Segundo seminario de estructuras algebráicas

Aitor Moreno Rebollo y Andoni Latorre Galarraga

18/03/2021

EJERCICIO 1

Dar explícitamente todos los subgrupos de $\mathbb{Z}/n\mathbb{Z}$ para los siguientes valores de n, y decir a qué grupos son isomorfos los respectivos cocientes.

Recordemos antes de empezar, que los subgrupos de $\mathbb{Z}/n\mathbb{Z}$ son de la forma $r\mathbb{Z}/n\mathbb{Z}$, con $r|n$.

b) $n = 8$. Los divisores positivos de 8 son 1, 2, 4 y el propio 8. Por tanto los subgrupos son $\mathbb{Z}/8\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}, \overline{7}\}$, $2\mathbb{Z}/8\mathbb{Z} = \{\overline{0}, \overline{2}, \overline{4}, \overline{6}\}$, $4\mathbb{Z}/8\mathbb{Z} = \{\overline{0}, \overline{4}\}$, $8\mathbb{Z}/8\mathbb{Z} = \{\overline{0}\}$. Aplicamos el segundo teorema de isomorfía de grupos, para ver a qué son isomorfos los respectivos cocientes (se pueden tomar, por ser normal todo subgrupo de un grupo abeliano).
$\frac{\mathbb{Z}/8\mathbb{Z}}{\mathbb{Z}/8\mathbb{Z}} \simeq \mathbb{Z}/\mathbb{Z}$
$\frac{\mathbb{Z}/8\mathbb{Z}}{2\mathbb{Z}/8\mathbb{Z}} \simeq \mathbb{Z}/2\mathbb{Z}$
$\frac{\mathbb{Z}/8\mathbb{Z}}{4\mathbb{Z}/8\mathbb{Z}} \simeq \mathbb{Z}/4\mathbb{Z}$
$\frac{\mathbb{Z}/8\mathbb{Z}}{8\mathbb{Z}/8\mathbb{Z}} \simeq \mathbb{Z}/8\mathbb{Z}$

c) $n = 10$. Los divisores positivos de 10 son 1, 2, 5, y el propio 10. Por tanto los subgrupos son $\mathbb{Z}/10\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}, \overline{7}, \overline{8}, \overline{9}\}$, $2\mathbb{Z}/10\mathbb{Z} = \{\overline{0}, \overline{2}, \overline{4}, \overline{6}, \overline{8}\}$, $5\mathbb{Z}/10\mathbb{Z} = \{\overline{0}, \overline{5}\}$, $10\mathbb{Z}/10\mathbb{Z} = \{\overline{0}\}$. Al igual que en el apartado anterior, aplicamos el segundo teorema de isomorfía de grupos para ver los cocientes.
$\frac{\mathbb{Z}/10\mathbb{Z}}{\mathbb{Z}/10\mathbb{Z}} \simeq \mathbb{Z}/\mathbb{Z}$
$\frac{\mathbb{Z}/10\mathbb{Z}}{2\mathbb{Z}/10\mathbb{Z}} \simeq \mathbb{Z}/2\mathbb{Z}$
$\frac{\mathbb{Z}/10\mathbb{Z}}{5\mathbb{Z}/10\mathbb{Z}} \simeq \mathbb{Z}/5\mathbb{Z}$
$\frac{\mathbb{Z}/10\mathbb{Z}}{10\mathbb{Z}/10\mathbb{Z}} \simeq \mathbb{Z}/10\mathbb{Z}$

EJERCICIO 2

Dadas las permutaciones siguientes σ, τ de Σ_n, dar la descomposición en producto de ciclos disjuntos de $\sigma, \tau, \sigma\tau, \tau\sigma$, y dar el orden de cada una de las cuatro permutaciones y decir si son permutaciones pares o impares, así como sus respectivos inversos. Decir cuáles de ellas son conjugadas en Σ_n y, cuando x, y sean conjugadas, encontrar una permutación ϵ tal que $x^\epsilon = y$.

