Segundo Taller Algebra Abstracta

Jonathan Andrés Niño Cortés

20 de octubre de 2014

1. I.) ψ tal que $\psi(x) = \gamma_x$ es un homomorfismo $\psi : H \longmapsto Aut(N)$.

En primer lugar, debemos verificar que si $x \in H$, entonces $\gamma_x \in Aut(N)$, es decir, que γ_x sea un isomorfismo de N a N.

Tomemos cualquier γ_x. Como N es normal sabemos que $gNg^{-1} = N$ para cualquier $g \in G$. En particular, $\gamma_x(N) = xNx^{-1} = N$.

γ_x esta bien definida pues si $a = b$, entonces $xax^{-1} = xb^{-1}$ ya que la operación de grupo esta bien definida. Además si $a \in N$ entonces $xax^{-1} \in N$ pues $xax^{-1} \in xNx^{-1} = N$.

γ_x es inyectiva pues si $xax^{-1} = xbx^{-1}$, entonces $a = b$ por propiedad cancelativa.

γ_x es sobreyectiva. Si tomamos cualquier elemento $a \in N$ y como $N = xNx^{-1}$, entonces $a \in xNx^{-1}$, es decir, existe un $b \in N$ tal que $a = xbx^{-1}$. Por lo tanto, $\gamma_x(b) = a$.

Por lo tanto γ_x es una biyección.

Además γ_x es un homomorfismo ya que $\gamma_x(a)\gamma_x(b) = xax^{-1}xbx^{x-1} = xabx^{-1} = \gamma_x(ab)$. Por lo tanto γ_x es un automorfismo de N.

Ahora solo falta ver que ψ es un homomorfismo de grupos. Para eso tomemos γ_x y γ_y. En la tarea anterior se demostró que $\gamma_x \circ \gamma_y = \gamma_{xy}$. Por lo tanto, ψ es un homomorfismo.

II.) Primero demostremos que si $(N \cap H) = \{e\}$, entonces $(x, y) \mapsto xy$ es una biyección de $N \times H$ a NH. Denotamos la anterior aplicación por τ.

En primer lugar la aplicación esta bien definida pues si $(x, y) = (x'y')$ entonces $xy = x'y'$ porque la operación de grupo esta bien definida.

En segundo lugar la aplicación es inyectiva. Supongamos que $(x, y), (x', y') \in N \times H$ y $xy = x'y'$. Multipliquemos a la izquierda por $(x')^{-1}$ y a la derecha por y^{-1} y obtenemos

$$\begin{aligned} xy &= x'y' \\ (x')^{-1}xyy^{-1} &= (x')^{-1}x'y'y^{-1} \\ (x')^{-1}x &= y'y^{-1} \end{aligned}$$

La parte de la izquierda de la anterior igualdad pertenece claramente a N y la de la derecha a H, pues N y H son grupos. Al ser iguales significa que ambas pertenecen a $N \cap H$ pero esto implica que $(x')^{-1}x = y'y^{-1} = e$ por nuestra suposición. Finalmente como el inverso en un grupo es único, los inversos de $(x')^{-1}$, que son x y x' son iguales y los inversos de y^{-1}, y, y y' también son iguales. Luego, $(x, y) = (x'y')$.

En tercer lugar la aplicación es sobreyectiva. Tomemos cualquier elemento $x \in NH$, por definición existe $n \in N$ y $h \in H$ tales que $nh = a$. Por lo tanto, existe una preimagen de x que sería (n, h).

Ahora supongamos que $\psi(x) = id_N$ para cualquier $x \in H$. Esto significa que $\gamma_x(y) = xyx^{-1} = y$ para todo $y \in N$. Por lo tanto podemos demostrar que τ es un homomorfismo de grupos. Sean $(x, y), (x', y') \in N \times H$. Tenemos lo siguiente

$$\tau(x, y)\tau(x', y') = xyx'y' = xyx'(y^{-1}y)y' = xx'yy' = \tau(xx', yy').$$

Como podemos ver el hecho de que $\psi(x) = id_N$ implica que todos los elementos de N conmutan con los elementos de H. En conclusión τ es un isomorfismo.

2. El conjunto $N \ltimes_\psi H$ con la operación * es un grupo. Para demostrar la anterior afirmación demostremos que los axiomas de grupo se cumplen.

- * es asociativa: * se define como $(x_1, h_1) * (x_2, h_2) = (x_1\psi(h_1)(x_2), h_1h_2)$.
  Sean $(x_1, h_1), (x_2, h_2), (x_3, h_3) \in N \ltimes_\psi H$. Por un lado

$$\begin{aligned} [(x_1, h_1) * (x_2, h_2)] * (x_3, h_3) &= [(x_1\psi(h_1)(x_2), h_1h_2)] * (x_3, h_3) \\ &= (x_1\underline{\psi(h_1)(x_2)\psi(h_1h_2)(x_3)}, h_1h_2h_3) \qquad (1) \end{aligned}$$

Por otro lado

$$\begin{aligned} (x_1, h_1) * [(x_2, h_2) * (x_3, h_3)] &= (x_1, h_1) * [(x_2\psi(h_2)(x_3), h_2h_3)] \\ &= (x_1\underline{\psi(h_1)\big(x_2\psi(h_2)(x_3)\big)}, h_1h_2h_3) \qquad (2) \end{aligned}$$

Como se puede observar para demostrar que la operación es asociativa basta con demostrar que las partes subrayadas en las ecuaciones anteriores son iguales. Por otra parte, sabemos que $\psi(h_1)$ es un automorfismo de N. Además, $x_2 \in N$ y $\psi(h_2)(x_3) \in N$ tambien porque $x_3 \in N$ y $\psi(h_2)$ también es un automorfismo de N que por lo tanto mapea elementos de N a N. Las anteriores observaciones os permiten concluir lo siguiente:

$$\psi(h_1)\big(x_2\psi(h_2)(x_3)\big) = \psi(h_1)(x_2)(\psi(h_1)\big(\psi(h_2)(x_3)\big)$$

Como ψ es un homomorfismo tenemos que $\psi(h_1h_2) = \psi(h_1) \circ \psi(h_2)$. Es decir que

$$\psi(h_1)(x_2)\psi(h_1)\big(\psi(h_2)(x_3)\big) = \psi(h_1)(x_2)\psi(h_1h_2)(x_3)$$

Por lo que (1) y (2) son equivalentes.

