Estructuras Algebraicas

Andoni Latorre Galarraga

1. Grupos

Definición: Un grupo $(G,*)$ son un conjunto no vacío G y una operación $\begin{array}{rccc} *: & G\times G & \longrightarrow & G \\ & (a,b) & \longmapsto & a*b\in G \end{array}$ tales que

$$\begin{array}{ll} \text{i)} & (a*b)*c = a*(b*c) \quad \forall a,b,c\in G \\ \text{ii)} & \exists e: \quad e*x = x = x*e \quad \forall x\in G \quad \text{se dice que } e \text{ es el elemento neutro} \\ \text{iii)} & \forall a\in G \quad \exists a'\in G: \quad a*a' = e = a'*a \quad \text{se dice que } a' \text{ es el simétrrico de } a. \end{array}$$

Con $*=+$ al simétrico se le llama opuesto. Con $*=\cdot$ al simétrico se le llama inverso.

Proposición: El elemento neutro y el simétrico son únicos.
Dem: Supongamos que e_1, e_2 son elementos neutros. Por ser e_1 elemento neutro $e_2 = e_2 * e_1$ y por ser e_2 elemento neutro $e_2 = e_2 * e_1 = e_1$, se tiene que el elemento neutro es único. Supongamos que a', a'' son simetricos de a. Por definición de simétrico $a*a' = e = a*a''$, operando con a' por la izquierda $a'(a*a') = a'(a*a'')$. Por la propiedad asociativa, $(a'*a)*a' = (a'*a)*a''$. Por definición de simétrico $e*a' = e*a''$. Por definición de elemento neutro $a' = a''$.

Definición: Si G es un grupo finito, $G = \{g_1, \cdots, g_n\}$, la tabla de grupo G es:

$\cdot$	g_1	g_2	$\cdots$	g_j	$\cdots$	g_n
g_1				$\vdots$		
g_2				$\vdots$		
$\vdots$				$\vdots$		
g_1	$\cdots$	$\cdots$	$\cdots$	$g_i \cdot g_j$		
$\vdots$						
g_n						

Definición: En $(G,*)$

$$\forall a\in G \quad \begin{cases} a^0 = e & \\ a^n = \overbrace{a*\cdots*a}^{n} & \text{si } n\geq 1 \\ a^n = \overbrace{a^{-1}*\cdots*a^{-1}}^{n} & \text{si } n<0 \end{cases} \quad \forall n\in\mathbb{Z}$$

Definición: Si $\emptyset \neq H \subsetneq G$ decimos que H es subgrupo de $(G,*)$ si $(H, *_{|H\times H})$ es grupo. Se escribe $H \leq G$.

Definición: Si $\exists m \geq 0$ tal que $g^m = 1$ llamamos orden de $g\in G$ al menor entero positivo n tal que $g^n = e$ y escribimos $o(g) = n$.

Definición: Si $a\in G$ llamamos subgrupo cíclico generado por a a

$$<a> = \{a^n \mid n\in\mathbb{Z}\}$$

Veamos que $<a>$ es subgrupo. Cumple $i)$ ya que se cumple en en G. Para $ii)$ tenemos que $a^0 = e$ y para $iii)$ tenemos que $a^{-n}*a^n = e = a^n * a^{-n}$.

$$\overbrace{a^{-1}*\cdots*a^{-1}}^{n} * \overbrace{a*\cdots*a}^{n} = e = \overbrace{a*\cdots*a}^{n} * \overbrace{a^{-1}*\cdots*a^{-1}}^{n}$$

Proposición: $| < g > | = o(g)$
Dem: Sabemos que $\forall n \in \mathbb{N}$ existen $q, r \in \mathbb{N}$ con $0 \leq r < o(g)$ tales que $n = q\dot{o}(g) + r$. Entonces

$$< g >) = \{1, g, g^2, \cdots, g^{o(g)-1}, g^{o(g)}, g^{o(g)+1}, \cdots, g^{o(g)+(o(g)-1)}, g^{2o(g)}, g^{2o(g)+1}, \cdots\}$$
$$= \{1, g, g^2, \cdots, g^{o(g)-1}, 1, 1 \cdot g, \cdots, 1 \cdot g^{o(g)-1}, 1^2, 1^2 g, \cdots\} = \{1, g, \cdots, g^{o(g)-1}\}$$

Se tiene que $| < g > | = 1 + o(g) - 1 = o(g)$.

