

## AYUDANTÍA 4 ESTRUCTURAS ALGEBRAICAS

4 DE ABRIL DE 2023

**Problema 1.** Sea  $G$  grupo finito,  $S \subseteq G$  un  $p$ -subgrupo de Sylow y  $H \leq G$  subgrupo arbitrario. Demuestre que existe  $g \in G$  tal que  $gSg^{-1} \cap H$  es un  $p$ -subgrupo de Sylow.

*Demostración.* Podemos definir la acción  $H \curvearrowright X$  donde  $X := G/S$  mediante  $h \cdot (gS) = (hg)S$ . Los estabilizadores vienen dados por

$$H_{gS} = \{h \in H | (hg)S = gS\} = \{h \in H | g^{-1}hg \in S\} = gSg^{-1} \cap H$$

Además, escribiendo  $|G| = p^\alpha m$ , del teorema de Lagrange tenemos que  $|X| = |G|/|S| = m$ . La fórmula de clases nos dice que

$$|G/S| = \sum_{gS \in R} [H : H_{gS}]$$

y dado que  $p$  no divide a  $|X|$  (pues  $\alpha$  es maximal) entonces existe  $gS \in X$  tal que  $p$  no divide a  $[H : H_{gS}]$ . Ahora, por otro lado tenemos que  $H_{gS} = gSg^{-1} \cap H \leq gSg^{-1}$  el cual es un  $p$ -grupo y en consecuencia el estabilizador  $H_{gS}$  también lo es. Como  $[H : H_{gS}] = |H|/|H_{gS}|$  no es divisible por  $p$  necesariamente  $H_{gS}$  debe ser de orden  $p$ -maximal.  $\square$

**Problema 2.**

1. Suponga que  $G$  es un grupo simple y que  $p$  es un divisor primo de  $|G|$ . Demuestre que  $|G|$  divide a  $n_p!$  donde  $n_p$  denota la cantidad de  $p$ -subgrupos de Sylow de  $G$ .
2. Si  $G$  es un grupo de orden  $|G| = 48$  pruebe que  $G$  no es simple.
3. Demuestre que no existen grupos simples de orden 1000000.

*Demostración.*

1. Sea  $G$  un grupo finito tal que  $p$  divide a  $|G|$  con  $p$  primo. Podemos entonces definir el conjunto  $X = \{S \leq G | S \text{ es un } p\text{-subgrupo de Sylow de } G\}$  y considerar la acción de grupo  $G \curvearrowright X$  por conjugación  $g \cdot S := gSg^{-1}$ , la cual gracias al teorema de Sylow sabemos está bien definida puesto todos los  $p$ -subgrupos de Sylow son conjugados entre sí. Más aún, este hecho implica que la acción definida es transitiva (posee una única órbita) y por lo tanto el morfismo de grupos asociado  $\Phi : G \rightarrow \text{Bij}(X)$  es no trivial, es decir,  $\ker(\Phi) \neq G$ . Ahora, si suponemos que  $G$  es un grupo simple, esto es, no posee subgrupos normales no triviales, dado que el kernel de un morfismo de grupos es siempre normal, necesariamente se deberá tener que  $\ker(\Phi) = \{e\}$ . En otras palabras, tenemos un morfismo inyectivo  $\Phi : G \hookrightarrow \text{Bij}(X)$  por lo que  $G$  se identifica con un subgrupo de  $\text{Bij}(X)$  y del teorema de Lagrange se sigue la conclusión pues  $|\text{Bij}(X)| = n_p!$ .
2. Considere la descomposición prima  $|G| = 48 = 2^4 \cdot 3$ . El teorema de Sylow entonces afirma la existencia de 2-subgrupos de Sylow de  $G$ , y además nos dice que  $n_2 | 3$ , por lo que  $n_2 = 1$  o bien  $n_2 = 3$ . Por contradicción, si suponemos que  $G$  es un grupo simple, dado que un  $p$ -subgrupo de Sylow es normal si y sólo si es único, entonces únicamente es posible que  $n_2 = 3$ , de modo que  $G$  se mantenga libre de subgrupos normales. Sin embargo, el punto anterior implicaría que  $|G| = 48$  es divisor de  $n_2! = 6$ , lo cual es una clara contradicción.
3. Suponer por contradicción que existe  $G$  simple de orden  $|G| = 1000000$ . Tenemos la descomposición prima  $|G| = 2^6 5^6$  y el teorema de Sylow implica que se cumplen las condiciones siguientes:

$$n_5 \equiv 1 \pmod{5} \quad \text{y} \quad n_5 | 2^6$$

donde  $n_5$  denota el número de  $p$ -subgrupos de Sylow. Por verificación directa se puede ver que los únicos números que cumplen ambas condiciones son 1, 16, pues como  $n_5 | 2^6$  solo se puede tener  $n_5 \in \{1, 2, 4, 8, 16, 32, 64\}$  y la primera condición descarta el resto de valores. Dado que  $G$  es simple necesariamente se debe tener  $n_5 = 16$  pues de lo contrario habría un único 5-Sylow y sería normal. Además, sabemos que entonces  $|G|$  divide a  $n_p!$  lo cual supone una contradicción (16! no posee suficientes factores de 5).

□

**Problema 3.** Sea  $G$  un grupo finito de orden  $|G| = 231$ . Demuestre que  $|Z(G)| \geq 11$ .

*Demostración.* Podemos hacer la descomposición  $|G| = 3 \cdot 7 \cdot 11$ . Si  $n_{11}$  denota el número de 11-Sylow de  $G$  entonces el teorema de Sylow afirma que  $n_{11} \equiv 1 \pmod{11}$  y además  $n_{11} | 3 \cdot 7 = 21$  y directamente se puede notar que la única posibilidad es  $n_{11} = 1$ . Así,  $G$  posee un único 11-Sylow  $H$  el cual es normal. Probaremos que  $H \subseteq Z(G)$ . Por contradicción suponer que existe  $h \in H \setminus Z(G)$ , es decir, existe  $g \in G$  tal que  $gh \neq hg$ . Multiplicando tenemos  $h \neq ghg^{-1}$ , y  $H$  es normal así que  $ghg^{-1} \in H$ . Por otro lado,  $|H| = 11$  por lo tanto es cíclico (ver Ayudantía 2) y, más aún, cualquier elemento distinto de la identidad es un generador, en particular  $H = \langle h \rangle$ . Así, existe  $n \in \{2, \dots, 10\}$  tal que  $ghg^{-1} = h^n$ . Similarmente tenemos  $gh^m g^{-1} = h^{mn}$  y conjugando repetidas veces  $g^k h g^{-k} = h^{n^k}$  para  $k \in \mathbb{N}$ . Tomando  $k = |g|$  como el orden de  $g \in G$  tenemos

$$h^{n^{|g|}} = g^{|g|} h g^{-|g|} = h$$

y como  $h$  es un elemento de orden 11 (pues  $|H| = 11$ ) entonces  $n^{|g|} \equiv 1 \pmod{11}$ . Viendo  $n$  como un elemento del grupo  $(\mathbb{Z}/11\mathbb{Z})^\times$ , lo anterior implica que su orden en  $(\mathbb{Z}/11\mathbb{Z})^\times$  divide a  $|g|$ , y como este último es de orden 10 (ver Ayudantía 2) tenemos por teorema de Lagrange que  $n$  es de orden 2, 5 o bien 10. De esta manera llegamos a una contradicción pues ninguno de estos números puede dividir al orden de un elemento de  $G$ . □

**Problema 4.** Determinar todos los grupos abelianos de orden 360.

*Demostración.* Notar que  $360 = 2^3 \cdot 3^2 \cdot 5$ . Dado que estamos buscando grupos abelianos finitos, por el teorema de estructura de grupos abelianos finitamente generados, se tendrá que

$$G \cong \prod_{i=1}^s \mathbb{Z}/d_i \mathbb{Z}$$

donde los enteros  $d_1, \dots, d_s$  son tales que  $1 < d_1 | \dots | d_s$ . Por ende, los grupos abelianos de orden 360 son aquellos que vienen determinados por las secuencias  $1 < d_1 | \dots | d_s$  de tal forma que  $d_1 \cdot \dots \cdot d_s = 360$ . Entonces tenemos los siguientes casos

- $s = 1$ :  $d_1 = 360$ .
- $s = 2$ : Tenemos las posibilidades  $d_1 = 2, d_2 = 180$ ;  $d_1 = 3, d_2 = 120$ ;  $d_1 = 6, d_2 = 60$ .
- $s = 3$ : Son posibles  $d_1 = 2, d_2 = 2, d_3 = 90$  y  $d_1 = 2, d_2 = 6, d_3 = 30$ .