- Identidad: El elemento (e, e') es la identidad de este grupo, donde e es la identidad de N y e' es la identidad de H. Para probar esto tomemos cualquier elemento $(x, h) \in N \ltimes_\psi H$.

$$(x, h) * (e, e') = (x\psi(h)(e), he')$$

  Como $\psi(h)(e)$ es un automorfismo, $\psi(h)(e) = e$. Por lo tanto,

$$(x\psi(h)(e), he') = (xe, he') = (x, h)$$

  Ahora tomemos

$$(e, e') * (x, h) = (e\psi(e')(x), e'h)$$

  Como ψ es un homorfismo, tenemos que $\psi(e')$ debe ser igual a la identidad de $Aut(N)$, es decir, id_N. Por lo tanto, $\psi(e')(x) = id_N(x) = x$.
  Finalmente, tenemos

$$(e\psi(e')(x), e'h) = (ex, e'h) = (x, h)$$

  Por lo cual (e, e') es la identidad de $N \ltimes_\psi H$.

- Inverso: Tomemos cualquier elemento $(x, h) \in N \ltimes_\psi H$. Probamos que el elemento $([\psi(h^{-1})(x)]^{-1}, h^{-1})$ es el inverso de (x, h).
  Estamos buscando un elemento $(a, b) \in N \ltimes_\psi H$ tal que $(a, b) * (x, h) = (e, e')$. Se puede observar facilmente que b debe ser igual a h^{-1}. Por otra parte a debe ser tal que $a\psi(h^{-1})(x) = e$. Por lo tanto, $a = [\psi(h^{-1})(x)]^{-1}$. Se puede observar que $[\psi(h^{-1})(x)]^{-1} \in N$ porque $\psi(h^{-1})(x) \in N$ y como N es grupo, el inverso también pertenece a N.
  Por otra parte observemos que $(x, h) * ([\psi(h^{-1})(x)]^{-1}, h^{-1}) = (e, e')$

$$(x, h) * ([\psi(h^{-1})(x)]^{-1}, h^{-1}) = (x\psi(h)([\psi(h^{-1})(x)]^{-1}), hh^{-1})$$

  Como $\psi(h^{-1})$ es un automorfismo tenemos que $[\psi(h^{-1})(x)]^{-1} = \psi(h^{-1})(x^{-1})$. Por otro lado como ψ es un homomorfismo tenemos que $\psi(h)([\psi(h^{-1})(x^{-1})]) = \psi(hh^{-1})(x^{-1}) = \psi(e')(x^{-1}) = id_N(x^{-1}) = x^{-1}$. Por lo tanto,

$$(x\psi(h)([\psi(h^{-1})(x)]^{-1}), hh^{-1}) = (xx^{-1}, hh^{-1}) = (e, e')$$

Por ultimo, hay que observar que $N \ltimes_\psi H$ sea el producto semidirecto de N y H.

Identificando H con $e \times H$ y N con $N \times e'$ podemos ver que $N \cap H = \{e\}$.

Además, $N \ltimes_\psi H = NH$. Tomemos un elemento $(x_1, h_1) \in N \ltimes_\psi H$. Se puede ver que $(x_1, h_1) = (x_1, e) * (e', h_1)$.

$$(x_1, e') * (e, h_1) = (x_1\psi(e')(e), e'h_1) = (x_1 e, e'h_1) = (x_1, h_1)$$

Por lo tanto $(x_1, h_1) \in NH)$. Por otra parte tomemos un elemento $a \in NH$ Por lo tanto, $a = (x, e') * (e, h)$ para algun $x \in N$ y $h \in H$. Vemos que $(x, e') \in N \ltimes_\psi H$ y $(e, h) \in N \ltimes_\psi H$. Por lo tanto, como a es producto de estos elementos también pertenece a $N \ltimes_\psi H$.

Por ultimo veamos que $\psi(h)(x) = h * x * h^{-1}$.

Por nuestras identificaciones tenemos que $h * x * h^{-1} = (e, h) * (x, e') * (e, h^{-1}) = (e\psi(h)(x), he') * (e, h^{-1}) = (\psi(h)(x)\psi(h)(e), hh^{-1}) = (\psi(h)(x)e, e') = (\psi(h)(x), e') = \psi(h)(x)$.

3. I.) Sean m, n enteros primos relativos. Si un elemento x de un grupo G satisface $x^m = x^n = 1$, entonces es cierto que $x = 1$.

Demostración. Sabemos que el orden de x debe dividir tanto a m como a n. Luego $|{<}x{>}|$ es un divisor común de m y n. Por propiedades del máximo común divisor sabemos que $|{<}x{>}| \leq (m, n)$. Pero como $(m, n) = 1$ la única posibilidad es que $|{<}x{>}| = 1$. Lo que implica que $x = 1$. □

II.) Demostrar que si m, n son enteros primos relativos la aplicación

$$\phi : (\mathbb{Z}/mn, +) \to (\mathbb{Z}/m, +) \times (\mathbb{Z}/n, +),$$

definida por $\phi(\bar{a}) := (\bar{a}, \bar{a})$, es un isomorfismo de grupos.

Demostración. Para esto demostraremos que ϕ es un homomorfismo biyectivo.

- ϕ esta bien definida.
  Sean $\bar{a}, \bar{b} \in \mathbb{Z}/mn$, tales que $\bar{a} = \bar{b}$. Esto significa que $a \equiv b \pmod{mn}$. Esto a su vez significa que $mn|b - a$. Pero de aqui podemos deducir que $m|b - a$ y $n|b - a$. Por lo tanto, $a \equiv b \pmod{m}$ y $a \equiv b \pmod{n}$. Esto equivale a que $\phi(\bar{a}) = (\bar{a}, \bar{a}) = (\bar{b}, \bar{b}) = \phi(\bar{b})$.
- ϕ es inyectiva.
  Sean $\bar{a}, \bar{b} \in \mathbb{Z}/mn$, tales que $\phi(\bar{a}) = \phi(\bar{b})$. Por lo mostrado anteriormente esto equivale a que $a \equiv b \pmod{m}$ y $a \equiv b \pmod{n}$. Ahora tenemos que $m|(b-a)$ y $n|(b - a)$. Por lo tanto, $[m, n]|(b - a)$. Pero tenemos que $mn = (m, n)[m, n]$ y como $(m, n) = 1$, $mn = [m, n]$. Por lo tanto $mn|(b - a)$, es decir, $a \equiv b \pmod{mn}$. Por lo tanto, $\bar{a} = \bar{b}$.
- ϕ es sobreyectiva.
  Sean $(\bar{a}, \bar{b}) \in (\mathbb{Z}/m, +) \times (\mathbb{Z}/n, +)$. Ahora estamos buscando un $x \in \mathbb{Z}$ tal que $x \equiv a \pmod{m}$ y $x \equiv b \pmod{n}$. Por el teorema chino del residuo este x existe y además es único módulo mn. Entonces tenemos que $\phi(\bar{x}) = (\bar{x}, \bar{x}) = (\bar{a}, \bar{b})$.

