4. Grupos cociente. Teoremas de isomorfía

4.1 Grupos normales

Definición

Un subgrupo H de un grupo G se dice que es un subgrupo normal ($H \lhd G$) si $xH = Hx$. En ese caso $G/_{\sim_H} = G/_{\tilde{H}}$ que notaremos por G/H y llamaremos conjunto de las clases laterales de H en G

Caracterización

Sea G un grupo y $H < G$. Son equivalentes:

i) $H \lhd G$

$\downarrow xh = h'x$

ii) $\forall x \in G,\ h \in H \Rightarrow xhx^{-1} \in H$ → Podemos probarlo sólo con los generadores

$\updownarrow$ trivial

iii) $\forall x \in G \Rightarrow xHx^{-1} \subset H$

$\downarrow x^{-1}H(x^{-1})^{-1} \subset H$

iv) $\forall x \in G \Rightarrow xHx^{-1} = H$ (H coincide con todos sus conjugados)

$xhx^{-1} = h' \in H$

Nota: xHx^{-1} es el conjugado de H según x.

-Demostración-

i) ⇒ ii)

Como H es normal $\Rightarrow xH = Hx$ luego $xh \in Hx$ luego $xh = h'x$, $h' \in H$. De aquí obtenemos que $xhx^{-1} = h' \in H$

ii) ⇔ iii) Es trivial

iii) ⇒ iv) Sabemos de iii) que $xHx \subset H$ luego vamos a ver que $H \subset xHx^{-1}$. Sabemos que $\forall x \in G,\ x^{-1} \in G,\ x^{-1}H(x^{-1})^{-1} \subset H \Rightarrow x^{-1}Hx \subset H$. Como $H = x(\underbrace{x^{-1}Hx}_{\subset H})x^{-1} \subseteq xHx^{-1}$

x^{-1} toma el papel de x

Aplicar inversos

iv) ⇒ i) $\forall h \in H$ $xhx^{-1} \in xHx^{-1} = H$, entonces $xhx^{-1} = h' \in H$. Entonces $xh = h'x \in Hx$, es decir $xH \subset Hx$ y la otra inclusión se hace igual y por tanto $xH = Hx$

> Nota: todo grupo tiene subgrupos normales

Veamos algunos ejemplos:

i) Los subgrupos impropios siempre son normales

ii) Todo subgrupo de un grupo abeliano es normal.

iii) Todo subgrupo de índice 2 es normal, es decir, $H < G$ $[G:H] = 2 \Rightarrow H \lhd G$

Razonamiento por particiones

Sea $x \in G \mid x \notin H \Rightarrow$ existen dos clases, es decir $G = H \cup xH = H \cup Hx$ en ambos casos xH y Hx son el complemento de H en G luego deben ser iguales.

iv) $G = S_3$, $H = \langle (12) \rangle$ H no es normal pues $(23)(12)(23)^{-1} = (13) \notin H$

Lo mismo ocurrirá con $\langle (23) \rangle$, $\langle (13) \rangle$.

En este caso $K = \{1, (123), (132)\} \trianglelefteq S_3$ entonces $S_3/_K \cong \{H, H(12)\} \Rightarrow [S_3 : K] = 2 \Rightarrow$ normal

v) Ser normal no es una relación transitiva.

Intuición: La situación puede darse

$$\begin{tikzcd} G \arrow[dr, "\text{normal}"] \arrow[d, dash, "\text{no normal}"'] & \\ K \arrow[r, "\text{normal}"'] & H \end{tikzcd}$$

Contraejemplo: A_4, V, $\langle (12)(34) \rangle$ donde se cumple que $\langle (12)(34) \rangle \trianglelefteq V \trianglelefteq A_4$ pero $\langle (12)(34) \rangle \ntrianglelefteq A_4$

índice 2

$A_4 = \langle (123), (124) \rangle$, basta con comprobar con que $(123)\, x\, (123)^{-1} \in V \quad \forall x \in V$

vi) Para un grupo G definimos $Z(G) = \{a \in G \mid ax = xa, \forall x \in G\}$ centro de G

- $Z(G)$ es un subgrupo.
- $Z(G) \trianglelefteq G$
- Si G es abeliano $\Rightarrow Z(G) = G$

Ejercicio 6 $Z(S_n)$, $Z(A_n)$

Vamos a ver que $Z(S_n) = 1$ si $n \geq 3$ y $Z(A_n) = 1$ si $n \geq 4$

- Si $n \geq 3$ y $\sigma \in S_n$ $\sigma \neq 1 \Rightarrow \exists\, i, j \in \{1, \ldots, n\}, i \neq j \mid \sigma(i) = j \Rightarrow \exists k \neq i, k \neq j$ $k \in \{1, \ldots, n\}$

considero la trasposición $\tau = (j\,k)$.

Vamos a ver que $\underbrace{\sigma(\tau(i))}_{= j} \neq \underbrace{\tau(\sigma(i))}_{= k}$ luego $\sigma\tau \neq \tau\sigma$ y tenemos que $\sigma = 1$

- Si $n \geq 4$ y $\sigma \in A_n \Rightarrow \exists\, i \neq j \in \{1, \ldots, n\} \mid \sigma(i) = j \Rightarrow \exists k, l \in \{1, \ldots, n\}$ $k \neq i, k \neq j$ tomamos $\tau = (j\,k\,l) \in A_n$

$\sigma(\tau(i)) \neq \tau(\sigma(i))$ luego $Z(A_n) = \{1\}$

Caracterización

Sea G un grupo, $H < G$. Son equivalentes

i) $H \trianglelefteq G$

ii) $\forall x, y \in G \mid xy \in H \Rightarrow yx \in H$

$x \sim_H y \Leftrightarrow xy^{-1} \in H$

por?