b) $n = 5$ y

$$(1)\sigma = 3,\ (2)\sigma = 5,\ (3)\sigma = 1,\ (4)\sigma = 4,\ (5)\sigma = 2$$
$$(1)\tau = 5,\ (2)\tau = 3,\ (3)\tau = 2,\ (4)\tau = 1,\ (5)\tau = 4$$

es decir, $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 1 & 4 & 2 \end{pmatrix}$, y $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 2 & 1 & 4 \end{pmatrix}$
Por tanto, $\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 5 & 1 & 3 \end{pmatrix}$, y $\tau\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 5 & 3 & 4 \end{pmatrix}$.
Veamos su descomposición en ciclos disjuntos:
$\sigma = (1\ 3)(2\ 5)(4) = (1\ 3)(2\ 5)$
$\tau = (1\ 5\ 4)(2\ 3)$
$\sigma\tau = (1\ 2\ 4)(3\ 5)$
$\tau\sigma = (1\ 2)(3\ 5\ 4)$
Veamos ahora los órdenes (sabiendo que el orden de una permutación cualquiera de Σ_n es el mínimo común múltiplo de los órdenes de cada uno de los ciclos disjuntos en que se descompone):
$o(\sigma) = 2$
$o(\tau) = 6$
$o(\sigma\tau) = 6$

$o(\tau\sigma) = 6$
Veamos ahora las signaturas:
$\sigma = (1\ 3)(2\ 5) \Longrightarrow sig(\sigma) = 1$ (es par).
$\tau = (1\ 5\ 4)(2\ 3) = (4\ 5)(5\ 1)(2\ 3) \Longrightarrow sig(\tau) = -1$ (es impar).
$\sigma\tau = (1\ 2\ 4)(3\ 5) = (4\ 2)(2\ 1)(3\ 5) \Longrightarrow sig(\sigma\tau) = -1$ (es impar).
$\tau\sigma = (1\ 2)(3\ 5\ 4) = (1\ 2)(4\ 5)(5\ 3) \Longrightarrow sig(\tau\sigma) = -1$ (es impar).
Veamos los inversos:
$\sigma^{-1} = (1\ 3)(2\ 5)(4) = (1\ 3)(2\ 5) = \sigma$
$\tau^{-1} = (1\ 4\ 5)(2\ 3) = (4\ 5\ 1)(3\ 2)$
$(\sigma\tau)^{-1} = (1\ 4\ 2)(3\ 5) = (4\ 2\ 1)(5\ 3)$
$(\tau\sigma)^{-1} = (1\ 2)(3\ 4\ 5) = (2\ 1)(4\ 5\ 3)$
Veamos ahora cuáles de ellos son conjugados entre sí:
Sabemos que dos permutaciones están relacionadas por conjugación si y solo si tienen el mismo tipo. Por tanto, las permutaciones $\tau, \sigma\tau$, y $\tau\sigma$ están relacionadas por conjugación. Vamos a hallar una permutación ϵ_1 tal que $\tau^{\epsilon_1} = \sigma\tau$:

$$\epsilon_1 = \begin{pmatrix} 1 & 5 & 4 & 2 & 3 \\ 1 & 2 & 4 & 3 & 5 \end{pmatrix} = (1)(2\ 3\ 5)(4) = (2\ 3\ 5)$$

Por tanto, $\tau^{\epsilon_1} = \sigma\tau \Longleftrightarrow \tau = (\sigma\tau)^{{\epsilon_1}^{-1}}$, y ${\epsilon_1}^{-1} = (2\ 5\ 3) = (5\ 3\ 2)$.
Vamos a hallar ahora una permutación ϵ_2 tal que $\tau^{\epsilon_2} = \tau\sigma$:

$$\epsilon_2 = \begin{pmatrix} 1 & 5 & 4 & 2 & 3 \\ 3 & 5 & 4 & 1 & 2 \end{pmatrix} = (1\ 3\ 2)(4)(5) = (1\ 3\ 2)$$

Por tanto, $\tau^{\epsilon_2} = \tau\sigma \Longleftrightarrow \tau = (\tau\sigma)^{{\epsilon_2}^{-1}}$, y ${\epsilon_2}^{-1} = (1\ 2\ 3) = (2\ 3\ 1)$.
Podría deducirse la relación de conjugación entre $\sigma\tau$ y $\tau\sigma$ igualando a partir de las dos relaciones que ya tenemos. Sin embargo, volvemos a hacer el mismo proceso:
Vamos a hallar una permutación ϵ_3 tal que $\sigma\tau^{\epsilon_3} = \tau\sigma$:

$$\epsilon_3 = \begin{pmatrix} 1 & 2 & 4 & 3 & 5 \\ 3 & 5 & 4 & 1 & 2 \end{pmatrix} = (1\ 3)(2\ 5)(4) = (1\ 3)(2\ 5)$$

