



Tarea 1

P1. (a) Sea G grupo y $H, K \trianglelefteq G$, entonces $H = K \Leftrightarrow G/H \cap G/K \neq \emptyset$.

R: Claramente para la izquierda no hay nada que demostrar. Para el otro lado, si es que $G/H \cap G/K \neq \emptyset$, entonces existen $x, y \in G$ tales que $Hx = Ky$, es decir $Hxy^{-1} = K$ y como $e \in H$, en particular $xy^{-1} \in K \Rightarrow yx^{-1} \in K$. Sigue directamente que $K = Kxy^{-1} = H$.

(b) Indicación: Para esta pregunta, puede utilizar sin demostrar los resultados de la pregunta 2 del control 1.

i. Demuestre que si $G/Z(G)$ es cíclico, entonces $|G/Z(G)| = 1$.

R: De la P2 i) del control sabemos que $Z(G) \trianglelefteq G$, luego el cociente está bien definido. Para ver que $|G/Z(G)| = 1$, basta demostrar que $G = Z(G)$, es decir que G es abeliano. En efecto, sean $x_1, x_2 \in G$, recordemos que $G/Z(G)$ es una partición y que por hipótesis es cíclico, digamos que su generados es $yZ(G)$, luego, existen $n_1, n_2 \in \mathbb{Z}$ y $z_1, z_2 \in Z(G)$ tales que $x_i = y^{n_i} z_i$, y por ende

$$x_1 x_2 = y^{n_1} z_1 y^{n_2} z_2 = y^{n_1} y^{n_2} z_1 z_2 = y^{n_1+n_2} z_2 z_1 = y^{n_2} y^{n_1} z_2 z_1 = y^{n_2} z_2 y^{n_1} z_1 = x_2 x_1.$$

Donde el segundo, tercer y penúltimo igual fueron debido a que z_i conmuta con todos (por estar en el centro), y el cuarto por propiedad conocida.

ii. Pruebe que si $|G| = p^2$, entonces es abeliano.

R: De la P2iv) del control, sabemos que si $|G| = p^r$, con $r \geq 1$ entonces G no tiene centro trivial, es decir $|Z(G)| \neq 1$. Si a esto, le agregamos el teorema de Lagrange (y el hecho de que el centro es subgrupo), entonces $|Z(G)| \in \{p, p^2\}$. Si llegase a ocurrir el primer caso entonces $|G/Z(G)| = p$, y como todo grupo de orden primo es cíclico, podemos utilizar la parte anterior para llegar a una contradicción. Luego, la única posibilidad es que $|Z(G)| = p^2$ y por lo tanto $G = Z(G)$, es decir G es abeliano.

(c) Sea $\mu_n = \{z \in \mathbb{C} : z^n = 1\}$, el grupo de las raíces n -ésimas de la unidad. Demuestre que μ_n es un grupo cíclico de $(\mathbb{C}^*, \cdot)$, y que $\mathbb{C}^*/\mu_n \cong \mathbb{C}^*$.

R: Sabemos que

$$\mu_n = \{e^{\frac{i2k\pi}{n}}, k \in 0, \dots, n-1\}$$

Luego, $\forall z \in \mu_n, \exists \bar{k} \in \mathbb{Z}$ tal que

$$z = e^{\frac{i2\bar{k}\pi}{n}} = (e^{\frac{i2\pi}{n}})^{\bar{k}} \Rightarrow \mu_n = \{e^{\frac{i2\pi}{n}}\} \Rightarrow \mu_n$$

es subgrupo cíclico (Claramente $\emptyset \neq \mu_n \subseteq \mathbb{C}^*$).

Como $(\mathbb{C}^*, \cdot)$ es abeliano, todo subgrupo es normal y por ende el cociente $\mathbb{C}^*/\mu_n$ está bien definido. Para ver que $\mathbb{C}^*/\mu_n \cong \mathbb{C}^*$ consideremos $f : \mathbb{C}^*/\mu_n \rightarrow \mathbb{C}^*$ tal que $f(z\mu_n) = z^n$ y veamos que es isomorfismo.