-Demostración-

da igual

$\Rightarrow)$ Si $xy \in H \Rightarrow x \sim_H y^{-1} \Rightarrow Hx = Hy^{-1} \Rightarrow \exists h, h' \in H \mid hx = h'y^{-1}$. Como H es normal $xH = Hx \wedge y^{-1}H = Hy^{-1}$ luego

no puedo asegurar que sea h — es h'

$hx = xh''$, $h'' \in H$ y de la misma forma $h'y^{-1} = y^{-1}h'''$, $h''' \in H$. Es decir, $xh'' = y^{-1}h''' \Leftrightarrow yx = h'''h''^{-1} \in H$

$\Leftarrow)$ $\forall x \in G$, $\forall h \in H$ $\underbrace{x x^{-1}}_{g} h \in H$ (x, y) luego, por hipótesis $xhx^{-1} \in H$, es decir, $H \trianglelefteq G$

Idea feliz

Teorema

Sea G un grupo y $H \trianglelefteq G$. Entonces en el conjunto G/H podemos definir una operación binaria $G/H \times G/H \longrightarrow G/H$ que convierte a G/H en grupo y de forma que la proyección canónica $p: G \longrightarrow G/H$ es un homomorfismo de grupos

A G/H lo podemos llamar el grupo cociente de G sobre H

-Demostración-

$$\left.\begin{array}{rcl} G/H \times G/H & \longrightarrow & G/H \\ (xH, yH) & \longmapsto & xyH \end{array}\right\}$$ Defino esta op. binaria que será la usual del cociente

$h_1 = h(h')^{-1}$ — no dist. — $h_2 = h(h')^{-1}$

Que está bien definido, pues si $xH = x'H$ y $yH = y'H \Rightarrow xyH = x'y'H$ ya que $x' = xh_1$ y $y' = yh_2$ con $h_1, h_2 \in H$ $\forall h \in H$ $x'y'h = \underbrace{xh_1}_{x'}\underbrace{yh_2}_{y'}h \overset{?}{=} xyh_1'h_2h = xy\bar{h}$ $\bar{h} \in H \Rightarrow xy\bar{h} \in xyH$. La otra inclusión igual.

$H \trianglelefteq G$? $h_1 y \in h = yh_1 \in H$?

La asociativa es clara, el neutro es H y el simétrico es $(xH)^{-1} = x^{-1}H$.

La proyección canónica es un homomorfismo de grupos pues $p(xy) = xyH = xHyH = p(x)p(y)$ luego es un homomorfismo de grupos

$\square$

En grupos cualesquiera?

Ahora ya podemos hablar de orden y se da que $|G/H| = [G:H] = \frac{|G|}{|H|}$ y además $\ker(p) = H$, realmente $\ker(p) = \{x \in G \mid p(x) = 1\} = \{x \in G \mid xH = H\} = \{x \in H\}$

Algunos ejemplos de cocientes son:

i) S_3, $H = \{1, (123), (132)\}$, $S_3/H = \{H, H(12)\} \cong \mathbb{Z}_2$

ii) $H < \mathbb{Z} \Rightarrow H \trianglelefteq \mathbb{Z}$, $H = n\mathbb{Z}$ luego $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$

iii) A_4 no tiene subgrupos de orden 6. Si $H < A_4 \mid |H| = 6 \Rightarrow [A_4 : H] = \frac{|A_4|}{|H|} = 2 \Rightarrow H \trianglelefteq A_4$ luego puedo hacer un cociente $A_4/H \cong \mathbb{Z}_2$ porque tiene 2 clases $\Rightarrow (xH)^2 = x^2H = H$ $\forall x \in A_4/H$ luego lo que estamos diciendo es que los cuadrados de los 8 3-ciclos de A_4 serían los 3-ciclos de $H \Rightarrow |H| \geq 8$ ↯ ? Por qué $|H| \geq 8$? si tenemos 8 3-ciclos ya bastaría no?

Caracterización

$H < \mathcal{G}$ es normal sii $\exists f: \mathcal{G} \longrightarrow \mathcal{G}'$ homomorfismo de grupos tal que $\operatorname{Ker} f = H$

-Demostración-

$\Rightarrow]$ $p: \mathcal{G} \longrightarrow \mathcal{G}/H$, $\operatorname{Ker}(p) = H$, teorema anterior.

$\Leftarrow]$ Sea $H = \operatorname{Ker}(f)$ para $f: \mathcal{G} \longrightarrow \mathcal{G}'$, $\forall x \in \mathcal{G}$, $h \in H$ $\quad x h x^{-1} \overset{??}{\in} H$.

$$f(xhx^{-1}) = f(x) f(h) \cdot f(x)^{-1} \underset{\substack{\uparrow \\ h \in \operatorname{Ker}(f)}}{=} f(x) f(x)^{-1} = 1 \Rightarrow xhx^{-1} \in \operatorname{Ker}(f) = H \Rightarrow H \trianglelefteq \mathcal{G}$$

Propiedad universal del grupo cociente

Sea $\mathcal{G}$ un grupo, $H \trianglelefteq \mathcal{G}$ y $p: \mathcal{G} \longrightarrow \mathcal{G}/H$ la proyección canónica. Entonces $\forall f\ \mathcal{G} \longrightarrow \mathcal{G}'$ homomorfismo de manera que $H \subseteq \operatorname{Ker} f$ $\exists! \varphi: \mathcal{G}/H \longrightarrow \mathcal{G}'$ homomorfismo tal que $\varphi \circ p = f$

Además, f es sobreyectivo $\Leftrightarrow$ φ es sobreyectivo y $H = \operatorname{Ker} f$ sii φ es inyectivo

-Gráficamente-

$$\begin{tikzcd}
\mathcal{G} \arrow[r, "i"] \arrow[dr, "f \,|\, H \subseteq \operatorname{Ker} f"'] & \mathcal{G}/H \arrow[d, dotted, "\exists! \varphi"] \\
& \mathcal{G}'
\end{tikzcd}$$

-Demostración-

Definimos $\varphi: \mathcal{G}/H \longrightarrow \mathcal{G}'$ como $\varphi(xH) = f(x)$ y vemos que está bien definido.

