Tema 2

Problemas complementarios

Ejercicio 1. *Sea H un subgrupo de un grupo G. Supongamos que el producto de dos clases cualesquiera de la forma xH y yH es otra clase de la forma zH. Demostrar que H es un subgrupo normal de G.*

Solución. Si el producto de las clases xH y yH está bien definido y es zH, como xy ha de estar en la clase zH, los elementos xy y z, definen la misma clase y por tanto podemos suponer que el producto de las clases dadas es xyH.

Dado ahora $a \in G$, hemos de ver que $aHa^{-1} \subseteq H$. El producto de las dos clases aH y $a^{-1}H$, ha de ser la clase H, con lo que

$$aHa^{-1}H = \left(aHa^{-1}\right) H = H,$$

lo que implica que $aHa^{-1} \subseteq H$.

Ejercicio 2. *Si un elemento a de un grupo G tiene exactamente dos conjugados, entonces G admite un subgrupo normal propio.*

Solución. Sea b el conjugado de a distinto de a. Entonces bab^{-1} es también conjugado de a. Además $bab^{-1} \neq b$, ya que si fuera $bab^{-1} = b$ entonces $ab^{-1} = 1$, con lo que $a = b$, que es una contradicción. De esta forma $bab^{-1} = a$, con lo que $ab = ba$. Considermos el subgrupo $H = \langle a, b \rangle$ de G. Dado que a y b conmutan, cada elemento $x \in H$ es de la forma $x = a^m b^n$ para ciertos enteros m y n.

Veamos que $H \neq G$. En efecto, si H fuese igual a G como existe $x \in G$ tal que $b = xax^{-1}$, x ha de ser de la forma $x = a^n b^m$, con lo que

$$b = xax^{-1} = a^m b^n a b^{-n} a^{-m} = a,$$

que es absurdo.

Para concluir es suficiente demostrar que H es un subgrupo normal de G. Hemos de ver que si $x \in H$ e $y \in G$, entonces $yxy^{-1} \in H$. Como $x = a^m b^n$, basta ver que $ya^m y^{-1}$, $yab^n y^{-1} \in G$, pues $ya^m b^n y^{-1} = ya^m y^{-1} yb^n y^{-1}$.

Ahora bien, $ya^m y^{-1} = \left(yay^{-1}\right)^m$, y como yay^{-1} es un conjugado de a, se tiene $yay^{-1} \in \{a, b\}$. Análogamente con $yb^n y^{-1}$ y se concluye.

Ejercicio 3. *Sea N un subgrupo normal de índice finito en un grupo G :*

$$[G : N] = n.$$

Sea t un elemento de G y sea h el mínimo entero positivo tal que $t^h \in N$. Demostrar que h divide a n.

Solución. Si h es el mínimo entero positivo tal que $t^h \in N$ entonces también es el mínimo entero positivo tal que $(tN)^h = N$. Luego $h = o(tN)$ es el orden del elemento tN en el grupo cociente G/N. De esta forma, el teorema de Lagrange concluye que h divide a n.

Ejercicio 4. *Sea G un grupo finito y sean H y K subgrupos cuyos índices son primos entre sí. Probar que $G = HK$.*

Solución. Por el segundo teorema de isomorfismo podemos escribir:

$$[G : H \cap K] = [G : H][H : H \cap K] = [G : K][K : H \cap K].$$

De esta forma, puesto que $[G : H]$ y $[G : K]$ son primos entre sí, cada uno de los factores primos que aparece en la descomposición de $[G : H]$ ha de estar en $[K : H \cap K]$, y por tanto

$$[G : H] \text{ divide a } [K : H \cap K],$$

con lo que

$$[G : H]o(H) \text{ divide a } [K : H \cap K]o(H),$$

lo que significa que $o(G)$ divide a $card(HK)$, lo que implica que $G = HK$.

Ejercicio 5. *En las mismas condiciones del ejercicio anterior probar que*

$$G/(H \cap K) \simeq G/H \times G/K.$$

Solución. Sabemos por la teoría (observación 1.12.12) que existe un morfismo inyectivo de grupos

$$G/(H \cap K) \hookrightarrow G/H \times G/K,$$

y por tanto basta ver que ambos grupos tienen el mismo orden. Por ser $card(HK)o(H \cap K) = o(H)o(K)$, invirtiendo y multiplicando por $o(G)^2$ tendremos

$$\frac{o(G)}{card(HK)} \frac{o(G)}{o(H \cap K)} = \frac{o(G)}{o(H)} \frac{o(G)}{o(K)},$$

y por tanto $o(G/(H \cap K)) = o(G/H \times G/K)$.

