C. Propiedades Elementales de Homomorfismos

Sea G,H y K grupos. Probar:

1. Si $f : G \to H$ y $g : H \to K$ son homomorfismos, entonces su composición $g \circ f : G \to K$ es un homomorfismo.

Sea $a, b \in G$, luego $(g \circ f)(ab) = g(f(ab)) = g(f(a)f(b)) = g(f(a))g(f(b))$

2. Si $f : G \to H$ es un homomorfismo con kernel K, entonces f es inyectivo si y solo si $k = \{e\}$

Sea f inyectivo, entonces $f(a) = f(b)$ si $a = b$, luego, sea $x \in K$ tal que $f(x) = e$, luego como $f(e) = f(x)$, luego como f es inyectivo se tiene que $x = e$. Por lo que todo elemento del kernel es el neutro. $K = \{e\}$.

Luego supongamos que $K = \{e\}$, sea x, y tales que $f(x) = f(y) \iff f(x)f^{-1}(y) = e = f(xy^{-1})$. Por lo que $xy^{-1} \in K$, pero por hipótesis $K = \{e\}$, es decir $xy^{-1} = e$, o equivalentemente, $x = y$.

3. Si $f : G \to H$ es homomorfismo y K es cualquier subgrupo de G, entonces $f(K) = \{f(x)|x \in K\}$ es subgrupo de H.

Sea $e_G \in K$, luego $f(e_G) = e_K$. Luego, sean $a, b \in K$, como K es grupo, $ab \in K$, y como f es homomorfismo, $f(ab) = f(a)f(b) \in f(K)$. Al ser K grupo, para a elemento, existe su inverso a^{-1}, luego $f(aa^{-1}) = f(a)f(a^{-1}) = f(a)f^{-1}(a) = e$. Luego $f^{-1}(a) \in f(K)$.

4. Si $f : G \to H$ es un homomorfismo y J es cualquier subgrupo de H, entonces:

$$f^{-1}(J) = \{x \in G|f(x) \in J\}$$

es subgrupo de G. Además $\ker f \subseteq f^{-1}(J)$.

$f(e_G) = e_H$, luego en particular $e_H \in J$, por lo que $e_G \in f^1(J)$
$f(a), f(b) \in J$, $f(a)f(b) = f(ab)$ entonces $ab \in f^{-1}(J)$
$f(a), f^{-1}(a) \in J$, $f(a)f^{-1}(a) = f(a)f(a^{-1}) = e$, luego $a^{-1} \in f^{-1}(J)$.

Luego, como $e_H \in J$, todo elemento $x \in \ker f$ pertenece a $f^{-1}(J)$, es decir $\ker f \subseteq f^{-1}(J)$.

5. Si $f : G \to H$ es homomorfismo con kernel K y J es subgrupo de G, sea f_J la restricción de f a K. Entonces $\ker f_J = J \cap K$.

Como $f_J(x) = f(x)$ para todo $x \in J$, se tiene que $\ker f_J = \{x \in J|f(x) = e_H\}$, luego ver que $\{x \in G|f(x) = e_H\} = \ker f = K$. Asi que todos los elementos $x \in J$ que satisfacen $f(x) = e_H$ son precisamente los elementos de J que están en K. Luego $\ker f_J = J \cap K$.

6. Para cualquie grupo G, la función $f : G \to G$ definida por $f(x) = e$ es un homomorfismo.

Sea $a, b \in G$, luego $f(a)f(b) = e \cdot e = e = f(ab)$

7. Para cualquier grupo G, $\{e\}$ y G son imagenes homomorfas de G.

a) $f(ab) = e = e \cdot e = f(a)f(b)$, luego para e se puede definir siempre $g \in G$ tal que $f(g) = e$. b) $f(ab) = ab = f(a)f(b)$, para $g \in G$ se puede definir $g \in G$ mismo elemento donde $f(g) = g$.

8. La función $f : G \to G$ definida por $f(x) = x^2$ es un homomorfismo si y solo si G es abeliano.

Sea $a, b \in G$, luego $f(a)f(b) = a^2b^2 = f(ab) = (ab)^2 = abab$, luego $a^2b^2 = abab$ si y solo si $ab = ba$. Se puede leer en ambas direcciones de la proposición.