i. **Está bien definida y es inyectiva:**

$$z_1 \mu_n = z_2 \mu_n \Leftrightarrow z_1 \cdot z_2^{-1} \in \mu_n \Leftrightarrow (z_1 \cdot z_2^{-1})^n = 1 \Leftrightarrow z_1^n \cdot (z_2^{-1})^n = 1 \Leftrightarrow z_1^n = z_2^n.$$

ii. **Es sobreyectiva:** Sea $w \in \mathbb{C}^* \Rightarrow \exists z \in \mathbb{C}^* : z^n = w$, y por lo tanto

$$f(z\mu_n) = z^n = w.$$

iii. **Es morfismo:**

$$f(z_1\mu_n \cdot z_2\mu_n) = f(z_1z_2\mu_n) = (z_1z_2)^n = z_1^n z_2^n = f(z_1\mu_n) \cdot f(z_2\mu_n).$$

Como existe un morfismo biyectivo entre las dos estructuras, estas son isomorfas.

- (d) Demuestre que para G grupo y $N \trianglelefteq G$, se cumple que: G/N es simple, si y solo si, N es un subgrupo normal propio maximal de G .

R: Ambas implicancias son resultados directos del teorema de correspondencia. En efecto, para la implicancia de izquierda a derecha razonamos por contradicción, si N no es un subgrupo normal propio maximal, entonces existe $N_2 \trianglelefteq G$, con $N_2 \neq G$ tal que $N \leq N_2$, luego si consideramos $\pi : G \rightarrow G/N$, con $\pi(g) = Ng$, se cumple que $N_2 \trianglelefteq G \Leftrightarrow \pi(N_2) \trianglelefteq \pi(G) = G/N$ y por lo tanto G/N no es simple. Para la otra implicancia, sea $Q \trianglelefteq G/N$, como el teorema garantiza que π (visto como la imagen) es sobreyectiva, se tiene que $\exists H$, tal que $N \leq H \leq G$, y $\pi(H) = Q \trianglelefteq G/N = \pi(G)$, luego $H \trianglelefteq G$, es decir N no es un subgrupo normal propio maximal.

P2. Sea $(G, \cdot)$ un grupo:

- a) (1 pt.) Probar que el grupo de automorfismos interiores:

$$\text{Inn}(G) := \{\phi_g : G \rightarrow G, \text{ donde } \phi_g(h) = ghg^{-1}\}$$

Es un subgrupo normal del grupo de automorfismos con la composición $(\text{Aut}(G), \circ)$.

R: Para ver que los automorfismos internos son un subgrupo, como $\phi_e = \text{Id}_G$, basta ver que son cerrados bajo la composición, en efecto:

$$\phi_g \circ \phi_h(t) = g(hth^{-1})g^{-1} = (gh)t(gh)^{-1} = \phi_{gh}(t)$$

Para ver la normalidad, sea $\sigma \in \text{Aut}(G)$, luego:

$$\begin{aligned} \sigma \circ \phi_h \circ \sigma^{-1}(t) &= \sigma(g\sigma^{-1}(t)g^{-1}) \\ &= \sigma(g)\sigma(\sigma^{-1}(t))\sigma(g^{-1}) = \sigma(g)t\sigma(g)^{-1} = \phi_{\sigma(g)}(t) \end{aligned}$$

- b) (1 pt.) Sea G abeliano, ver que $\text{Inn}(G) = \{\text{Id}_G\}$.

R: Sea $\phi_g \in \text{Inn}(G)$, para algun $g \in G$, luego veamos que:

$$\phi_g(t) = gtg^{-1} = gg^{-1}t = t = \text{Id}_G(t)$$

- c) (2pt.) Si $G = \mathbb{Z}$, ¿A que grupo es isomorfo $\text{Aut}(\mathbb{Z})$?

Concluir que $\mathbb{Z}$ tiene algún automorfismo no interior.

R: Sabemos que si $\phi \in \text{Aut}(G)$ es un automorfismo, entonces $\phi(1)$ define únicamente al morfismo, esto es pues para todo $m \in \mathbb{Z}_+$, tenemos que:

$$\phi(m) = \phi(1 + 1 + \dots + 1) = m\phi(1)$$

Además, si m es negativo, tenemos que:

$$\phi(m) = -|m|\phi(1)$$

Luego, notemos que $\text{Im}(\phi) = \mathbb{Z}$, puesto que es sobreyectivo por ser automorfismo, además de lo anterior tenemos que:

$$\text{Im}(\phi) = \phi(1)\mathbb{Z}$$

Para tener ambas cosas al mismo tiempo, necesariamente $|\phi(1)| = 1$, luego $\phi(1) \in \{-1, +1\}$

d) (2 pt.) Si ahora G es un grupo cíclico finito, probar que:

$$\text{Out}(G) := \text{Aut}(G)/\text{Inn}(G) = \{T_g : g \in G \text{ tales que } \exists k \in G : kg = gh = 1\}$$

Donde T_g es la función dada por la multiplicación por g , esto es: $T_g(h) = gh$.