- ϕ es un homomorfismo.
  Observese que

$$\phi(\bar{a}) + \phi(\bar{b}) = (\bar{a}, \bar{a}) + (\bar{b}, \bar{b}) = (\bar{a} + \bar{b}, \bar{a} + \bar{b}) = \phi(\bar{a} + \bar{b})$$

$\square$

4. Demostrar que si m es un entero sin cuadrados, o sea m no es divisible por ningun cuadrado distinto de 1, entonces cada grupo abeliano G de orden m es cíclico.

Demostración. Como m es libre de cuadrados, se puede expresar de la forma $m = p_1 p_2 \cdots p_n$ con p_i primo y $p_i \neq p_j$ si $i \neq j$. Por el primer teorema de Sylow tenemos que existen p_i-subgrupos de Sylow para $1 \leq i \leq n$.

Además, sea S y S' p_i-subgrupos de Sylow. Por el segundo teorema de Sylow tenemos que $S' = gSg^{-1}$, pero como G es abeliano, tenemos qe $gSg^{-1} = S$ lo que implica que $S' = S$ y por lo tanto solo existe un p_i-subgrupo de Sylow para cada $1 \leq i \leq n$.

El orden de cada p_i-subgrupo de Sylow es p_i ya que m es libre de cuadrados. En clase se ha demostrado que los únicos grupos de orden algun primo son cíclicos. Por lo tanto, cada p_i-subgrupo de Sylow es isomorfo a $\mathbb{Z}/p_i$.

Vamos a demostrar por inducción que $\mathbb{Z}/p_1\mathbb{Z}/p_2 \cdots \mathbb{Z}/p_k$ es un subgrupo normal cíclico de G de orden $p_1 \cdots p_k$. El caso base es cuando $k = 1$. En cuyo caso claramente $\mathbb{Z}/p_1$ es un subgrupo normal cíclico de orden p_1. Para el paso inductivo supogamos que $\mathbb{Z}/p_1 \cdots \mathbb{Z}/p_k$ es un subgrupo normal cíclico y tomemos $\mathbb{Z}/p_1 \cdots \mathbb{Z}/p_k\mathbb{Z}/p_{k+1}$. Para mayor comodidad sea $S = \mathbb{Z}/p_1 \cdots \mathbb{Z}/p_k$, $T = \mathbb{Z}/p_{k+1}$ y $ST = \mathbb{Z}/p_1 \cdots \mathbb{Z}/p_k\mathbb{Z}/p_{k+1}$. Por un lado tenemos que si $x \in S \cap T$ entonces $x^{p_1 \cdots p_k} = x^{p_{k+1}} = e$ y $(p_1 \cdots p_k, p_{k+1}) = 1$. Por lo demostrado en el punto 3 I), tenemos que $x = e$, es decir, $S \cap T = \{e\}$. Por la formula del producto tenemos que $|ST||S \cap T| = |S||T|$, es decir, $|ST| = p_1 \cdots p_k p_{k+1}$.

Ahora para demostrar que ST es un subgrupo demostremos que la multiplicación esta cerrada y que los inversos estan incluidos.

Tomemos dos elementos $x, y \in ST$, entonces existen $s_1, s_2 \in S$ y $t_1, t_2 \in T$ tales que $x = s_1 t_1$ y $y = s_2 t_2$. Entonces tomemos $xy = s_1 t_1 s_2 t_2$. Como G es abeliano tenemos que $xy = s_1 t_1 s_2 t_2 = s_1 s_2 t_1 t_2 \in ST$.

Por otra parte tomemos $x = st \in ST$, como G es abeliano $x = st = ts \in ST$ por lo tanto, $x^{-1} = (st)^{-1} = (ts)^{-1} = s^{-1}t^{-1} \in ST$.

Por lo tanto ST es un subgrupo normal.

Ahora por producto directo como S y T son subgrupos normales tenemos que $ST \cong S \times T$. Y como S, T son cíclicos y sus ordenes son primos relativos entonces podemos aplicar lo demostrado en el punto 3 II) para concluir que $S \times T \cong \mathbb{Z}/p_1 p_2 \cdots p_k p_{k+1}$.

Una consecuencia de esto es que $\mathbb{Z}/p_1\mathbb{Z}/p_2 \cdots \mathbb{Z}/p_n \cong \mathbb{Z}/m$. Observese que el orden de $\mathbb{Z}/p_1\mathbb{Z}/p_2 \cdots \mathbb{Z}/p_n$ es m. Por lo tanto, tenemos un subgrupo de G cuyo orden es igual al de G. La única posibilidad es que $\mathbb{Z}/p_1\mathbb{Z}/p_2 \cdots \mathbb{Z}/p_n = G$. Por lo tanto, $G \cong \mathbb{Z}/m$.

□

5. Sea G un grupo finito de orden par. Demostrar que existe un elemento $x \in G$ tal que $x \not 1$ y $x^2 = 1$.

Demostración. Lo anterior quiere decir que existe un elemento x con orden 2. En el libro de Rotman se demuestra un teorema que dice que si p es un número primo que divide al orden de G entonces debe existir algun elemento de orden p. Aplicando este teorema para $p = 2$ obtenemos este resultado. □

6. Demostrar que un grupo G de orden 4 es isomorfo a $\mathbb{Z}/4$ o $\mathbb{Z}/2 \times \mathbb{Z}/2$.

Demostración. En primer lugar tenemos que G es un 2-grupo pues su orden es 2^2. Sabemos por un teorema que el número de subgrupos de orden p en un p-grupo es congruente a 1 módulo p. Por lo tanto el número de subgrupos de G de orden 2 es congruente a 1 módulo 2. Por otro lado el número de subgrupos de orden 2 no puede exceder 3 pues vemos que si hay tres subgrupos diferentes serian de la forma $\{e, x\}, \{e, y\}, \{e, z\}$ con x, y, z diferentes entre si y vemos que aqui ya estan incluidos los 4 elementos del grupo G. En otras palabras, un número mayor de subgrupos excederia el número de elementos de G. Denotemos como r el número de subgrupos de G de orden 2. Por lo tanto, tenemos dos casos: $r = 1$ o $r = 3$.