9. Las funciones $f_1(x, y) = x$ y $f_2(x, y) = y$ desde $G \times H$ a G y H respectivamente son homomorfismos.

$f_1((x_1,y_1)(x_2,y_2)) = f((x_1x_2, y_1y_2)) = x_1x_2 = f(x_1,y_1)f(x_2,y_2)$. El mismo procedimiento para f_2.

D. Propiedades Básicas de Subgrupos Normales

Sea G un grupo arbitrario.

1. Encontrar todos los subgrupos normales de S_3 y de D_4

S_3: $\{e\}$, $\{e,(123),(132)\}$ D_4: $\{e,r,r^2,r^3\}, \{e,r^2,s,r^2s\}, \{e,r^2,rs,r^3s\}$ y $\{e,r^2\}$

2. Cada subgrupo de un grupo abeliano es normal.

Sea H subgrupo de un brupo abeliano, sea $h \in H$, luego $eh = h = gg^{-1}h = ghg^{-1} \in H$

3. El centro de cualquier grupo G es un subgrupo normal de G.

Sea $C_G = \{a \in G | ax = xa \quad \forall x \in G\}$, luego sea $a \in G_G$, se tiene que $ax = xa \quad \forall x \in G$, pero esto es equivalente a $a = xax^{-1}$, es decir C_G es normal con respecto a conjugados.

4. Sea H un subgrupo de G. H es normal si y solo si posee la siguiente propiedad: Para todo $a, b \in G$, $ab \in H$ si y solo si $ba \in H$.

H es normal, entonces $xax^{-1} \in H$ para todo $x \in G$ y $a \in H$, sean $a, b \in H$ y $ab \in H$, como H es normal, $babb^{-1} = ba \in H$, luego como $ba \in H$, $abaa^{-1} = ab \in H$. Luego si $ab \in H \longleftrightarrow ba \in H$, entinces $ab = h_1$ y $ba = h_2$, luego $b = h_1a^{-1}$, por lo que $h_2 = ah_1a^{-1}$, por lo que H es normal.

5. Sea H un subgrupo de G. H es normal si y solo si $aH = Ha$ para todo $a \in G$

Si H es normal, entonces $xh_1x^{-1} \in H$ para $h_1 \in H, x \in G$, es decir $xh_1x^{-1} = h_2 \iff xh_1 = h_2x \iff xH = Hx$.

Si $aH = Ha$, entonces $ah_1 = h_2a$, luego $h_2 = ah_1a^{-1}$, es decir $ah_1a^{-1} \in H$.

6. Cualquier intersección de subgrupos normales es un subgrupo normal de G.

Sean H, K subgrupos normales de G, sea $H \cap K$ y a un elemento de este, luego como H y K son normales, $xax^{-1} \in H, K$, por lo que $xax^{-1} \in H \cap K$

E. Más Propiedades de Subgrupos Normales

Sea G un grupo y H subgrupo de G. Probar:

1. Si H posee índice 2 en G, entonces H es normal.

Como $(G : H) = 2$, existen dos cosets de H, tanto izquierdos como derechos, luego estos son respectivamente, H, aH y H, Ha con $a \notin H$, como $eH = He$, entonces solo queda que $aH = Ha$.

2. Suponer que un elemento $a \in G$ posee orden 2. Entonces $\langle a \rangle$ es subgrupo normal de G si y solo si a está en el centro de G.

Si $\langle a \rangle$ es subgrupo normal, entonces para $x \in G$, $xax^{-1} \in \langle a \rangle$, pero $\langle a \rangle = \{e, a\}$, como $xax^{-1} = e$ es imposible (ya que el orden es 2), entonces $xax^{-1} = a$, es decir $xa = ax$ y $a \in C_G$.

3. Si a es cualquier elemento de G, $\langle a \rangle$ es un subgrupo normal si y solo si a posee la siguiente propiedad: para cualquier $x \in G$, hay un entero positivo k tal que $xa = a^kx$.

Si $\langle a \rangle$ es subgrupo normal, entonces $xax^{-1} \in \langle a \rangle$, pero $\langle a \rangle = \{a^i | 1 \leq i \leq \operatorname{ord}(a)\}$m es decur $xax^{-1} = a^k \iff xa =$

$a^k x$ para algún k.

Directamente si $xax^{-1} = a^k$ para algún k, como $a^k \in \langle a \rangle$, $xax^{-1} = \langle a \rangle$.

