Ejercicios GyA - Cap. 4

Jose Antonio Lorencio Abril

4 Grupos

4.1 Definiciones y ejemplos

4.1.1 Construir la tabla de multiplicación de los grupos aditivos y de unidades de $\mathbb{Z}_7, \mathbb{Z}_{16}$, $GL_2(\mathbb{Z}_2)$.

$(\mathbb{Z}_7, +)$:

0	**1**	**2**	**3**	**4**	**5**	**6**
1	2	3	4	5	6	0
2	3	4	5	6	0	1
3	4	5	6	0	1	2
4	5	6	0	1	2	3
5	6	0	1	2	3	4
6	0	1	2	3	4	5

$(\mathbb{Z}_7, \cdot)$:

	1	**2**	**3**	**4**	**5**	**6**
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

Para $(\mathbb{Z}_{12}, +/\cdot)$ se hace igual.
$(GL_2(\mathbb{Z}_2), +/\cdot)$ también, pero con matrices. Bastante pesado de hacer, pero no tiene dificultad.

4.1.2 Sea G un grupo. Probar que son equivalentes:

(1) G es abeliano
(2) $(ab)^2 = a^2b^2 \ \forall a, b \in G$
(3) $(ab)^{-1} = a^{-1}b^{-1} \ \forall a, b \in G$
(4) $(ab)^n = a^n b^n \ \forall n \in \mathbb{N}, \ \forall a, b \in G$
'1 $\implies$ 2' $(ab)^2 = (ab)(ab) = a(ba)b = a(ab)b = (aa)(bb) = a^2b^2$
'2 $\implies$ 1' $a(ba)b = (ab)^2 = a^2b^2 = a(ab)b$
Como todo elemento es cancelativo, entonces $(ba)b = (ab)b$, y cancelando b, $ba = ab$
'1 $\implies$ 3' Por el lema 4.2, sabemos que $(ab)^{-1} = b^{-1}a^{-1} \overset{abeliano}{=} a^{-1}b^{-1}$
'3 $\implies$ 1' $(ba)^{-1} = b^{-1}a^{-1} = (ab)^{-1}$. Entonces

$$(ab)(ab)^{-1} = e = (ba)(ab)^{-1} \overset{cancelativa}{\implies} ab = ba$$

'1 $\implies$ 4' Inducción en n.

$n = 1$: Obvio, $ab = ab$

Supongamos se verifica para $n-1$ y la hipótesis de inducción:

$$(ab)^n = (ab)^{n-1+1} = (ab)^{n-1}(ab) = a^{n-1}b^{n-1}ab \overset{abeliano}{=} a^{n-1}ab^{n-1}b = a^n b^n$$

'4 $\implies$ 1' Es obvio que 4 $\implies$ 2, y 2 $\implies$ 1 ya lo hemos visto.

4.1.3 Desmotrar que si G es un grupo tal que $g^2 = 1$, $\forall g \in G$, entonces G es abeliano.

Sean $a, b \in G$, entonces $a^2 = 1 = b^2 \implies a^{-1} = a$, $b^{-1} = b$. Además, $abab = (ab)^2 = 1 \implies a^{-1}ababb^{-1} = a^{-1}b^{-1} \implies ba = a^{-1}b^{-1} = ab$.

4.2 Subgrupos

4.2.2 Probar que todo grupo G de orden menor o igual a cinco es abeliano

$|G| = 1$. Entonces, $G = \{e\}$. Y así, ee es la única operación posible y G es abeliano.

$|G| = 2, 3, 5$

Entonces, por el corolario del teorema de Lagrange, G es cíclico y cualquier elemento de G distinto de 1 es un generador de G.

Entonces, si es 5. $G = \langle g \rangle = \left\{1, g, g^2, g^3, g^4\right\}$, pero esto es conmutativo, pues

$$g^i g^j = g^{i+j} = g^{j+i} = g^j g^i$$

Para 2 y 3, el mismo argumento sirve.

Queda $|G| = 4$.

Si G es cíclico, como antes, es abeliano.

Si G no es cíclico, por el teorema de Lagrange, los subgrupos de G distintos del trivial y el total tienen orden 2.

Es decir, dado $g \in G \setminus \{1\}$, tenemos que $|\langle g \rangle| = 2$. Por tanto, $g^2 = 1$.

Ahora bien, $g_1 g_2$ no puede dar 1, porque $Xg_2 = 1$, tiene solución única, y sería $g_1 = g_2$.

Tampoco puede ser $g_1 g_2 = g_2$, pues implicaría $g_1 = 1$.

Por el mismo motivo no puede ser g_1.

Es decir, $g_1 g_2 = g_3$.

Y, entonces, razonando análogamente con las demás multiplicaciones, la tabla de multiplicación queda

	1	g_1	g_2	g_3
1	1	g_1	g_2	g_3
2	g_1	1	g_3	g_2
3	g_2	g_3	1	g_1
4	g_3	g_2	g_1	1

Y es abeliano.

4.2.3 Mostrar que la unión de dos subgrupos de un grupo no es necesariamente un subgrupo. Aún más, probar que un grupo nunca puede expresarse como unión de dos subgrupos propios.

Tomando $G/\,|G| = 4$, como en el ejercicio anterior, que no sea cíclico, entonces

$$A = \langle g_1 \rangle \cup \langle g_2 \rangle = \{1, g_1, g_2\}$$

Pero $g_1 g_2 = g_3 \notin A$. Por tanto, no es un subgrupo.

Para la segunda afirmación, sea G un grupo. Supongamos que puede expresarse como unión de dos subgrupos propios. O sea

$$G = G_1 \cup G_2$$

Como son propios, quiere decir que $\exists g_1 \in G \setminus G_1$ y $\exists g_2 \in G \setminus G_2$.

Pero, dado que la unión es el total, debe ser $g_1 \in G_2$ y $g_2 \in G_1$.

Fijémonos ahora en $g_1 g_2$.

Si perteneciese a G_2, entonces tendríamos que $g_1, g_1 g_2 \in G_2$. Pero $g_1^{-1} \in G_2$, también, por lo que $g_1^{-1} g_1 g_2 = g_2 \in G_2 \#$ Esto no puede ser.

Por tanto, $g_1 g_2 \notin G_2$.

Por el mismo razonamiento, $g_1 g_2 \notin G_1$.

Lo que quiere decir que $g_1 g_2 \notin G_1 \cup G_2$

Pero $g_1 g_2 \in G \# \; G \neq G_1 \cup G_2$.

