL.

PROPOSICIÓN 1.2.4.– Sea G un grupo, $\{H_i : \ i \in I\}$ una familia de subgrupos de G. Entonces $\bigcap_{i\in I} H_i$ es un subgrupo de G.

DEFINICIÓN 1.2.5.– Dado un subconjunto A de un grupo G, definimos :

$$\langle A\rangle = \bigcap\{H : \ H \text{ subgrupo de } G \text{ y } A \subseteq H\}.$$

PROPOSICIÓN 1.2.6.– Sean G un grupo y $A \subseteq G$. Se tiene lo siguiente:

1. $\langle A\rangle$ es un subgrupo de G.
2. $\langle A\rangle$ es el menor subgrupo de G que contiene a A, i.e. si H es un subgrupo de G que contiene a A, entonces también contiene a $\langle A\rangle$.

DEFINICIÓN 1.2.7.– Al subgrupo $\langle A\rangle$ se le llamará *subgrupo generado* por A. Se dirá que A es un sistema de generadores de $\langle A\rangle$. Si $G = \langle A\rangle$, se dirá que A es un sistema de generadores de G.

PROPOSICIÓN 1.2.8.– Sea G un grupo y A un subconjunto de G. Se tiene lo siguiente:

1. Si $A = \emptyset$ entonces $\langle\emptyset\rangle = \{1\}$.
2. Supongamos que $A \neq \emptyset$. Sea $A^{-1} = \{x^{-1} : \ x \in A\}$. Entonces:

$$\langle A\rangle = \{x_1 \cdot x_2 \cdot \cdots \cdot x_n : \ x_i \in A \cup A^{-1}, n \geq 1\},$$

esto es, $\langle A\rangle$ es el conjunto de todos los productos finitos de elementos de $A \cup A^{-1}$.

DEFINICIÓN 1.2.9.– Sea G un grupo y H, K subgrupos de G. Definimos:

$$H \cdot K = \langle H \cup K\rangle.$$

PROPOSICIÓN 1.2.10.– Sean $H, K \subseteq G$ subgrupos de G. Se tiene:

1. $H \cdot K = \{h_1 \cdot k_1 \cdot \cdots \cdot h_n \cdot k_n : \ n \geq 1, h_i \in H, k_i \in K\}$.
2. Si G es abeliano, $H \cdot K = \{h \cdot k : \ h \in H, \ k \in K\}$.

1.3. Grupos cíclicos. Orden de un elemento de un grupo

DEFINICIÓN 1.3.1.– Dado un grupo G cuya operación es notada multiplicativamente (resp. aditivamente), definimos la *potencia* (resp. el *múltiplo*) de un elemento $a \in G$ como sigue: para cada entero $n \geq 0$

$$\left\{ \begin{array}{lcl} a^n & = & \left\{ \begin{array}{ll} 1 & \text{si } n = 0 \\ a^m \cdot a & \text{si } n = m+1 \end{array} \right. \\ a^{-n} & = & (a^{-1})^n \end{array} \right.$$

(resp.

$$\left\{ \begin{array}{lcl} n \cdot a & = & \left\{ \begin{array}{ll} 0 & \text{si } n = 0 \\ (m \cdot a) + a & \text{si } n = m+1 \end{array} \right. \\ (-n) \cdot a & = & n \cdot (-a) \end{array} \right.)$$

Nótese que con la definición anterior, $(a^m)^n = a^{mn}, (a^m)(a^n) = a^{m+n}$.

PROPOSICIÓN 1.3.2.– Sean G un grupo, $a \in G$ y $A = \{a\}$. Entonces

$$\langle a \rangle \overset{not.}{=} \langle \{a\} \rangle = \{a^n : \ n \in \mathbb{Z}\}$$

y se le denomina *subgrupo cíclico* de G generado por a.

DEFINICIÓN 1.3.3.– Sea G un grupo. Diremos que G es un *grupo cíclico* si existe $a \in G$ tal que $G = \langle a \rangle$.

PROPOSICIÓN 1.3.4.– Si G es un grupo cíclico entonces G es abeliano.

DEFINICIÓN 1.3.5.– Sea G un grupo y $a \in G$. Diremos que:

1. a tiene orden infinito si todas las potencias de a son distintas entre sí.
2. a tiene orden finito si existen $0 \leq n < m$ tales que $a^n = a^m$.

EJEMPLO 1.3.6.–

1. Sea $a \in \mathbb{Z}$ con $a \neq 0$. Entonces a tiene orden infinito.
2. El elemento $a = \begin{pmatrix} i & 0 \\ 0 & i \end{pmatrix} \in \mathrm{GL}(2, \mathbb{C})$ tiene orden finito.

PROPOSICIÓN 1.3.7.– Sean G un grupo (con notación multiplicativa) y $a \in G$. Consideremos el subgrupo $\langle a \rangle$.

