Tema 2. Grupos.

1 Grupos

Definición 1 *Un grupo es una estructura algebraica $(G, *)$ tal que la operación binaria $*$ verifica:*

1. ** es asociativa*
2. ** tiene elemento neutro*
3. *todo elemento de G tiene simétrico.*

*Si, además, * es conmutativa se dice que $(G, *)$ es un grupo conmutativo o abeliano (en honor al matemático noruego Niels Henrik Abel, 1802-1829).*

Ejemplo 1 *Las siguientes estructuras algebraicas son grupos.*

1. $(\mathbb{Z}, +)$, $(Q, +)$, $(R, +)$, $(\mathbb{Z}_m, +)$.
2. $(Q^*, \cdot)$ $(R^*, \cdot)$, $(\mathbb{Z}_p^*, \cdot)$ *con p primo.*
3. *El conjunto de matrices de orden 2 con coeficientes enteros (o reales) con la suma es un grupo conmutativo.*
4. $(S_3, \circ)$, *con la operación dada por la tabla*

$$1 = \begin{pmatrix} a & b & c \\ a & b & c \end{pmatrix} \quad \alpha = \begin{pmatrix} a & b & c \\ a & c & b \end{pmatrix}$$

$$\beta = \begin{pmatrix} a & b & c \\ b & a & c \end{pmatrix} \quad \gamma = \begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix}$$

$$\delta = \begin{pmatrix} a & b & c \\ c & a & b \end{pmatrix} \quad \epsilon = \begin{pmatrix} a & b & c \\ c & b & a \end{pmatrix}$$

$\circ$	1	α	β	γ	δ	ϵ
1	1	α	β	γ	δ	ϵ
α	α	*1*	δ	ϵ	β	γ
β	β	γ	*1*	α	ϵ	δ
γ	γ	β	ϵ	δ	1	α
δ	δ	ϵ	α	1	γ	β
ϵ	ϵ	δ	γ	β	α	1

Nota $\delta = \alpha \circ \beta$.

Proposición 1.1 *En un grupo $(G, *)$ se verifica:*

1. *El elemento neutro es único (suele denotarse por e).*
2. *El simétrico de un elemento g de G es único (se escribe g^{-1}).*
3. *Para cada $g \in G$, $(g^{-1})^{-1} = g$.*
4. *Dados $g, h \in G$, $(g * h)^{-1} = h^{-1} * g^{-1}$.*
5. *Todo elemento de G es simplificable.*
6. *Para cualesquiera $g, h \in G$, la ecuación $g * x = h$ (también, $x * g = h$) tiene solución única en G.*
7. *El neutro es el único elemento idempotente de G.*
8. *Cada elemento de un grupo finito aparece exactamente una vez en cada fila y en cada columna de la tabla de la operación del grupo.*

Nota Cuando la operación del grupo es + (adición), el grupo se dice aditivo, el elemento neutro se denota por 0 y el simétrico de a se escribe $-a$.

Se llama orden de un grupo $(G, *)$ al cardinal del conjuinto G. Hay sólo un grupo de orden 1, 2 ó 3; ¿cuántos grupos de orden 4 puede haber?

Definición 2 *Sean $(G_1, *)$ y $(G_2, \circ)$ dos grupos. Consideremos, en el conjunto $G_1 \times G_2$, la operación interna $(x, y)\cdot(x', y') = (x * x', y \circ y')$. Se verifica que $(G_1 \times G_2, \cdot)$ tiene estructura de grupo, que llamaremos el grupo producto de $(G_1, *)$ y $(G_2, \circ)$. Observemos que su neutro es (e, e'); y para cada $(x, y) \in (G_1 \times G_2)$ su simétrico es $(x, y)^{-1} = (x^{-1}, y^{-1})$.*

2 Subgrupos

Sea $(G, *)$ un grupo y H un subconjunto no vacío de G.