Por tanto, $\sigma\tau^{\epsilon_3} = \tau\sigma \Longleftrightarrow \sigma\tau = (\tau\sigma)^{{\epsilon_3}^{-1}}$, y ${\epsilon_3}^{-1} = \epsilon_3$.

EJERCICIO 3

Dar las clases de conjugación en los grupos diédricos D_5 y D_6.

En un grupo diédrico de orden $2n$, hay dos tipos de elementos:
Tipo 1: $a^i b$, $0 \leqslant i < n$
Tipo 2: a^i, $0 \leqslant i < n$
Vamos a conjugar cada tipo de elemento con los demás, y así vemos qué elementos están relacionados entre sí por conjugación.
Démonos cuenta primero de las siguientes igualdades:
(i) $b^2 = 1 \Longrightarrow b = b^{-1}$
(ii) $a^b = a^{-1} \overset{\text{(i)}}{\Longrightarrow} bab = a^{-1} \overset{\text{(i)}}{\Longrightarrow} ab = ba^{-1} \Longrightarrow ba = a^{-1}b$. Más generalmente, $(a^i)^b = a^{-i} \Longrightarrow ba^i b = a^{-i} \Longrightarrow a^i b = ba^{-i} \Longrightarrow ba^i = a^{-i}b$, $i \in \mathbb{Z}$.
(iii) $(a^i b)^{-1} = b^{-1}a^{-i} \overset{(i)}{=} ba^{-i} \overset{(ii)}{=} a^i b$
(iv) $a^n = 1 \Longrightarrow a^{-n} = 1^{-1} = 1 \Longrightarrow 1 = a^n = a^{-n} = a^{-n-i+i} = a^{i-n}a^{-i} \Longrightarrow a^{-i} = a^{n-i}$, $0 \leqslant i < n$, $0 < n - i \leqslant n$
Conjuguemos:
Tipo 1 con tipo 1: $(a^i b)^{a^k b} = (a^k b)^{-1} a^i b a^k b \overset{\text{(iii)}}{=} a^k b a^i b a^k b = a^k b a^i (b a^k b) \overset{\text{(ii)}}{=} a^k b a^i a^{-k} = a^k b a^{i-k} = a^k (b a^{i-k}) \overset{\text{(ii)}}{=} a^k a^{k-i} b = a^{2k-i} b$, es decir, $(a^i b)^{a^k b} = a^{2k-i} b$, $0 \leqslant i, k < n$
Tipo 1 con tipo 2: $(a^i b)^{a^k} = (a^k)^{-1} a^i b a^k = a^{-k} a^i b a^k = a^{i-k} b a^k = (a^{i-k} b) a^k \overset{\text{(ii)}}{=} b a^{k-i} a^k = b a^{2k-i} \overset{\text{(ii)}}{=} a^{i-2k} b$,

es decir, $(a^ib)^{a^k} = a^{i-2k}b$, $0 \leqslant i, k < n$
Tipo 2 con tipo 1: $(a^i)^{a^kb} = (a^kb)^{-1}a^ia^kb \overset{\text{(iii)}}{=} a^kba^ia^kb = a^kba^{i+k}b = (a^kb)a^{i+k}b \overset{\text{(ii)}}{=} ba^{-k}a^{i+k}b = ba^ib \overset{\text{(ii)}}{=} a^{-i}$,
es decir, $(a^i)^{a^kb} = a^{-i} \overset{\text{(iv)}}{=} a^{n-i}$, $0 < n - i \leqslant n$
Tipo 2 con tipo 2: $(a^i)^{a^k} = (a^k)^{-1}a^ia^k = a^{-k}a^ia^k = a^i$, $0 \leqslant i, k < n$
En resumen, si $\overset{D_n}{\sim}$ es la relación de equivalencia 'estar relacionado por conjugación', entonces tenemos que:

$$\begin{cases} a^ib \overset{D_n}{\sim} a^{2k-i}b, & 0 \leqslant i, k < n \\ a^ib \overset{D_n}{\sim} a^{i-2k}b, & 0 \leqslant i, k < n \\ a^i \overset{D_n}{\sim} a^{n-i}, & 0 < n - i \leqslant n \end{cases}$$