1. Si a es de orden infinito, entonces
   a) $a^n = 1 \Leftrightarrow n = 0$.
   b) La aplicación $\varphi : \mathbb{Z} \to \langle a \rangle$ dada por $\varphi(n) = a^n$ es biyectiva.
   c) $\langle a \rangle$ es un grupo infinito.

2. Si a es de orden finito, entonces

   a) Existe $n > 0$ tal que $a^n = 1$.

   b) Sea m el menor entero estrictamente positivo tal que $a^m = 1$. Entonces los $a^i, 0 \leq i \leq m-1$ son distintos entre sí y $\langle a \rangle = \{a^0 = 1, a, a^2, \ldots, a^{m-1}\}$.

DEFINICIÓN 1.3.8.– Sea G un grupo y $a \in G$ de orden finito. El orden de a, notado $o(a)$, es el menor entero (estrictamente) positivo m tal que $a^m = 1$.

PROPOSICIÓN 1.3.9.– Sea G un grupo y $a \in G$. Se tienen las siguientes propiedades:

1. $o(a) = 1 \Leftrightarrow a = 1$.
2. Si $a \in G$ tiene orden finito, $o(a) = o(a^{-1})$.
3. Si $a \in G$ tiene orden infinito, a^{-1} tiene orden infinito.
4. Si G es finito, todo elemento de G tiene orden finito.
5. Si $o(a) = n$ y $a^m = 1$ entonces $n|m$.

1.4. Teorema de Lagrange

DEFINICIÓN 1.4.1.– Sean G un grupo y $H \subseteq G$ un subgrupo. Sobre G definimos las relaciones $\sim_H$ y ${}_H\sim$ de la manera siguiente: Dados $x, y \in G$,

$$x \sim_H y \Leftrightarrow x^{-1} \cdot y \in H \qquad x \,{}_H\!\sim y \Leftrightarrow x \cdot y^{-1} \in H.$$

PROPOSICIÓN 1.4.2.– En las condiciones de la definición anterior, las relaciones $\sim_H$ y ${}_H\sim$ son relaciones de equivalencia.

PROPOSICIÓN 1.4.3.– Sea G un grupo y $a \in G$. Notemos

$$a \cdot H \overset{not.}{=} \{a \cdot h : \ h \in H\}, \quad H \cdot a = \{h \cdot a : \ h \in H\}.$$

Se tiene:

1. $a \cdot H$ es la clase de equivalencia de a para la relación $\sim_H$.
2. $H \cdot a$ es la clase de equivalencia de a para la relación ${}_H\sim$.

DEFINICIÓN 1.4.4.– En las condiciones anteriores, introducimos la siguiente terminología:

1. Las clases de equivalencia $a \cdot H$ se llaman clases adjuntas (o laterales) a izquierda de G *módulo* H, y su conjunto, esto es, el conjunto cociente $G/\sim_H$, se designará por $G : H$.

2. Las clases de equivalencia $H \cdot a$ se llaman clases adjuntas (o laterales) a derecha de G *módulo* H, y el conjunto cociente $G/_{H}\sim$ se designará por $H : G$.

NOTA 1.4.5.– Si G es un grupo abeliano, entonces las relaciones a derecha e izquierda coinciden.

EJEMPLO 1.4.6.–

1. Sea $n \in \mathbb{Z}$, $n > 0$. Se tiene $\mathbb{Z} : \mathbb{Z}n = \mathbb{Z}n : \mathbb{Z} = \{0 + \mathbb{Z}n, \ldots, (n-1) + \mathbb{Z}n\}$, donde las clases anteriores son distintas entre sí.

   Si $n \in \mathbb{Z}$, $n \neq 0$, como $\mathbb{Z}n = \mathbb{Z}(-n)$, podemos suponer que $n > 0$.

2. Consideremos el subgrupo $H \subseteq \mathrm{GL}(2, \mathbb{C})$ dado por

$$H = \left\{ \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} : \ \lambda = 1, -1, i, -i \right\}.$$

   Para todo $A \in \mathrm{GL}(2, \mathbb{C})$, $A \cdot H = H \cdot A$. Por tanto, $\sim_H = {}_H\sim$, aún sin ser $\mathrm{GL}(2, \mathbb{C})$ un grupo abeliano.