Si es único siempre será así

$$\text{Si } xH = yH \Rightarrow y^{-1}x \in H \Rightarrow y^{-1} x \in \underset{\substack{\uparrow \\ \text{caracterización anterior}}}{\operatorname{Ker} f} \Rightarrow f(y^{-1}x) = 1 \Rightarrow f(y)^{-1} f(x) = 1 \Rightarrow f(x) = f(y)$$

Veamos ahora que φ es homomorfismo.

$$\varphi(xHyH) = \varphi(xyH) = f(xy) = f(x) f(y) = \varphi(xH)\varphi(yH) \quad \rightarrow \text{definición de } \varphi.$$

Veamos que el diagrama conmuta(?)

$$\varphi \circ p = f: \forall x \in \mathcal{G} \quad (\varphi p)(x) = \varphi(p(x)) = \varphi(xH) = f(x)$$

Unicidad: Si hubiera otro definido igual

$$\text{Sea } \overline{\varphi}: \mathcal{G}/H \longrightarrow \mathcal{G}' \mid \overline{\varphi} \circ p = f, \ \forall x \in \mathcal{G} \ (\overline{\varphi} \circ p)(x) = \overline{\varphi}(p(x)) = \underline{\overline{\varphi}(xH) = f(x)} = \varphi(xH) \Rightarrow \overline{\varphi} = \varphi$$

Veamos las equivalencias.

- f sobreyectivo $\Leftrightarrow$ φ sobreyectivo

  $\Leftarrow]$ La composición de sobreyectivos es sobreyectivo

  $\Rightarrow]$ Sea f sobreyectivo, $y \in \mathcal{G}' \Rightarrow \exists x \in \mathcal{G} \mid f(x) = y$, pero $\overset{y}{\overset{\shortparallel}{f(x)}} = \varphi(p(x)) = \varphi(xH)$, $xH \in \mathcal{G}/H$ y $\varphi(xH) = y$

  $\hookrightarrow \forall y \in \mathcal{G}' \ \exists xH \in \mathcal{G}/H \mid \varphi(xH) = y$.

- $H = \operatorname{Ker} f \Leftrightarrow \varphi$ es inyectivo

  $\Rightarrow]$ Si $H = \operatorname{Ker} f$ y $\varphi(xH) = 1 \Rightarrow 1 = \varphi(xH) = f(x) \Rightarrow x \in \operatorname{Ker} f = H \Rightarrow \boxed{xH = H} \Rightarrow \varphi$ inyectivo

$\Leftarrow$) $\operatorname{Ker} f \overset{??}{\subset} H$, sea $x \in \operatorname{Ker} f \Rightarrow \underset{\varphi(xH)}{\underset{\parallel}{f(x)}} = 1$ $\Big\} \Rightarrow xH \in \operatorname{Ker}\varphi = H \Rightarrow xH = H \Rightarrow x \in H$

$\hookrightarrow H \subset \operatorname{Ker} f$ por hipótesis

4.2. Teoremas de isomorfía

1^er^ Teorema de isomorfía (para grupos)

Sea $f: \mathcal{G} \to \mathcal{G}'$ homomorfismo de grupos. Entonces $\exists \varphi: \mathcal{G}/_{\operatorname{Ker} f} \longrightarrow \operatorname{Im} f$ isomorfismo y vendrá dado por $\varphi(x\operatorname{Ker} f) = f(x)$ $\forall x\operatorname{Ker} f \in \mathcal{G}/_{\operatorname{Ker} f}$

$\hookrightarrow \{y \in \mathcal{G} \mid xy^{-1} \in \operatorname{Ker}(f)\} = \{y \in \mathcal{G} \mid f(xy^{-1}) = 1$

-Demostración-

$\operatorname{Ker} f \triangleleft \mathcal{G}$ luego podemos considerar $p: \mathcal{G} \to \mathcal{G}/_{\operatorname{Ker} f}$ y definimos $f: \mathcal{G} \to \operatorname{Im} f$ un homomorfismo sobreyectivo. Hay que componerlo

Usando la propiedad universal del grupo cociente tenemos el siguiente diagrama

$$\begin{tikzcd}
\mathcal{G} \arrow[r, "p"] \arrow[dr, "f"', "\text{sobrey.}"] & \mathcal{G}/_{\operatorname{Ker} f} \arrow[d, dotted, "\text{sobrey. inyectiva}"] \\
& \operatorname{Im} f
\end{tikzcd}$$

$\hookrightarrow \exists! \varphi: \mathcal{G}/_{\operatorname{Ker} f} \longrightarrow \operatorname{Im} f$ isomorfismo.

solo me sirve la existencia.

Luego $\mathcal{G}/_{\operatorname{Ker} f} \cong \operatorname{Im} f$

-Ejemplo-

Sea K un cuerpo finito, $|K| = q$ y $\det: \mathcal{GL}_n(K) \longrightarrow K^*$ un homomorfismo de grupos

$\operatorname{Ker}(\det) = \underset{\text{lineal especial}}{\mathcal{SL}_n(K)}$

Luego $\mathcal{GL}_n(K)/_{\mathcal{SL}_n(K)} \cong \operatorname{Im}(\det) = K^*$. Lo usamos para calcular $|\mathcal{GL}_n(K)| = (q^n - 1)(q^n - q) \cdots (q^n - q^{n-1})$

es decir, $|\mathcal{SL}_n(K)| = \dfrac{|\mathcal{GL}_n(K)|}{|K^*|} = \dfrac{(q^n - 1)(q^n - q) \cdots (q^n - q^{n-1})}{q-1}$

2º Teorema de isomorfía (para grupos)

Sea $\mathcal{G}$ un grupo, $H, K < \mathcal{G}$ tal que $K \triangleleft \mathcal{G}$. Entonces $H \cap K \triangleleft H$ y $\exists \varphi: H/_{H \cap K} \longrightarrow \frac{HK}{K}$ isomorfismo

-Idea-

-Demostración-

Como $K \triangleleft \mathcal{G} \Rightarrow xK = Kx$ $\forall x \in \mathcal{G} \Rightarrow HK = KH \Rightarrow HK < \mathcal{G} \Rightarrow K \triangleleft HK$. Supongamos la siguiente situación

$$H \xhookrightarrow{i} \mathcal{G} \xrightarrow{p} \mathcal{G}/_K$$

Luego considerando este morfismo, $Im(p\circ i) = \{(p\circ i)(h) \mid h\in H\} = \{p(h) \mid h\in H\} = \{hK \mid h\in H\} = HK/_K$

y $ker(p\circ i) = \{h\in H \mid (p\circ i)(h) = K\} = \{h\in H \mid hK = K\} = \{h\in H \mid h\in K\} = H\cap K$

Aplicando el primer teorema de isomorfía sabemos que $\frac{H}{Ker(p\circ i)} \cong Im(p\circ i) \Rightarrow \frac{H}{H\cap K} \cong \frac{HK}{K}$

-Ejemplo- (Ejercicio 1)

Si $H < S_n$ tiene una permutación impar $\Rightarrow [H : H\cap A_n] = 2$, es decir, H tiene el mismo número de permutaciones pares que impares.