En el primer caso tenemos que el grupo es cíclico pues se demostró que si un grupo G es de tal manera que para cada divisor $d \big| |G|$ tenemos un único subgrupo de orden d , entonces G es cíclico. Los divisores de 4 son 1, 2, 4. Claramente solo hay un subgrupo de orden 1 que es el subgrupo trivial y un subgrupo de orden 4 que es G y por nuestra suposición como $r = 1$ solo hay un subgrupo de orden 2. Por lo tanto G es cíclico. Es decir, $G \cong \mathbb{Z}/4$.

Por otra parte, si $r = 3$ tenemos que hay tres subgrupos de orden 2. Veamos que si H es un subgrupo de G de orden 2 entonces H es normal. Por el teorema de Lagrange tenemos que $[G : H] = |G|/|H| = 4/2 = 2$. Ahora, en la tarea anterior demostramos que si el indice de un subgrupo era 2 entonces este subgrupo deberia ser normal. Por lo tanto, H es un subgrupo normal. Entonces sean S, T dos de los tres subgrupos de G de orden 2. Como S y T son diferentes tenemos que $S \cap T = \{e\}$, o de lo contrario S y T serian iguales.

Por otro lado resta probar que $ST = G$. Sea $S = \{e, s\}$ y $T = \{e, t\}$ con $s \neq t$ y $s, t \neq e$. Entonces, $ST = \{ee, et, se, st\} = \{e, t, s, st\}$. Ahora observemos que $st \neq e$, pues de lo contrario, s seria el inverso de t y viceversa, pero esto es una contradicción pues como el orden de s y t es dos, el inverso de s es s y el inverso de t es t. Por otra parte si $st = s$ entonces t=e, lo que contradice el hecho de que T sea subgrupo de orden 2. Lo mismo ocurre para S si $st = t$. Por lo tanto la única posibilidad es que st

sea un elemento distinto y por lo tanto $|ST| = 4$. Pero el único subconjunto de orden 4 de G es G. Por lo tanto, $ST = G$.

Finalmente, utilizando producto directo obtenemos que $G \cong S \times T$ y como el orden de S,T es 2, que es primo, estos a su vez son isomorfos a $\mathbb{Z}/2$. Por lo tanto, $G \cong \mathbb{Z}/2 \times \mathbb{Z}/2$. $\square$

7. Demostrar que el grupo de automorfismos de $\mathbb{Z}/2 \times \mathbb{Z}/2$ es isomorfo a S_3.

Demostración. Sea $\mathbb{Z}/2 \times \mathbb{Z}/2 = \{e, x, y, z\}$. Como se observo anteriormente cada elemento diferente de e es de orden 2. Asi sabemos que $x^2 = y^2 = z^2 = e$. Además tenemos que $xy = z; yz = x$ y $zx = y$. Por ultimo sabemos que $\mathbb{Z}/2 \times \mathbb{Z}/2$ es abeliano.

Ahora queremos probar que las biyecciones que fijan el elemento e son automorfismos de $\mathbb{Z}/2 \times \mathbb{Z}/2$ Sea $\alpha : \mathbb{Z}/2 \times \mathbb{Z}/2 \to \mathbb{Z}/2 \times \mathbb{Z}/2$ una biyección tal que $\alpha(e) = e$.

Para probar que es un isomorfismo tomemos cualquier elemento $s, t \in \mathbb{Z}/2 \times \mathbb{Z}/2$.

Tomemos $\alpha(st)$. Queremos demostrar que $\alpha(st) = \alpha(s)\alpha(t)$ En el caso en el que $s = e$ esto se cumple pues $\alpha(et) = \alpha(t) = e\alpha(t) = \alpha(e)\alpha(t)$. En el caso en el que $t = e$ también tenemos que $\alpha(se) = \alpha(s) = \alpha(t)e = \alpha(t)\alpha(e)$

Ahora para el caso en que $s \neq e$ y $t \neq e$. Tenemos otros dos casos, o bien $s = t$ o $s \neq t$. En el primer caso entonces $\alpha(st) = e$. Por otro lado como α esta bien definida y es inyectiva tenemos que $s = t$ si y solo si $\alpha(s) = \alpha(t)$. Por lo tanto, $\alpha(s)\alpha(t) = e$. En el segundo caso de nuevo como α esta bien definida e inyectiva $s \neq t$ si y solo si $\alpha(s) \neq \alpha(t)$. Esto nos permite concluir que $\alpha(s)\alpha(t) = \alpha(st)$, pues por la anterior condición $\alpha(s)\alpha(t)$ no es ni $\alpha(s)$ ni $\alpha(t)$ ni $\alpha(e)$. La única posibilidad es que sea $\alpha(st)$.

Por otro lado si la biyección no fija a e entonces no es un isomorfismo pues la anterior condición es necesaria para que sea un isomorfismo.

Por lo tanto vemos que los automorfismos son permutaciones de los tres elementos x, y y z distintos de e. Por lo tanto $Aut(\mathbb{Z}/2 \times \mathbb{Z}/2) \cong S_3$. $\square$

8. En la anterior tarea demostramos que γ_a (conjugación por a) es un automorfismo. Por lo tanto si H es caracteristico entonces se cumple que $aHa^{-1} = H$ para todo $a \in H$. Pero vemos que esto es una de las caracterizaciones de que H sea normal.

Ahora para demostrar que un subgrupo caracteristico K de un subgrupo normal N de G es normal en N, vamos a demostrar que $\gamma_a \in Aut(N)$ para todo $a \in G$.

Por un lado ya sabemos que γ_a esta bien definida y es inyectiva en el dominio G. Si nos restringimos al dominio N estas propiedades todavia se siguen cumpliendo.

Por otro lado sabemos que $\gamma_a(N) = N$, pues como N es normal tenemos que $aNa^{-1} = N$. De aqui se deduce que γ_a es sobreyectiva con dominio N y rango N.