3. Sea $H \subseteq \mathrm{GL}(2, \mathbb{C})$ el subgrupo

$$H = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix} \right\}.$$

   Sea $A = \begin{pmatrix} 3 & 2 \\ 5 & 4 \end{pmatrix}$. Se tiene que:

$$A.H = \left\{ \begin{pmatrix} 3 & 2 \\ 5 & 4 \end{pmatrix}, \begin{pmatrix} 2i & 3i \\ 4i & 5i \end{pmatrix}, \begin{pmatrix} -3 & -2 \\ -5 & -4 \end{pmatrix}, \begin{pmatrix} -2i & -3i \\ -4i & -5i \end{pmatrix} \right\}$$

$$H.A = \left\{ \begin{pmatrix} 3 & 2 \\ 5 & 4 \end{pmatrix}, \begin{pmatrix} 5i & 4i \\ 3i & 2i \end{pmatrix}, \begin{pmatrix} -3 & -2 \\ -5 & -4 \end{pmatrix}, \begin{pmatrix} -5i & -4i \\ -3i & -2i \end{pmatrix} \right\}$$

   Como $A.H \neq H.A$, es $\sim_H \neq {}_H\sim$.

DEFINICIÓN 1.4.7.– Dado un grupo finito G, definimos su *orden*, que notaremos $|G|$, como el cardinal del conjunto G.

TEOREMA 1.4.8.– (Teorema de Lagrange) Sea G un grupo finito, $H \subset G$ un subgrupo. Entonces $|H|$ divide a $|G|$.

Demostración. Consideremos la relación $\sim_H$ sobre G. Como G es finito, habrá sólo un número finito de clases de equivalencia distintas. Sean éstas $a_1.H, \ldots, a_r.H$. Como G es unión disjunta de estas clases, será

$$|G| = |a_1.H| + \cdots + |a_r.H|.$$

Sea $H = \{h_1, \ldots, h_n\}$; fijado un entero i, $1 \leq i \leq r$, de $a_i \cdot h_j = a_i \cdot h_l$ se deduce que $h_j = h_l$. Por tanto los elementos de la clase $a_i.H$ son todos distintos, ya que

$$a_i \cdot H = \{a_i \cdot h_1, \ldots, a_i \cdot h_n\}.$$

Así, $|a_i \cdot H| = |H|$, luego $|G| = r \cdot |H|$. □

Nótese que podíamos haber hecho parecido razonamiento con ${}_H\sim$. Habríamos obtenido, en particular, que el número de clases adjuntas a izquierda coincide con el de clases adjuntas a derecha, y es igual a $|G|/|H|$.

DEFINICIÓN 1.4.9.– Sea G un grupo finito, $H \subset G$ un subgrupo. Al número $|G : H| = |H : G| = |G|/|H|$ se le llama índice de H en G, y se le representa por $i(H, G)$.

COROLARIO 1.4.10.– Sea G grupo finito y $H, K \subset G$ subgrupos. Se tienen las siguientes propiedades:

1. Para cada $a \in G$ se tiene que $o(a)$ divide a $|G|$.
2. Si el orden de G es primo, entonces G es cíclico y no tiene más subgrupos que los triviales.
3. Si $|H|$ y $|K|$ son primos entre sí, entonces $H \cap K = \{e\}$.
4. $|H \cdot K| \geq \dfrac{|H||K|}{|H \cap K|}$, y se tiene la igualdad cuando $H \cdot K = \{hk \ : \ h \in H, k \in K\}$ (por ejemplo, cuando G es abeliano).

Demostración. Sea $L = \{hk \mid h \in H, k \in K\}$. Notemos que L es la unión de las clases a izquierda de K, es decir,

$$L = \bigcup_{h \in H} hK.$$

Cada clase a izquierda tiene $|K|$ elementos. Por tanto, debemos calcular el número de clases distintas de la forma hK, cuando $h \in H$. Pero $h_1K = h_2K$ si y solamente si $h_2^{-1}h_1 \in K$. Entonces

$$h_1K = h_2K \Leftrightarrow h_2^{-1}h_1 \in H \cap K \Leftrightarrow h_1(H \cap K) = h_2(H \cap K).$$

El número de clases a izquierda hK distintas es igual al número de clases a izquierda $h(H \cap K)$ distintas, para $h \in H$. Este último número, por le teorema de Lagrange, es igual a $\frac{|H|}{|H \cap K|}$. Entonces L contiene $\frac{|H|}{|H \cap K|}$ clases distintas de K, cada una de las cuales tiene $|K|$ elementos. Por tanto,

$$|L| = \frac{|H|}{|H \cap K|}|K|.$$

Si G es abeliano, entonces $HK = L$. □

1.5. Operaciones con grupos

DEFINICIÓN 1.5.1.– Sean $G_1, \ldots, G_n$ grupos. En el conjunto $G_1 \times \cdots \times G_n$ definimos operación binaria:

$$(a_1, \ldots, a_n) \cdot (b_1, \ldots, b_n) = (a_1 \cdot b_1, \ldots, a_n \cdot b_n).$$

Proposición 1.5.2.– $G_1 \times \cdots \times G_n$ con la operación binaria que acabamos de definir es un grupo.

Proposición 1.5.3.– En las condiciones anteriores, son equivalentes:

1. $G_1 \times \cdots \times G_n$ es abeliano.
2. Para todo i, $1 \leq i \leq n$, G_i es abeliano.