Como tiene perm. impar $H \not< A_n$ y $HA_n = S_n$. Aplicando el segundo teorema de isomorfía tenemos que $\frac{H}{H\cap A_n} = \frac{S_n}{A_n} \cong \mathbb{Z}_2$ luego tiene índice 2 como se quería.

3^er Teorema de isomorfía (para grupos) o del doble cociente

Dado $\mathcal{G}$ un grupo, $N \trianglelefteq \mathcal{G}$. Entonces existe una biyección entre los subgrupos de $\mathcal{G}$ que contienen a N y los subgrupos de $\mathcal{G}/_N$; que viene dada por $\varphi: H \longrightarrow H/_N$.

Además, $H \trianglelefteq \mathcal{G}$ si y solo si $H/_N \trianglelefteq \mathcal{G}/_N$, y en ese caso, $\frac{\mathcal{G}/_N}{H/_N} \cong \mathcal{G}/_H$

-Demostración-

Sea $p: \mathcal{G} \longrightarrow \mathcal{G}/_N$ la proyección canónica y los siguientes conjuntos

$$\{N\subset H < \mathcal{G}\} \xrightarrow[p_*]{} \{J < \mathcal{G}/_N\}$$

$$\{J < \mathcal{G}/_N\} \xrightarrow[p^*]{} \{N\subset H < \mathcal{G}\}$$

Y vamos a ver que la composición es la identidad. Pero primero veamos que están bien definidos:

$p_*)$

$\forall H < \mathcal{G}$ $p_*(H) = \{p(h) \mid h\in H\} = \{hN \mid h\in N\} = H/_N < \mathcal{G}/_N$

$p^*)$

$\forall J < \mathcal{G}/_N$ $p^*(J) = \{x\in \mathcal{G} \mid p(x)\in J\} < \mathcal{G}$. Vamos a ver que $p(N)$ es subgrupo de J

$p(u) = uN = N \in J$, $u \in p^*(J)$, $N \subseteq p^*(J)$

Vemos la composición:

- $p_* \circ p^* = J$ pues p es sobreyectiva
- $H \overset{??}{=} p^* p_*(H)$, $H \subseteq p^* p_*(H)$ ocurre siempre pues $h = p^* p_*(h) \subset p^* p_*(H)$

$p^* p_*(H) \overset{?}{\subseteq} H$, si $x \in p^* p_*(H) \Rightarrow p(x) \in p_*(H) \Rightarrow xN \in H/N = \{hN \mid h \in H\} \Rightarrow x \in H \Rightarrow p^* p_*(H) \subseteq H$.

Veamos ahora el además:

$\Rightarrow$] $\forall xN \in \mathcal{G}/N, hN \in H/N$ veamos que $xNhN(xN)^{-1} \in H/N$ pero:

$$xNhN(xN)^{-1} = xNhNx^{-1}N = xhx^{-1}N \in N/N$$

$\Leftarrow$] $\forall x \in \mathcal{G}, h \in H$ veamos que $xhx^{-1} \in H$. Consideramos la clase de equivalencia $xhx^{-1}N = xNhN(xN)^{-1} \in H/N$

luego $xhx^{-1} \in H \Rightarrow H \trianglelefteq \mathcal{G}$

Para ver ese isomorfismo del doble cociente:

$$\begin{tikzcd} \mathcal{G} \arrow[r, "p_N"] \arrow[dr, "p_H"'] & \mathcal{G}/N \arrow[d, dashed, "\exists! \varphi"] \\ & \mathcal{G}/H \end{tikzcd}$$

$\exists! \varphi \mid \varphi p_N = p_H$ por la propiedad universal del grupo cociente

Ahora, aplicando el 1TI aplicado a φ, tenemos que $\dfrac{\mathcal{G}/N}{\operatorname{Ker}\varphi} \cong \operatorname{Im}\varphi$ pues $\operatorname{Ker}\varphi = H/N$.

-Ejemplo-

Utilidad para ver los retículos sobre el cociente

$$\begin{tikzcd} & D_4 \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\ \langle s, sr^2 \rangle \arrow[dr, dash] & \langle r \rangle \arrow[d, dash] & \langle sr, sr^3 \rangle \arrow[dl, dash] \\ & \langle r^2 \rangle & \end{tikzcd}$$

Si tomamos el cociente sobre $\langle r^2 \rangle$ obtenemos el mismo retículo tomando cocientes

$$\begin{tikzcd} & D_4/\langle r^2 \rangle \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\ \langle s, sr^2 \rangle/\langle r^2 \rangle \arrow[dr, dash] & \langle r \rangle \arrow[d, dash] & \langle sr, sr^3 \rangle/\langle r^2 \rangle \arrow[dl, dash] \\ & \langle r^2 \rangle/\langle r^2 \rangle & \end{tikzcd}$$

4.2.1. Cuarto teorema de isomorfía

4.2.1.1 Lema (Ley modular o regla de Dedekind)

Basta pedir $A \subseteq C$ pues se deduce

Sea $\mathcal{G}$ un grupo y $A, B, C < \mathcal{G}$ con $A < C$. Entonces

$$A(B \cap C) = (AB) \cap C$$

-Demostración-

$\subseteq$] Sea $z \in A(B \cap C) \Rightarrow \exists a \in A, x \in B \cap C \mid z = ax \Rightarrow ax \in AB \wedge ax \in AC$, pero $a \in A < C \Rightarrow ax \in C$, luego $z \in AB \cap C$