4. En un grupo G, un conmutador es cualquier producto de la forma $aba^{-1}b^{-1}$, donde a y b son elementos cualquiera de G. Si un subgrupo H de G contiene todos los conmutadores de G, entonces H es normal.

Si $H = \{aba^{-1}b^{-1} | a, b \in G\}$, luego $g(aba^{-1}b^{-1})g^{-1} = (aha^{-1})(aga^{-1})(ah^{-1}a^{-1})(ag^{-1})a^{-1} =$
$(aha^{-1})(aga^{-1})(aha^{-1})^{-1}(aga^{-1})^{-1} \in H$

5. Si H y K son subgrupos de G y K es normal, entonces HK es un subgrupo de G. (HK denota el conjunto de todos los productos hk cuando h para por H y k por K)

$e \in KH$ ya que $e = e \cdot e$
Sea h_1k_1 y $h_2k_2 \in HK$, luego $h_1k_1h_2k_2$, como K es normal $k_1h_2 = h_2k_1'$, luego $h_1k_1h_2k_2 = (h_1h_2)(k_1'k_2) \in HK$
El inverso se ve directo al ser H, K grupos.

6.

F. Homomorfismos y El Orden de Elementos

Si $f : G \to H$ es un homomorfismo, probar:

1. Por cada elemento $a \in G$, el orden de $f(a)$ es divisor del orden de a.

Sea $a^n = e$ para algún $n \in \mathbb{N}$ minimal, luego $f(a^n) = f(e) = e = f^n(a)$, luego, esto quiere decir que $m \mid n$ con m el orden de $f(a)$.

2. El orden de cualquier elemento $b \neq e$ en el grando de f es un divisor común de $|G|$ y $|H|$.

Se vió en (1) que si $\operatorname{ord}(f(a)) = m$ y $\operatorname{ord}(a) = n$, entonces $m \mid n$, luego como $n \mid |G|$, en particular $m \mid |G|$ a su vez $m \mid |H|$.

3. Si el rango de f posee n elementos entonces $x^n \in \ker f$ para todo $x \in G$.

Como $|\operatorname{ran} f| = n$, se tiene que $\operatorname{ord} f(x) \mid n$, por lo que $f^n(x) = f(x^n) = e$. Luego $x^n \in \ker f$.

4. Sea m un entero tal que m y $|H|$ son coprimos. Para cualquier $x \in G$, si $x^m \in \ker f$, entonces $x \in \ker f$.

Sea $x^m \in \ker f$, entonces $f(x^m) = f^m(x) = e$, luego, se sabe que $\operatorname{ord} f(x) | m$ y $\operatorname{ord} f(x) \mid |H|$, pero como son coprimos, $\operatorname{ord} f(x) = 1$, luego $f(x) = e$ y $x \in \ker f$.

5. Sea el rango de f de tamano m. Si $a \in G$ posee orden n, donde m, n coprimos, entonces a está en el kernel de f.

Sea $|\operatorname{ran} f| = m$, sea $a^n = e$, luego $f^n(a) = e$, luego se sabe que $\operatorname{ord} f(a) \mid n$, luego como m, n son corpimos, no poseen factores primos, pero a la vez $\operatorname{ord} f(a) \mid m$, por lo que $\operatorname{ord} f(a) = 1$, es decir $f(a) = e$ y $a \in \ker f$.

6. Sea p primo. Si $\operatorname{ran} f$ posee un elemento de orden p, entonces G posee un elemento de orden p.

Se tiene que $\operatorname{ord} a \mid |G|$, luego $p = \operatorname{ord} f(a) \mid \operatorname{ord} a$, es decir $p \mid |G|$, luego G posee un elemento de orden p (teorema de Cauchy).

G. Propiedades Preservadas bajo Homomorfismo

Si $f : G \to H$ es un homomorfismo de G a H sobreyectivo. Probar:

1. Si G es abeliano, entonces H es abeliano.

$f(ab) = f(a)f(b) = f(ba) = f(b)f(a)$. Luego $f(a)f(b) = f(b)f(a)$.

2. Si G es cíclico, entonces H es cíclico.

Si G es cíclico, entonces $G = \{a_i \mid i \in I\}$ con I conjunto de enteros positivos contables, luego $f(a^i) = f^i(a)$, por lo que H posee generador $f(a)$.

