Álgebra I: Teoría de Grupos
Examen parcial 1. Soluciones

Universidad de El Salvador. Ciclo impar 2018

Problema 1 (1 punto)**.** Consideremos los grupos simétricos S_n y grupos alternantes A_n. ¿Para cuáles valores de n son abelianos? Cuando no son abelianos, encuentre un par de permutaciones específicas σ, τ tales que $\sigma \circ \tau \neq \tau \circ \sigma$.

Solución. El grupo S_n no es abeliano para $n \geq 3$. En este caso tenemos, por ejemplo,

$$(1\ 2) \circ (2\ 3) = (1\ 2\ 3), \quad (2\ 3) \circ (1\ 2) = (1\ 3\ 2).$$

El grupo A_n no es abeliano para $n \geq 4$. Por ejemplo,

$$(1\ 2\ 3) \circ (1\ 2\ 4) = (1\ 3) \circ (2\ 4), \quad (1\ 2\ 4) \circ (1\ 2\ 3) = (1\ 4) \circ (2\ 3).$$

El grupo

$$A_3 = \{\mathrm{id}, (1\ 2\ 3), (1\ 3\ 2)\}$$

es abeliano. ■

Problema 2 (1 punto)**.** Demuestre que un grupo G es abeliano si y solamente si para cualesquiera $g, h \in G$ se cumple

$$(gh)^2 = g^2 h^2.$$

Solución. Si G es abeliano, entonces

$$(gh)^2 = ghgh = gghh = g^2 h^2.$$

En la otra dirección, si en G se cumple

$$ghgh = (gh)^2 = g^2 h^2 = gghh$$

para cualesquiera $g, h \in G$, entonces, podemos cancelar g en la izquierda y h en la derecha y obtener

$$hg = gh.$$

■

Problema 3 (2 puntos)**.** Supongamos que $\sigma = (i_1\ \cdots\ i_k)$ y $\tau = (j_1\ \cdots\ j_\ell)$ son dos ciclos *disjuntos* en el grupo simétrico S_n; es decir,

$$\{i_1, \ldots, i_k\} \cap \{j_1, \ldots, j_\ell\} = \emptyset.$$

Demuestre que el mínimo exponente $m = 1, 2, 3, \ldots$ tal que $(\sigma \circ \tau)^m = \mathrm{id}$ es igual a $\mathrm{mcm}(k, \ell)$.

Solución. Dado que los ciclos disjuntos conmutan entre sí, para cualquier $m = 1, 2, 3, \ldots$ se cumple

$$(\sigma \circ \tau)^m = \sigma^m \circ \tau^m.$$

De hecho, podemos notar que las potencias σ^i y τ^j son disjuntas para todo i, j. Luego,

$$k = \mathrm{mín}\{m = 1, 2, 3, \ldots \mid \sigma^m = \mathrm{id}\}, \quad \ell = \mathrm{mín}\{m = 1, 2, 3, \ldots \mid \tau^m = \mathrm{id}\}$$

y la división con resto de m por k y ℓ respectivamente demuestra que

$$\sigma^m = \mathrm{id} \iff k \mid m, \quad \tau^m = \mathrm{id} \iff \ell \mid m.$$

Ahora

$$(\sigma \circ \tau)^m = \sigma^m \circ \tau^m = \mathrm{id} \iff \sigma^m = \mathrm{id} \text{ y } \tau^m = \mathrm{id} \iff k \mid m \text{ y } \ell \mid m.$$

Entonces,

$$\text{mín}\{m = 1, 2, 3, \dots \mid (\sigma \circ \tau)^m = \mathrm{id}\} = \text{mín}\{m = 1, 2, 3, \dots \mid k \mid m \text{ y } \ell \mid m\} =: \mathrm{mcm}(k, \ell).$$

■

Problema 4 (2 puntos)**.** Para el grupo simétrico S_5 calcule cuántas diferentes permutaciones $\sigma \in S_5$ satisfacen la propiedad $\sigma \circ \sigma = \mathrm{id}$.