Este esquema de relaciones por conjugación nos da una manera constructiva de encontrar las clases de conjugación en un grupo diédrico cualquiera de orden $2n$. Veamos ahora las clases de conjugación en los casos particulares $n = 5$ y $n = 6$:
En D_5:

$$\begin{cases} 1 \\ a \overset{D_5}{\sim} a^4 \\ a^2 \overset{D_5}{\sim} a^3 \\ ab \overset{D_5}{\sim} a^2b \overset{D_5}{\sim} b \overset{D_5}{\sim} a^3b \overset{D_5}{\sim} a^4b \end{cases}$$ y estas son las 4 clases de conjugación.

En D_6:

$$\begin{cases} 1 \\ a \overset{D_6}{\sim} a^5 \\ a^2 \overset{D_6}{\sim} a^4 \\ a^3 \\ ab \overset{D_6}{\sim} a^3b \overset{D_6}{\sim} a^5b \\ a^2b \overset{D_6}{\sim} a^4b \overset{D_6}{\sim} b \end{cases}$$ y estas son las 6 clases de conjugación.

EJERCICIO 4

En la primera relación de problemas vimos que en un grupo, dos elementos conjugados tienen el mismo orden. Demostrar que el recíproco es falso dando un contraejemplo en un grupo simétrico.

Tenemos que encontrar dos permutaciones que tengan tipo distinto (dos permutaciones son conjugadas si y solo si tienen el mismo tipo), pero mismo orden. Es decir, que los mínimos comunes múltiplos de los ciclos disjuntos en que se descompone cada permutación sean iguales.
Tomamos, por ejemplo, en Σ_{69}:

$$\sigma = (1\ 2)(3\ 4\ 5)$$
$$\tau = (1\ 2)(3\ 4)(5\ 6\ 7)$$

Estas dos permutaciones no son conjugadas, pero tienen el mismo orden ($o(\sigma) = o(\tau) = 6$).

EJERCICIO 5

Probar que si $|G| = p^m$, con p primo y $m \in \mathbb{N}$, entonces $Z(G) \neq \{1\}$.

Trivial por T$^{\text{a}}$ (2.39).
Basta considerar la ecuación de clases, y, sabiendo que $|Cl_G(S)| = |G : N_G(S)|$, entonces el sumatorio de la ecuación de clases es múltiplo de p. Por tanto $|Z(G)|$ es múltiplo de p y por tanto $Z(G) \neq \{1\}$.

EJERCICIO 6

Demostrar que si $H_1, H_2 \trianglelefteq G$, entonces $H_1 \cap H_2 \trianglelefteq G$.

$\forall h_i \in H_i,\ gh_i \in H_i g \quad \forall g \in G$, por ser H_i normales en G, y por tanto, $\forall h \in H_1 \cap H_2,\ gh \in (H_1 \cap H_2)g \quad \forall g \in G$.
Recíprocamente, $\forall h_i \in H_i,\ h_i g \in g H_i \quad \forall g \in G$, y entonces $\forall h \in H_1 \cap H_2,\ hg \in g(H_1 \cap H_2) \quad \forall g \in G$. Por tanto, $(H_1 \cap H_2)^g = H_1 \cap H_2 \quad \forall g \in G$, y por tanto $H_1 \cap H_2 \trianglelefteq G$.

EJERCICIO 7

Demostrar que si $H \leqslant G$ y $|G : H| = 2$, entonces H es subgrupo normal de G.