3. Si cada elemento de G posee orden finito, entonces cada elemento de H posee orden finito.

Si para cada $a \in G$ existe $k \in \mathbb{N}$ tal que $a^k = e$, entonces $f(a^k) = f(e) = e = f^k(a)$, luego cada elemento de H posee orden finito.

4. Si cada elemento de G es su propio inverso, cada elemento de H es su propio inverso.

Si para todo $a \in G$, $a = a^{-1}$, luego $f(a) = f(a^{-1}) = (f(a))^{-1}$.

5. Si cada elemento de G pose una raíz cuadrada, entonces cada elemento de H posee una raíz cuadrada.

Todo elemento x posee raíz cuadrada, es decir existe $y \in G$ tal que $x = y^2$, luego $f(x) = f(y^2) = f^2(y)$.

6. Si G es finitamente generado, entonces H es finitamente generado.

Sea $G = \langle g_1, \ldots, g_n \rangle$, por lo que $a \in G$ se puede expresar como $a = g_1^{i_1} g_2^{i_2} \ldots g_n^{i_n}$ donde cada g_i está en el generador y los exponentes son $0, 1$ o -1, luego como f es sobreyectiva, para cada $h \in H$ hay g tal que $f(g) = h$, tomando g como antes y considerando que f es homomorfismo:

$$h = f(g) = f(g_1^{i_1} g_2^{i_2} \ldots g_n^{i_n}) = f(g_1^{i_1}) f(g_2^{i_2}) \ldots f(g_n^{i_n})$$

Luego como h fué arbitrario, todo elemento de H se puede expresar de esta forma, por lo que $H = \langle f(g_1), f(g_2), \ldots, f_{g_n} \rangle$.

H. Producto Directo Interno

Si G es un grupo cualquiera, sea H, K subgrupos normales de este tal que $H \cap K = \{e\}$. Probar:

1. Si h_1, h_2 son dos elementos cualquiera de H y k_1, k_2 elementos cualquiera de K.

$$h1k_1 = h_2k_2 \text{ implica } h_1 = h_2 \text{ y } k_1 = k_2$$

Como $k_1k_1 = h_2k_2 \iff h_2^{-1}h_1k_1 = k_2 \iff h_2^{-1}h_1 = k_2k_1^{-1} \in H \cap K$, luego como $H \cap K = \{e\}$, $h_2^{-1}h_1 = e$ y $k_2k_1^{-1} = e$, es decir, $h_2 = k_1, k_2 = k_1$.

2. Para cualquier $h \in H$ y $k \in K$, $hk = kh$.

Como H y K son normales, $H \cap K = \{e\}$ es normal, luego $hkh^{-1}k^{-1} = e$, es decir, $hk = kh$.

3. Ahora, hacer la suposición adicional que $G = HK$, eso es, cada $x \in G$ puede ser expresado como $x = hk$, para algún $h \in H$ y $k \in K$. Luego la función $\phi(h, k) = hk$ es un isomorfismo de $H \times K$ sobre G.

Sea $\phi(h_1, k_1)\phi(h_2, k_2) = h_1k_1h_2k_2 = h_1h_2k_1h_2$ (por punto anterior conmutan), por lo que $\phi(h_1, k_1)\phi(h_2, k_2) = \phi(h_1h_2, k_1k_2)$.
Sea $\phi(h_1, k_1) = \phi(h_2, k_2)$, es decir $h_1k_1 = h_2k_2$, por punto anterior, $h_1 = h_2$ y $k_1 = k_2$, por lo que $(h_1, k_1) = (h_2, k_2)$, por lo que la inyectividad de cumple. Para ver la sobreyectividad ver que para todo producto hk se puede definir (h, k).

I. Subgrupos Conjugados

Sea H un subgrupo de G. Para cualquier $a \in G$, sea $aHa^{-1} = \{axa^{-1} \mid x \in H\}$. aHa^{-1} se denomina un conjunto de H. Probar:

1. Por cada $a \in G$, aHa^{-1} es subgrupo de G.

$e \in aHa^{-1}$ ya que $e \in H$, se tiene luego que $aea^{-1} = aa^{-1} = e$.
Sea $aha^{-1} \in aHa^{-1}$, y $h^{-1} \in H$, luego se puede definir $ah^{-1}a^{-1}$, luego $(aha^{-1})(ah^{-1}a^{-1}) = (ah)(h^{-1}a^{-1}) = aa^{-1} = e$
Sea ah_1a^{-1} y $ah_2a^{-1} \in aHa^{-1}$, luego $(ah_1a^{-1})(ah_2a^{-1}) = a(h_1h_2)a^{-1}$.