$\supseteq$] Sea $z \in AB \cap C \Rightarrow \begin{cases} z = ab \mid a \in A, b \in B \\ z = c \mid c \in C \end{cases}$ como $A < C \Rightarrow a \in C \Rightarrow a^{-1} \in C \Rightarrow \begin{cases} b = a^{-1}z \in C \\ b \in B \end{cases} \Rightarrow b \in B \cap C \Rightarrow z \in A(B \cap C)$

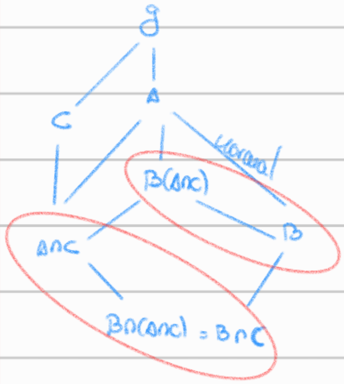
4.2.12 Lema

Sea G un grupo y $A,B,C<G$ con $B\triangleleft A$. Entonces

i) $B\cap C \triangleleft A\cap C$ ∧ $\frac{A\cap C}{B\cap C} \cong \frac{B(A\cap C)}{B}$

ii) Si además $C\triangleleft G$ entonces $BC\triangleleft AC$ y $\frac{AC}{BC}\cong \frac{A}{B(A\cap C)}$

-Demostración-

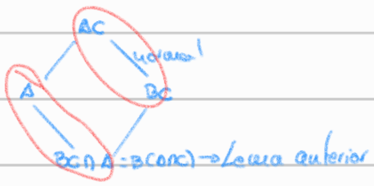


i) Aplicando el 2TI obtenemos que $\frac{A\cap C}{B\cap C}\cong\frac{B(A\cap C)}{B}$

ii) Si $C\triangleleft G \Rightarrow BC, AC<G$ y $BC<AC$ pues $B<A$. Vamos a ver que $BC\triangleleft AC$, sean $x=ac$ y $y=bc$

$$xyx^{-1}=acbc'c^{-1}a^{-1}=\underbrace{aca^{-1}}_{\substack{C\triangleleft G\\ \uparrow\\ C}}\underbrace{aba^{-1}}_{\substack{B\triangleleft A\\ \uparrow\\ B}}\underbrace{ac'c^{-1}a^{-1}}_{\substack{C\triangleleft G\\ \uparrow\\ C}}\in CBC$$

Entonces, hemos visto que $xyx^{-1}\in CBC$ pero $BC=CB$ pues $C\triangleleft G$ luego $BC\triangleleft AC$



$BC\cap A\triangleleft BC$ $\qquad \frac{A}{BC\cap A}\cong\frac{AC}{BC}$

Usando 2TI tenemos que $\frac{A}{B(A\cap C)}\cong\frac{AC}{BC}$

4º Teorema de Isomorfía (de la mariposa o zassenhaus)

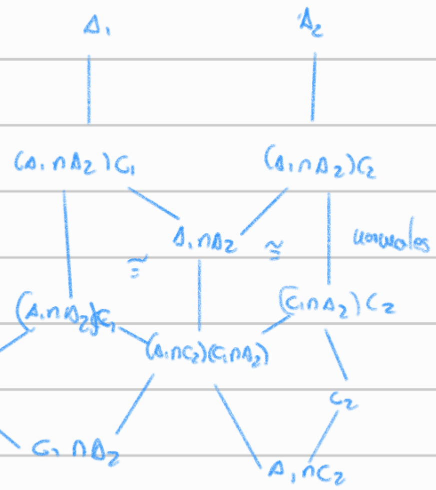
Sea G un grupo, $A_1, C_1, A_2, C_2 < G$ cumpliendo $C_1\triangleleft A_1$, $C_2\triangleleft A_2$. Entonces

i) $(A_1\cap C_2)C_1 \triangleleft (A_1\cap A_2)C_1$

ii) $(A_2\cap C_1)C_2 \triangleleft (A_1\cap A_2)C_2$ } Es lo mismo cambiando 1 por 2

iii) $\frac{(A_1\cap A_2)C_1}{(A_1\cap C_2)C_1}\cong\frac{A_1\cap A_2}{(A_1\cap C_2)(A_2\cap C_1)}\cong\frac{(A_1\cap A_2)C_2}{(A_2\cap C_1)C_2}$

- Demostración -



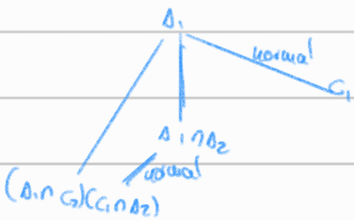
i) Nos fijamos en el siguiente retículo

Usando el 2TI tenemos que $\frac{A_1 \cap A_2}{A_1 \cap C_2} \cong \frac{(A_1 \cap A_2)C_2}{C_2}$ y $A_1 \cap C_2 \trianglelefteq A_1 \cap A_2$.

Usando ahora, el apartado ii) del lema 4.2.1.2 obtenemos que $(A_1 \cap C_2)C_1 \trianglelefteq (A_1 \cap A_2)C_1$

ii) De forma análoga cambiando el retículo se obtiene lo buscado

iii) Vamos a demostrar una de las isomorfías, la otra es análoga. Consideramos el subretículo



Usando ahora el apartado ii) del lema 4.2.1.2 tenemos que $(A_1 \cap C_2)(C_1 \cap A_2) \trianglelefteq A_1 \cap A_2$,

$A_1 \cap C_2 \trianglelefteq A_1 \cap A_2$, $C_1 \cap A_2 \trianglelefteq A_1 \cap A_2$ $\Rightarrow$ tenemos que $\frac{(A_1 \cap A_2)C_1}{(A_1 \cap C_2)C_1} \cong \frac{A_1 \cap A_2}{(A_1 \cap C_2)(A_2 \cap C_1)}$ $\square$