Definición 3 *Se dice que H es un subgrupo de G si, considerando $*$ restringida a H, se verifica que $(H, *)$ es un grupo. Es decir:*

1. $\forall h, h' \in H,\ h * h' \in H$
2. $e \in H$
3. $\forall h \in H,\ h^{-1} \in H$.

Proposición 2.1 *Son equivalentes,*

1. *H es subgrupo de G*
2. *$\forall h, h' \in H,\ h * h' \in H$ y $\forall h \in H,\ h^{-1} \in H$.*
3. *$\forall h, h' \in H,\ h * (h')^{-1} \in H$*

Ejemplo 2

1. *G y $\{e\}$ son subgrupos de $(G, *)$; se llaman subgrupos triviales de G.*
2. *$(\mathbb{Z}, +)$ es subgrupo de $(Q, +)$.*
3. *$H = \{0, 2\}$ es subgrupo de $(\mathbb{Z}_4, +)$; sin embargo, $H' = \{0, 1\}$ no lo es.*
4. *$H = \{1, 6\}$ es un subgrupo de $(\mathbb{Z}_7^*, \cdot)$, pero $H' = \{1, 5\}$ no lo es.*
5. *$H = \{1, \alpha\}$ y $H' = \{1, \gamma, \delta\}$ son subgrupos de $(S_3, \circ)$; sin embargo $H' = \{1, \alpha, \beta\}$ no lo es.*

3 Orden de un elemento y grupos cíclicos

Notación. Dado un elemento de un grupo G, se definen las potencias g^n, para cualquier entero n, de la forma siguiente:

$$g^0 = e,\ \text{ y para } n \geq 1,\ g^n = g * \overset{n}{\cdots} * g;\ g^{-n} = (g^n)^{-1}$$

Usando inducción se prueba que para todo $n \geq 1,\ g^n = g * g^{n-1};\ (g^n)^{-1} = (g^{-1})^n$.

Además, se cumple que:

$$g^n * g^m = g^{n+m} \text{ y } (g^n)^m = g^{nm},\ \forall\, n, m \in \mathbb{Z}.$$

3.1 *Aunque g^n es un elemento de G para cada entero n, no significa que todas las potencias g^n representen elementos distintos de G. De hecho, si G es finito, algunas de las potencias han de ser iguales: Supongamos que $g^a = g^b$ con $a > b$, entonces $g^{a-b} = e$, donde $a - b > 0$. En consecuencia, se puede asegurar que $g^s = e$ para algún entero positivo s; por el axioma del buen orden, existe el menor entero positivo con esa propiedad.*

Definición 4 *Sea g un elemento de un grupo G. Si para todo entero positivo n, $g^n \neq e$ se dice que g tiene orden infinito. En caso contrario, se dice que g tiene orden finito y al menor entero positivo m para el cual $g^m = e$ se llama orden de g, denotado por ord g.*

Por lo señalado anteriormente, en un grupo finito todo elemento tiene orden finito y el orden del elemento neutro es 1.

Ejemplo 3 *1. En $(\mathbb{Z}, +)$: ord $0 = 1$, pero n es de orden infinito $\forall\, n \in \mathbb{Z}, n \neq 0$.*

2. En $(\mathbb{Z}_4, +)$: ord $0 = 1$, ord $1 = 4 =$ ord 3, ord $2 = 2$.

3. En $(\mathbb{Z}_7*, \cdot)$: ord $1 = 1$, ord $2 = 3 =$ ord 4, ord $3 = 6 =$ ord 5, ord $6 = 2$.

4. En $(S_3, \circ)$: ord $1 = 1$, ord $\alpha = 2 =$ ord $\beta =$ ord ϵ, ord $\gamma = 3 =$ ord δ.

5. En $(\mathbb{Z}_2 \times \mathbb{Z}_2, +)$ todos los elementos, salvo el neutro, tienen orden 2.

6. En $(C^*, \cdot)$: ord $i = 4$, ord $(-1) = 2$, ord $((-1 + i\sqrt{3})/2) = 3$.

Proposición 3.2 *Sea $g \in G$.*

1. ord $g = 1$ si, y sólo si, $g = e$.