Además sigue siendo un homomorfismo pues si $x, y \in N$ entonces $x, y \in G$ y como γ_a es un homomorfismo de G se cumple que $\gamma_a(x)\gamma_a(y) = \gamma_a(xy)$.

Por lo tanto $\gamma_a \in Aut(N)$. Ahora si tomamos un subgrupo caracteristico K de N sabemos que $f(K) = K$ para todo $f \in Aut(N)$. En particular sabemos que $\gamma_a(K) = K$ para todo $a \in G$. Pero esto significa que $aKa^{-1} = K$, es decir, K es normal en G.

Veamos que si no es caracteristico entoces no es normal necesariamente. Tomemos el grupo V_4. En la tarea anterior demostramos que V_4 es normal en S_4. Además, demostramos que el subgrupo generado por un elemento de V_4 diferente a la identidad es normal en V_4, pues $[V_4 : <x>] = |V_4|/|<x>| = 4/2 = 2$ y se demostro que un subgrupo con indice 2 es normal. Pero también se demostro que $<x>$ no es un subgrupo normal de S_4.

9. Sea G un grupo y $H \leq G$. Demostrar que el nucleo del homomorfismo $\rho : g \to S_{G/H}$ correspondiente a la acción de G por translación sobre las clases laterales izquierdas de H en G (que denotamos por G/H) tiene por nucleo el subgrupo normal de G más grande contenido en H.

Demostración. Sea K el kernel de ρ por definición es el conjunto de los elementos en G tales que $\rho(g) = (1)$, donde (1) es la permutación identidad de $S_{G/H}$. Por definición de ρ esto quiere decir que $g \cdot x = x$ para todo $x \in G/H$.

La primera observación es que K es normal porque el kernel de cualquier homomorfismo es normal. La segunda observación es que $K \subset H$. Para esto tomemos cualquier elemento $k \in K$. En particular se cumple que $kH = H$. Como H es subgrupo de G tenemos que $e \in H$ y por lo tanto $ke \in kH$ finalmente como $kH = H, ke \in H$, es decir $k \in H$.

La tercera observación es que si $a \in G$ es un elemento tal que $a \in H$ y $a \in N$ donde $N \trianglelefteq G$ y $N \subset H$ entonces $a \in K$.

Tomemos cualquier elemento $x \in G/H$. Por propiedades de las clases laterales izquierdas sabemos que $x = gH$ para algun $g \in G$. Ahora aplicamos la acción de translación con el elemento a. Tenemos que $a \cdot gH = agH$. Pero como a pertenece a un subgrupo normal de G tenemos que $ag = ga'$ para algun $a' \in N$. Por lo tanto, $agH = ga'H$. Por ultimo tenemos que como $a' \in H$, $a'H = H$. Luego $ga'H = gH$. Como gH era cualquier elemento en G/H esto significa que $a \in K$.

Las tres observaciones anteriores implican que K debe ser el subgrupo normal más grande de G contenido en H. □

10. I.) Si H y K son subgrupos de G de indice finito, entonces $H \cap K$ tiene también indice finito en G. Ademas, $[G : H \cap K] \leq [G : H][G : K]$.

Demostración. Sea $\rho : G/H\cap K \to G/H \times G/K$ una función tal que $\rho(g(H\cap K)) = (gH, gK)$. Demostramos que la función esta bien definida y es inyectiva.

Tomemos $g, g' \in G$ tales que $g(H \cap K) = g'(H \cap K)$. Esto equivale a qu $g^{-1}g' \in (H \cap K)$. Esto a su vez equivale a que $g^{-1}g' \in H$ y $g^{-1}g' \in K$. Es decir que $gH = g'H$ y $gK = g'K$.

Como tenemos una función inyectiva concluimos que $[G : H \cap K] \leq [G : H][G : K]$. $\square$

II.) Si H tiene indice finito en G, entonces la intersección de todos los conjugados de H es un subgrupo normal de G de indice finito.

Demostración. En primer lugar debemos demostrar que el conjugado de H tendra un indice finito. Esto se puede observar porque existe una biyección entre G/H (las clases laterales izquierdas de G en H) y $G/(gHg^{-1})$. Sea esta biyección denotada por ρ y definida de tal manera que $\rho(g'H) = gg'g^{-1}(gHg^{-1}) = gg'Hg^{-1}$.

ρ esta bien definida: Sea $g_1H = g_2H$, por lo tanto $gg_1Hg^{-1} = gg_2Hg^{-1}$.

ρ es inyectiva: Sea $gg_1Hg^{-1} = gg_2Hg^{-1}$. Esto implica que $g^{-1}gg_1Hg^{-1}g = g^{-1}gg_2Hg^{-1}g$, es decir que $g_1H = g_2H$

ρ es sobreyectiva. Tomemos cualquier $g'gHg^{-1}$. La preimagen de este elemento bajo ρ sería $g^{-1}g'g$. En efecto $\rho(g^{-1}g'g) = gg^{-1}g'gg^{-1}gHg^{-1} = g'gHg^{-1}$.

Esto demuestra que $[G : H] = [G : gHg^{-1}]$.

Ahora sea $I = \bigcap_{g \in G} gHg^{-1}$. Por lo demostrado en el punto anterior, como la intersección de subgrupos con índice finito da un indice finito, el índice de I debe ser finito.

Ahora para demostrar que I es normal en G, demostremos que $I = gIg^{-1}$ para cualquier $g \in G$.

Primero demostremos que para cualquier $g \in G$, $gIg^{-1} \subseteq I$. Sea $a \in gIg^{-1}$, es decir que $a = gig^{-1}$ para algun $i \in I$. Ahora para demostrar que $a \in I$, demostramos que $a \in fHf^{-1}$ para todo $f \in G$. En efecto como $i \in I$, $i \in g^{-1}fHf^{-1}g$. Es decir que $i = g^{-1}fhf^{-1}g$ para algun $h \in H$. Luego $a = gig^{-1} = gg^{-1}fhf^{-1}gg^{-1} = fhf^{-1}$, es decir que $a \in fHf^{-1}$. Como esto se demostro para cualquier f concluimos que $a \in I$.

Ahora para demostrar que $I \subseteq gIg^{-1}$, tomemos un elemento $i \in I$. Tenemos que $g^{-1}ig \in g^{-1}Ig$, y por lo demostrado justo antes tenemos que $g^{-1}ig \in I$. Por lo tanto, $gg^{-1}igg^{-1} = i \in gIg^{-1}$.