Solución. El grupo S_5 tiene $5! = 120$ elementos y por supuesto, no nos conviene analizarlos uno por uno. Enumeremos todos los posibles tipos de ciclo de las permutaciones en S_5 (recordemos que estos corresponden a las particiones de 5):

$$\begin{aligned}
1+1+1+1+1 &\longleftrightarrow \mathrm{id},\\
1+1+1+2 &\longleftrightarrow (\bullet\ \bullet),\\
1+1+3 &\longleftrightarrow (\bullet\ \bullet\ \bullet),\\
1+2+2 &\longleftrightarrow (\bullet\ \bullet)\,(\bullet\ \bullet),\\
1+4 &\longleftrightarrow (\bullet\ \bullet\ \bullet\ \bullet),\\
2+3 &\longleftrightarrow (\bullet\ \bullet\ \bullet)\,(\bullet\ \bullet),\\
5 &\longleftrightarrow (\bullet\ \bullet\ \bullet\ \bullet\ \bullet).
\end{aligned}$$

Solamente las permutaciones id, $(\bullet\ \bullet)$ y $(\bullet\ \bullet)\,(\bullet\ \bullet)$ satisfacen la condición $\sigma^2 = \mathrm{id}$:

$$\mathrm{id}^2 = \mathrm{id}, \quad (a\ b)^2 = \mathrm{id}, \quad ((a\ b) \circ (c\ d))^2 = (a\ b)^2 \circ (c\ d)^2 = \mathrm{id}.$$

Para las demás permutaciones se tiene

$$\begin{gathered}
(a\ b\ c)^2 = (a\ c\ b) \neq \mathrm{id}, \quad (a\ b\ c\ d)^2 = (a\ c) \circ (b\ d) \neq \mathrm{id},\\
((a\ b\ c) \circ (d\ e))^2 = (a\ b\ c)^2 \circ (d\ e)^2 = (a\ c\ b) \neq \mathrm{id},\\
(a\ b\ c\ d\ e)^2 = (a\ c\ e\ b\ d) \neq \mathrm{id}.
\end{gathered}$$

Entonces, necesitamos contar cuántas permutaciones de la forma $(a\ b)$ y $(a\ b) \circ (c\ d)$ hay en S_5. Para las transposiciones, es fácil: necesitamos escoger un par de índices diferentes $a, b \in \{1, 2, 3, 4, 5\}$ y estos definen una transposición $(a\ b) = (b\ a)$. Tenemos

$$\binom{5}{2} = \frac{5!}{2! \cdot 3!} = \frac{4 \cdot 5}{2} = 10$$

posibilidades. Para contar las permutaciones de la forma $(a\ b) \circ (c\ d)$ (productos de dos transposiciones disjuntas), podemos escribirlas como $(a\ b) \circ (c\ d) \circ (e)$. Hay 5! posibilidades de poner números diferentes en lugar de a, b, c, d, e. Luego, ya que $(a\ b) = (b\ a)$ y $(c\ d) = (d\ c)$, tenemos que dividir 5! por $2 \cdot 2$. De la misma manera, el orden de múltiplos $(a\ b)$ y $(c\ d)$ no cambia el resultado, y hay que dividir todo por 2. Entonces, hay

$$\frac{5!}{2 \cdot 2 \cdot 2} = \frac{2 \cdot 3 \cdot 4 \cdot 5}{2 \cdot 2 \cdot 2} = 15$$

diferentes permutaciones de la forma $(a\ b) \circ (c\ d)$.

Podemos concluir que en S_5 hay precisamente

$$1 + 10 + 15 = 26$$

permutaciones que satisfacen $\sigma \circ \sigma = \mathrm{id}$. ■

Problema 5 (2 puntos)**.**

1) Para un grupo G demuestre que el centro $Z(G)$ es un subgrupo de G.

2) Sea G un grupo y H su subgrupo. ¿Es cierto que $Z(H)$ es un subgrupo de $Z(G)$? (Demuéstrelo o encuentre un contraejemplo.)