Por definición, $|G : H| = |C_d(H, G)| = |C_i(H, G)|$, donde $C_d(H, G) = \{gH \mid g \in G\}$ y $C_i(H) = \{Hg \mid g \in G\}$. Trabajaremos con coclases a izquierda. Por tanto, $|G : H| = 2$ supone que $C_i(H) = \{H, g_1 H\}$, pues una de las coclases es la coclase trivial necesariamente. Además, esto construye una partición de G. Es también evidente que $g_1 H \neq H \iff g_1 \notin H$, y esto para todo representante de $g_1 H$, es decir, para todo elemento no trivial de $g_1 H$. Veamos ahora que $H^g = H\ \forall g \in G$. Dos casos:
i) Si $g \in H$, entonces es trivial que $H^g = H$.
ii)Si $g \notin H$, entonces $g \in g_1 H$. Primero, es trivial que $\forall h \in H,\ \forall g \in G,\ gh \in H \iff g \in H$. Análogamente, $\forall h \in H,\ \forall g \in G,\ hg \in H \iff g \in H$. Entonces, $g \notin H \iff g \in g_1 H \iff gH = g_1 H$. Ahora, $\forall h \in H,\ gh \notin H$. Y por tanto, si consideramos ahora las coclases a derecha ($C_d(H, G) = \{H, Hg_2\}$), entonces $gh \in Hg_2 \implies \exists h_1 \in H$ tal que $gh = h_1 g_2$, y por tanto, para cada $g \in g_1 H,\ \forall h \in H,\ gH \subseteq Hg_2$. Análogamente, $\forall g \in Hg_2,\ \forall h \in H,\ Hg \subseteq g_1 H$, y por tanto, $Hg = Hg_1 = g_2 H = gH\ \forall g \in g_1 H \iff g \notin H$. Y por tanto $H^g = H\ \forall g \in G$, y H es normal en G.

EJERCICIO 8

Demostrar que en el grupo de cuaterniones Q_8 de la relación anterior, el subgrupo $H =< i >$ es normal en G.

Recordemos antes de empezar, que $Q_8 =< i, j, k \mid ij = k, jk = i, ki = j, i^2 = j^2 = k^2 \overset{\text{not}}{=} m >$, y que $Q_8 = \{1, i, j, k, m, mi, mj, mk\}$. Veremos que $< i > \leqslant Q_8$ viendo que $\forall x \in Q_8,\ i^x \in < i >$, ya que entonces trivialmente todo elemento de $< i >$ cumple que al conjugarlo con elementos de Q_8, pertenecen al propio $< i >$ (por ser i el generador). Entonces:
$i^1 = 1^{-1} i 1 = i$
$i^i = i^{-1} i i = i$
$i^j = j^{-1} i j = j^{-1} k = j^{-1} j i^{-1} = i^{-1}$
$\quad\quad\quad\ \downarrow \quad\quad\ \downarrow$
$\quad\quad\ ij = k \quad\ \downarrow$
$\quad\quad\quad ki = j \implies k = j i^{-1}$
$i^k = k^{-1} i k = j^{-1} k = i^{-1}$
$\quad\quad\quad\ \downarrow \quad\quad\ \downarrow$
$ij = k \implies k^{-1} i = j^{-1}$
$\quad\quad\quad\ \downarrow$
$\quad\quad ki = j \implies j^{-1} k = i^{-1}$
$i^m = m^{-1} i m = i^{-2} i i^2 = i$
$\quad\quad\quad\ \downarrow$
$\quad i^2 = m \implies i^{-2} = m^{-1}$
$i^{mi} = (mi)^{-1} i m i = i^{-1} m^{-1} i m i = i^{-1} i^{-2} i i^2 i = i$
$i^{mj} = (mj)^{-1} i m j = j^{-1} m i m j = j^{-1} i^{-2} i i^2 j = j^{-1} i j = i^j = i^{-1}$
$i^{mk} = (mk)^{-1} i m k = k^{-1} m^{-1} i m k = k^{-1} i^{-2} i i^2 k = k^{-1} i k = i^k = i^{-1}$

EJERCICIO 9

Sea G un grupo ¿Cuál es la condición necesaria y suficiente para que la aplicación

$$\begin{array}{rccc} f: & G & \longrightarrow & G \\ & x & \rightsquigarrow & x^{-1} \end{array}$$

sea un automorfismo?

Queremos que $f(x_1x_2) = f(x_1)f(x_2)$, para que sea automorfismo. En nuestro caso, $f(x_1x_2) = (x_1x_2)^{-1} = x_2^{-1}x_1^{-1} = f(x_2)f(x_1)$, entonces queremos que $f(x_2)f(x_1) = f(x_1)f(x_2)\ \forall x_i \in G$. Como $f(x_i)$ son elementos de G, y f es claramente biyectiva, la condición necesaria y suficiente es que G sea abeliano.