Concluimos que I es normal. $\square$

III.) Si $([G : H], [G : K]) = 1$, entonces $[G : H \cap K] = [G : H][G : K]$.

Demostración. Para esto utilizamos el teorema de Lagrange generalizado: *Sea $H \leq K \leq G$, entonces $[G : H] = [G : K][K : H]$.*

Como demostramos el la parte I), $[G : H \cap K]$ es finito. Denotemos por comodidad, $a = [G : H]$, $b = [G : K]$ y $c = [G : H \cap K]$. Tenemos que $c \leq ab$. Además por el teorema de Lagrange tenemos que $c = a * [H : H \cap K]$ y $c = b * [K : H \cap K]$, es decir que $a|c$ y $b|c$. Por lo tanto, el minimo comun múltiplo $[a, b] \leq c$. Pero como $(a, b) = 1$, tenemos que $[a, b] = ab$. Es decir que $ab \leq c$ y como $ab \geq c$ concluimos que $ab = c$. $\square$

11. Demostrar que A_6 no contiene subgrupos de indice primo.

Demostración. El orden de A_6 es $|A_6| = 6!/2 = 2^3 * 3^2 * 5 = 360$. Como el indice debe ser un divisor del orden del grupo, las posibilidades son 2, 3 y 5. Ahora en el libro de Rotman tenemos el siguiente corolario:

Si G es un grupo simple, y $[G : H] = n$ entonces existe un homomorfismo inyectivo $\rho : G \to S_n$.

De este resultado se concluye que $|G|\big||S_n| = n!$ pues la imagen del homomorfismo debe ser un subgrupo de S_n y además al ser inyectivo tenemos que G es isomorfo a este subgrupo. Finalmente aplicamos el teorema de Lagrange.

Asi que supongamos por contradicción que exista un subgrupo H tal que $[A_6 : H] = 2, 3$ ó 5.

Por lo discutido anteriormente tendriamos que $|A_6|$ divide a $2!, 3!$ o $5!$. Pero $2! = 4, 3! = 6$ y $5! = 120$ son menores y por lo tanto no divisibles por 360. Llegamos a una contradicción y por lo tanto H no puede existir. □

12. Sea G un grupo finito que contenga un subgrupo H de indice p, donde p es el divisor primo mas pequeño de $|G|$. Demostrar que H es un subgrupo normal de G.

Demostración. Tomemos el homomorfismo asociado a la acción de translación de las clases laterales izquierdas (el del punto 9). Sea ρ este isomorfismo. Tenemos que $\rho : G \to S_{G/H} = S_p$. Por lo demostrado en el punto 9 tenemos que el kernel de ρ es el subgrupo normal de G más grande contenido en H.

Por otra parte, por el primer teorema de isomorfismo $G/ker(\rho) \cong \mathrm{Img}_\rho(G)$. Donde $\mathrm{Img}_\rho(G)$ es la imagen de G en S_p por el homomorfismo ρ. Sabemos que $\mathrm{Img}_\rho(G)$, es un subgrupo de S_p. Por lo tanto, tenemos que $|\mathrm{Img}_\rho(G)|\big|p!$ Además, tenemos que $|G|/|ker(\rho)| = |\mathrm{Img}_\rho(G)|$. Así que $|G|/|ker(\rho)|\big|p!$.

Por otra parte tenemos que $|G|/|ker(\rho)| = (|G|/|H|)(|H|/|ker(\rho)|) = p[H : ker(p)]$.

Es decir que $p[H : ker(p)]|p!$, lo que implica que $[H : ker(p)]|(p-1)!$.

Ahora si suponemos que $[H : ker(p)] > 1$, tenemos que $[H : ker(\rho)]$ es divisible por algun primo p' menor que p. Pero podemos ver que $|G| = (|G|/|H|)|H| = p|ker(\rho)|[H : ker(\rho)]$, es decir que $[H : ker(\rho)]$ divide a $|G|$ y por transitividad tenemos que p' divide a $|G|$. Esto ultimo contradice la minimalidad de p.

Por lo tanto $[H : ker(\rho)] = 1$ lo que significa que $H = ker(\rho)$ y como el kernel de un homomorfismo es normal tenemos que H es normal.

□

13. Sea G un grupo finito que actue sobre un conjunto finito X.

I.) Suponiendo que cada órbita contenga al menos 2 elementos, que $|G| = 15$ y que $|X| = 17$, determinar el numero de órbitas y la cardinalidad de cada una.

Demostración. Sabemos que por cada orbita hay un estabilizador correspondiente y que los estabilizadores son subgrupos de G. Sabemos además por el teorema de Lagrange que el orden de subgrupo debe dividir el orden del grupo. Por lo tanto podemos tener estabilizadores de orden 1, 3, 5 o 15.

El 15 lo podemos descartar porque si hubiera un estabilizador con dicho orden entonces el orden de la orbita correspondiente sería $|O_x| = [G : G_x] = 1$. Pero por nuestras suposiciones no pueden haber orbitas de un solo elemento.

Los subgrupos de orden 3 y 5 serian p-subgrupos de Sylow. Por lo tanto, podemos utilizar el primer teorema de Sylow para afirmar que dichos subgrupos existen.

Ahora si tenemos estabilizadores de orden 3 entonces las orbitas correspondientes tendria tamaño igual a $|O_x| = [G : G_x] = 15/3 = 5$.

Si tenemos estabilizadores de orden 5 entonces las orbita correspondientes tendria tamaño igual a $|O_x| = [G : G_x] = 15/5 = 3$.

Y si tenemos el estabilizador de orden 1 entonces las orbitas correspondientes tendrian tamaño igual a $|O_x| = [G : G_x] = 15/1 = 15$.

Pero la suma del tamaño de todas las orbitas debe ser igual a 17. La única manera de escribir 17 como combinación lineal con coeficientes enteros positivos de 3,5 y 15 es 17 = 4*3+1*5+0*15. Por lo tanto hay 4 orbitas de orden 3 y 1 orbita de orden 5. □

II.) Suponiendo que $|G| = 33$ y que $|X| = 19$, demostrar que existe al menos una órbita que contenga un solo elemento.