R: Sabemos que si G es cíclico finito, entonces:

$$G \simeq \mathbb{Z}/m\mathbb{Z}, \text{ para algún } m \in \mathbb{Z}$$

Análogamente al caso anterior, tenemos que si $\phi \in \text{Aut}(G)$, este queda determinado únicamente por $\phi(1 + m\mathbb{Z})$, luego de la sobreyectividad, tenemos que:

$$\text{Im}(\phi) = \phi(1 + m\mathbb{Z})\mathbb{Z}/m\mathbb{Z} = \mathbb{Z}/m\mathbb{Z}$$

Así, como $1 + m\mathbb{Z} \in \mathbb{Z}/m\mathbb{Z}$, luego existe $k + m\mathbb{Z} \in \mathbb{Z}/m\mathbb{Z}$ tal que:

$$\phi(1 + m\mathbb{Z})(k + m\mathbb{Z}) = (1 + m\mathbb{Z})$$

Denotemos $\phi(1 + m\mathbb{Z}) = \varphi(1) + m\mathbb{Z}$, con $\varphi(1) \in \{0, \dots, m-1\}$, luego la ecuación anterior se lee como:

$$\varphi(1)k + m\mathbb{Z} = 1 + m\mathbb{Z}$$

$$\implies \exists n \in \mathbb{Z}, \text{ tal que: } \varphi(1)k - 1 = mn \implies \varphi(1)k - mn = 1$$

Luego el máximo común divisor entre $\varphi(1)$ y m es 1, por el lema de Bezout.

Finalmente, recordemos que en los grupos cíclicos finitos de la forma $\mathbb{Z}/m\mathbb{Z}$, los elementos invertibles son justamente aquellos $k + m\mathbb{Z}$, donde k es coprimo con m .

En lo anterior probamos que si ϕ es un automorfismo de $\mathbb{Z}/m\mathbb{Z}$, entonces $\phi(1 + m\mathbb{Z})$ es tal que el representante $\varphi(1)$ de $\phi(1 + m\mathbb{Z})$ en $\{0, \dots, m-1\}$ es coprimo a m , luego $\varphi(1) + m\mathbb{Z}$ es invertible en $\mathbb{Z}/m\mathbb{Z}$.

P3. [Subgrupos de Sylow, automorfismos y grupos simétricos]

(a) Sea G un grupo, $p \in \mathbb{N}$ primo y $\text{Syl}_p(G)$, el conjunto de p -subgrupos de Sylow de G .

i. Muestre que todo automorfismo $\varphi \in \text{Aut}(G)$ induce una permutación $\sigma_\varphi \in S_{\text{Syl}_p(G)}$, donde $\sigma_\varphi(S) = \varphi(S)$, para $S \in \text{Syl}_p(G)$.

R: Para todo subgrupo $H < G$, φ induce un isomorfismo $\varphi|_H : H \rightarrow \varphi(H)$. En particular, si S es p -Sylow, entonces $\varphi(S)$ es p -Sylow (los órdenes de grupos isomorfos coinciden). Luego $\sigma_\varphi(S) \in \text{Syl}_p(G)$.

Por otro lado, es claro que $\sigma_\varphi \in S_{\text{Syl}_p(G)}$, puesto que $\sigma_{\varphi^{-1}}$ es su inversa ($\sigma_\varphi \circ \sigma_{\varphi^{-1}}(S) = \varphi(\varphi^{-1}(S)) = S$).

ii. Muestre que para todo $S, S' \in \text{Syl}_p(G)$, existe $\varphi \in \text{Aut}(G)$ tal que $\sigma_\varphi(S) = S'$.