Notar que los anteriores son los únicos casos posibles, pues en otro caso no se cumple la condición de divisibilidad. De esta forma existen solo 6 grupos abelianos de orden 360, los cuales corresponde, salvo isomorfismo, a

$$\begin{aligned} & \mathbb{Z}/360\mathbb{Z} \\ & \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/180\mathbb{Z} \\ & \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/120\mathbb{Z} \\ & \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/60\mathbb{Z} \\ & \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/90\mathbb{Z} \\ & \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/30\mathbb{Z} \end{aligned}$$

□

El teorema que se presenta a continuación es una generalización del Pequeño Teorema de Fermat el cual es válido en  $\mathbb{Z}/n\mathbb{Z}$  incluso cuando  $n$  no es primo. Su demostración es análoga a la del Pequeño Teorema de Fermat (Ayudantía 2) y por lo tanto queda como ejercicio.

**Teorema 1** (Teorema de Euler). *Sea  $n \in \mathbb{N} \geq 1$  entero positivo. Definimos la función  $\varphi$  de Euler como  $\varphi(n) = |\{m \in \mathbb{N} | m \leq n, \text{mcd}(m, n) = 1\}|$ . Si  $a, n \in \mathbb{Z}$  son enteros primos relativos con  $n \geq 1$ , entonces*

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

**Problema 5.** Utilice el Teorema chino del resto y el Teorema de Euler para calcular los dos últimos dígitos de  $17^{17^{17}}$ .

*Solución.* Calcular los últimos dos dígitos equivale a calcular módulo 100, es decir, buscamos calcular  $17^{17^{17}} \pmod{100}$ . Dado que  $100 = 2^2 \cdot 5^2$ , el Teorema chino del resto nos da la existencia de un isomorfismo  $\mathbb{Z}/100\mathbb{Z} \cong (\mathbb{Z}/4\mathbb{Z}) \times (\mathbb{Z}/25\mathbb{Z})$ , así que calcularemos  $17^{17^{17}}$  módulo 4 y 25, y finalmente uniremos estos resultados mediante el isomorfismo.

En primer lugar, notamos que  $17 \equiv 1 \pmod{4}$ , así que  $17^{17^{17}} \equiv 1 \pmod{4}$ . Calculamos ahora  $17^{17^{17}} \pmod{25}$ . Notemos ahora que  $\varphi(25) = 20$ , así que por el Teorema de Euler tenemos que  $17^{20} = 17^{\varphi(25)} \equiv 1 \pmod{25}$ . Calculemos entonces  $17^{17^{17}} \pmod{20}$ . Para ello notamos

$$17^{17} \equiv 17 \cdot 289^8 \equiv 17 \cdot 9^8 \equiv 17 \cdot 81^4 \equiv 17 \pmod{20}$$

Por lo tanto, tenemos que  $17^{17} = 20k + 17$  para cierto  $k \in \mathbb{Z}$ , así que

$$\begin{aligned} 17^{17^{17}} &\equiv 17^{20k+17} \equiv (17^k)^{20} \cdot 17^{17} \\ &\equiv 17^{17} \equiv 17 \cdot 289^8 \\ &\equiv 17 \cdot 14^8 \equiv 17 \cdot (196)^4 \\ &\equiv 17 \cdot 21^4 \equiv 17 \cdot 441^2 \\ &\equiv 17 \cdot 16^2 \equiv 17 \cdot 256 \\ &\equiv 17 \cdot 6 \equiv 2 \pmod{25} \end{aligned}$$

Así, tenemos un elemento  $(1, 2) \in ((\mathbb{Z}/4\mathbb{Z}) \times (\mathbb{Z}/25\mathbb{Z}))$  y vemos que en este anillo  $(1, 2) = (77, 77)$  y por lo tanto el Teorema chino del resto nos da que  $17^{17^{17}} \equiv 77 \pmod{100}$  □

**Problema 6.** Sea  $G$  un grupo y considere el grupo de raíces complejas de la unidad, denotado por  $\mathbb{T}^1$ . Se define el **grupo dual** de  $G$ , denotado  $\widehat{G}$ , como

$$\widehat{G} := \{\chi : G \rightarrow \mathbb{T}^1 \mid \chi \text{ morfismo de grupos}\}$$

Como su nombre lo indica, este conjunto es un grupo abeliano, cuya ley de composición corresponde al producto puntual de funciones, es decir,

$$(\chi\psi)(g) = \chi(g)\psi(g) \quad \forall g \in G$$

Demuestre que si  $G$  es un grupo abeliano finito, entonces  $\widehat{\widehat{G}} \cong G$ .