4.3. El producto directo de grupos

Producto directo externo o producto directo

Tomamos dos grupos cualesquiera, $\mathcal{G}$ y H y consideramos $H \times \mathcal{G}$ con una operación binaria

$$(H \times \mathcal{G}) \times (H \times \mathcal{G}) \longrightarrow (H \times \mathcal{G})$$
$$(h_1, k_1)(h_2, k_2) \longmapsto (h_1 h_2, k_1 k_2)$$

que cumple la asociatividad, la existencia de neutro que será $(1,1)$ y para cada elemento de $H \times \mathcal{G}$ consideramos su inverso como el inverso componente a componente

Por tanto, $(H \times \mathcal{G})$ con esta operación tiene estructura de grupo que llamamos producto directo de H y $\mathcal{G}$

↳ Es un grupo y es el prod directo externo

Si H y $\mathcal{G}$ son finitos entonces:

•) $|H \times \mathcal{G}| = |H||\mathcal{G}|$

•) $o((h,k)) = \text{mcm}(o(h), o(k))$ → se deduce de la operación binaria

Vamos a definir cuatro aplicaciones según el siguiente diagrama.

$$\begin{tikzcd} H \arrow[r, shift left, "i_1"] & H\times\mathcal{G} \arrow[l, shift left, "p_1"] \arrow[r, shift left, "p_2"] & \mathcal{G} \arrow[l, shift left, "i_2"] \end{tikzcd}$$

definidas por:

Proyecciones	Inyecciones
$p_1(h_1,k)=h_1$	$i_1(h_1)=(h_1,1)$
$p_2(h,k_1)=k_1$	$i_2(k_1)=(1,k_1)$

Lema

Se cumple que:

i) $p_j, j=1,2 \wedge i_j, j=1,2$ son homomorfismos de grupos

ii) $p_j i_j = id \quad j=1,2 \quad \wedge \; p_j i_k$ con $j\neq k$ es trivial

iii) p_j es ~~inyectiva~~ sobreyectiva $j=1,2$ e i_j son inyectivas $j=1,2$

Expresar H como $H\times\{1\}$

iv) Si consideramos $H'=Im(i_1)=Ker(p_2)=\{(h,1)\mid h\in H\}\trianglelefteq H\times\mathcal{G}$ y $H'\cong H$

Expresar $\mathcal{G}$ como $\{1\}\times\mathcal{G}$

v) Si consideramos $K'=Im(i_2)=Ker(p_1)=\{(1,k)\mid k\in\mathcal{G}\}\trianglelefteq H\times\mathcal{G}$ y $K'\cong\mathcal{G}$

vi) $H'\cap K'=\{1\}$ y $\forall x\in H', y\in K' \quad xy=yx$

Propiedad universal del producto directo

Sea $\mathcal{G}$ un grupo y $f_1:\mathcal{G}\longrightarrow H$, $f_2:\mathcal{G}\longrightarrow K$ dos homomorfismos de grupos. Existe un único homomorfismo de grupos $f:\mathcal{G}\longrightarrow H\times K$ de manera que $p_1 f=f_1 \wedge p_2 f=f_2$

-Demostración-

$$\begin{tikzcd} & \mathcal{G} \arrow[dl, "f_1"'] \arrow[d, dashed, "\exists! f"] \arrow[dr, "f_2"] & \\ H & H\times K \arrow[l, "p_1"] \arrow[r, "p_2"'] & K \end{tikzcd}$$

$\forall g\in\mathcal{G} \quad f(g)=(h,k)=(f_1(g),f_2(g))$

$h=p_1 f(g)=f_1(g)$

$k=p_2 f(g)=f_2(g)$

Está construida f para que se cumpla y sea única. □

Teorema

Sea L un grupo y $\ell_1:L\longrightarrow H$, $\ell_2:L\longrightarrow K$ dos homomorfismos que cumplen: para todo grupo $\mathcal{G}$ y para todo par de homomorfismos $f_1:\mathcal{G}\to H$, $f_2:\mathcal{G}\to K$, existe un único homomorfismo $f:\mathcal{G}\longrightarrow L$ tal que $\ell_1 f=f_1 \wedge \ell_2 f=f_2$ entonces $L\cong H\times K$

- Demostración -

$$\begin{tikzcd} & L \cong H\times K \arrow[dl, "\ell_1"'] \arrow[dr, "\ell_2"] & \\ H \arrow[r, phantom, "="] & & K \\ & \mathcal{G} \arrow[ul, "p_1"] \arrow[ur, "p_2"'] \arrow[uu, dashed, "\exists! p"] & \end{tikzcd}$$

Por la propiedad universal del producto directo $\exists! : L \longrightarrow H\times K$ tal que $p_2\ell = \ell_2 \wedge p_1\ell = \ell_1$.

¿Por hipótesis, para cualquier grupo $H\times K$ con p_1 y p_2 $\exists! p$ $\mathcal{G}\to L$ tal que $p_1 p = \ell_1$ y $p_2 p = \ell_2$? Es la idea

Tomando $p_1 1_{H\times K} = p_1 = \ell_1 p = p_1 \ell p \Rightarrow \ell p = 1_{H\times K}$

y $\ell_1 1_{\mathcal{G}} = \ell_1 = p_1\ell = \ell_1 p\ell \Rightarrow 1_{\mathcal{G}} = p\ell$

Teorema

Sea $\mathcal{G}$ un grupo y $f_1 : H \longrightarrow \mathcal{G}$, $f_2 : K \longrightarrow \mathcal{G}$ dos homomorfismos de grupos. Existe un único homomorfismo de grupos $f : H\times K \longrightarrow \mathcal{G}$ de manera que $f i_1 = f_1 \wedge f i_2 = f_2$

- Demostración -

Pensar en [illegible]

$$\begin{tikzcd} & \mathcal{G} & \\ H \arrow[ur, "f_1"] \arrow[r, "p_1"'] & H\times K \arrow[u, dashed, "\exists! f"] & K \arrow[ul, "f_2"'] \arrow[l, "p_2"] \end{tikzcd}$$