R: Por el segundo teorema de Sylow, S y S' son conjugados, de modo que basta tomar el automorfismo interior correspondiente I_a tal que $S' = aSa^{-1} = I_a(S)$.

iii. Muestre que la función $\Sigma : \text{Aut}(G) \rightarrow S_{\text{Syl}_p(G)}$, donde $\Sigma(\varphi) = \sigma_\varphi$, para $\varphi \in \text{Aut}(G)$, es un morfismo de grupos.

R: $(\Sigma(\phi) \circ \Sigma(\varphi))(S) = \phi(\varphi(S)) = (\phi \circ \varphi)(S) = \Sigma(\phi \circ \varphi)(S)$.

- (b) Recuerde que la función $\mathcal{I} : G \rightarrow \text{Aut}(G)$, $g \mapsto I_g$, es un morfismo, donde $I_g : G \rightarrow G$ es el automorfismo interior $I_g(x) = gxg^{-1}$. Se tiene que $\text{Int}(G) = \text{Im}(\mathcal{I})$ es el grupo de automorfismos interiores y

$$\mathcal{Z}(G) = \{g \in G : \forall x \in G, gx = xg\} = \ker(\mathcal{I}) \triangleleft G$$

es el centro de G .

- i. Muestre que el centro de S_2 es todo S_2 , es decir $\mathcal{Z}(S_2) = S_2$.

R: $S_2 \cong C_2$ es Abelian, por lo tanto $\mathcal{Z}(S_2) = S_2$.

- ii. Muestre que para todo $n \geq 3$, el centro de S_n es trivial, es decir $\mathcal{Z}(S_n) = \{id\}$.

R: Sea $\sigma \in S_n \setminus \{id\}$. Luego, existen $i, j \in \{1, \dots, n\}$ tal que $\sigma(i) = j \neq i$. Sea $k \in \{1, \dots, n\} \setminus \{i, j\}$ ($\neq \emptyset$, puesto que $n \geq 3$).

Sea $\tau = (jk) \in S_n$. Se tiene que $\sigma \circ \tau(i) = \sigma(i) = j$ y $\tau \circ \sigma(i) = \tau(j) = k \neq j$. De modo que $\sigma \circ \tau \neq \tau \circ \sigma$ y por lo tanto $\sigma \notin \mathcal{Z}(S_n)$.

- (c) Para todo lo que sigue, sea $p = 2$ ó 3 y $n = p + 1$.

- i. Describa explícitamente todos los p -subgrupos de Sylow de S_n , es decir, calcule $\text{Syl}_2(S_3)$ y $\text{Syl}_3(S_4)$.

R: Los p -subgrupos de Sylow de S_{p+1} son de orden p (ya que $p^2 \nmid (p+1)!$). En particular, son cíclicos.

Por otro lado, todo p -ciclo en S_{p+1} genera un grupo cíclico de orden p , de modo que hay más de un p -subgrupo de Sylow.

Recordemos que si $\sigma \in S_n$ se escribe como composición de ciclos disjuntos $\sigma = c_1 \circ \dots \circ c_k$, entonces $\text{Ord}(\sigma) = \text{mcm}(\text{Ord}(c_i))$. Luego, todo elemento de orden p debe escribirse como composición de p -ciclos disjuntos. Como $2p > p + 1$, sigue que todo elemento de orden p en S_{p+1} es necesariamente un p -ciclo.

Así,

$$\text{Syl}_p(S_{p+1}) = \{\langle c \rangle : c \in S_{p+1} \text{ es un } p\text{-ciclo}\}.$$

En el caso particular de $p = 2, 3$, se tiene que

$$\text{Syl}_2(S_3) = \{\langle (12) \rangle, \langle (23) \rangle, \langle (31) \rangle\},$$

$$\text{Syl}_3(S_4) = \{\langle (123) \rangle, \langle (234) \rangle, \langle (341) \rangle, \langle (412) \rangle\}.$$

- ii. Muestre que en estos casos el morfismo $\Sigma : \text{Aut}(S_n) \rightarrow S_{\text{Syl}_p(S_n)}$ en (a.iii) es un isomorfismo.

R: En (b.ii) vimos que $\mathcal{Z}(S_{p+1}) = \{id\}$. En particular $\mathcal{I}$ es inyectiva y por lo tanto, $|\text{Aut}(S_{p+1})| \geq |S_{p+1}| = (p+1)!$. Por otro lado, en (i) vimos que $\#\text{Syl}_p(S_{p+1}) = p+1$, por lo que $|\text{Syl}_p(S_{p+1})| = (p+1)!$.