2. ord $g = 2$ si, y sólo si, $g \neq e$ y $g = g^{-1}$.

3. Si G es finito, entonces ord $g \leq |G|$.

4. $g^s = e$ si, y sólo si, s es múltiplo del orden de g.

5. ord $g =$ ord g^{-1}.

Definición 5 *Sea g un elemento de un grupo $(G, *)$. El conjunto $< g >= \{g^n,\ n \in \mathbb{Z}\}$ es un subgrupo de G, llamado subgrupo cíclico generado por g.*

Definición 6 *Se dice que un grupo $(G, *)$ es cíclico si existe $x \in G$ tal que $G =< x >$, es decir, todos los elementos de G pueden expresarse como potencias de x.*

Ejemplo 4 *Los grupos $(\mathbb{Z}, +)$ y $(\mathbb{Z}_7^*, \cdot)$ son cíclicos generados por 1 y 3, respectivamente.*

3.3 *Sea g un elemento del grupo G tal que ord $g = m$.*

1. Para $0 \leq i < j < m$, se verifica que, $g^i \neq g^j$.

2. Para cualquier entero n, $g^n = g^r$ siendo r el resto de dividir n por m $(0 \leq r < m)$.

Por lo tanto, $< g >= \{e, g^1, g^2, ..., g^{m-1}\}$ y el cardinal del conjunto $< g >$ coincide con el orden del elemento g.

Ejemplo 5 *1. En un grupo, $(G, *)$, $< e >= \{e\}$ y para todo $g \in G$, $< g >=< g^{-1} >$.*

2. En $(\mathbb{Z}, +)$, $< 1 >= \mathbb{Z} =< -1 >$ y $< a >$ es el conjunto de los múltiplos del elemento a.

3. En $(\mathbb{Z}_4, +)$, $< 1 >= \mathbb{Z}_4 =< 3 >$, $< 2 >= \{0, 2\}$.

4. En $(\mathbb{Z}_{12}, +)$, $< 1 >= \mathbb{Z}_{12} =< 5 >=< 7 >=< 11 >$ (nótese que 1, 5, 7, 11 son primos con 12), $< 2 >= \{0, 2, 4, 6, 8, 10\}$, $< 3 >= \{0, 3, 6, 9\}$.

5. En $(\mathbb{Z}_7^*, \cdot)$, $< 1 >= \{1\}$, $< 2 >= \{1, 2, 4\} =< 4 >$, $< 3 >= \mathbb{Z}_7^* =< 5 >$, $< 6 >= \{1, 6\}$.

6. En $(S_3, \circ)$, $< 1 >= \{1\}$, $< \alpha >= \{1, \alpha\}$, $< \beta >= \{1, \beta\}$, $< \epsilon >= \{1, \epsilon\}$, $< \gamma >= \{1, \gamma, \delta\} =< \delta >$.

Proposición 3.4 *1. Si G es cíclico, entonces G es conmutativo. Pero el recíproco no es cierto, por ejemplo, $(\mathbb{R}, +)$ es conmutativo, pero no cíclico.*

2. Todo subgrupo de un grupo cíclico es cíclico (está generado por la menor potencia positiva del generador del grupo que pertenezca al subgrupo).

Demostración (del primer enunciado). Para $n, m \in \mathbb{Z}$, se tiene $g^n * g^m = g^{n+m} = g^m * g^n$.

Proposición 3.5 *Sean $(G, \cdot)$ es un grupo finito y H un subconjunto no vacío de G. H es subgrupo de G si, y sólo si, la operación es interna en H.*

Demostración. Si H es subgrupo de G entonces la operación es interna en H por definición de subgrupo. Supongamos que la operación es interna en H. Para demostrar que H es subgrupo basta con justificar que dado cualquier elemento $h \in H$ se tiene que su inverso también pertenece a H (ver Proposición **??**). Fijemos $h \in H$ y veamos que su inverso también pertenece a H. Sabemos que el orden del elemento h es finito, supongamos ord $h = m$. Si $m = 1$ entonces h es el elemento neutro y su inverso es el mismo. Si $m > 1$ entonces $e = h^m = h^{m-1} \cdot h = h \cdot h^{m-1}$. Por lo tanto, $h^{-1} = h^{m-1} \in H$.

