P5 Sea $f : G \to G$, $x \mapsto x^{-1}$ $\quad$ f es biyección

¡Cuidado! f no necesariamente es morfismo. De hecho, f es morfismo ssi G es abeliano.

Sea $H \leq G$, $\mathcal{H}^- = \{xH : x \in G\}$, $\mathcal{H}^+ = \{Hx : x \in G\}$

Notemos que $f(xH) = \{hx^{-1}, h \in H\} = h^{-1}x^{-1}, h \in H\} = \{hx^{-1}, h \in H\} = \{hf(x) : h \in H\} = \{Hf(x)$. Veamos que $\tilde{f}_1 : \mathcal{H}^- \to \mathcal{H}^+$, $\tilde{f}_1(xH) = f(xH) = Hf(x)$ esta bien definida.

Para ello hay que mostrar que $xH = yH \Rightarrow \tilde{f}_1(xH) = \tilde{f}_1(yH)$.

Si $xH = yH \Rightarrow y^{-1}x \in H \Rightarrow x^{-1}y = (y^{-1}x)^{-1} \in H \Rightarrow x^{-1} \in Hy^{-1} \Rightarrow Hx^{-1} = Hy^{-1}$
$\Rightarrow \tilde{f}_1(xH) = \tilde{f}_2(xH)$

Un procedimiento análogo muestra que $\tilde{f}_2 \; \mathcal{H}^+ \to \mathcal{H}^-$, $\tilde{f}_2(Hx) = f(Hx) = f(x)H$ está bien definida. Es claro que $\tilde{f}_1 \circ \tilde{f}_2 = id_{\mathcal{H}^+}$, $\tilde{f}_2 \circ \tilde{f}_1 = id_{\mathcal{H}^-}$ $\therefore \tilde{f}_1$ es biyección ∎

P1 $|G| \leq 5 \Rightarrow G$ abeliano

Gracias al teorema de Lagrange, sabemos que los grupos de orden 1, 2, 3 y 5 son cíclicos y por lo tanto, abelianos. Si $|G| = 4$, tomemos $g \in G$, $H = \langle \{g\} \rangle$. Nuevamente, Lagrange nos dice que $|H| \in \{1, 2, 4\}$. $g \neq 1 \Rightarrow |H| \neq 1$.

Si $|H| = 4 \Rightarrow H = G \Rightarrow G$ cíclico $\Rightarrow G$ abeliano

Si $|H| = 2$. Sea $h \in G \setminus H$. Se compreba que $gh, hg \notin \{1, g, h\} \Rightarrow gh = hg \Rightarrow$ G abeliano

P3 (c) Sea

$$\begin{aligned} f_g : G &\to G \\ x &\mapsto f_g(x) = gx \end{aligned}$$

Es fácil porque $f_g \circ f_h = f_{gh}$, $f_1 = id\, G$ (1)

$\Rightarrow f_g \circ f_{g^{-1}} = f_{g^{-1}} \circ f_g = id\, G$ (2)

(2) muestra que f_g es biyección, $\forall g \in G$

(1) muestra que $\varphi : G \to Biy\, G$ es morfismo.

$$g \mapsto f_g$$

Es fácil ~~por~~ ver que φ es inyectiva, y como $Biy\, G \cong S_n$, concluimos.

P6 (a) Dados $n \in N_1$, $g \in G_2$, hay que probar que $gng^{-1} \in N_1$.

$gng^{-1} \in N_1 \Leftrightarrow (1, gng^{-1}) \in H$. Como P_2 es epiyectiva, existe $(x,y) \in H : P_2(x,y) = g \Rightarrow y = g$.

$\Rightarrow (1, gng^{-1}) = (x,g)(1,n)(x,g)^{-1} \in N_1$

(b) Sea $\hat{H} = \{([g],[h]) \in G_1/N_2 \times G_2/N_1 : g \in G_1, h \in G_2\}$, la imagen de H en $G_1/N_2 \times G_2/N_1$. Debemos demostrar que $\forall [g] \in G_1/N_2 \ \exists! \ [h] \in G_2/N_1 : ([g],[h]) \in G_1/N_2 \times G_2/N_1$ y que $\forall [h] \in G_2/N_1 \ \exists! \ [g] \ G_1/N_2 : ([g],[h]) \in G_1/N_2 \times G_2/N_1$.

Dada la simetría en las hipótesis bastará probar lo primero.

- Existencia: si $g \in G_1$, P_1 epi $\Rightarrow \exists (g',h) \in H : P_1(g',h) = g \Rightarrow g' = g \Rightarrow (g,h) = (g',h) \in H$
- Unicidad: Si $([g],[x]), ([g],[y]) \in G_1/N_2 \times G_2/N_1$, hay que probar que $[x] = [y]$, o, que es igual, que $xy^{-1} \in N_1$.

Como $(g,x);(g,y) \in H \Rightarrow (1, xy^{-1}) = (g,x)(g,y)^{-1} \in H \Rightarrow xy^{-1} \in N_1$

Se deja propuesto al lector comprobar que $\hat{H}$ es un morfismo.

$\boxed{P7}$ $|G| = n \mid m = \exp(G) = \min\{k \geq 1 : \forall g \in G \cdot g^k = 1\}$ ← **Nota**: $\forall G$ finito $\exists$ exponente de G (porque?)

Por inducción: Los casos base se pueden comprobar a mano gracias al $\boxed{P1}$

Si es cierto para todo $K<n$, probemos que se cumple para n.

Sea $x \in G \setminus \{1\}$, $H = \langle\{x\}\rangle$. $H \trianglelefteq G$ pues G es abeliano. Sea ℓ el exponente de G/H. La hipótesis de inducción que $n = |G| = |G/H| \cdot |H| \mid \ell^\alpha \cdot |H|$, para algún $\alpha \in \mathbb{N}$. Nos gustaría decir algo del tipo $\ell |H| \mid m^\beta$. Veamos que sí se puede hacer:

(i) $|H| \mid m$. Como $\forall g \in H: g^m = 1$ y H cíclico, $|H| \mid m$

(ii) $\ell \mid m^\beta$. Como $\forall [g] \in G/H: [g]^m = 1 \Rightarrow \ell \leq m$. Del colegio sabemos que existen $p, q \in \mathbb{N}: m = p\ell + q$, $0 \leq q < p$. Para todo $g \in G$ se tiene $1 = [g]^m = [g]^{p\ell+q} = ([g]^\ell)^p \cdot [g]^q = [g]^q$. Que $\forall g \in G: [g]^q = 1$ implica $q = 0 \vee \ell \leq q$ (lo anterior ~~es~~ por la definición de ℓ). $q < \ell \Rightarrow q = 0 \Rightarrow m = p\ell \Rightarrow \ell \mid m$

$\Rightarrow n \mid \ell^\alpha |H| \mid \ell^\alpha |H|^\alpha \mid m^\alpha m^\alpha = m^{2\alpha}$ ■