EJERCICIO 10

Sea G un grupo.

a) Demostrar que $\mathrm{Aut}(G)$ es un subgrupo de Σ_G

b) Si $a \in G$, demostrar que la aplicación $c_a: G \longrightarrow G$ definida por $c_a(x) = x^a$ es un automorfismo de G.

c) Demostrar que la aplicación $f: G \longrightarrow \mathrm{Aut}(G)$ definida por $f(a) = c_a$ es un homomorfismo. ¿Cuál es su núcleo?

d) Deducir del apartado anterior que $\{c_a \mid a \in G\}$ es un subgrupo de $\mathrm{Aut}(G)$.

e) Demostrar que el subgrupo del apartado anterior es, de hecho, un subgrupo normal.

a) Trivial por Tª (3.21). La demostración es la siguiente:
$1 \in \mathrm{Aut}(G)$, luego $\mathrm{Aut}(G) \neq \emptyset$. Además, si $f, g \in \mathrm{Aut}(G)$, entonces $g^{-1} \in \mathrm{Aut}(G)$ y $fg \in \mathrm{Aut}(G)$. Por tanto, $\mathrm{Aut}(G)$ es un subgrupo de Σ_G, y en consecuencia tiene estructura de grupo con respecto a la operación composición de aplicaciones. ■
b) $c_a(x_1) = c_a(x_2) \iff x_1^a = x_2^a \iff x_1 = x_2$, por tanto está bien definida y es inyectiva. Es trivialmente suprayectiva, pues, si $x \in G$, consideramos $x^{a^{-1}}$, y trivialmente $c_a(x^{a^{-1}}) = (x^{a^{-1}})^a = x^1 = x$, y por tanto $\exists x' = x^{a^{-1}} \in G$ tal que $c_a(x') = x$. Finalmente, $c_a(x_1x_2) = (x_1x_2)^a = a^{-1}x_1x_2a = a^{-1}x_1 1 x_2 a = a^{-1}x_1aa^{-1}x_2a = (a^{-1}x_1a)(a^{-1}x_2a) = x_1^a x_2^a = c_a(x_1)c_a(x_2)$, por tanto es automorfismo.
c) Si tomamos $a, b \in G$, $a = b$, entonces necesariamente $a^{-1} = b^{-1}$ y por tanto, conjugar por a o por b es la misma operación, es decir, $c_a = c_b$. Por tanto está bien definida. Veamos que es homomorfismo:
$f(ab) = c_{ab}: G \longrightarrow G$. Para cada $x \in G$, $(f(ab))(x) = c_{ab}(x) = x^{ab} = (ab)^{-1}xab = b^{-1}a^{-1}xab = b^{-1}x^a b = (x^a)^b = c_a(x)^b = c_b(c_a(x)) = (c_b \circ c_a)(x) = (f(a)f(b))(x)$, por tanto es homomorfismo. Veamos ahora el núcleo:
$ker f = \{a \in G \mid f(a) = c_a = 1_{\mathrm{Aut}(G)} = Id_G\}$, es decir, son los elementos a de G tales que $\forall x \in G$, $c_a(x) = x^a = x$. Es decir, tales que $a^{-1}xa = x \iff xa = ax\ \forall x \in G$. $\{a \in G \mid xa = ax\ \forall x \in G\} = Z(G)$. Es decir, $ker f = Z(G)$.
d) Trivial por Prop (2.21). Básicamente, la imagen por un homomorfismo de un subgrupo es un subgrupo, y $G \leqslant G \Longrightarrow f(G) \leqslant \mathrm{Aut}(G)$, pues f es homomorfismo.
e) Llamamos $H = f(G) = \{c_a \mid a \in G\}$. Hay que ver que $\forall c_a \in H$, $c_a^g \in H\ \forall g \in \mathrm{Aut}(G)$. Es evidente que, para cada automorfismo, su inverso es también un automorfismo ($\mathrm{Aut}(G)$ es un grupo). Entonces, $\forall x \in G \quad (g^{-1} \circ c_a \circ g)(x) = g^{-1}(c_a(g(x))) = g^{-1}(g(x)^a) = g^{-1}(a^{-1}g(x)a) = g^{-1}(a^{-1})g^{-1}(g(x))g^{-1}(a) = g^{-1}(a)^{-1}g^{-1}(g(x))g^{-1}(a) = g^{-1}(a)^{-1}xg^{-1}(a) = x^{g^{-1}(a)} \quad \forall g \in \mathrm{Aut}(G)$, y como $g^{-1}(a) = b \in G$, entonces tenemos que $c_a^g = c_b$, para cierto $b \in G$, y se tiene el resultado.