*Demostración.* Si  $G$  es un grupo abeliano finito, el Teorema de estructura de grupos abelianos finitamente generados nos dice que existen  $d_1, \dots, d_s \in \mathbb{N}^{>1}$  tales que

$$G \cong \prod_{i=1}^s \mathbb{Z}/d_i\mathbb{Z}$$

<sup>1</sup>Geoméricamente, este grupo corresponde a la esfera unitaria de  $\mathbb{C}$

Dado que cada factor anterior es cíclico, podemos elegir generadores  $x_1 \in \mathbb{Z}/d_1\mathbb{Z}, \dots, x_s \in \mathbb{Z}/d_s\mathbb{Z}$  y por lo tanto  $G \cong \langle x_1 \rangle \times \dots \times \langle x_s \rangle$ . Para cada  $i \in \{1, \dots, s\}$  podemos definir el morfismo de grupos

$$\chi_i : G \rightarrow \mathbb{T}, \quad (x_1^{m_1}, \dots, x_i^{m_i}, \dots, x_s^{m_s}) \mapsto e^{2\pi i m_i / d_i}$$

Notemos que

$$\chi_i^{d_i}(g) = (\chi_i(g))^{d_i} = \chi_i(g^{d_i}) = e^{2\pi i m} = 1 \quad \forall g \in G$$

donde  $(g_1, \dots, g_s)$  con  $g_i = x_i^m$  para cierto  $m \in \mathbb{N}$ . Tenemos entonces que el orden  $|\chi_i|$  divide a  $d_i$ , y por otro lado, notando que

$$\chi_i(g^{|\chi_i|}) = (\chi_i(g))^{|\chi_i|} = 1 \quad \forall g \in G$$

entonces tomando  $g = (1, \dots, x_i, \dots, 1)$  tenemos que  $|\chi_i| = d_i$  divide a  $|\chi_i|$ , así que  $|\chi_i| = d_i$  y por lo tanto  $|\langle x_1 \rangle \times \dots \times \langle x_s \rangle| = |\langle \chi_1 \rangle \times \dots \times \langle \chi_s \rangle|$ . Definamos

$$\begin{aligned} \varphi : \langle x_1 \rangle \times \dots \times \langle x_s \rangle &\rightarrow \langle \chi_1 \rangle \times \dots \times \langle \chi_s \rangle \\ (x_1^{m_1}, \dots, x_s^{m_s}) &\mapsto (\chi_1^{m_1}, \dots, \chi_s^{m_s}) \end{aligned}$$

que es un morfismo de grupos pues

$$\varphi((x_1^{m_1}, \dots, x_s^{m_s})(x_1^{k_1}, \dots, x_s^{k_s})) = (\chi_1^{m_1+k_1}, \dots, \chi_s^{m_s+k_s}) = (\chi_1^{m_1}, \dots, \chi_s^{m_s})(\chi_1^{k_1}, \dots, \chi_s^{k_s}) = \varphi((x_1^{m_1}, \dots, x_s^{m_s}))\varphi((x_1^{k_1}, \dots, x_s^{k_s}))$$

Ahora,

$$\ker(\varphi) = \{(x_1^{m_1}, \dots, x_s^{m_s}) : \chi_i^{m_i} = 1 \quad \forall i\} = \{(x_1^{m_1}, \dots, x_s^{m_s}) : d_i | m_i \quad \forall i\} = \{1\}$$

pues  $x_i$  y  $\chi_i$  son del mismo orden. Así, tenemos un morfismo de grupos inyectivo entre dos grupos del mismo orden y por tanto es un isomorfismo. Para concluir basta con probar entonces que  $\widehat{G} = \langle \chi_1 \rangle \times \dots \times \langle \chi_s \rangle$ . Para realizar esto probaremos el siguiente lema más general:

**Lema 2.** Sean  $G, G_1, \dots, G_n$  grupos abelianos y denote por  $\text{Hom}(G, H)$  el conjunto de morfismos de grupo  $G \rightarrow H$ . Demuestre que

$$\text{Hom}\left(\prod_{i=1}^n G_i, G\right) \cong \prod_{i=1}^n \text{Hom}(G_i, G)$$