Definición: Si $S \subset G$ llamamos subgrupo generado por el conjunto S a

$$< S >= \{s_{i_1}^{t_1} \cdots s_{i_n}^{t_n} \mid s_{i_j} \in S, t_j \in \{1, -1\}, n \in \mathbb{Z}\}$$

Veamos que $< S >$ es subgrupo. Cumple $i)$ ya que se cumple en en G. Para $ii)$ tenemos que $s^1 s^{-1} = e$ y para $iii)$ tenemos que $(s_{i_1}^{t_1} \cdots s_{i_n}^{t_n}) \cdot (s_{i_n}^{-t_n} \cdots s_{i_1}^{-t_1}) = e = (s_{i_n}^{-t_n} \cdots s_{i_1}^{-t_1}) \cdot (s_{i_1}^{t_1} \cdots s_{i_n}^{t_n})$.

Observación: $< a >=< \{a\} >$

Definición: Si $(G, \cdot)$ es grupo y $H \leq G$ definimos la coclase por la izquierda $gH = \{gh \mid h \in H\}$.

Lema: $hH = H$. Como $h^{-1}\tilde{h} \in H$ se tiene que $h\underbrace{h^{-1}\tilde{h}}_{\in H} = \tilde{h}$

Proposición: $\mathcal{P} = \{gH = \{gh \mid h \in H\} \mid g \in G\}$ es una partición de G.
Dem: Evidentemente $\bigcup_{g \in G} gH = G$ ya que $G \supset \bigcup_{g \in G} gH \supset \bigcup_{g \in G} g\underbrace{e}_{\in H} = \bigcup_{g \in G} g = G$. Ahora, veamos que si $g_1 H \cap g_2 H \neq \emptyset$, entonces $g_1 H = g_2 H$. Sabemos que existen $h_1, h_2 \in H$ tales que $g_1 h_1 = g_2 h_2$, entonces $g_1 = g_2 h$ con $h = h_2 h_1^{-1} \in H$. Ahora, $g_1 H = (g_2 h)H = g_2(hH) = g_2 H$.

Proposición $|gH| = |H|$
Dem: Veamos que existe una biyección entre gH y H.

$$\begin{array}{cccc} \varphi & H & \longrightarrow & gH \\ & h & \longmapsto & gh \end{array}$$

Tenemos que es suprayectiva ya que $\varphi(H) = \{gh \mid h \in H\} = gH$. Es inyectiva ya que si $h_1 = h_2$, entonces $gh_1 = gh_2$.

Definición: Si $(G, \cdot)$ es grupo y $H \leq G$ definimos la coclase por la derecha $Hg = \{hg \mid h \in H\}$.

Lema: $Hh = H$. Como $\tilde{h}h^{-1} \in H$ se tiene que $\underbrace{\tilde{h}h^{-1}}_{\in H} h = \tilde{h}$

Proposición: $\mathcal{P} = \{Hg = \{hg \mid h \in H\} \mid g \in G\}$ es una partición de G.
Dem: Evidentemente $\bigcup_{g \in G} Hg = G$ ya que $G \supset \bigcup_{g \in G} Hg \supset \bigcup_{g \in G} \underbrace{e}_{\in H} g = \bigcup_{g \in G} g = G$. Ahora, veamos que si $Hg_1 \cap Hg_2 \neq \emptyset$, entonces $Hg_1 = Hg_2$. Sabemos que existen $h_1, h_2 \in H$ tales que $h_1 g_1 = h_2 g_2$, entonces $g_1 = hg_2$ con $h = h_1^{-1} h_2 \in H$. Ahora, $Hg_1 = H(hg_2) = (Hh)g_2 = Hg_2$.

Proposición $|Hg| = |H|$
Dem: Veamos que existe una bijección entre gH y H.

$$\begin{array}{cccc} \varphi & H & \longrightarrow & Hg \\ & h & \longmapsto & hg \end{array}$$

Tenemos que es suprayectiva ya que $\varphi(H) = \{hg \mid h \in H\} = Hg$. Es inyectiva ya que si $h_1 = h_2$, entonces $h_1 g = h_2 g$.

Definición: Como $G = \dot{\bigcup\limits_{g\in I}} gH = \dot{\bigcup\limits_{g\in \tilde{I}}} Hg$ y $|Hg| = |H| = |gH|$ se tiene que $|H| \mid |G|$. Tiene sentido definir $|G| = \underbrace{|I|}_{|G:H|} |H| = \underbrace{|\tilde{I}|}_{|G:H|} |H|$ y se dice que $|G:H|$ es el índice de H en G.

Obsevación: $|G:H| \mid |G|, |H| \mid |G| \quad \forall H \leq G$

Proposición: $o(g) \mid |G| \quad \forall g \in G$
Dem: Tenemos que $o(g) = | < g > |$ y como $< g >$ es subgrupo, por la observación anterior $| < g > | \mid |G|$, entonces $o(g) \mid |G|$.

Definición: Para cada $x \in G$ si $H, K \leq G$ definimos $HxK = \{hxk \mid h \in H, k \in K\}$.