Ejercicio 6. *Si N es un subgrupo normal de índice finito de un grupo G y H es un subgrupo de orden finito de tal forma que $[G : N]$ y $o(H)$ son primos entre sí, entonces HN.*

Solución. Sabemos que NH es un subgrupode G, con lo que NH/N es también un subgrupo de G/N, y por tanto $d = o(NH/N)$ divide a $[G : N]$. Ahora bien, por ser:

$$d = o(NH/N) = o(H/(H \cap N)) = \frac{o(H)}{o(H \cap N)},$$

se tiene que también d divide a $o(H)$ y por tanto $d = 1$ con lo que $NH = N$, lo que implica que $H \subset N$.

Ejercicio 7. *Sea G un grupo y $Z(G)$ su centro. Probar que si $G/Z(G)$ es un grupo cíclico, entonces G es abeliano.*

Solución. Que $G/Z(G)$ sea cíclico, quiere decir que está generado por una clase de la forma $tZ(G)$ para cierto $t \in G$. Esto proporciona la siguiente descomposición en clases de G:

$$G = \bigsqcup_r t^r Z(G).$$

De esta manera, dados $a, b \in G$, serán de la forma $a = t^r c$, $b = t^s c'$ para ciertos enteros r y s y ciertos elementos $c, c' \in Z(G)$. Ahora tenemos

$$ab = t^r c t^s c' = t^{r+s} cc' = t^s t^r c' c = t^s c' t^r c = ba,$$

donde hemos usado que c y c', al ser elementos del centro, conmutan entre sí y con las potencias de t. Con ello se concluye.

Ejercicio 8. *Sea G un grupo H y K dos subgrupos suyos. Consideremos la aplicación*

$$f : H \times K \to G : \; f(h, k) = hk.$$

Probar que f es un isomorfismo si y sólo si:
i) $hk = kh$, para todo $h \in H$ y $k \in K$.
ii) $H \cap K = \{1\}$
iii) $G = HK$.

Solución. Veamos en primer lugar los siguientes puntos.

a) f es un morfismo de grupos si y sólo si se cumple la condición i).

En efecto si f es un morfismo entonces $f(h', k) \cdot f(h, k') = f(h'h, kk')$, lo que equivale a que $h'khk' = h'hkk'$, esto es $kh = hk$.

b) Se cumple que $\ker(f) = H \cap K$.

En efecto si $h \in H \cap K$, entonces $(h, h^{-1}) \in \ker(f)$. Recíprocamente si $(h, k) \in \ker(f)$ entonces $hk = 1$, con lo que $h = k^{-1} \in H \cap K$.

Con ello se concluye fácilmente el enunciado del ejercicio.

Ejercicio 9. *Si G es un grupo y H es un subgrupo normal tal que $[G:H]=n$, probar que para todo elemento $g\in G$ se tiene $g^n\in H$. Dar un ejemplo que muestre que lo anterior no es cierto si H no es normal.*

Solución. Puesto que G/H es un grupo de orden n, cualquier elemento suyo $gH\in G/H$ cumple que $(gH)^n=g^nH=H$, de donde $g^n\in H$.

Un contraejemplo a este hecho viene dado por el grupo D_3, cuyo subgrupo $H=\langle f\rangle$ no es normal y cumple $[G:H]=3$, pero $(gf)^3=gf\notin H$.

Ejercicio 10. *Sea* $\mathbb{R}^*=\mathbb{R}\backslash\{0\}$ y consideremos el grupo multimplicativo $(\mathbb{R}^*,\cdot)$. Demostrar que no existe ningún subgrupo de índide finito impar en $(\mathbb{R}^*,\cdot)$.

Solución. Procedamos por reducción al absurdo y supongamos que existe un subgrupo H de índice impar $m\geq 3$. Entonces podemos escribir a $\mathbb{R}^*$ como unión disjunta

$$\mathbb{R}^*=H\cup g_1H\cup...\cup g_{m-1}H, g_i\notin H\ (1\leq i\leq m-1).$$

Ahora por ser m impar, existe un valor real para $a=\sqrt[m]{g_1}$. Como $[\mathbb{R}^*:H]=m$, por el ejercicio anterior, todo elemento de $\mathbb{R}^*$ elevado a m pertenece a H; en particular $a^m=g_1\in H$, lo que supone una contradicción.