4.2.4 Para $n = 1, ..., 10$ determinar cuales de los grupos $\mathbb{Z}_n^*$ son cíclicos.

Claramente para $n = 1$ es cíclico.

$\mathbb{Z}_2^* = \{1\}$ cíclico

$\mathbb{Z}_3^* = \{1, 2\} = \langle 2 \rangle$ cíclico

$\mathbb{Z}_4^* = \{1, 3\} = \langle 3 \rangle$ cíclico

$\mathbb{Z}_5^* = \{1, 2, 3, 4\}$. $\langle 1 \rangle = \{1\}$, $\langle 2 \rangle = \{1, 2, 3, 4\}$cíclico

$\mathbb{Z}_6^* = \{1, 5\} = \langle 5 \rangle$ cíclico

$\mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$. $\langle 1 \rangle = \{1\}$, $\langle 2 \rangle = \{1, 2, 4\}$, $\langle 3 \rangle = \{1, 2, 3, 4, 5, 6\}$ cíclico

$\mathbb{Z}_8^* = \{1, 3, 5, 7\}$. $\langle 1 \rangle = \{1\}$, $\langle 3 \rangle = \{1, 3\}$, $\langle 5 \rangle = \{1, 5\}$, $\langle 7 \rangle = \{1, 7\}$ no cíclico

$\mathbb{Z}_9^* = \{1, 2, 4, 5, 7, 8\}$. $\langle 1 \rangle = \{1\}$, $\langle 2 \rangle = \{1, 2, 4, 5, 7, 8\}$cíclico

$\mathbb{Z}_{10}^* = \{1, 3, 7, 9\}$. $\langle 1 \rangle = \{1\}$, $\langle 3 \rangle = \{1, 3, 7, 9\}$ cíclico

4.2.5 Demostrar que si el grupo G no es abeliano, entonces existe un subgrupo abeliano de G que contiene estrictamente al centro $Z(G)$.

Como G no es abeliano, $\exists g \in G \setminus Z(G)$.

Consideramos $\langle \{g\} \cup Z(G) \rangle = A$.

Entonces

$$Z(G) \subsetneq A \leq G$$

Por lo que hay que ver que A es abeliano.

Para ello, basta ver que g conmuta con los elementos de $Z(G)$.

Sea $x \in Z(G)$, entonces $gx = xg$ porque $x \in Z(G)$. Y lo tenemos.

4.2.6 Calcular los centros de $GL_n(\mathbb{R})$, $GL_n(\mathbb{C})$, $SL_n(\mathbb{R})$, $SL_n(\mathbb{C})$.

$\boldsymbol{GL_n(\mathbb{R})}$: serán las matrices $A / AX = XA, \forall X \in GL_n(\mathbb{R})$.

$$AX_{ij} = \sum_{k=0}^{n} a_{ik} x_{kj}$$

$$XA_{ij} = \sum_{k=0}^{n} x_{ik} a_{kj}$$

Y deben ser iguales

$$\sum_{k=0}^{n} a_{ik}x_{kj} = \sum_{k=0}^{n} x_{ik}a_{kj}$$

Pero debe verificarse para cualquier matriz cuadrada no singular.

Podemos, por tanto, ir seleccionando matrices con todo 0 excepto $x_{1j} = 1$ y $x_{j1} = 1$ y la diagonal a 1, otra todo 0 excepto x_{2j} y x_{j2} y la diagonal a 1,... De forma que, para cada una obtendríamos las igualdades

$$a_{ii} + a_{i1} = a_{11} + a_{1i}$$

$$a_{ii} + a_{i2} = a_{22} + a_{2i}$$

$$...$$

Pero también podemos hacer $x_{1j} = 1$ y $x_{j1} = -1$,... siempre que j no sea la columna que hace que estos elementos estén en la diagonal. De aquí obtenemos

$$a_{ii} + a_{i1} = a_{11} - a_{1i}$$

$$a_{ii} + a_{i2} = a_{22} - a_{2i}$$

$$...$$

Juntando la información anterior con esta:

$$a_{11} + a_{1i} = a_{11} - a_{1i} \implies a_{1i} = -a_{1i} \implies a_{1i} = 0$$

$$a_{2i} = 0$$

$$...$$

Por lo que todos los elementos fuera de la diagonal tienen que ser 0. Por tanto, son matrices diagonales.

Pero esto no es todo, consideremos dos elementos de la diagonal $a_{ii},\ a_{jj}$. Entonces

$$AX_{ij} = a_{ii}x_{ij}$$

$$XA_{ij} = x_{ij}a_{jj}$$

Por lo que, tomando una matriz con $x_{ij} = 1$, vemos que ha de ser

$$a_{ii} = a_{jj}$$

Es decir, el centro son las matrices diagonales con el mismo escalar en toda la diagonal, o sea, de la forma aI_n.

$\boldsymbol{GL_n}\ (\mathbb{C})$: ahora tenemos que verlo en los complejos. Podemos expresarlo como

$$AX = XA \iff (A_r + iA_i)(X_r + iX_i) = (X_r + iX_i)(A_r + iA_i)$$

Separando las partes reales de las imaginarias, entonces

$$(A_r + iA_i)(X_r + iX_i) = A_rX_r + iA_rX_i + iA_iX_r - A_iX_i = (A_rX_r - A_iX_i) + i(A_rX_i + A_iX_r)$$

$$(X_r + iX_i)(A_r + iA_i) = (X_rA_r - X_iA_i) + i(X_rA_i + X_iA_r)$$

Y esto ya son matrices reales, tales que

$$A_r X_r - A_i X_i = X_r A_r - X_i A_i$$

Esto se verifica para todo X_r, X_i, por lo que tenemos que

$$A_r X_r = X_r A_r, \quad A_i X_i = X_i A_i$$

por lo que A_r y A_i deben ser como las anteriores, de la forma aI_n.
O sea, son las matrices $A = a_1 I_n + i a_2 I_n = (a_1 + i a_2) I_n$.
$\boldsymbol{SL_n}(\mathbb{R})$: deben ser diagonales, como hemos visto antes, y tener determinante 1.
O sea, $A = aI_n$, con $a^n = 1$. Si n es impar, la única matriz que verifica esto es I_n.
Si n es impar, lo verifican I_n y $-I_n$.
$\boldsymbol{SL_n}(\mathbb{R})$: igual, diagonales tales que $a^n = 1$. Pero en $\mathbb{C}$, 1 tiene n raíces n-ésimas, por lo que el centro estará formado por n matrices con estas raíces en su diagonal y lo demás 0.