Proposición: $x \sim y \Leftrightarrow \exists h \in H, \exists k \in K \mid x = hyk$ es una relación de equivalencia.
Dem: Reflexividad, $e \in H, e \in K$ y $x = exe$. Simetría, si $\exists h \in H, \exists k \in K \mid x = hyk$, entonces $h^{-1} \in H, k^{-1} \in K$ y $y = h^{-1}xk^{-1}$. Transitividad, si $x = h_1 y k_1, y = h_2 z k_2$, entonces $x = \underbrace{h_1 h_2}_{\in H} z \underbrace{k_2 k_1}_{\in K}$.

Corolario: $\mathcal{P} = \{HxK \mid x \in G\}$ es una partición de G.

Definición: Llamamos conjugado a $H^g = g^{-1}Hg$ con $g \in G$ y también $x^g = g^{-1}xg$ para $x, g \in G$.

Proposición: Si H es subgrupo de G, entonces H^x es subgrupo de G.
Dem: La propiedad asociativa se cumple ya que se cumple enn todo G. Veamos que el elemento neutro esta en H^x, $e \in H$ por ser H subgrupo, entonces $e = x^{-1}x = x^{-1}ex \in H^x$. Veamos que existe el inverso, $(x^{-1}hx)^-1 = x^{-1} \underbrace{\overset{-1}{h}}_{\in H} x \in H^x$

Proposición: Si $H, K \leq G$ entonces $H \cap K \leq G$
Dem: La propiedad asociativa se cumple ya que se cumple en todo G. El eleemto neutro está en la intersección ya que esta en ambos subgrupos. Veamos que existe inverso en la intersección, si $x \in H \cap K$, entonces $x \in H, x \in K$ y $x^{-1} \in H, x^{-1} \in K \Rightarrow x^{-1} \in H \cap K$.

Proposición: $\mathcal{P} = \{Hxk \mid k \in K\}$ es una partición de HxK.

Dem: Por la definicón de coclase a la derecha.

$$\bigcup_{k\in K} Hxk = \bigcup_{k\in K} \{hxk \mid h\in H\} = \{hxk \mid h\in H, k\in K\} = HxK$$

Ahora, veamos que si $Hxk_1 \cap Hxk_2 \neq \emptyset$ entonces $Hxk_1 = Hxk_2$. Sabemos que existen h_1, h_2 tales que $h_1xk_1 = h_2xk_2$. Entonces, $xk_1 = \underbrace{h_1^{-1}h_2}_{=h\in H} xk_2$ y $Hxk_1 = Hhxk_2 = Hxk_2$.También sabemos que $|Hxk| = |H|$.
Veamos cuantos elementos tiene la partición. Si $k_1, k_2 \in K$,

$$Hxk_1 = Hxk_2 \Leftrightarrow Hx(k_1k_2^{-1}) = Hx \Leftrightarrow Hx(k_1k_2^{-1})x^{-1} = H$$

$$\Leftrightarrow x(k_1k_2^{-1})x^{-1} \in H \Leftrightarrow x^{-1}\underbrace{x(k_1k_2^{-1})x^{-1}}_{\in H} x \in x^{-1}Hx = H^x$$

$$\Leftrightarrow k_1k_2^{-1} \in H^x \Leftrightarrow k_1k_2^{-1} \in H^x \cap K \Leftrightarrow (H^x\cap K)k_1 = (H^x \cap K)k_2$$

Por lo tanto $|\mathcal{P}| = |K : H^x \cap K|$. Entonces $|HxK| = |H||K : H^x \cap K|$.

Proposición: $|G| = \sum_{i\in I} |H||K : H^x \cap K|$.
Dem: $\mathcal{P} = \{HxK \mid x \in G\} = \{Hx_iK \mid i \in I\}$ entonces,

$$|G| = \sum_{i\in I} |Hx_iK| = \sum_{i\in I} |H||K : H^{x_i} \cap K|$$

Corolario: $|G : H| = \sum_{i\in I} |K : H^x \cap K|$.

Definición: Sean $S, T \neq \emptyset$, entonces $ST = \{st \mid s \in S, t \in T\}$

Obeservación: $SS = S$

Proposición: Sean $H, K \leq G$, entonces $HK \leq G \Leftrightarrow HK = KH$
Dem: $\Rightarrow$: $HK \ni hk = ((hk)^{-1})^{-1} = (\underbrace{k^{-1}h^{-1}}_{\in KH})^{-1} \in KH$, entonces $HK = KH$
$\Leftarrow$: Se cumple la asociativa ya que se cumpre en todo G. El elemento neutro esta en HK ya que $e \in H, e \in K$ por ser H, K subgrupos, entonces $HK \ni ee = e$. El inverso esta en HK, $(hk)^{-1} = k^{-1}h^{-1} \in KH = HK$

Definición: Se dice que $N \leq G$ es normal en G si $gN = Ng \quad \forall g \in G$, equivalentemente $gNg^{-1} = N \quad \forall G \in G$. Se escribe $N \trianglelefteq G$ cuando N es normal en G y $N \ntrianglelefteq G$ cuando N no es normal en G.