4 Teorema de Lagrange

En este apartado demostraremos el Teorema de Lagrange, que afirma que el orden de un subgrupo de un grupo finito divide al orden del grupo. La idea de la demostración es construir una partición del grupo en la que todas las partes tengan el mismo número de elementos que el subgrupo.

Sea $(G, *)$ un grupo (no necesariamente finito) y sea H un subgrupo de G. Se define la siguiente relación $\sim$ en G. Para $x, y \in G$

$$x \sim y \Leftrightarrow x^{-1} * y \in H.$$

1. La relación $\sim$ es de equivalencia:

   (a) $\sim$ es reflexiva (equivale a que el neutro sea un elemento de H)
   $g \sim g \Leftrightarrow g^{-1} * g \in H \Leftrightarrow e \in H$

   (b) $\sim$ es simétrica (equivale a que el inverso de cualquier elemento de H pertenece a H)
   $x \sim y \Leftrightarrow x^{-1} * y \in H \Leftrightarrow (x^{-1} * y)^{-1} \in H \Leftrightarrow y^{-1} * x \in H \Leftrightarrow y \sim x$

   (c) $\sim$ es transitiva
   $x \sim y, y \sim z \Leftrightarrow x^{-1} * y, y^{-1} * z \in H \Rightarrow (x^{-1} * y) * (y^{-1} * z) \in H \Rightarrow (x^{-1} * z) \in H \Leftrightarrow x \sim z$

2. Sea $g \in G$. La clase lateral (por la izquierda) de g respecto a H es:

   $[g] = \{x \in G / \, g \sim x\} = \{x \in G / \, g^{-1} * x \in H\} = \{x \in G / \, g^{-1} * x = h$, para algún h de $H\}$.

   Luego $[g] = \{x = g * h$, para algún h de $H\}$.

   Denotaremos $[g] = g * H$.

   Observemos que, $[e] = [h] = H$ para todo $h \in H$.

3. Todas las clases de equivalencia tienen el mismo cardinal, que coincide con el cardinal de H.

   Sea $g \in G$ veamos que $[g]$ y H son conjuntos con el mismo cardinal. En efecto, teniendo en cuenta que el elemento g es simplificable y la caracterización de $[g]$ en el punto anterior, se concluye que la aplicación $\psi : H \to g * H$ definida por $\psi(h) = g * h$ es biyectiva.

4. Se llama índice de H en G al número de clases de equivalencia de la relación inducida por H en G. Se representa por $[G : H]$.

Como todas las clases tienen el mismo cardinal que H y las clases distintas forman una partición de G, se obtiene el siguiente Teorema de Lagrange.

Teorema 4.1 *Sea $(G, \cdot)$ un grupo finito y H un subgrupo de G. Entonces, $|G| = [G : H] \cdot |H|$.*

Corolario 4.2 *Sea $(G,\cdot)$ un grupo finito*

1. *El orden de un subgrupo divide al orden del grupo.*
2. *El orden de un elemento de un grupo finito divide al orden del grupo.*
3. *Si G es un grupo finito de orden n, entonces $g^n = e$, para todo g de G.*
4. *Si $|G|$ es un número primo, entonces G es cíclico (y, por lo tanto, conmutativo).*

Ejemplo 6 1. *El subgrupo $H = \{1, \alpha\}$ de $(S_3, \circ)$ da lugar a las siguientes clases:*
$[1] = [\alpha] = H$; $[\beta] = \{\beta \circ 1, \beta \circ \alpha\} = \{\beta, \gamma\} = [\gamma]$; $[\delta] = \{\delta \circ 1, \delta \circ \alpha\} = \{\delta, \epsilon\} = [\epsilon]$.