*Demostración.* Para cada coordenada  $i = 1, \dots, n$  podemos definir el morfismo de grupos

$$\mu_i : G_i \rightarrow G_1 \times \dots \times G_n, \quad x_i \mapsto (1, \dots, x_i, \dots, 1)$$

y la aplicación

$$\varphi : \text{Hom}\left(\prod_{i=1}^n G_i, G\right) \rightarrow \prod_{i=1}^n \text{Hom}(G_i, G), \quad f \mapsto (f \circ \mu_1, \dots, f \circ \mu_n)$$

para cada  $f \in \text{Hom}(G_1 \times \dots \times G_n, G)$ . Demostramos primero que  $\varphi$  es morfismo de grupos. Sean  $f, g \in \text{Hom}(G_1 \times \dots \times G_n, G), x_i \in G_i$ . Tenemos

$$(f \circ \mu_i + g \circ \mu_i)(x_i) = f(\mu_i(x_i)) + g(\mu_i(x_i)) = (f + g)(\mu_i(x_i))$$

y luego

$$\begin{aligned} \varphi(f + g) &= ((f + g) \circ \mu_1, \dots, (f + g) \circ \mu_n) = (f \circ \mu_1 + g \circ \mu_1, \dots, f \circ \mu_n + g \circ \mu_n) \\ &= (f \circ \mu_1, \dots, f \circ \mu_n) + (g \circ \mu_1, \dots, g \circ \mu_n) \\ &= \varphi(f) + \varphi(g) \end{aligned}$$

Probemos ahora que  $\varphi$  es inyectivo. Suponer  $\varphi(f) = \varphi(g)$  con  $f, g \in \text{Hom}(G_1 \times \dots \times G_n, G)$ . Por definición  $f \circ \mu_i = g \circ \mu_i$  para todo  $i = 1, \dots, n$ . Luego

$$\begin{aligned} f(x_1, \dots, x_n) &= f(\mu_1(x_1) + \dots + \mu_n(x_n)) = f(\mu_1(x_1)) + \dots + f(\mu_n(x_n)) \\ &= g(\mu_1(x_1)) + \dots + g(\mu_n(x_n)) \\ &= g(\mu_1(x_1) + \dots + \mu_n(x_n)) \\ &= g(x_1, \dots, x_n) \end{aligned}$$

así que  $f = g$ . Finalmente, vemos que  $\varphi$  es sobreyectivo. Para ello consideramos morfismos  $f_i : G_i \rightarrow G$  y definimos

$$f(x_1, \dots, x_n) := f_1(x_1) + \dots + f_n(x_n)$$

Usando que los  $f_i$  son morfismos y que los  $G_i$  son abelianos tenemos que  $f \in \text{Hom}(G_1, \dots, G_n, G)$  y

$$f \circ \mu_i(x_i) = f(1, \dots, x_i, \dots, 1) = f_1(1) \cdots f_i(x_i) \cdots f_n(1) = f_i(x_i)$$

de donde tenemos que

$$\varphi(f) = (f \circ \mu_1, \dots, f \circ \mu_n) = (f_1, \dots, f_n)$$

□

El lema anterior nos indica que

$$\widehat{G} \cong \widehat{\langle x_1 \rangle} \times \dots \times \widehat{\langle x_n \rangle}$$

así que basta notar que cada factor cumple  $\widehat{\langle x_i \rangle} \cong \langle \chi_i \rangle$ . En efecto, note que un elemento  $\chi \in \widehat{\mathbb{Z}/d_i\mathbb{Z}}$  corresponde a un morfismo  $\chi : \mathbb{Z}/d_i\mathbb{Z} \rightarrow \mathbb{T}$ , y dado que  $\mathbb{Z}/d_i\mathbb{Z}$  es cíclico el morfismo viene determinado por la imagen de un generador, en este caso  $x_i$ , y como los morfismos de grupos preservan el orden de los elementos  $x_i$  debe ir a parar a una raíz  $d_i$ -ésima de la unidad, y como los elementos del grupo dual están definidos con la multiplicación puntual, vemos que  $x_i \mapsto e^{2\pi i/d_i}$  es un generador de  $\widehat{\langle x_i \rangle}$  □