Demostración. Supongamos por contradicción que no hay orbitas con un solo elemento. Entonces utilizando los mismos argumentos del punto anterior tenemos que los estabilizadores pueden ser de orden 1, 3 o 11, y por lo tanto las orbitas pueden ser de tamaño 33, 11 o 3. Pero la suma del tamaño de todas las órbitas debe ser igual a 19. Claramente no pueden haber órbitas de 33 elementos. Pero 19 no se puede escribir como combinación lineal de 11 y 3.

Si suponemos que no hay orbitas de tamaño 11, entonces solo podrian haber orbitas de 3 pero $3 \nmid 19$.

Si suponemos que hay una orbita de tamaño 11, entonces el resto de las órbitas serian de tamaño 3 pero $3 \nmid 19 - 11 = 8$.

Y no pueden haber dos órbitas de tamaño 11 porque 22 excede el tamaño del conjunto X.

Por lo tanto, G no podría actuar sobre X. Por lo tanto deben existir órbitas de un elemento. □

14. Sea G un grupo no abeliano de orden 12 y sea H un 3-Sylow de G. Consideremos el homomorfismo $\theta : G \to S_{G/H}$ correspondiente a la acción de G por translación sobre

G/H. Demostrar que θ no es injectivo si y solo si H es normal en G. Concluir que, si H no es normal en G, entonces el grupo G es isomorfo a A_4.

Demostración. Consideremos primero el número de 3-subgrupos de Sylow posibles. Por el segundo teorema de Sylow tenemos que $n_3 \equiv 1 \pmod 3$ y $n_3|4$. Asi que $n_3 = 1 o n_3 = 4$.

Ahora empecemos suponiendo que H es normal. Por lo demostrado en el punto 9, el kernel de θ es el subgrupo de H más grande que es normal en G. Así que si H es normal el kernel debe ser igual a H. Como el kernel tiene más de un elemento el homomorfismo no es inyectivo.

Ahora empecemos suponiendo que el homomorfismo no es inyectivo. Esto implica que el kernel de θ es diferente de la identidad. Pero sabemos por lo probado en el punto 9 que el el kernel es un subgrupo de H. Ahora por el teorema de Lagrange tenemos que el orden del kernel divide a $|H|$ pero como $|H| = 3$ esto implica que el orden del kernel debe ser igual a 3. Es decir, que el kernel es igual a H. Y como un kernel es normal tenemos que H es normal.

Ahora si H no es normal entonces H es isomorfo a A_4, entonces sabemos que el homomorfismo es inyectivo. Esto quiere decir que $G \cong \theta(G)$ donde $\theta(G)$ es la imagen de G por θ. Además tenemos que $\theta(G) \leq S_{G/H} = S_4$. Pero el único subgrupo de S_4 con orden 12 es A_4. Por lo tanto, $G \cong A_4$.

□

15. Sea G y H el grupo y el subgrupo del problema anterior. Ahora supongamos que G no es isomorfo a A_4. Demostrar que entonces G tiene un único 3-Sylow $H = 1, a, a^2$. Demostrar después que si g contiene un elemento b de orden 4, entonces a y b satisfacen las relaciones $a^3 = b^4 = 1$ y $bab^{-1} = a^2 = a^{-1}$.

Demostración. Si G no es isomorfo a A_4 es porque el homomorfismo no es inyectivo. Por lo tanto, el subgrupo H es normal en G. Claramente podemos escribir $H = \{1, a, a^2\}$ pues H es cíclico. Ahora si suponemos que existe un elemento b de orden 4, entonces existiria un subgrupo cíclcio $K = \{1, b, b^2, b^3\}$. Además tenemos que $HK = G$ por el mismo argumento expuesto en el punto 18 de esta tarea.

Claramente, $a^3 = b^4 = 1$ pues el orden de a es tres y el orden de b es cuatro. Ahora para demostrar que $bab^{-1} = a^2$. Como H es normal, $bab^{-1} = a^i$ para $i = 0, 1 o 2$. Ahora el primer caso no puede ser porque si lo fuera $bab^{-1} = 1$ implicaria que $a = b^{-1}1b = 1$, pero esto es una contradicción porque el orden de a es tres.

Ahora si $bab^{-1} = a$ entonces $ba = ab$. Es decir que a y b conmutan entre sí. Pero $G = HK$ implica que cualquier elemento puede expresarse como la multiplicación de un elemento de H y uno de K. Ahora tomemos cualquier $g_1, g_2 \in G$. Por lo anterior, $g_1 = a^i b^j$ y $g_2 = a^k b^l$. Ahora tomemos $g_1 g_2 = a^i b^j a^k b^l$. Como a y b conmutan entre si podemos reordenar los elementos en esta expresión y obtener $a^ib^ja^kb^l = a^kb^la^ib^j = g_2g_1$. Esto implicaria que G es abeliano, lo cual contradice nuestras suposiciones. La única posibilidad es que $bab^{-1} = a^2$.

$\square$

16. Sea p un número primo. Determinar el número de p-subgrupos de Sylow del grupo simétrico S_p.

Demostración. En primer lugar tenemos que los p-subgrupos de Sylow serían cíclicos. Ahora sabemos que los únicos elementos de orden p en S_p son p-cíclos. Por lo tanto, un subgrupo generado por un p-cíclos es un subgrupo de Sylow. Además sabemos que cualquier elemento en un grupo cíclico primo, distinto del 1, tiene grado p. Por lo tanto los demás elementos son p-ciclos también. Por ultimo si tomamos la intersección de dos p-subgrupos de Sylow, y suponemos que en esta intersección existe un elemento $x \neq 1$, entonces este elemento tiene grado igual a p. Esto significa que la intersección debe incluir todas las potencias de $1, ..., p$ de x pero esto implica que los dos subgrupos son iguales.

Finalmente tenemos que cada p-ciclo pertenece a un único subgrupo diferente. El número de p-ciclos en S_p es igual a $p!/p$=$(p-1)!$. La estructura de cada p-subgrupo es $\{1, p, p^2, ...p^{p-1}\}$ entonces vemos que cada subgrupo tiene $p-1$ $p-ciclos$. Por lo tanto el número de subgrupos es $(p-1!)/(p-1) = (p-2)!$ $\square$

17. Determinar los subgrupos de Sylow del grupo alterno A_5.

Demostración. El orden de A_5 es igual a $5!/2 = 60 = 2^2 * 3 * 5$.