4.3 Subgrupos normales y grupos cociente

4.3.1 Construir la tabla de multiplicación del grupo cociente $\frac{G}{\langle -I \rangle}$, donde G es cualquier de los tres primeros grupos del 4.1.1 e I es la matriz identidad.

$\frac{\mathbb{Z}_7}{\langle -1 \rangle}, +$: hay una única clase de equivalencia, porque todo elemento no nulo genera el conjunto, en particular el -1, y por tanto el cociente tiene un único elemento. La tabla de multiplicación es trivial.

$\frac{\mathbb{Z}_7^*}{\langle -1 \rangle}, \cdot$: tenemos que $H = \langle -1 \rangle = \{1, -1\}$. Ahora, $a \equiv b$ mod $H \iff ab^{-1} \in H \iff ab^{-1} = 1, -1 \iff b = \pm x$ Entonces $H1 = \{1, 6\}$, $H2 = \{2, 5\}$, $H3 = \{3, 4\}$. Es decir, hay dos clases de equivalencia. La tabla queda

	1	**2**	**3**
1	1	2	3
2	2	2	1
3	3	1	2

$\frac{\mathbb{Z}_{16}}{\langle -1 \rangle}, +$: igual, la tabla trivial.

$\frac{\mathbb{Z}_{16}^*}{\langle -1 \rangle}, \cdot$: $\mathbb{Z}_{16}^* = \{1, 3, 5, 7, 9, 11, 13, 15\}$, $H = \{1, 15\}$. Entonces $H1 = \{1, 15\}$, $H3 = \{3, 13\}$, $H5 = \{5, 11\}$ $H7 = \{7, 9\}$.

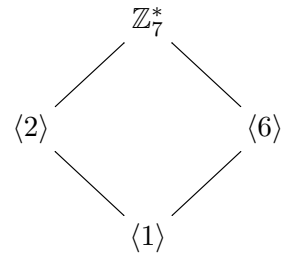
	1	**3**	**5**	**7**
1	1	3	5	7
3	3	7	1	3
5	5	1	7	3
7	7	3	3	1

4.3.2 Construir el diagrama de los subgrupos de cada uno de los grupos de los problemas 4.1.1, 4.2.1 y 4.3.1 indicando cuáles de ellos son normales.

$(\mathbb{Z}_7, +)$ **:** por el teorema de Lagrange, el orden subgrupos de $\mathbb{Z}_7$ debe ser divisor de 7. Es decir, su orden es 1 o 7. El único elemento que no genera todo el conjunto es 0.

$\left(\mathbb{Z}_{\mathbf{7}}^{*}, \cdot\right)$ **:** $\langle 1\rangle = \{1\}$, $\langle 2\rangle = \{1,2,4\}$, $\langle 3\rangle = \mathbb{Z}_7^*$, $\langle 4\rangle = \{1,2,4\} = \langle 2\rangle$, $\langle 5\rangle = \{1,2,3,4,5,6\} = \mathbb{Z}_7^*$, $\langle 6\rangle = \{1,6\}$

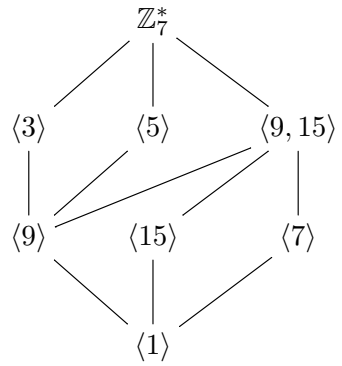
$\langle 2,6\rangle = \mathbb{Z}_7^*$ y realmente no hay más conjuntos que generen algo que nos aporte nueva información. Entonces



y todos son subgrupos normales.

$\left(\mathbb{Z}_{\mathbf{16}}^{*}, \cdot\right)$ **:** $\mathbb{Z}_{16}^* = \{1,3,5,7,9,11,13,15\}$,$\langle 1\rangle = \{1\}$, $\langle 3\rangle = \{1,3,9,11\}$, $\langle 5\rangle = \{1,5,9,13\}$, $\langle 7\rangle = \{1,7\}$, $\langle 9\rangle = \{1,9\}$, $\langle 11\rangle = \{1,3,9,11\} = \langle 3\rangle$, $\langle 13\rangle = \{1,5,9,13\} = \langle 5\rangle$, $\langle 15\rangle = \{1,15\}$.

Veamos los subgrupos generados por varios elementos, $\langle 3,5\rangle = \langle 3,7\rangle = \langle 3,15\rangle = \langle 5,7\rangle = \langle 5,15\rangle = \mathbb{Z}_{16}^*$, porque generan conjuntos de al menos 5 elementos. El teorema de Lagrange implica que deben generar el total. Los únicos que quedan y podrían aportar algo de información son$\langle 9,15\rangle = \langle 1,7,9,15\rangle$, $\langle 7,9\rangle = \{1,7,9,15\}$, $\langle 7,15\rangle = \{1,7,9,15\}$. Y ya está.



todos son normales.

4.3.3 Demostrar que la intersección de una familia de subgrupos normales de un grupo normal también es un subgrupo normal.

Sea $N = \cap_{i\in I} N_i$ el subgrupo intersección de subgrupos normales.

Entonces, se tiene que $\forall x \in G$, $x^{-1}N_i x = N_i$, $\forall i$.

Entonces, dado $a \in N$, se tiene que $a \in N_i, \forall i$. Entonces $x^{-1}ax \in N_i$, $\forall i$ y entonces $x^{-1}ax \in N$. Es decir $x^{-1}Nx \subset N$.

Por la proposición 4.9, tenemos el resultado.

4.3.4 Demostrar que todo subgrupo de un subgrupo cíclico normal de G es normal en G.

Sea N el subgrupo normal, $N = \langle a \rangle$. Entonces, dado $g \in G$ se tiene que $a^g \in N \implies a^g = a^r,\ r \in \mathbb{Z}$.

H subgrupo de N. Entonces H es cíclico generado por algún $a^n,\ n \in \mathbb{Z}$.

Dado $h \in H = \langle a^n \rangle$, entonces $h = (a^n)^m = a^{nm}$.