2. *La relación dada por el subgrupo $H =< m >= \{zm / \ z \in \mathbb{Z}\}$ en $(\mathbb{Z}, +)$, es la relación "ser congruente módulo m"*

$$x \sim y \Leftrightarrow -x + y \in H \Leftrightarrow x - y \in H \Leftrightarrow \exists z \in \mathbb{Z}, \text{ tal que } x - y = zm \Leftrightarrow x \equiv_m y.$$

Las clases de equivalencia son las clases de resto módulo m, $[x] = \{x + zm / \ z \in \mathbb{Z}\} = x + < m >$.

5 Relaciones de congruencia y grupo cociente

Sea $(G, *)$ un grupo conmutativo y sea H un subgrupo de G.

5.1 1. *La relación de equivalencia definida por H en G, $x \sim y \Leftrightarrow x^{-1} * y \in H$ es una relación de congruencia, es decir, compatible con la operación $*$. En efecto, si $x \sim y$ e $z \sim t$ entonces $(x * z)^{-1} * (y * t) = z^{-1} * x^{-1} * y * t = (x^{-1} * y) * (z^{-1} * t) \in H$ ya que es el resultado de operar dos elementos de H. Luego $(x * z) \sim (y * t)$.*

En ese caso, el conjunto cociente tiene estructura de grupo, llamado grupo cociente, que se representa por G/H. La operación está definida por $[g] * [g'] = [g * g']$ (ó $(g * H) * (g' * H) = (g * g') * H$). Observemos que el elemento neutro es $[e] = H$.

2. *Recíprocamente, si $\sim$ es una relación de congruencia en G entonces*

   (a) *$[e]$ es un subgrupo.*
   En efecto, $[e]$ es no vacío pues contiene al neutro. Veamos que la operación es interna: si $x, y \in [e]$ entonces $x \sim e$ e $y \sim e$ de donde se tiene que $x * y \sim e * e$ por ser $\sim$ una relación de congruencia. Luego $x * y \in [e]$. Finalmente, veamos que para todo $x \in [e]$, su simétrico también pertenece a $[e]$: si $x \in [e]$ entonces $x \sim e$. Por otro lado, $x^{-1} \sim x^{-1}$ (por ser $\sim$ una relación de equivalencia), luego $x^{-1} * x \sim x^{-1} * e$. Es decir, $e \sim x^{-1}$ o equivalentemente, $x^{-1} \in [e]$.

   (b) *Además, para todo $x \in G$ se verifica $[x] = x * [e]$. Es decir, $\sim$ coincide con la relación definida por el subgrupo $[e]$.*
   En efecto, si $y \in [x]$ entonces $y \sim x$. Por otro lado, $x^{-1} \sim x^{-1}$ y la relación es compatible con la operación, luego $x^{-1} * y \sim x^{-1} * x^{-1} = e$ de donde se tiene que $x^{-1} * y \in [e]$ o equivalentemente, $y \in x * [e]$.
   Veamos la inclusión $x * [e] \subset [x]$. Si $y \in x * [e]$ entonces $x^{-1} * y \in [e]$ o equivalentemente, $x^{-1} * y \sim e$. Usando que $x \sim x$ y que la relación es compatible con la operación tenemos que $x * x^{-1} * y \sim x * e$. Luego $y \sim x$ y por tanto $y \in [x]$.

Ejemplo 7 *El subgrupo $H =< m >$ de $(\mathbb{Z}, +)$ define la relación de equivalencia ser congruente módulo m y la operación en el cociente $\mathbb{Z}_m$ es la suma módulo m.*

6 Morfismos de grupos

Sean $(G, *)$ y $(G', \#)$ grupos.