Proposición: Si $N \trianglelefteq G$ y $H \leq G$, entonces $NH \leq G$
Dem: Sabemos que $NH \leq G \Leftrightarrow NH = HN$. Por ser N subgrupo normal, $NH = HN$ ya que $NH = \bigcup\{Nh \mid h \in H\} = \bigcup\{hN \mid h \in H\} = HN$.

Definición: Sea $N \trianglelefteq G$ entonces definimos el grupo cociente $G/N = \{gN \mid g \in G\} = \{Ng \mid g \in G\}$.
Veamos que $(G/N, \cdot)$ es grupo. Para la propiedad asociativa, sean $[a], [b], [c] \in G/N$

$$([a][b])[c] = \{(\alpha\beta)\gamma \mid \alpha \in [a], \beta \in [b], \gamma \in [c]\} = \{\alpha(\beta\gamma) \mid \alpha \in [a], \beta \in [b], \gamma \in [c]\} = [a]([b][c])$$

Para el elemento neutro, $e_{G/N} = \underbrace{e_G}_{\in N} N = N$,

$$N[a] = \{n\alpha \mid n \in N, \alpha \in [a]\}\{n\alpha \mid n \in N, \alpha \in Na\} = nNa = Na = [a]$$

$$[a]N = \{\alpha n \mid n \in N, \alpha \in [a]\}\{\alpha n \mid n \in N, \alpha \in aN\} = aNn = aN = [a]$$

Para el inverso de $[a]$, tenemos que $[a]^{-1} = [a^{-1}]$,

$$[a][a^{-1}] = aNNa^{-1} = aNa^{-1} = N = e_{G/N}$$

Proposición: $|G/N| = |G : N|$
Dem: $|G/N|$ es el número de coclases que es $|G : N|$.

Definición: Dado un subgrupo H de G definimos $N_G(H) = \{g \in G \mid H^g = H\}$ y lo llamamos subgrupo normalizador de H en G. Veamos que es subgrupo. La asociativa se cumple ya que se cumple en todo G. Veamos que $e \in N_G(H)$, $H^e = e^{-1}He = eHe = H$. Veamos que si $a \in N_G(H)$ entonces $a^{-1} \in N_G(H)$, por ser H subgrupo, $H^{a^{-1}} = (H^{a^{-1}})^{-1} = (aHa^{-1})^{-1} = a^{-1}H^{-1}a = a^{-1}Ha = H$.

Definición: Se dice que G es abeliano si la L.C.I. es conmutativa, es decir, $ab = ba \quad \forall a, b \in G$

Proposición: Si G es abeliano y $H \leq G$, entonces $H \trianglelefteq G$.
Dem: $gH = \{gh \mid h \in H\} = \{hg \mid h \in H\} = Hg$.

Observación: $(\mathbb{Z}, +)$ es abeliano.

Proposición: La totalidad de los subconjuntos de $(\mathbb{Z}, +)$ es $\{0\} \cup \{n\mathbb{Z} \mid n \in \mathbb{N}\}$.
Dem: $\{0\}$ es el subgrupo trivial, veamos que $n\mathbb{Z}$ es subgrupo. $0 = 0n \in n\mathbb{Z}$, veamos que suma está bien definida $nz_1 + nz_2 = n(z_1 + z_2)$, claramente si z es múltiplo de n, entonces $-z \in n\mathbb{Z}$. Reciprocamente, si $H \leq \mathbb{Z}$ supongamos que H es diferente del trivial, entonces $a \in H$ para algún $a \neq 0$. Además $-a \in H$ por lo que H tiene enteros positivos. Ahora, sea n el menor entero positivo en H, supongamos que $x \in H$, ahora $x = zn + r$ con $0 \leq r < n$ si $r \neq 0$ hay contradicción con que n es el menor entero positivo, por lo tato, x es múltipolo de n y $H = n\mathbb{Z}$.

Proposición: $n\mathbb{Z} \leq m\mathbb{Z} \Leftrightarrow m|n$.
Dem: $\Rightarrow$) Si $n\mathbb{Z} \leq m\mathbb{Z}$, entonces $n \in m\mathbb{Z}$ por lo que n es múltiplo de m y $m \mid n$.
$\Leftarrow$) Si $m \mid n$, entonces existe $z \in \mathbb{Z}$ tal que $n = zm$ por lo que n es múltiplo de m y se tiene que $n \in m\mathbb{Z}$.