2. Por cada $a \in G$, $H \cong aHa^{-1}$.

Sea $\varphi : H \to aHa^{-1} : h \mapsto aha^{-1}$. Se tiene por punto anterior que φ es homomorfismo.

Inyectividad: $ah_1a^{-1} = ah_2a^{-1} \Longrightarrow h_1 = h_2$
Sobreyectividad: Sea aha^{-1}, siempre se puede definir $h \in H$ tal que $\varphi(h) = aha^{-1}$.

3. H es subgrupo normal de G si y solo $H = aHa^{-1}$, para todo $a \in G$.

Si H es subgrupo normal de G, entonces $aH = Ha$, es decir $ah_1 = h_2a \Longleftrightarrow h_2 = ah_1a^{-1}$, luego $H = aHa^{-1}$.

(*) En los ejercicios restantes, sea G un grupo finito. Por el normalizador de H nos referimos al conjunto $N(H) = \{a \in G \mid axa^{-1} \in H \quad \forall x \in H\}$

4. Si $a \in N(H)$, entonces $aHa^{-1} = H$ (recordar que G es un grupo finito).

Sea $a \in N(H)$, entonces $aha^{-1} \in H$ para todo $h \in H$, por lo que $aHa^{-1} \subseteq H$, como $H \cong aHa^{-1}$, $|H| = |aHa^{-1}|$, por lo que $aHa^{-1} = H$.

5. $N(H)$ es subgrupo de G.

$e \in H$, luego $aea^{-1} = aa^{-1} = e$, por lo que $e \in N(H)$.
Sea $h^{-1} \in H$, se tiene que $ah^{-1}a^{1} \in H$, ya que $(aha^{-1})(ah^{-1}h^{-1}) = e$
Sean $h_1, h_2 \in N(H)$, luego ah_1a^{-1} y $ah_2a^{-1} \in H$, por lo que $(ah_1a^{-1})(ah_2a^{-1}) = a(h_1h_2)a^{-1} \in H$.

6. $H \subseteq N(H)$. Además, H es subgrupo normal de $N(H)$.

Sea $h \in H$, nortar que para $h' \in H$, $h'hh'^{-1} \in H$, luego $h \in N(H)$, por lo que $H \subseteq N(H)$. Para ver que H es normal, tomar $a \in N(H)$ y $h \in H$, luego $aha^{-1} \in H$, luego es normal.

7. Para cualquier $a, b \in G$, $aHa^{-1} = bHb^{-1}$ si y solo si $b^{-1}a \in N$ si y solo si $aN = bN$.

Si $aHa^{-1} = bHb^{-1}$, $ah_1a^{-1} = bh_2b^{-1} \Longleftrightarrow b^{-1}ah_1a^{-1}b = (b^{-1}a)h_1(b^{-1}a)^{-1} = h_2 \in H$, luego $b^{-1}a \in N$, es decor $aN = bN$. Ambas implicancias se leen en sus respectivas direcciones.

8. Hay una correspondencia uno-a-uno entre en conjunto de los conjugados de H y el conjunto de cosets de N. (Entonces hay tantos conjugados de H como cosets de N).

Sea $\varphi : \{aHa^{-1} \mid a \in G\} \to \{aN \mid a \in G\} : aHa^{-1} \mapsto aN$.

Inyectividad: Si $aN = bN$, entonces $aHa^{-1} = bHb^{-1}$ (punto anterior)
Sobreyectividad: Luego por cada aN se puede definir siempre aHa^{-1} tal que $\varphi(aHa^{-1}) = aN$).

9. H posee exactamente $(G : N)$ conjugados, en particular, el número de conjugados distintos de H es divisor de G.

$\frac{|G|}{|H|} = (G : H) = |\{aN \mid a \in G\}| = |\{aHa^{-1} \mid a \in G\}|$, luego $|G| = |\{aHa^{-1} \mid a \in G\}| \cdot |H|$ y por lo tanto es divisor de $|G|$.

10. Lo mismo pero con la restricción φ_J.