Entonces

$$h^g = (a^{nm})^g = g^{-1}a^{(nm)}ag = g^{-1}a\left(gg^{-1}\right)a...a\left(gg^{-1}\right)ag = \left(g^{-1}ag\right)\left(g^{-1}ag\right)\overset{nm}{...}\left(g^{-1}ag\right) =$$

$$= \left(g^{-1}ag\right)^{nm} = (a^r)^{nm} = a^{rnm} = (a^n)^{rm} \in H$$

Y H es normal.

4.3.5 Sean N, M subgrupos normales de un grupo tales G tales que $N \cap M = \{1\}$. Probar que $nm = mn,\ \forall n \in N, m \in M$.

Es lo mismo que demostrar que $m^{-1}nm = n$, que es lo mismo que demostrar que $m^{-1}nmn^{-1} = 1$.

Como N es normal, entonces $m^{-1}nm \in N$, y $n \in N$, entonces $m^{-1}nmn^{-1} \in N$.

Como M es normal, entonces $nmn^{-1} \in M$ y $m^{-1} \in M$, entonces $m^{-1}nmn^{-1} \in M$.

Como en la intersección solo está el uno, entonces ha de ser $m^{-1}nmn^{-1} = 1$, como queríamos ver.

4.3.7 Si N es un subgrupo normal en un grupo G y $a \in G$ tiene orden n, probar que el orden de Na en G/N es un divisor de n.

Sea $m = |Na|$.
$a^n = 1 \implies (Na)^n = Na^n = N = 1_{G/N} \iff m = |Na|\,|n$, como queríamos ver.

4.4 Homomorfismos de grupo y Teoremas de Isomorfía

4.4.1 Si G, H son grupos, $Hom(G, H)$ denota el conjunto de los homomorfismos de G a H.

(1) Demostrar que si H es abeliano, entonces $Hom(G, H)$ es un grupo con la operación natural:

$$(fg)(a) = f(a)\,g(a),\ a \in G$$

Antes de nada tenemos que ver que el producto de dos homomorfismos es un homomorfismo.

$$fg(ab) = f(ab)\,g(ab) \overset{f,g\ hom}{=} f(a)\,f(b)\,g(a)\,g(b) \overset{H\ abel}{=} f(a)\,g(a)\,f(b)\,g(b) = fg(a)\,fg(b)\ \checkmark$$

Y ahora veamos que se forma un grupo:

- Asociativa

$$(fg)\,h(a) = fg(a)\,h(a) = f(a)\,g(a)\,h(a) = f(a)\,gh(a) = f(gh)(a)\ \checkmark$$

- Neutro

$$f1\,(a) = f\,(a)\,1\,(a) = f\,(a)$$
$$1f\,(a) = 1\,(a)\,f\,(a) = f\,(a)\,\checkmark$$

- Inverso, si definimos $g\,(a) = f\,(a)^{-1}$, entonces
  $g\,(ab) = f\,(ab)^{-1} = (f\,(a)\,f\,(b))^{-1} = f\,(b)^{-1}\,f\,(a)^{-1} = f\,(a)^{-1}\,f\,(b)^{-1} = g\,(a)\,g\,(a)$, por lo que g es un homomorfismo, y tenemos que

$$fg\,(a) = f\,(a)\,g\,(a) = f\,(a)\,f\,(a)^{-1} = 1 = f\,(a)^{-1}\,f\,(a) = g\,(a)\,f\,(a) = gf\,(a)\,\checkmark$$

- Conmutativa

$$fg\,(a) = f\,(a)\,g\,(a) = g\,(a)\,f\,(a) = gf\,(a)$$

(2) Demostrar que si G es abeliano, entonces $Hom\,(\mathbb{Z}, G) \simeq G$ y $Hom\,(\mathbb{Z}_n, G) \simeq \{g \in G : g^n = e\}$.

$\mathbb{Z} = \langle 1 \rangle$, por tanto, dado un homomorfismo f, conociendo $f\,(1)$ conocemos toda la imagen, pues (notación aditiva) $f\,(n) = nf\,(1)$.

Tomamos entonces

$$\begin{array}{ccc} Hom\,(\mathbb{Z}, G) & \overset{\psi}{\to} & G \\ f & \mapsto & f\,(1) \end{array}$$

Es inyectiva porque si dos homomorfismos coinciden en el 1, entonces coinciden en toda la imagen, por lo explicado antes.

Dado $x \in G$, definimos $f\,(n) = nx$, ¿es un homomorfismo?

$$f\,(n+m) = (n+m)\,x = nx + mx = f\,(n) + f\,(m)\,\checkmark$$

Luego $f\,(1) = x$. Y tenemos que ψ es una biyección y tenemos la equivalencia buscada.

Ahora $\mathbb{Z}_n = \langle 1 \rangle$, también. Vamos a tomar la misma aplicación

$$\begin{array}{ccc} Hom\,(\mathbb{Z}, G) & \overset{\psi}{\to} & G \\ f & \mapsto & f\,(1) \end{array}$$

Es inyectiva por la misma razón que antes.

Sea ahora $x \in Im\psi \implies \exists f \in Hom\,(\mathbb{Z}, G)\,/\,f\,(1) = \psi\,(f) = x$. Entonces

$$1 = f\,(0) = f\,(n \cdot 1) = f\,(1 + \overset{n}{\ldots} + 1) = f\,(1) \cdot \overset{n}{\ldots} \cdot f\,(1) = f\,(1)^n = x^n$$

O sea, que $Imf \subset \{x \in G : x^n = 1\} = A$.

Ahora, dado $x \in A$, entonces $x^n = 1$, definimos $f : \mathbb{Z}_n \to G$, de la forma $f\,(a) = x^a$. ¿Está bien definido?

Sean $a + (n) = b + (n)$, entonces $b - a \in (n) \implies b - a = nt,\ t \in \mathbb{Z}$. Entonces

$$f\,(b + (n)) = x^b = x^{a+nt} = x^a\,(x^n)^t = x^a = f\,(a + (n))\ \checkmark$$

Como queríamos ver. Y claramente es homomorfismo. Luego queda probado el resultado.

4.4.2 Un subgrupo H del grupo G es característico si, para cualquier automorfismo f de G, se verifica $f(H) \subseteq H$. Se pide:

(1) Demostrar que todo subgrupo característico de G es un subgrupo normal de G.

Debe ser $g^{-1}Hg \in H,\ \forall g \in G$. Esto son los automorfismos internos. Por tanto, los subgrupos característico son normales.