De modo que, basta mostrar que Σ es inyectiva (en tal caso se tendría que ambos grupos tienen el mismo orden y por lo tanto, todo monomorfismo es un isomorfismo).

Supongamos entonces que $\Sigma(\varphi) = id$, es decir, $\varphi(S) = S$ para cada $S \in \text{Syl}_p(S_{p+1})$.

Caso $p = 2$: De (i) sabemos que si $S \in \text{Syl}_2(S_3)$, entonces S es un grupo cíclico generado por una transposición. Luego, si $\varphi(S) = S$, entonces φ fija la transposición (el único otro elemento en S es la identidad que necesariamente es fija por φ). Luego, si $\varphi \in \ker(\Sigma)$, entonces φ fija todas las transposiciones. Pero, como las transposiciones generan S_3 , se tiene que φ fija cada elemento de S_3 , es decir, $\varphi = id$. Sigue que $\ker(\Sigma) = \{id\}$.

Caso $p = 3$: De (i) sabemos que si $S \in \text{Syl}_3(S_4)$, entonces S es un grupo cíclico generado por un 3-ciclo. Luego, si $\varphi(S) = S$, entonces φ o bien fija el 3-ciclo, o bien lo envía a su inverso (el único otro elemento en S es la identidad que necesariamente es fija por φ).

Sea (ijk) un 3-ciclo en S_4 . Entonces $\varphi((ijk)) = (ijk)$ o (kji) . Si $\varphi((ijk)) = (ijk)$, como $(ijk) = (ij)(jk)$, entonces

$$(ij)(jk) = (ijk) = \varphi((ijk)) = \varphi((ij))\varphi((jk)).$$

Si $\varphi((ijk)) = (kji)$, entonces

$$(kj)(ji) = (kji) = \varphi((ijk)) = \varphi((ij))\varphi((jk)).$$

Notemos que en general, en S_n , todo automorfismo preserva la paridad de los elementos y en S_4 se tiene que los únicos elementos impares son las transposiciones (justificar) y, por lo tanto, todo elemento par puede escribirse como producto de dos transposiciones.

Sigue entonces que φ induce una permutación en las transposiciones de S_4 .

Como $\varphi((ij))\varphi((jk)) = \varphi((ijk)) = (ijk)$ o (kji) , entonces $\varphi((ij)) \in \{(ij), (jk), (ki)\}$. Por otro lado, si $l \in \{1, 2, 3, 4\} \setminus \{i, j, k\}$, entonces $(ij)(kl) = \varphi((ij))\varphi((kl))$ (justificar) son disjuntas, de modo que $\varphi((ij)) \in \{(ij), (kl)\}$.

Se concluye que $\varphi((ij)) = (ij)$, es decir, φ fija las transposiciones y, por lo tanto, $\varphi = id$. Sigue que $\ker(\Sigma) = \{id\}$.

Así, para $p = 2, 3$, $\Sigma : \text{Aut}(S_{p+1}) \rightarrow S_{\text{Syl}_p(S_{p+1})}$ es un monomorfismo y como $|\text{Aut}(S_{p+1})| \geq |S_{\text{Syl}_p(S_{p+1})}|$ son finitos, se concluye que Σ es un isomorfismo.

iii. Concluya que $\text{Aut}(S_n) = \text{Int}(S_n) \cong S_n$.

R: De (ii) se tiene que $|\text{Aut}(S_{p+1})| = |S_{\text{Syl}_p(S_{p+1})}|$ y en (i) vimos que $\#\text{Syl}_p(S_{p+1}) = p + 1$. Luego, $|\text{Aut}(S_{p+1})| = (p + 1)!$.

De (b.ii) sabemos que $\mathcal{I} : S_{p+1} \rightarrow \text{Aut}(S_{p+1})$ es inyectiva, de modo que $S_{p+1} \cong \text{Im}(\mathcal{I}) = \text{Int}(S_{p+1})$.

Pero $|\text{Aut}(S_{p+1})| = (p + 1)! = |S_{p+1}|$, de modo que $\mathcal{I}$ es de hecho un isomorfismo y, en particular, sobreyectiva. Sigue que $\text{Int}(S_{p+1}) = \text{Im}(\mathcal{I}) = \text{Aut}(S_{p+1})$.