EJERCICIO 11

Sea $f: G \longrightarrow G'$ un homomorfismo de grupos.

a) Si $H' \trianglelefteq G'$, probar que $f^{-1}(H') \trianglelefteq G$.

b) Si f es suprayectiva y $H \trianglelefteq G$, probar que $f(H) \trianglelefteq G'$ ¿Sigue siendo cierto el resultado si eliminamos

la condición de que f sea suprayectiva?

a) Por el Tª (2.21), $f^{-1}(H') \leqslant G$, por tanto es subgrupo. Veamos ahora que es normal. Vamos a ver que $\forall h \in f^{-1}(H'),\ h^g \in f^{-1}(H')\ \ \forall g \in G$. Efectivamente, si $h \in f^{-1}(H')$, entonces $f(h^g) = f(g^{-1}hg) = f(g^{-1})f(h)f(g) = f(g)^{-1}f(h)f(g) = f(h)^{f(g)} \in H'$, por ser $H' \trianglelefteq G'$ y $f(h) \in H'$. Por tanto, $f(h^g) \in H'\ \forall g \in G,\ \forall h \in f^{-1}(H') \Longrightarrow h^g \in f^{-1}(H')\ \forall g \in G,\ \forall h \in f^{-1}(H')$, y por tanto se tiene que $f^{-1}(H') \trianglelefteq G$.
b) Por el Tª (2.21), $f(H) \leqslant G'$, por tanto es subgrupo. Veamos ahora que es normal. Vamos a ver que $\forall h' \in f(H),\ h'^{g'} \in f(H)\ \forall g' \in G'$. Por ser $h' \in f(H),\ \exists h \in H$, tal que $f(h) = h'$. Entonces, $h'^{g'} = f(h)^{g'} =$
$\downarrow$
Por ser f suprayectiva, $\exists g \in G$ tal que $f(g) = g'$
$f(h)^{f(g)} = f(g)^{-1}f(h)f(g) = f(g^{-1})f(h)f(g) = f(g^{-1}hg) = f(h^g) \in f(H)$, por ser $H \trianglelefteq G$, y $h \in H$.
Si f no es suprayectiva, entonces no necesariamente se puede mantener h' en H' al conjugar por elementos de G', pues la condición de que H sea normal en G no es suficientemente fuerte (podrían haber $g' \in G'$ tales que $\nexists g \in G,\ f(g) = g'$ y entonces es posible que $h'^{g'} \notin f(H)$).

EJERCICIO 12

Demostrar que si G es un grupo abeliano y $n \in \mathbb{Z}$, entonces la aplicación $f : G \longrightarrow G$ definida por $f(x) = x^n$ es un homomorfismo. ¿Es siempre un automorfismo?

Esta aplicación está bien definida trivialmente. Veamos que es un homomorfismo: $f(x_1x_2) = (x_1x_2)^n = \underbrace{(x_1x_2)(x_1x_2)\cdots(x_1x_2)}_{\text{n veces}} \underset{\text{G abeliano}}{\downarrow} = x_1\cdots x_1x_2\cdots x_2 = x_1^n x_2^n = f(x_1)f(x_2)$, por tanto es homomorfismo.
No siempre es automorfismo. Por ejemplo, si $n = |G|$ (si G es finito), entonces $f(x) = x^{|G|} = 1\ \forall x \in G$, y por tanto no es suprayectiva, pues $f(G) = \{1\} \neq G$ (si G es no trivial).