(2) Dar un ejemplo de un grupo con un subgrupo normal que no sea característico

En un grupo abeliano todo subgrupo es normal.

Tomamos un grupo abeliano G, y hacemos $G \times G$. Tomamos $H = G \times 1$, y tomamos el automorfismo $f(x,y) = (y,x)$.

(3) Demostrar que si H es un subgrupo característico de G y K es un subgrupo característico de H, entonces K es un subgrupo característico de G.

Sea f un automorfismo de G, entonces f_H es un automorfismo de H, ya que $f(H) \subset H$, por ser H característico y $|f(H)| = |H|$, por ser f automorfismo.

Entonces $f_H(K) \subset K$, por ser K característico en H. Pero $f(K) = f_H(K)$, por lo que K es característico en G.

(4) Si H es un sugrupo característico de K y K es un subgrupo normal de G, entonces H es normal en G.

Dado $g \in G$, ¿$g^{-1}Hg \subset H$?

Sabemos que $g^{-1}Kg = K$.

Entonces $i_g \in Aut(K)$. Como H es subgrupo característico de K, tenemos que $g^{-1}Hg = i_g(H) \subset H$✓

(5) Demostrar que el centro de un grupo es un subgrupo característico.

Sea f un automorfismo de G, ¿se tiene $f(Z(G))) \subset Z(G)$?

Para que se dé la inclusión, ha de cumplirse que, dado $a \in Z(G)$, se verifique $f(a)\,b = bf(a)\,,\ \forall b \in G$.

Como f es automorfismo, es sobreyectiva, entonces $\exists g \in G / f(g) = b$. Entonces

$$f(a)\,b = f(a)\,f(g) = f(ag) = f(ga) = f(g)\,f(a) = bf(a)$$

como queríamos ver.

(6) Supongamos que H es el único subgrupo de G con el mismo cardinal que H. Demostrar que H es característico en G.

Si $f \in Aut(G) \implies f(H) \subset H\ y\ |f(H)| = |H| \implies f(H) = H$.

4.4.3 Demostrar que si G es D_4 o el grupo de cuaterniones Q_8, entonces $Z(G) \simeq \mathbb{Z}_2$ y $\frac{G}{Z(G)} \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$, y sin embargo $D_4 \not\simeq Q_8$.

$$D_4 = \left\{1, a, a^2, a^3, b, ab, a^2b, a^3b\right\},\ a^4 = b^2 = 1,\ ba = a^3b = a^{-1}b$$

$$Q_8 = \left\{1, A, A^2, A^3, B, AB, A^2B, A^3B\right\},\ A^4 = 1,\ B^2 = A^2,\ BA = A^3B$$

$ba^i = a^{-1}ba^{i-1} = a^{-i}b$

$ba^2 = a^{-2}b = a^2b$

Y en Q_8 ocurre lo mismo.

Es decir, que $a^2 \in Z(D_4) = \left\{1, a^2\right\}$ y $A^2 \in Z(Q_8) = \left\{1, A^2\right\}$.

$a \notin Z(D_4)$ porque $ba = a^{-1}b \neq ab$, por la misma razón $a^{-1}, b \notin Z(D_4)$. Y $aba = aa^{-1}b = b \neq a^2b$, por lo que $ab \notin Z(G)$. Como a^2 si está en el centro y b no, entonces a^2b no puede estar, y de igual forma no puede estarlo $a^3b = a^2ab$, pues a^2 está pero ab no.

Razonando de forma análoga vemos que $Z(Q_8) = \left\{1, A^2\right\}$. Y tenemos trivialmente la isomorfía $Z(G) \simeq \mathbb{Z}_2$.

Ahora

$$\frac{D_4}{\langle a^2 \rangle} = \left\{\overline{1}, \overline{a}, \overline{b}, \overline{a}\overline{b}\right\}$$

y se tiene que $\overline{a}^2 = \overline{a^2} = 1$ y $b^2 = a^2$, por lo que $\overline{b}^2 = 1$. Y $\overline{b}\overline{a} = \overline{ba} = \overline{a^3b} = \overline{ab} = \overline{a}\overline{b}$.

Ahora, haciendo la asociación $(0,0) \mapsto \overline{1}, \quad (0,1) \mapsto \overline{b}, \quad (1,0) \mapsto \overline{a}, \quad (1,1) \mapsto \overline{ab}$, tenemos el isomorfismo buscado.

Y en el Q_8 ocurre exactamente lo mismo.

Resta ver que $D_4 \not\simeq Q_8$. Para esto, nos vamos a fijar en los órdenes de los elementos de cada grupo:

$$|a| = 4 = \left|a^3\right|, \ \left|a^2\right| = |b| = |ab| = \left|a^2b\right| = \left|a^3b\right| = 2$$

$$|A| = 4 = \left|A^3\right|, \ \left|A^2\right| = 2, \ |B| = 4$$

y aquí podemos parar. Ya que el primer grupo tiene 2 elementos de orden 4, y el segundo tiene, al menos, 3. Esto implica que no pueden ser isomorfos.

4.4.4 Probar que, salvo isomorfismos, solo hay dos grupos no abelianos de orden 8. ¿Cuáles son?

Sea G un grupo no abeliano de orden 8.

$Exp(G) = min\{n \in \mathbb{N} / g^n = 1, \ \forall g \in G\}$.

Debe ser $Exp(G) \,|8 \implies Exp(G) \in \{1, 2, 4, 8\}$.

No puede ser 1, pues el único elemento sería el 1.

No puede ser 8, porque entonces sería cíclico, y, por tanto, abeliano.

Si $Exp(G) = 2 \implies g^2 = 1 \ \forall g \implies (gh)^2 = 1, \ \forall g, h \in G$. Entonces $hg = h^{-1}g^{-1} = (gh)^{-1} = gh$. Y G es abeliano.

Por tanto, ha de ser $Exp(G) = 4$.

G tiene un elemento a de orden 4. Se tiene que $\langle a \rangle_4 \trianglelefteq G$ y tiene índice 2, por lo que es normal.

Sea $b \in G \setminus \langle a \rangle$, como a tiene orden 4, entonces $\langle a, b \rangle = G$.

El orden de b debe ser divisor de 8, pero no puede ser 1 porque entonces $b \in \langle a \rangle$, y no puede ser 8 porque entonces G es cíclico. Es decir, $|b| = 2$ *ó* 4.