Proposición: $\forall m, n \in \mathbb{Z}, n\mathbb{Z} + m\mathbb{Z} = a\mathbb{Z}$ donde $a = m.c.d.(n, m)$.
Dem: $n\mathbb{Z}+m\mathbb{Z}$ es subgrupo ya que $n\mathbb{Z}+m\mathbb{Z} = m\mathbb{Z}+n\mathbb{Z}$ por ser $\mathbb{Z}$ es abeliano. Tenemos que $n, m \in n\mathbb{Z}+m\mathbb{Z}$, por lo que $a \mid m$ y $a \mid n$, entonces $a \mid a' = m.c.d.(m, n)$. Por otra parte, existen $z_1, z_2 \in \mathbb{Z}$ tales que $n = z_1a'$ y $m = z_2a'$, entonces $a\mathbb{Z} = n\mathbb{Z} + m\mathbb{Z} = z_1a'\mathbb{Z} + z_2a'\mathbb{Z} \subseteq a'\mathbb{Z}$ por lo que $a' \mid a$ y se tiene que $a' = a$.

Proposición: $\forall m, n \in \mathbb{Z}, n\mathbb{Z} \cap m\mathbb{Z} = b\mathbb{Z}$ donde $b = m.c.m.(n, m)$.
Dem: Sabemos que $nm \in n\mathbb{Z} \cap m\mathbb{Z}$ por lo que $n\mathbb{Z} \cap m\mathbb{Z}$ es no nulo. Además $n\mathbb{Z}, m\mathbb{Z} \leq b\mathbb{Z}$ por lo que $n, \mid b$ y $b'\mathbb{Z} \subseteq n\mathbb{Z}, m\mathbb{Z}$. Ahora, $b'\mathbb{Z} \subseteq n\mathbb{Z} \cap m\mathbb{Z}$, por lo tanto $b \mid b'$. Si $b' = m.c.m.(n, m)$, entonces $b' \mid b$ y se tiene que $b = b'$.

Proposición: Para cada $n \in \mathbb{N}$, $\mathbb{Z}/n\mathbb{Z}$ es un grupo abeliano de orden n.
Dem: $\mathbb{Z}/n\mathbb{Z} = \{m + n\mathbb{Z} \mid m \in \mathbb{Z}\}$. Tenemos que $m = nq + r$ con $0 \leq r < n$,

$$m + n\mathbb{Z} = (nq + r) + n\mathbb{Z} = (nq + n\mathbb{Z}) + (r + n\mathbb{Z}) = r + n\mathbb{Z}$$

por lo que,

$$\mathbb{Z}/n\mathbb{Z} = \{0 + n\mathbb{Z}, 1 + n\mathbb{Z}, \cdots, (n-1) + n\mathbb{Z}\}$$

Veamos que estos elementos son distintos dos a dos, $i + n\mathbb{Z} = j + n\mathbb{Z} \Leftrightarrow i - j \in n\mathbb{Z}$ pero $|i - j| < n$ por lo que $i = j$. Se tiene que $|\mathbb{Z}/n\mathbb{Z}| = n$.

Proposición: Sean $n, m \in \mathbb{N}$, Entonces existen enteros r y s tales que $1 = nr + ms$ si y solo si $m.c.d.(n, m) = 1$.
Dem: Sabemos que $n\mathbb{Z} + n\mathbb{Z} = m.c.d.(n, m)\mathbb{Z}$ y $1 \in m.c.d.(n, m)\mathbb{Z} \Leftrightarrow m.c.d = (n, m) = 1$. (También es posible $m.c.d = (n, m) = -1$, depende de como se defina $m.c.d.$, independientemente, es lo mismo.)

Proposición: La ecuación difántica $ax + by = c$ tiene al menos una solución en $\mathbb{Z} \times \mathbb{Z}$ si y solo si $m.c.d.(a, b)$ divide a c. Si (x_0, y_0) es una solución, entonces el conjunto de todas las soluciones es

$$\{(x_0 - (d/b)z + (a/d)z) \mid z \in \mathbb{Z}\}$$

*Dem:*Sabemos que $n\mathbb{Z} + n\mathbb{Z} = m.c.d.(a, b)\mathbb{Z}$, entonces existe solución si y solo si $m.c.d.(a, b) \mid c$. Ahora, supongamos que (x_0, y_0) es una solución,

$$ax_0 + by_0 = c$$

$$ax + by = c$$

Restando, obtenemos

$$a(x - x_0) = -b(y - y_0)$$

$$(\frac{a}{m.c.d.(a, b)})(x - x_0) = -(\frac{b}{m.c.d.(a, b)})(y - y_0)$$

Y como $m.c.d.(\frac{a}{m.c.d.(a,b)}, \frac{b}{m.c.d.(a,b)}) = 1$, se tiene que $\frac{a}{m.c.d.(a,b)}$ divide a

Definición: Sean $(G_1, \cdot)$ y $(G_2, *)$ grupos. Decimos que $f : G_1 \longrightarrow G_2$ es un homomorfismo de de grupos, si verifica

$$f(x \cdot y) = f(x) * f(y) \quad \forall x, y \in G_1$$

Ejemplo: Homomorfismo trivial $f(x) = e_2 \quad \forall x \in G_1$.