Solución. Recordemos la definición del centro:

$$Z(G) := \{g \in G \mid gh = hg \quad \text{para todo } h \in G\}.$$

Primero, $1 \in Z(G)$, puesto que para todo $h \in G$ se cumple

$$1 \cdot h = h \cdot 1 = h.$$

Ahora supongamos que $g_1, g_2 \in Z(G)$. Entonces, para todo $h \in G$ se cumple

$$(g_1 g_2)\, h \overset{\text{asoc.}}{=} g_1\, (g_2\, h) \overset{g_1 \in Z(G)}{=} (g_2\, h)\, g_1 \overset{\text{asoc.}}{=} g_2\, (h\, g_1) \overset{g_2 \in Z(G)}{=} (h\, g_1)\, g_2 \overset{\text{asoc.}}{=} h\, (g_1 g_2).$$

Ahora si $g \in Z(G)$, entonces para todo $h \in G$ tenemos

$$g^{-1}\, h = (h^{-1}\, g)^{-1} \overset{g \in Z(G)}{=} (g\, h^{-1})^{-1} = h\, g^{-1}.$$

Esto demuestra la primera parte (de hecho, ya lo habíamos hecho en clase). La segunda parte es totalmente falsa. Por ejemplo, como vimos en clase,

$$Z(S_n) = \{\mathrm{id}\} \quad \text{para } n \geq 3,$$

pero S_n puede contener subgrupos abelianos

$$\{\mathrm{id}\} \subsetneq H \subsetneq S_n$$

para los cuales $Z(H) = H$. El ejemplo mínimo es el de S_3 donde tenemos cuatro subgrupos propios

$$\{\mathrm{id}, (1\ 2)\}, \quad \{\mathrm{id}, (1\ 3)\}, \quad \{\mathrm{id}, (2\ 3)\}, \quad A_3 = \{\mathrm{id}, (1\ 2\ 3), (1\ 3\ 2)\}.$$

Todos estos subgrupos son abelianos. ■

Problema 6 (2 puntos)**.** Se dice que un número complejo $z \in \mathbb{C}$ es una **raíz n-ésima de la unidad** si $z^n = 1$.

1) Demuestre que todas las raíces n-ésimas de la unidad forman un grupo abeliano respecto a la multiplicación compleja. Denotémoslo por $\mu_n(\mathbb{C})$.

2) Demuestre que todas las raíces de la unidad

$$\mu_\infty(\mathbb{C}) := \bigcup_{n \geq 1} \mu_n(\mathbb{C})$$

también forman un grupo.

Solución. Sabemos que los números complejos no nulos $\mathbb{C} \setminus \{0\}$ forman un grupo abeliano respecto a la multiplicación, así que será suficiente ver que $\mu_n(\mathbb{C})$ es un subgrupo. Obviamente, 1 es una raíz n-ésima de la unidad para cualquier n: tenemos $1^n = 1$. Luego, si z y w son raíces n-ésimas de la unidad, entonces su producto zw es también una raíz n-ésima de la unidad:

$$(zw)^n = z^n\, w^n = 1.$$

Por fin, si z es una raíz n-ésima de la unidad, entonces $z \neq 0$ y z es invertible: existe z^{-1} tal que $z^{-1}\, z = 1$. Luego,

$$(z^{-1})^n = (z^n)^{-1} = 1,$$

así que z^{-1} es también una raíz n-ésima de la unidad.

De la misma manera, podemos ver que todas las raíces de la unidad forman un subgrupo

$$\mu_\infty(\mathbb{C}) := \bigcup_{n\geq 1} \mu_n(\mathbb{C}) \subset \mathbb{C} \setminus \{0\}.$$

Obviamente, $1 \in \mu_\infty(\mathbb{C})$. Luego, si $z \in \mu_\infty(\mathbb{C})$, entonces $z \in \mu_n(\mathbb{C})$ para algún n y, como acabamos de ver, $z^{-1} \in \mu_n(\mathbb{C})$. Finalmente, si $z, w \in \mu_\infty(\mathbb{C})$, esto quiere decir que $z^m = 1$ y $w^n = 1$ para algunos m y n. Sea ℓ algún número tal que $m \mid \ell$ y $n \mid \ell$. En particular, podemos tomar $\ell = \text{mcm}(m, n)$. Luego, $\ell = am = bn$ para algunos a y b y tenemos

$$(zw)^\ell = z^{am}\, w^{bn} = (z^m)^a\, (w^n)^b = 1,$$

así que zw es una raíz ℓ-ésima de la unidad.

(Esencialmente, acabamos de ver que $m \mid \ell$ implica $\mu_m(\mathbb{C}) \subset \mu_\ell(\mathbb{C})$; en particular, $\mu_m(\mathbb{C}), \mu_n(\mathbb{C}) \subset \mu_\ell(\mathbb{C})$ donde $\ell = \text{mcm}(m, n)$.) ■