Como el índice de $\langle a \rangle$ es 2, entonces $b^2 \in \langle a \rangle$.

$$b^2 = \begin{cases} 1 & |b| = 2 \\ a^2 & |b| = 4 \end{cases}$$

Si $|b| = 4$, entonces $b^2 = a^2$, porque $b^2 \in \left\langle 1, a, a^2, a^3 \right\rangle$, con $|1| = 1, \ \left|a^2\right| = 2$ y $|a| = \left|a^3\right| = 4$. Como $\left|b^2\right| = 2$, debe ser $b^2 = a^2$.

Solo falta calcular $b^{-1}ab$.

Debe ser $\left|b^{-1}ab\right| = |a| = 4$, luego $b^{-1}ab = a$ *ó* a^3, pero no puede ser a, pues en tal caso G sería abeliano, porque $ab = bb^{-1}ab = ba$.

Luego ha de ser a^3.

Recapitulando, G es un grupo de orden 8, que no es abeliano, tiene exponente 4, por lo que $\exists a \in G / \, |a| = 4$.

Además, $\forall b \notin \langle a \rangle$, se tiene que $b^{-1}ab = a^{-1}$ y $b^2 = \begin{cases} 1 \\ a^2 \end{cases}$.

En el primer caso de esta última igualdad, el grupo será isomorfo a D_4 y en el segundo lo es a Q_8.

4.4.5 Probar que todo grupo no abeliano de orden 6 es isomorfo a S_3.

Como en el ejercicio anterior, ha de ser $Exp\,(G) \in \{1, 2, 3, 6\}$, no puede ser ni 1 ni 2 ni 6 por los mismos razonamientos que antes. Por lo que debe ser 3.

Es decir, G tiene, al menos, un elemento a de orden 3. Se tiene que $\langle a \rangle_4 \trianglelefteq G$ y tiene índice 2, por lo que es normal.

Sea $b \in G \setminus \langle a \rangle$, se tiene que $\langle a, b \rangle = G$.

El orden de b debe dividir a 6, pero no puede ser 1 porque entonces $b \in \langle a \rangle$ y no puede ser 6 porque entonces G sería cíclico. Ha de ser $|b| = 2$ *ó* 3.

Como el índice de $\langle a \rangle$ es 2, entonces $b^2 \in \langle a \rangle = \left\{1, a, a^2\right\}$, con $|1| = 1, \ |a| = 3, \ \left|a^2\right| = 3$.

Si el orden de b es 2, entonces el orden de $b^2 = 1$ es 1.

Si el orden de b es 3, entonces el orden de b^2 debe ser, también, 3.

Si fuera $b^2 = a$, entonces $ab^{-1} = b = b^{-1}a \implies ab = ab^{-1}a = ba$, por lo que esto no puede ser.

Si fuera $b^2 = a^2$, entonces $b = b^2b^2 = a^2b^2 \implies 1 = a^2b \implies b = \left(a^2\right)^{-1} = a\#$ Esto tampoco puede ser, pues $b \notin \langle a \rangle$.

Es decir, que la única posibilidad es que $|b| = 2$.

Es decir, que cualquier grupo no abeliano de orden 6 es de la forma

$$\left\{1, a, a^2, b, c, d\right\}$$

con $|b| = |c| = |d| = 2, \ a^3 = 1$, por lo que es isomorfo a S_3.

4.4.6 Demostrar que si H es un subgrupo abeliano de un grupo G tal que $HZ\,(G) = G$, entonces G es abeliano. Deducir que si $\frac{G}{Z(G)}$ es cíclico, entonces G es abeliano.

Dados $x, y \in G \implies \begin{cases} x = hu \\ y = kv \end{cases} \quad h, k \in H, u, v \in Z\,(G) \implies xy = hu \cdot kv = hkuv = khvu = kvhu = yx \implies G \ abeliano$

Para la segunda afirmación:

Si tenemos $H = \langle g \rangle$ cíclico, entonces es abeliano. Y entonces

$$x \in G \implies xZ\,(G) = (gZ\,(G))^n = g^nZ\,(G)$$

para algún $n \in \mathbb{Z}$.

$$x = g^nz, \ g^n \in H, z \in Z\,(G) \implies G = HZ\,(G)$$

y por lo anterior es abeliano.

4.5 El orden de un elemento de un grupo

4.5.1 Sea G un grupo cíclico y sea g un generador de G. Demostrar:

1. **Si G tiene orden infinito entonces para cada grupo H y cada elemento $h \in H$ existe un único homomorfismo $f : G \to H$ tal que $f(g) = h$.**

   Supongamos que k es otro homomorfismo con $k(g) = h$.

   Entonces, como G es cíclico, todo elemento es de la forma g^j para cierto j natural.

   Por tanto, dado $a \in G$, se tiene que

   $$k(a) = k\left(g^j\right) = (k(g))^j = (f(g))^j = f\left(g^j\right) = f(a)$$

   y $k = f$. Por tanto, en caso de existir, es único.

   Además, existe pues la aplicación dada por $f\left(g^j\right) = h^j$ es claramente un homomorfismo.

2. **Si G tiene orden finito n entonces para cada grupo H y cada elemento $h \in H$ las siguientes condiciones son equivalentes:**

   (a) **n es múltiplo del orden de h**

   (b) **existe un homomorfismo $f : G \to H$ tal que $f(g) = h$**

   (c) **existe un único homomorfismo $f : G \to H$ tal que $f(g) = h$.**

   '$(a) \implies (b)$' Sea m el orden de h y f dada por $f\left(g^k\right) = h^{\lfloor k \rfloor_m}$. Entonces, dados $a, b \in G$ se tiene que $a = g^i,\ b = g^j$, luego

   $$f(a) f(b) = f\left(g^i\right) f\left(g^j\right) = h^{\lfloor i \rfloor_m} h^{\lfloor j \rfloor_m} = h^{\lfloor i+j \rfloor_m}$$

   $$f(ab) = f\left(g^i g^j\right) = f\left(g^{\lfloor i+j \rfloor_n}\right) = h^{\left\lfloor \lfloor i+j \rfloor_n \right\rfloor_m} = h^{\lfloor i+j \rfloor_m}$$

   esta igualdad se debe que $m|n$. Por lo que es un homomorfismo, y existe.