Definición: Un homomorfismo inyectivo se llama monomorfismo.
Un homomorfismo suprayectivo se llama epimorfismo.
Un homomorfismo biyectivo se llama isomorfismo.
Si existe un isomorfismo entre G_1 y G_2 decimos que son isomorfos y escribimos $G_1 \simeq G_2$.

Proposición: Ser isomorfo es relación de equivalencia.
Dem: Propiedad reflexiva: $\begin{array}{rccc} 1_G : & G & \longrightarrow & G \\ & g & \longmapsto & g \end{array}$ es isomorfismo.

Propiedad simétrica: Si existe φ isomorfismo $\begin{array}{cccc}\varphi: & G_1 & \longrightarrow & G_2\\ & g & \longmapsto & \varphi(g)\end{array}$ Por ser biyectiva existe $\tilde{\varphi}$ bien definida $\begin{array}{cccc}\tilde{\varphi}: & G_2 & \longrightarrow & G_1\\ & \varphi(g) & \longmapsto & g\end{array}$ Veamos que $\tilde{\varphi}$ es isomorfismo.

$$\tilde{\varphi}(\underbrace{x}_{=\varphi(g)} * \underbrace{y}_{=\varphi(h)}) = \tilde{\varphi}(\varphi(g) * \varphi(h)) = \tilde{\varphi}(\varphi(g \cdot h)) = g \cdot h = \tilde{\varphi}(\varphi(g)) \cdot \tilde{\varphi}(\varphi(h)) = \tilde{\varphi}(x) \cdot \tilde{\varphi}(y)$$

Propiedad transitiva: Sabemos que la composición de funciones biyectivas es biyectiva. Veamos que la composición de homomorfismos es homomorfismo. Sean $(G_1, \overset{1}{*})$, $(G_2, \overset{2}{*})$ y $(G_3, \overset{3}{*})$ grupos. Si f y g son homomorfismos, entonces $g \circ f$ es homomorfismo.

$$\begin{array}{ccccc} G_1 & \xrightarrow{g} & G_2 & \xrightarrow{f} & G_3\\ g_1 & \longmapsto & g_2 & \longmapsto & g_3\end{array}$$

$$f(g(x \overset{1}{*} y)) = f(g(x) \overset{2}{*} g(y)) = f(g(x)) \overset{3}{*} f(g(y))$$

Definición: Si $(G_1, \cdot) = (G_2, *) = G$ se llama endomorfismo, y si es biyectivo automorfismo.

Ejemplo: Automorfismo identidad $1_G(x) = x \quad \forall x \in G$.

Proposición: Si $f\ :\ G_1 \longrightarrow G_2$ es un homomorfismo de de grupos, entonces se verifican

$$\begin{array}{ll} \textit{i)} & f(e_1) = e_2\\ \textit{ii)} & f(a^{-1}) = f(a)^{-1}\\ \textit{iii)} & \text{Si } o(a) = n < \infty, \text{ entonces } f(a)^n = e_2\\ \textit{iv} & \text{Si } H_1 \leq G_1, \text{ entonces } f(H_1) \leq G_2\\ \textit{v)} & \text{Si } H_2 \leq G_2, \text{ entonces } f^1(H_2) \leq G_1 \end{array}$$

Dem: i) $f(e_1) = f(e_1 \cdot e_1) = f(e_1) * f(e_1)$, entonces $f(e_1) = f(e_1) * f(e_1) \Leftrightarrow f(e_1)^{-1} * f(e_1) = f(e_1)^{-1} * f(e_1) * f(e_1) \Leftrightarrow e_2 = e_2 * f(e_1) = f(e_1)$.
ii) Veamos que $f(a) * f(a^-1) = e_2 = f(a^{-1}) * f(a)$.Aplicando *i)* $f(a) * f(a^{-1}) = f(a \cdot a^{-1}) = f(e_1) = e_2 = f(e_1) = f(a^{-1} \cdot a) = f(a^{-1}) * f(a)$.
iii) $f(a^n) = f(a) * \overset{n}{\cdots} * f(a) = f(a)^n$,entonces $e_2 = f(e_1) = f(a^{o(a)}) = f(a)^{o(a)}$
iv)

$$\begin{array}{ll} e_2 \in f(H_1) & f(\underbrace{e_1}_{\in H_1}) = e_2\\ f(y) \in f(H_1) \Rightarrow f(y)^{-1} \in f(H_1) & f(y)^{-1} = f(\underbrace{y^{-1}}_{\in H_1}) \in f(H_1) \end{array}$$

v)

$$\begin{array}{ll} e_1 \in f^{-1}(H_2) & f^{-1}(\underbrace{e_2}_{\in H_2}) \ni e_1\\ y \in f^{-1}(H_2) \Rightarrow y^{-1} \in f^{-1}(H_1) & f(y) \in H_2 \Rightarrow f(y)^{-1} \in H_2 \Rightarrow f(y^{-1}) \in H_2 \Rightarrow y^{-1} \in f^{-1}(H_2) \end{array}$$