EJERCICIO 13

Probar que si G es un grupo finito cuyo único automorfismo es la identidad, entonces

$$G \simeq \mathbb{Z}/2\mathbb{Z} \times \cdots \times \mathbb{Z}/2\mathbb{Z}$$

Tenemos que $\mathrm{Aut}(G) = \{Id_G = 1_{\Sigma_G}\}$. Sabemos que $\mathrm{Int}(G) \trianglelefteq \mathrm{Aut}(G)$, pero el único subgrupo posible es el trivial. Por tanto $\mathrm{Int}(G) = \{1_{\Sigma_G}\}$. Además, $G/Z(G) \simeq \mathrm{Int}(G)$, y por tanto $G/Z(G) = \{1\}$. Es decir, todo elemento de G está en el centro, y por tanto G es abeliano.
Por el ejercicio 9, la aplicación

$$\begin{array}{rccc} f: & G & \longrightarrow & G \\ & x & \rightsquigarrow & x^{-1} \end{array}$$

es un automorfismo. Pero como el único automorfismo es la identidad, entonces $f = Id_G = 1_{\Sigma_G}$. Es decir, $\forall x \in G \setminus \{1\},\ x = Id_G(x) = f(x) = x^{-1} \Longrightarrow x^2 = 1 \Longrightarrow o(x) = 2$. Por el ejercicio 2 de la relación anterior, concluimos. Esta es la resolución de dicho ejercicio:

Demostrar que un grupo G en el que todo elemento distinto del neutro es de orden 2 es abeliano y que si además G es finito, entonces $G \simeq \frac{\mathbb{Z}}{2\mathbb{Z}} \times \cdots \times \frac{\mathbb{Z}}{2\mathbb{Z}}$.

$\forall a \in G$, como $o(a) = 2$, $aa = 1 \Leftrightarrow a\underbrace{aa^{-1}}_{1} = 1a^{-1} = a^{-1} \Leftrightarrow a^{-1} = a$. Consideramos ahora el conmutador de dos elementos cualesquiera $a, b \in G$ y veamos que es la identidad:
$[a,b] = a^{-1}b^{-1}ab \underset{\left\{\begin{smallmatrix} a^{-1}=a \\ b^{-1}=b \end{smallmatrix}\right.}{\downarrow} = abab = (ab)(ab) = (ab)^2 = 1$, por ser $ab \in G$, $(o(ab) = 2)$.Por tanto el grupo G es

abeliano.
$\forall g \in G$, $o(g) = 2 \Rightarrow g^2 = 1 \Rightarrow < g >= \{1, g\}$, y, además, $< g > \trianglelefteq G$, (pues, por ser G abeliano, todos sus subgrupos son normales). Si G es finito, $G = \{g_1, \cdots, g_n\}$. Consideramos ahora el subconjunto $K \subseteq G$, que construiremos de la siguiente manera:
Primero, $K = \{g_1, g_2\}$. Ahora, para cada $g_i \in G$, si $g_i \notin < K >$, entonces lo añadimos al conjunto K y continuamos con g_{i+1}. Repetimos este proceso hasta obtener un conjunto $K = \{g_{k_1} = g_1, g_{k_2} = g_2, g_{k_3}, \cdots, g_{k_l}\}$, tal que $G =< K >$. Este proceso es posible por ser G finito. Ahora, para cada $g_{k_i} \in K$, consideramos $< g_{k_i} >$. Trivialmente $G =< g_{k_1} >< g_{k_2} > \cdots < g_{k_l} >$ pues, si $g_i \in G$, entonces $g_i \in < K >$. La intersección entre ellos es trivial y son normales en G. Por tanto G queda construido mediante un producto directo interno. Sabemos entonces que $G \simeq < g_{k_1} > \times < g_{k_2} > \times \cdots \times < g_{k_l} >$, donde hablamos ahora de producto cartesiano. Como además, se satisface que $< g_{k_i} > \simeq \frac{\mathbb{Z}}{2\mathbb{Z}}$, $\forall i,\ 1 \leqslant i \leqslant l$, por ser $< g_{k_i} >$ grupos cíclicos de orden 2, entonces se tiene que $G \simeq \frac{\mathbb{Z}}{2\mathbb{Z}} \times \cdots \times \frac{\mathbb{Z}}{2\mathbb{Z}}$.