   '$(b) \implies (c)$' Supongamos que k es otro homomorfismo con $k(g) = h$. Entonces, como todo $a \in G$ es $a = g^j$, tenemos que

   $$k(a) = k\left(g^j\right) = (k(g))^j = (f(g))^j = f\left(g^j\right) = f(a)$$

   y el homomorfismo es único.

   '$(c) \implies (a)$' Tenemos que $h^n = f(g)^n = f(g^n) = f(1) = 1$, por lo que el orden de h divide a n.

4.5.2 Demostrar que si G es cíclico infinito entonces G tiene exactamente dos generadores, es decir, existen exactamente dos elementos $g \in G$ que verifican $G = \langle g \rangle$. Decid cuáles son en función de un generador $a \in G$.

Dado un generador $a \in G$, entonces a^{-1} también es generador.

Veámoslo, dado $g \in G$, entonces $g = a^n$, en particular, $a^{-1} = a^m$, luego $a^{-m} = a \implies \left(a^{-1}\right)^m = a$.

Entonces $g = \left(a^{-1}\right)^{mn},\ \forall g \in G$.

Por tanto, a^{-1} es generador.

Obsérvese que no puede haber generadores que sean su propio inverso, ya que entonces $aa = a^2 = 1$, por lo que el orden de a es 2 o 1 (si $a = 1$) y a no es generador, si excluimos, claro $\{1\}$ y $\{1, a\}$, que son finitos.

Por tanto, todo grupo cíclico tiene, al menos, dos generadores.

Supongamos que hay más generadores. Sea b uno de estos.

Como G es cíclico, entonces es isomorfo a $(\mathbb{Z}, +)$, y sabemos que 1 es generador, también sabemos que -1 lo es, como hemos visto.

Supongamos que la isomorfía nos da la imagen de b como k. Entonces $\exists m/mk = 1$, luego $k|1$ y $k \neq 1$. Esto no puede ser.

4.5.3 La función $\phi : \mathbb{N} \to \mathbb{N}$ que asocia a cada número n el cardinal de $\mathbb{Z}_n^*$ se llama función de Euler. Demostrar que:

(1) Si n, m son coprimos, entonces $\phi(nm) = \phi(n)\,\phi(m)$

Por el teorema chino de los restos:

$$\mathbb{Z}_{nm} \simeq \mathbb{Z}_n \times \mathbb{Z}_m \implies \mathbb{Z}_{nm}^* \simeq \mathbb{Z}_n^* \times \mathbb{Z}_m^*$$

Luego

$$\phi(nm) = |\mathbb{Z}_{nm}^*| = |\mathbb{Z}_n^*|\,|\mathbb{Z}_m^*| = \phi(n)\,\phi(m)$$

(2) Si p es primo, entonces $\phi(p^n) = p^{n-1}(p-1)$

$$\mathbb{Z}_{p^n}^* = \{a \in \mathbb{Z}_{p^n} : (a, p^n) = 1\}$$

Los múltiplos de p en $\mathbb{Z}_{p^n}$ son $0, p, 2p, 3p, ..., (p-1)\,p, p^2, ..., p^{n-1}, 2p^{n-1}, ..., (p-1)\,p^{n-1}$. O sea, que para cada potencia de p, tenemos p múltiplos de p. Por tanto, hay p^{n-1} múltiplos de p.

Por tanto, $\phi(p^n) = p^n - p^{n-1} = p^{n-1}(p-1)$.

(3) Si $n = p_1^{a_1} \cdot ... \cdot p_k^{a_k}$ con p_i primos entonces $\phi(n) = n\frac{p_1-1}{p_1} \cdot ... \cdot \frac{p_k-1}{p_k}$

Aplicando 1 y después 2, sale

$$\phi(n) = \phi(p_1^{a_1}) \cdot ... \cdot \phi\left(p_k^{a_k}\right) = p_1^{a_1-1}(p_1-1) \cdot ... \cdot p_k^{a_k-1}(p_k-1) = p_1^{a_1}\frac{p_1-1}{p_1} \cdot ... \cdot p_k^{a_k}\frac{p_k-1}{p_k} = n\frac{p_1-1}{p_1} \cdot ... \cdot \frac{p_k-1}{p_k}$$

4.5.4 Sea G un grupo cíclico de orden n generado por a. Demostrar que G tiene $\phi(|G|)$ generadores y describir cuáles son esos generadores en términos de a.

$G \simeq (\mathbb{Z}_n, +)$ y $a \in \mathbb{Z}_n \iff \langle a \rangle = a\mathbb{Z}_n$

a es generador de $(\mathbb{Z}_n, +)$ si, y solo si $a\mathbb{Z}_n = \mathbb{Z}_n$ si, y solo si $a \in \mathbb{Z}_n^*$

Luego hay $\phi(\mathbb{Z}_n^*) = |\mathbb{Z}_n^*|$ generadores.

4.5.5 Encontrar todos los grupos cíclicos G, salvo isomorfismos, que tengan exactamente dos generadores.

Si G es infinito, hemos visto en 1.5.2 que tiene dos generadores, y es isomorfo a $(\mathbb{Z}, +)$.

Si G es finito, por ser cíclico, es isomorfo a $(\mathbb{Z}_n, +)$.

Por el ejercicio 1.5.3, sabemos que tendrá $\phi(n)$ generadores. O sea, buscamos $n/\phi(n) = 2$.

La fórmula es

$$\phi(n) = n \prod_{p_i | n} \left(1 - \frac{1}{p_i}\right) \text{ con } p_i \text{ primo}$$

Los primos dan $\phi(p) = p - 1$, luego $\mathbb{Z}_3$ sirve, y no sirve ningún $p > 3$.

$$\phi(1) = 1$$

luego tampoco sirve.

$$\phi(4) = 4\left(1 - \frac{1}{2}\right) = 4 \cdot \frac{1}{2} = 2$$

Por lo que $\mathbb{Z}_4$ también funciona.

$$\phi(6) = 6\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right) = 6\frac{1}{2}\frac{2}{3} = 2$$

Y $\mathbb{Z}_6$ también vale.