Ejercicio 11. *Un grupo abeliano finito G (que supondremos dado en notación aditiva) se dice que es $p-$elemental (donde p es primo) si $p\cdot g=0$ para todo elemento $g\in G$. Probar que todo grupo abeliano $p-$elemental es suma directa de grupos cíclicos de orden p.*

Solución. Por el teorema de estructura podemos escribir

$$G=\mathbb{Z}/m_1\mathbb{Z}.\times\mathbb{Z}/m_2\mathbb{Z}.\times...\times\mathbb{Z}/m_r\mathbb{Z}$$

De esta forma si denotamos por $e_i\in G$ al generador correspondiente a $(0,...,1,...0)$, se tiene que su orden es m_i, pero por ser también $p\cdot e_i=0$, ha de cumplirse que p es múltiplo de m_i, con lo que $p=m_i$ y se concluye.

Ejercicio 12. *Clasificar todos los grupos abelianos de orden* $5^3\cdot 7^2$.

Solución. En primer lugar realizamos todas las particiones posibles de los dos exponentes, 3 y 2, en sumandos decrecientes:

$$\begin{array}{cc} 3=3 & 2=2\\ 3=2+1 & 2=1+1\\ 3=1+1+1 & \end{array}$$

y combinamos cada partición de la primera columna con cada una de la segunda, para obtener las siguientes descomposiciones de 5^37^2 en factores decrecientes: $\{5^37^2\}$, $\{5^37,7\}$, $\{5^27^2,5\}$, $\{5^27,5\cdot 7\}$, $\{5\cdot 7^2,5,5\}$, $\{5\cdot 7,5\cdot 7,5\}$, lo que proporciona los factores de torsión de todos los grupos abelianos de orden $5^3\cdot 7^2$.

Ejercicio 13. *Supongamos que G es un grupo de orden pq, con p,q primos distintos, y que existe un homomorfismo sobreyectivo*

$$g:G\rightarrow\mathbb{Z}_q.$$

Dempostrar que G tiene un subgrupo H isomorfo a $\mathbb{Z}_q$.
Solución. Puesto que g es sobreyectivo, existe $a \in G$ tal que $g(a) = \overline{1}$ (la clase del 1 en $\mathbb{Z}_q$ y generador de este grupo). De esta forma, puesto que $o(G) = pq$ se tiene $a^{pq} = 1$, esto es $(a^p)^q = 1$. De esta forma tenemos dos posibilidades

$$\begin{aligned} a^p &= 1 \\ a^p &\neq 1. \end{aligned}$$

En el primer caso se tiene que $g(a^p) = 0$, esto es $pg(a) = p \cdot \overline{1} = \overline{0}$. Como $\overline{1}$ es el generador del grupo cíclico $\mathbb{Z}_q$, ello implica que p es múltiplo de q, lo que es una contradicción.

De esta forma, $b = a^p \neq 1$, y como $b^q = 1$, el subgrupo $\langle b \rangle \subset G$ es cíclico de orden q, y por tanto isomorfo a $\mathbb{Z}_q$.

Ejercicio 14. *Sean p, q números primos distintos y supongamos que $o(G) = pq$, y que existen homomorfismo sobreyectivos $f : G \to \mathbb{Z}_p$ y $g : G \to \mathbb{Z}_q$. Demostrar que entonces $G \cong \mathbb{Z}_{pq}$, esto es, G es cíclico.*
Solución. Si llamamos $H = \ker(f)$, entonces $H \lhd G$, y como $G/H \cong \mathbb{Z}_p$, se sigue $o(H) = q$. Análogamente si llamamos $K = \ker(g)$, se tiene $K \lhd G$ y $o(K) = p$.

Por otra parte, se tiene que $HK = KH$ (ya que H y K son normales), con lo que HK es un subgrupo de G. Calculemos su orden:

$$o(HK) = \frac{o(H)o(K)}{o(H \cap K)} = \frac{pq}{1} = o(G).$$

Así $G = HK$. Veamos que $ab = ba$. Por una parte $ab \in aK = Ka$, con lo que

$$ab = b^j a, \text{ para cierto } j < ord(b).$$

Pero también $ab \in Hb = bH$, y por tanto

$$ab = ba^i, \text{ para cierto } i < ord(a).$$

En conclusión $b^j a = ba^i$, esto es $b^{j-1} = a^{i-1} \in H \cap K$ con lo que $j = 1$ e $i = 1$, y así $ab = ba$.

De esta forma, por la proposición 1.10, $ord(ab) = pq$, lo que implica que G es el grupo cíclico de orden pq.