Definimos ahora $f(h,k) = f_1(h) f_2(k)$ y cumple lo que queremos

Idea de construcción:

$f(h,k) = f((h,1)(1,k)) = f_{i_1}(h,k) f_2(h,k)$

Teorema

Sea L un grupo y $\ell_1 : H \longrightarrow L$, $\ell_2 : K \longrightarrow L$ dos homomorfismos tales que $\forall h\in H$, $\forall k\in K$ $\ell_1(h)\ell_2(k) = \ell_2(k)\ell_1(h)$ que cumplen. para todo grupo $\mathcal{G}$ y para todo par de homomorfismos $f_1 : H\to\mathcal{G}$, $f_2 : K\to\mathcal{G}$ tales que $\forall h\in H$, $\forall k\in K$, $f_1(h)f_2(k) = f_2(k)f_1(h)$, existe un único homomorfismo $f : L \longrightarrow \mathcal{G}$ tal que $\ell_1 f = f_1 \wedge \ell_2 f = f_2$ entonces $L \cong H\times K$

$f\ell_1 = f_1$ $\quad f\ell_2 = f_2$

- Demostración -

Es similar al anterior de proyecciones

Producto directo interno

Lo que vamos a ver es cuando, dado $\mathcal{G}$ grupo y $K, H < \mathcal{G}$, se tiene que $H\times K \cong \mathcal{G}$. En ese caso, tendremos un producto directo interno

sólo tendremos producto directo interno cuando se da esa condición

Teorema (caracterizaciones del grupo directo interno)

Sea $\mathcal{G}$ un grupo, $H, K < \mathcal{G}$. Equivalen:

i) $\phi : H\times K \longrightarrow \mathcal{G} \mid \phi(h,k) = hk$ es un isomorfismo $\quad H\times K \cong \mathcal{G} = HK$

ii) $H, K \lhd \mathcal{G}$, $HK = \mathcal{G}$ y $H\cap K = \{1\}$ $\quad$ Subgrupo más pequeño que contiene a $H\cup K$

iii) $\forall h\in H$, $k\in K$ $hk = kh$, $H\vee K = \mathcal{G} \wedge H\cap K = \{1\}$ $\quad H\vee K = HK$ ↳ cuando $HK < \mathcal{G}$

iv) $\forall h\in H, k\in K$ $hk = kh \wedge \forall g\in\mathcal{G}$ $\exists! h\in H, k\in K \mid hk = g$

En el caso de que se cumpla alguna podremos decir que $H \times K$ es producto directo interno en $\mathcal{G}$

-Demostración-

i) $\Rightarrow$ ii) ϕ es sobreyectiva $\Rightarrow \forall g \in \mathcal{G}, \exists h \in H, k \in K \mid \phi(h,k) = hk = g \Rightarrow \mathcal{G} \subseteq HK$, pero $HK \subseteq \mathcal{G} \Rightarrow \mathcal{G} = HK$

Sea $g \in H \cap K \Rightarrow g = \phi(g,1) = \phi(1,g) = g$, como ϕ es inyectiva $(g,1) = (1,g) \Rightarrow g = 1$

$$\begin{tikzcd} & \mathcal{G} & \\ H & H \times K \arrow[l, "p_1"] \arrow[u, "\phi"] \arrow[r, "p_2"'] & K \end{tikzcd}$$

$H \cong Ker(p_2 \phi^{-1}) = (h,1)$ $\quad$ $K \cong Ker(p_1 \phi^{-1}) = (1,k) \Rightarrow H, K \trianglelefteq \mathcal{G}$

ii) $\Rightarrow$ iii) Sólo debemos ver que $hk = kh$, para lo que definimos el conmutador de h y k $[h,k] = hkh^{-1}k^{-1}$

Vamos a ver que $[h,k] = 1$ $\forall k \in K, h \in H$; pero $hkh^{-1}k^{-1} = hk(kh)^{-1}$, es decir, debemos ver que $hk(kh)^{-1} = 1$.

$$[h,k] = \underbrace{(hkh^{-1})}_{\in K,\ K \trianglelefteq \mathcal{G}} k^{-1} = h\underbrace{(kh^{-1}k^{-1})}_{\in H,\ H \trianglelefteq \mathcal{G}} \underbrace{\in H \cap K = \{1\}}_{H,K \trianglelefteq \mathcal{G}}$$

Luego $hk = kh$

iii) $\Rightarrow$ iv) $\forall g \in \mathcal{G}$ $g = h_1k_1 \ldots h_mk_m$ pues $H \cup K = \mathcal{G}$, como h_i, k_j conmutan, podemos ver que

$g = h_1 \ldots h_m k_1 \ldots k_m \in HK$

Veamos la unicidad; si $g = h_1k_1 = h_2k_2 \Rightarrow h_2^{-1}h_1 = k_2k_1^{-1} \in H \cap K = \{1\} \Rightarrow h_1 = h_2, k_1 = k_2$.

iv) $\Rightarrow$ i) $\phi((h_1,k_1)(h_2,k_2)) = \phi(h_1h_2, k_1k_2) = h_1h_2k_1k_2 = h_1k_1h_2k_2 = \phi(h_1,k_1)\phi(h_2,k_2)$ luego ϕ es un homomorfismo y biyectiva por cómo está definido $\mathcal{G}$, de forma única pues $\forall g \in \mathcal{G}\ \exists! h_1 \in H, k_1 \in K$ tal que $g = h_1k_1$

-Ejemplo- (Ejercicio 18)

1) $\mathcal{G} = \mathbb{R}^*$, $H = \{\pm 1\}$ $\quad K = \{x \in \mathbb{R} \mid x > 0\}$ $\mathcal{G} = HK$, $\mathcal{G}$ abeliano $\Rightarrow H, K \trianglelefteq \mathcal{G}$ y $H \cap K = 1$

2) $\mathcal{G} = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in GL_2(\mathbb{R}) \right\}$ $\quad H = \left\{ \begin{pmatrix} a & 0 \\ 0 & c \end{pmatrix} \in GL_2(\mathbb{R}) \right\}$ $\quad K = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \in GL_2(\mathbb{R}) \right\}$