Por otro lado, está la propiedad de que si $n = p_1^{a_1} \cdot \ldots \cdot p_k^{a_k}$, entonces $\phi(n) = n\frac{p_1 - 1}{p_1} \cdot \ldots \cdot \frac{p_k - 1}{p_k}$

Esto quiere decir que si $n > 6$, entonces:

- Si $2|n$, se tiene que $\phi(n) = n\frac{2-1}{2} \cdot \ldots \cdot \frac{p_k - 1}{p_k} = \frac{n}{2} \cdot \ldots \cdot \frac{p_k - 1}{p_k} \geq \frac{n}{2} > \frac{6}{3} = 3 > 2$
- Si $3|n$, entonces $\phi(n) \geq n\frac{2}{3} > \frac{12}{3} = 4 > 2$
- Y, en general si $p|n$, con $p > 3$ y $n > 6$, entonces, si llamamos $k = \frac{n}{p}$, tenemos $\phi(n) \geq n\frac{p-1}{p} = k(p-1) > 2 \cdot 2 > 2$.

4.5.7 ¿Es cíclico el producto directo de dos grupos cíclicos infinitos?

No. Contraejemplo: $\mathbb{Z} \times \mathbb{Z}$, con la suma. $\mathbb{Z} = \langle 1 \rangle$. Pero, supongamos que $\mathbb{Z} \times \mathbb{Z} = \langle a, b \rangle$, entonces, dado (x, y) ha de ser $(x, y) = k(a, b) = (ka, kb)$, pero basta tomar $(x, 1)$, entonces la k debe ser la misma, porque $x = ka$. Pero no puede ser la misma, pues podemos tomar $y \neq 1$.

4.5.8 Describir $Aut(\mathbb{Z})$ y probar que $Aut(\mathbb{Z}_n) \simeq \mathbb{Z}_n^*$.

Los automorfismos de $\mathbb{Z} = \langle 1 \rangle$ deben verificar $f(1) = 1$ y $f(ab) = f(a) f(b)$, pero todo elemento $a = a1$, entonces el único automorfismo es la identidad, pues el 1 va al 1, y este genera todos los elementos.

En $\mathbb{Z}_n$ ocurre algo similar, pero $\mathbb{Z}_n = \langle a \rangle$ si $a \in \mathbb{Z}_n^*$. Es decir, que hay tantos automorfismos como elementos ivnertibles, y, además, cada automorfismo está determinado por la imagen de un invertible, de ahí la isomorfía, que vendría dada por

$$\begin{array}{ccc} \mathbb{Z}_n^* & \to & Aut(\mathbb{Z}_n) \\ a & \mapsto & f : f(a) = 1 \end{array}$$

4.5.9 Mostrar con un ejemplo que, aun cuando G sea cíclico, $Aut(G)$ no tiene por qué ser cíclico.

4.5.10 Probar que si G, H son grupos cíclicos finitos entonces las siguientes condiciones son equivalentes

1. **El orden de G divide al orden de H**
2. **Existe un homomorfismo inyectivo $G \to H$**
3. **Existe homomorfismo suprayectivo $H \to G$**

4.5.11 Sea G un grupo abeliano finito en el que, para cada $n \in \mathbb{Z}^+$, la ecuación $x^n = e$ tiene a lo sumo n soluciones. Demostrar que G es cíclico. Deducir que un subgrupo finito del grupo de unidades de un dominio es cíclico.

Sea $g \in G$ de orden máximo, llamémosle $|g| = n$. Entonces $\langle g \rangle$ tiene n soluciones de la ecuación $x^n = 1$.
¿$G = \langle g \rangle$?

Supongamos que no, entonces $\exists h \in G \setminus \langle g \rangle$.

Sea p un primo que divide a $|h|$.

Si $p \nmid n$ entonces $\langle h \rangle$ tiene un elemento k de orden p y $\langle k, g \rangle$ es un cíclico de orden pn en contra de la maximalidad de n.

Por lo que $p|n$.

Si

$$|g| = p_1^{a_1} \cdot \ldots \cdot p_k^{a_k}, \quad |h| = p_1^{b_1} \cdot \ldots \cdot p_k^{b_k}$$

Entonces

$$\langle h \rangle = C_{p_1^{b_1}} \times \ldots \times C_{p_k^{b_k}}, \quad \langle g \rangle = C_{p_1^{a_1}} \times \ldots \times C_{p_k^{a_k}}$$

En $C_{p_1^{a_1}}$ hay $p_1^{a_1}$ soluciones de $x^{p_1^{a_1}} = 1$

4.6 Conjugación y acciones de grupos en conjuntos

4.6.2 Sea p un número primo. Demostrar las siguientes afirmaciones:

1. **Todos los grupos de orden p^2 son abelianos**
2. **El centro de cualquier grupo no abeliano de orden p^3 tiene orden p.**

4.6.3 Demostrar las siguientes afirmaciones para un $p-grupo$ finito G.

1. **Si n divide al orden de G entonces G tiene un subgrupo de orden n**

   Inducción en $|G|$:

   - $|G| = 1$, es obvio
   - $|G| = p$ primo, también obvio. Los únicos subgrupos son el total y el 1.
   - Supongamos la hipótesis de inducción y $|G| = p^m > p$, con $p^k = n|p^m$. Entonces
     Si G es abeliano y H es un subgrupo de orden p. Entonces $|H| = p \leq p^k$, entonces G/H tiene orden p^{m-1} y la hipótesis de inducción nos dice que tiene subgrupos de cualquier orden divisor de p^{m-1}, en particular lo tiene de orden n y el teorema de correspondencia nos da el resultado, ya que H es normal.
     Si G no es abeliano, consideramos $Z(G)$, que no es trivial por ser un p-grupo y H un subgrupo de $Z(G)$ de orden p, que será normal, y hacemos lo mismo que antes.

2. **Existe una cadena $\mathbf{1 = G_0 \subset G_1 \subset ... \subset G_n = G}$ de subgrupos normales de G tales que cada $\frac{G_i}{G_{i-1}} \subset Z\left(\frac{G}{G_{i-1}}\right)$, $\forall i = 1, ..., n$.**

   $1 = G_0$

   Debe ser $G_1 = G_1/G_0 \subset Z(G/G_0) = Z(G)$, tomamos $G_1 = Z(G)$, que es normal.

   Debe ser $G_2/G_1 \subset Z(G/G_1)$. Elegimos el único subgrupo G_2 de G que contiene a G_1de forma que $G_2/G_1 = Z(G/G_1)$.

   Procedemos por inducción en $|G|$.

   Si $|G| = 1$ ó p, entonces es trivial.

   En otro caso

   $$|G/G_1| < |G|$$

   y tenemos $H_0 \subset H_1 \subset ... \subset H_{m-1} \subset H_m = G/G_1$ por la hipótesis de inducción.