Definición: Dado un homorfismo f de $(G_1, \cdot)$ en $(G_2, *)$. Llamamos núcleo de f a $Ker(f) = \{g \in G_1 \mid f(g) = e_2\}$.

Proposición: Dado un homorfismo f de $(G_1, \cdot)$ en $(G_2, *)$. $Ker(f) \trianglelefteq G_1$
Dem: Primero veamos que es subgrupo. $e_1 \in Ker(f)$ ya que $f(e_1) = e_2$. Si $x \in Ker(f)$, entonces

$x^{-1} \in Ker(f)$ ya que $e_2 = f(e_1) = f(x^{-1}x) = f(x^{-1}) * f(x) = f(x^{-1}) * e_2 = f(x^{-1})$. Ahora veamos que es subgrupo normal probando que $x \in Ker(f) \Rightarrow y^{-1}xy \in Ker(f)$. Observamos que $f(y^{-1}xy) = f(y^{-1}) * f(x) * f(y) = f(y)^{-1} * e - 2 * f(y) = e_2$.

Proposición: Dado un homorfismo f de $(G_1, \cdot)$ en $(G_2, *)$. f es inyectivo sii $Ker(f) = \{e_1\}$.
Dem: Si f es inyectiva $f(a) = e_2 = f(e_1)$, entonces $a = e_1$. Si $f(a) = f(b)$, entonces $e_2 = f(a) * f(b)^{-1} = f(a) * f(b^{-1}) = f(ab^{-1}) \in Ker(f) = \{e_1\}$, ahora $ab^{-1} = e_1$ y $a = b$.

Primer teorema de isomorfía de grupos: Dado un homorfismo f de $G_1, \cdot)$ en $(G_2, *)$. $G_1/Ker(f) \simeq f(G_1)$.
Dem: Consideramos la siguiente aplicación

$$\begin{array}{rccc} \bar{f}: & G_1/Ker(f) & \longrightarrow & f(G_1) \\ & aKer(f) & \longmapsto & f(a) \end{array}$$

Veamos que es isomorfismo.Primero que es suprayectiva pues todo elemento de $f(G_1)$ es de la forma $f(x)$ con $x \in G_1$. Veamos que es inyectiva, si $aKer(f) \in Ker(\bar{f})$ entonces $f(a) = e_2$ por lo que $a \in Ker(f)$ y $aKer(f) = Ker(f)$. Veamos que es homomorfismo $\bar{f}(aKer(f) \cdot bKer(f)) = \bar{f}((ab)Ker(f)) = f(ab) = f(a) * f(b) = \bar{f}(aKer(f)) * \bar{f}(bKer(f))$.

Definición: Sea G un grupo y $N \trianglelefteq G$. Definimos el epimorfismo canónico

$$\begin{array}{rccc} \pi: & G & \longrightarrow & G/N \\ & g & \longmapsto & gN \end{array}$$

Es epimorfismo ya que todo elemento de G/N es de la forma xN y por lo tanto es imagen de x. Por otra parte, $\pi(xy) = (xy)N = (xN)(yN) = \pi(x)\pi(y)$.

Proposición: Si $f : G \longrightarrow H$ es homomorfismo, entonces $Ker(f) \trianglelefteq G$ y $\begin{array}{rccc} \pi: & G & \longrightarrow & g/Ker(f) \\ & a & \longmapsto & aKer(f) \end{array}$ es un epimorfismo con $Ker(\pi) = Ker(f)$.
Dem: $Ker(f) \trianglelefteq G$ ya está probado, y $x \in Ker(\pi)$ entonces $xKer(f) = Ker(f)$ y $x \in Ker(f)$. Ahora, si $x \in Ker(f)$, entonces $\pi(x) = xKer(f) = Ker(f)$ y $x \in Ker(\pi)$.