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & c \end{pmatrix}\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & ab \\ 0 & c \end{pmatrix} \neq \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & 0 \\ 0 & c \end{pmatrix}$$

3) $\mathcal{G} = \mathbb{C}^*$ $\quad H = \{z \in \mathbb{C} \mid |z| = 1\}$ $\quad K = \{x \in \mathbb{R} \mid x > 0\}$

$z = \frac{z}{|z|}|z|$ luego $HK = \mathcal{G}$, como $\mathbb{C}$ abeliano $\Rightarrow H, K \trianglelefteq \mathcal{G}$, y $H \cap K = \{1\}$

Lema

Sean $H_1 < H$, $K_1 < K$ entonces:

i) $H_1 \times K_1 < H \times K$

ii) Existe un monomorfismo $Aut(H) \times Aut(K) \longrightarrow Aut(H \times K)$

$$\begin{tikzcd} H \arrow[d, "f"'] & \times & K \arrow[d, "g"] & \arrow[r, "\varphi"', "\varphi(f,g)=(f,g)"] & \, & H \times K \arrow[d] \\ H & & K & & & H \times K \end{tikzcd}$$

-Demostración-

i) $H_1 \times K_1 < H \times K$ $\Rightarrow$ cerrado para el producto, unidad, inverso

ii) Sea $\varphi: Aut(H) \times Aut(K) \longrightarrow Aut(H \times K)$

$(\alpha, \beta) \longmapsto \varphi(\alpha, \beta): H \times K \longrightarrow H \times K$

$(h,k) \longmapsto (\alpha(h), \beta(k))$

Teorema

Sean H, K dos grupos finitos tales que $mcd(|H|,|K|)=1$ entonces:

i) $\forall L < H \times K$, $\exists!\, H_1 < H$, $K_1 < K$ tales que $L = H_1 \times K_1$

ii) $\varphi: Aut(H) \times Aut(K) \longrightarrow Aut(H \times K)$ isomorfismo

-Demostración-

i)

$$H \xleftarrow{p_1} H \times K \xrightarrow{p_2} K$$

Sea $L < H \times K \Rightarrow H_1 = p_1(L)$ y $K_1 = p_2(L)$, pero $L < H_1 \times K_1$. Veamos que $H_1 \times K_1 < L$, $\forall h \in H_1 \Rightarrow \exists (h,k) \in L$, si $n = |H|$, $m = |K|$ y $mcd(n,m)=1$, por el Teorema de Bezout $\exists r,s \in \mathbb{Z} \mid nr + ms = 1$. Entonces

$$L \ni (h,k)^{ms} = (h^{ms}, k^{ms}) = (h^{1-nr}, 1) = (h,1) \text{, entonces } (h,1) \in L$$

Análogamente $\forall k \in K_1$, $(1,k) \in L$, entonces $\forall (h,k) \in H_1 \times K_1$ $(h,k) = (h,1)(1,k) \in L$.

ii) ¿Dicho de palabra?

4.4 Producto directo de grupos cíclicos (ya nos "olvidamos del producto directo interno)

Denotaremos por $\oplus$ al producto directo y nos preguntamos: ¿el producto directo de 2 grupos cíclicos es un grupo cíclico? No, vamos a ver un contraejemplo:

- Supongamos que $\mathbb{Z} \oplus \mathbb{Z} = \langle (r,s) \rangle$ luego $(1,0) = n(r,s)$, es decir, $nr = 1$ y $ns = 0$ luego $s = 0$ y $n = \pm 1 = r$. Entonces $(r,s) = (-1,0)$ ó $(1,0)$, veamos ahora cómo se escribe $(0,1)$

$$(0,1) = m(1,0) \Rightarrow m = 0 \wedge 1 = 0 \;!!$$

Entonces $\mathbb{Z} \oplus \mathbb{Z}$ no es cíclico

- Supongamos que $\mathbb{Z}_2 \oplus \mathbb{Z}_2 = \langle (r,s) \rangle$, $o(r,s) = mcm(o(r), o(s)) \in \{1,2\}$, si $o(r,s) = 1 \Rightarrow r = s = 0$ y si $o(r,s) = 2 \Rightarrow r \neq 0 \vee s \neq 0$. Pero estoy diciendo que en $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ no tiene elementos de orden 4 luego no puede ser cíclico

-Ejemplo-

- $\mathbb{Z}_2 \oplus \mathbb{Z}_3 = \langle (1,1) \rangle$, en general se cumple para cuando $\mathbb{Z}_n, \mathbb{Z}_m$ n y m son coprimos

Proposición

Si G y H son grupos cíclicos finitos, $G \oplus H$ es cíclico $\Leftrightarrow$ $mcd(|G|, |H|) = 1$

-Demostración-

Sean $G = \langle x \rangle$ con $o(x) = n$ y $H = \langle y \rangle \mid o(y) = m$.

$\Leftarrow)$ Si $mcd(n,m) = 1 \Rightarrow mcm(n,m) = n \cdot m \Rightarrow o(xy) = mcm(o(x), o(y)) = nm = o(G \oplus H) \Rightarrow G \oplus H = \langle (x,y) \rangle$

$\Rightarrow)$ Si $G \oplus H$ es cíclico $\Rightarrow G \oplus H = \langle (a,b) \rangle$ con $o(a,b) = mcm\{o(a), o(b)\} = nm = |G \times H| \Rightarrow o(a) | n \wedge o(b) | m$

y por tanto $o(a) = n \wedge o(b) = m$. Entonces $mcd(m,n) = mcd(o(a), o(b)) = \frac{nm}{mcm} = 1$

↳ por el mcm

Proposición

$\bigoplus_i G_i$ es cíclico $\Leftrightarrow$ $mcd(G_i, G_j) = 1$ $\forall i \neq j$; siendo G_i cíclico $\forall i$

↳ si mcd dos a dos es 1

-Ejemplo-

- $\mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5 \cong \mathbb{Z}_{30}$ es cíclico
- $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5$ no es cíclico