Los 5-subgrupos de Sylow son cíclicos asi que son generados por los elementos de A_5 de orden 5, es decir los 5-cíclos. Por el segundo teorema de de Sylow tenemos que $n_5 \equiv 1 \pmod 5$ y $n_5|12$. Las opciones son $n_5 = 1$ o $n_5 = 6$ pero claramente como hay 24 5-ciclos diferentes la opción correcta debe ser la segunda.

Del mismo modo los 3-subgrupos de Sylow son cíclicos asi que son generados por los elementos de A_5 de orden 3, es decir los 3-cíclos. Por el segundo teorema de de Sylow tenemos que $n_3 \equiv 1 \pmod 5$ y $n_3|20$. Las opciones aqui son $n_3 = 1$, $n_3 = 4$ o $n_3 = 10$.

Ahora para los 2-subgrupos de Sylow, estos serian de orden 4. En esta tarea demostramos que cualquier subgrupo de orden 4 es isomorfo a $\mathbb{Z}/4$o $\mathbb{Z}/2 \times \mathbb{Z}/2$. Pero en A_5 no hay elementos de orden 4. Es decir, que los 2-subgrupos de Sylow son isomorfos a $\mathbb{Z}/2 \times \mathbb{Z}/2$. En particular obtenemos un 2-subgrupo de Sylow si tomamos las permutaciones de dos transposiciones disjuntas que fijan un mismo elementos. Por ejemplo, si tomamos las que fijan el elemento 5 tenemos $\{(1), (12)(34), (13)(24), (14)(23)\}$ que el grupo V_4. Como hay 5 elementos diferentes que se pueden fijar, tenemos 5 2-subgrupos de Sylow diferentes. $\square$

18. Sean $p < q$ dos números primos distintos y G un grupo de orden pq. Demostrar que G tiene un único q-Sylow Q que es normal en G y que $G = QP$, donde P es un p-Sylow de G. Demostrar que G es isomorfo a un producto semidirecto de un grupo cíclico de orden q por un grupo cíclico de orden p.

Demostración. Por el primer teorema de Sylow tenemos que Q y P existen. También podemos observar que estos subgrupos son cíclicos pues sus ordenes son primos.

Ahora sea n_q el número de q-subgrupos de Sylow. Por el segundo teorema de Sylow tenemos que $n_q \equiv 1(\text{mod } q)$ y $n_q|p$. Ahora como p es primo tenemos que $n_q = 1$ o $n_q = p$ Pero el segundo caso no es posible pues como $1 < p < q$ el residuo de la división de p por q es p y $p \neq 1$. Por lo tanto, $p \not\equiv 1 \pmod p$.

Entonces n_q es el único subgrupo de Sylow. Utilizando la parte del segundo teorema de Sylow que enuncia que todos los conjugados son q-subgrupos de Sylow concluimos que Q es normal.

Observece que $P \cap Q = \{e\}$. Para esto tomemos cualquier elemento $x \in P \cap Q = \{e\}$. Tenemos que $x^p = x^q = e$ y claramente $(p, q) = 1$ pues son primos distintos. Por lo demostrado en el punto 3 I), esto implica que $x = e$ lo cual demuestra la observación.

Ahora necesitamos observar que $G = QP$. Para esto observece que $QP = \bigcup_{a \in P} Qa$. Ahora observece que los Qa son disjuntos entre si. Tomemos Qa y Qb tales que $a, b \in P$. En primer lugar podemos escribir $a = x^n$ y $b = x^m$ para algun $x \in P$ y $0 \geq n, m < p$ pues P es cíclico. En segundo lugar como Qa y Qb son clases laterales tenemos o que son iguales o son disjuntas entre si. Ahora si $Qa = Qb$ tenemos que $qa = q'b$ para algunos $q, q' \in Q$. Es decir que $qx^n = q'x^m$. Manipulando esta expresión tenemos que

$$\begin{aligned}
qx^n &= q'x^m \\
qx^n x^{-n} &= q'x^m x^{-n} \\
q &= q'x^m x^{-n} \\
(q')^{-1}q &= (q')^{-1}q'x^m x^{-n} \\
(q')^{-1}q &= x^m x^{-n} \\
(q')^{-1}q &= x^{m-n}
\end{aligned}$$

Por la tanto tenemos que $x^{m-n} \in P \cap Q$ pero esto implica que $x^{m-n} = e$. Como el orden de x es p la única forma es que $m = n$ y por lo tanto $a = x^n = x^m = b$. Lo anterior nos permite concluir que por cada $a \in P$ hay una clase lateral Qa disyunta. Por lo tanto tenemos que $|QP| = \sum_{a \in P} |Qa| = \sum_{a \in P} q = pq$. Pero el orden de G es pq, luego $QP = G$.

Todo lo anterior nos permite concluir que G es el producto semidirecto de P y Q. Por lo tanto, $G \cong \mathbb{Z}/q \ltimes_\psi \mathbb{Z}/p$.

$\square$

19. En la situación del problema anterior, demostrar que si $q-1$ no es divisible por p, es cierto $G \cong \mathbb{Z}/p \times \mathbb{Z}/q$.

Demostración. Sea n_p el número de subgrupos de p-Sylow. Por el segundo teorema de Sylow tenemos que $n_p \equiv 1 \pmod p$ y $n_p|q$. Como q es primo tenemos que $n_p = 1$ o $n_p = q$. Pero si $n_p = q$, y como $n_p \equiv 1 \pmod p$ tendriamos que $p|q-1$ lo cual contradice la suposición que agregamos en este punto. Por lo tanto, $n_q = 1$ y bajo los mismos argumentos que en el punto anterior tendriamos que P es normal. Con este nuevo dato y lo demostrado anteriormente concluimos que G es el producto directo de P y Q. Es decir que $G \cong \mathbb{Z}/p \times \mathbb{Z}/q$. □

20. Demostrar que un grupo de orden 35 es cíclico.

Demostración. Sea G dicho grupo. Observese que $35 = 5 * 7$. Además $5 \not| 7 - 1 = 6$. Por lo tanto podemos utilizar el resultado obtenido en el punto anterior para concluir que $G \cong \mathbb{Z}/5 \times \mathbb{Z}/7$. Pero además utilizando el resultado del punto 3 II) tenemos que $\mathbb{Z}/5 \times \mathbb{Z}/7 \cong \mathbb{Z}/35$. Como la relación $\cong$ es de equivalencia tenemos que es transitiva. Por lo tanto G es cíclico. □