Definición: Dado un homorfismo f de $G_1, \cdot)$ en $(G_2, *)$.Se tiene la descomposición canonica del homomorfismo

$$f = \underbrace{\iota}_{\text{monomorfismo inclusión}} \circ \underbrace{\bar{f}}_{\text{isomorfismo}} \circ \underbrace{\pi}_{\text{epimorfismo canónico}}$$

$$\begin{array}{ccccccc} \multicolumn{7}{c}{\xrightarrow{\hspace{12em} f \hspace{12em}}} \\ G_1 & \xrightarrow{\pi} & G_1/Ker(f) & \xrightarrow{\bar{f}} & f(G_1) & \xrightarrow{\iota} & G_2 \\ a & \longmapsto & aKer(f) & \longmapsto & f(a) & \longmapsto & f(a) \end{array}$$

Teorema: Sea $N \trianglelefteq G$. Entonces todo subgrupo de G/N es de la forma H/N con $N \subseteq H \leq G$.
Dem: Suponganmos que $K \leq G/N$, Sea $H = \{x \in G \mid xN \in K\}$. Veamos que H es subgrupo. Tenemos que $e \in H$ ya que $e_1N = N$ que es el elemento neutro en G/N y por lo tanto esta en K. Veamos que si $y \in H$, entonces $y^{-1} \in H$. Tenemos que $yN \in K$ entonces por ser N subgrupo normal $K \ni (yN)^{-1} = N^{-1}y^{-1} = Ny^{-1} = y^{-1}N$ por lo que $y^{-1} \in H$. Para ver que $N \subseteq H$, si $n \in N$, entonces $nN = N \in K$ por ser el elemento neutro y $n \in H$.

Teorema: Sea $N \trianglelefteq G$. Entonces si $N \leq H \leq G$ entonces $H/N \leq G/N$.
Dem: Veamos que es subgrupo. Si $x, y \in H$, $xN, yN \in H/N$ entonces $xy \in H$ y $(xy)N \in H/N$. Si $e \in H$, entonces $eN = N$. Si $x \in H$, $xN \in H/N$, entonces $x^{-1} \in H$ y $x^{-1}N \in H/N$, $(xN)(x^{-1}N) = (Nx)(x^{-1}) = N$.

Segundo teorema de isomorfía de grupos: Sea G un grupo, $N \trianglelefteq G$ y $H \leq G$, entonces

$$\begin{array}{ll} i) & N \trianglelefteq NH \\ ii) & N \cap H \trianglelefteq H \\ iii) & NH/N \simeq H/(N \cap H) \end{array}$$

Dem: i) Veamos que $(nh)^{-1}N(nh) = N$. $(nh)^{-1}N(nh) = h^{-1}n^{-1}Nnh = h^{-1}Nh = N$.
ii) Veamos que si $h \in H$, entonces $h^{-1}(N \cap H)h = N \cap H$. $(h^{-1}Nh) \cap (h^{-1}Hh) = N \cap H$.
iii) La aplicación $\begin{array}{rccc} \bar{f}: & NH/N & \longrightarrow & H/(N \cap H) \\ & hnN & \longmapsto & h(N \cap H) \end{array}$ es un isomorfismo de grupos. Está bien definida ya que si $hN = h'N$ entonces $h^{-1}h' \in N, H$ y $h(N \cap H) = h'(N \cap H)$. Es homomorfismo ya que $f((hN)(h'N)) = f((hh')N) = (hh')(N \cap H) = h(N \cap H)h'(N \cap H)) = f(hN)f(h'N)$. Es inyectiva ya que si $x \in Ker(f)$, entonces $x \in (N \cap H)$ y $xN = N$, es decir, $Ker(f) = \{N\}$. Es suprayectiva ya que dado un $h \in H$ existe hN tal que $f(hN) = h(N \cap H)$.

Tercer teorema de isomorfia de grupos: Sea G un grupo y $N \subseteq M$ dos subgrupos normales de G. Entonces se verifican

$$\begin{array}{ll} i) & M/N \trianglelefteq G/N \\ ii) & (G/N)/(M/N) \simeq G/M \end{array}$$

Dem: Sabemos que M/N es subgrupo.

$$(gN)^{-1}(mN)(gN) = (g^{-1}mg)N = mN$$

Consideramos la aplicación $\begin{array}{rccc} f: & G/N & \longrightarrow & G/M \\ & xN & \longmapsto & xM \end{array}$, esta bien definida ya que si $xN = yN$, entonces $x^{-1}y \in N \subseteq M$ y $xM = yM$. Es homomorfismo ya que $f((xN)(yN) = f((xy)N) = (xy)M = f(xN)f(yN)$. Es suprayectiva ya que para todo $xM \in G/M$ existe $xN \in G/N$ tal que $f(xN) = xM$. Calculamos $ker(f)$, si $N = f(xM) = xN$ se tiene que $x \in N$ por lo que

$$Ker(f) = \{xM \mid x \in N\} = M/N$$

Por el primer teorema de isomorfía, aplicado a f,

$$(G/N)/Ker(f) = (G/N)/(M/N) \simeq f(G/N) = G/M$$

$$(G/N)/(M/N) \simeq G/M$$