Definición 7 *Una aplicación $f : G \to G'$ se denomina morfismo de grupos si f conserva la operación. Es decir,*
$f(g_1 * g_2) = f(g_1)\#f(g_2)$, *para todos $g_1, g_2 \in G$.*

Proposición 6.1 *Sea $f : G \to G'$ un morfismo de grupos*

1. $f(e) = e'$, *siendo e y e' los elementos neutros de G y G', respectivamente.*
2. $f(g^{-1}) = f(g)^{-1}$, *para todo $g \in G$.*
3. *Si H es un subgrupo de G, entonces $f(H)$ es un subgrupo de G'.*
   En particular, $\mathrm{Im}(f) = f(G)$ *es un subgrupo de G'.*
4. *Si H'es un subgrupo de G',entonces $f^{-1}(H')$ es un subgrupo de G.*
   En particular, $\mathrm{Ker}(f) = \{g \in G / f(g) = e'\}$ *es un subgrupo de G.*
5. *f es inyectiva si, y sólo si,* $\mathrm{Ker}(f) = \{e\}$.

Ejemplo 8
1. *$f : (\mathbb{R}, +) \to (\mathbb{R}^+, \cdot)$, con $f(x) = e^x$ es un isomorfismo y $f^{-1}(x) = Ln(x)$.*
2. *$f : (\mathbb{Z}, +) \to (\mathbb{Z}_m, +)$, con $f(x) = [x]$ es un epimorfismo.*
3. *Para definir un morfismo de grupos desde un grupo cíclico $(G =< a >, *)$ a un grupo $(G', \#)$, $f : G \to G'$, basta definir la imagen del generador de G. Observemos que dicha imagen $f(a)$ será un elemento cualquier de G' en el caso de orden infinito. En el caso finito de orden n, tenemos que $f(a)^n = e'$ de donde se deduce que el orden de $f(a)$ debe ser un divisor de n.*

   Si f es inyectivo (es decir, monomorfismo) entonces el orden de un elemento coincide con el orden de su imagen (ver ejercicios). Luego, en este caso, ord a = ord $f(a)$.

   Por otro lado, f es un epimorfismo si, y sólo si, $f(a)$ es un generador de G'. En efecto, si $y \in G'$, existe un $x \in G$ tal que $y = f(x)$. Es decir, $y = f(a^s)$ para algún $s \in \mathbb{Z}$. Por ser f morfismo tenemos que $y = f(a)^s$ lo que justifica que $G' =< f(a) >$. Recíprocamente, si $f(a)$ es un generador de G' entonces f es sobreyectiva.

   Si ambos grupos son cíclicos y del mismo orden, el morfismo será biyectivo, (es decir, será un isomorfismo) si, y sólo si, $f(a)$ es un generador de G'.

   En particular, todo grupo cíclico infinito es isomorfo a $(\mathbb{Z}, +)$. Y, todo grupo cíclico de cardinal n es isomorfo a $(\mathbb{Z}_n, +)$.
4. *El morfismo de grupos $f : (\mathbb{Z}_4, +) \to (\mathbb{Z}_5^*, \cdot)$, con $f(1) = 2$ es un isomorfismo.*
5. *Sea $(G, *)$ un grupo cíclico de cardinal infinito. El morfismo $f : (\mathbb{Z}, +) \to (G, *)$, $f(1) = g$ con g generador de G es un isomorfismo.*
6. *Sea $(G, *)$ un grupo cíclico de cardinal n y generador g. El morfismo $f : (\mathbb{Z}_n, +) \to (G, *)$, dado por $f(1) = g$, es un isomorfismo.*
7. *El grupo $(\mathbb{Z}_4, +)$ no es isomorfo al grupo producto $(\mathbb{Z}_2 \times \mathbb{Z}_2, +)$, que se llama grupo de Klein. Este grupo es conmutativo, pero no cíclico, pues sus elementos tienen orden 1 ó 2.*
8. *$(\mathbb{Q}^*, \cdot)$ y $(\mathbb{Z}, +)$ no son isomorfos, ya que el orden de -1 en $\mathbb{Q}^*$ es 2, mientras que en $\mathbb{Z}$ ningún elemento tiene ese orden.*
9. *Si f es un isomorfismo, ord $(f(x))$ = ord (x), para todo $x \in G$.*