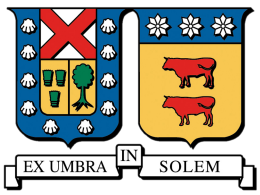

Ayudantia #1: Permutaciones y $\mathbb{Z}/n\mathbb{Z}$

MAT-214: Estructuras Algebraicas

Semestre 2026-1

Profesor: Pedro Montero **Ayudante:** Madeline Castro

Recuerdo

Recordamos algunas cositas de permutaciones.

Definición 1. Denotamos por S_n (o $\mathfrak{S}_n$ en el apunte del profe) al conjunto de funciones biyectivas $\sigma\colon \{1,\cdots,n\} \to \{1,\cdots,n\}$. Este conjunto puede ser dotado de una estructura de grupo considerando como producto la composicion de funciones $\circ$ (¿Por que?). Haremos uso de la notación:

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & n \end{pmatrix}$$

Para especificar elementos de este conjunto.

Sea $n \in \mathbb{N}^{\geq 1}$ fijo, durante el primer problema vamos a hacer uso de unos tipos especificos de permutación, definimos entonces:

Definición 2. Sea $\tau \in S_n$, diremos que τ es una **transposición** si existen $i \neq j \leq n$ tal que $\tau(i) = j, \tau(j) = i$ y $\tau(k) = k$ para todo $k \neq i, j$. En nuestra notación:

$$\tau = \begin{pmatrix} 1 & 2 & \cdots & i & \cdots & j & \cdots & n \\ 1 & 2 & \cdots & j & \cdots & i & \cdots & n \end{pmatrix}$$

Tambien denotamos $\tau = (i, j)$.

Definición 3. Sea $\sigma \in S_n$ y $k \leq n$ diremos que σ es un **k-ciclo** si existen $a_1, a_2, \cdots, a_k$ tal que $\sigma(a_1) = a_2, \sigma(a_2) = a_3, \cdots, \sigma(a_k) = a_1$ y deja todo el resto de elementos fijos. Al igual que antes, podemos escribir esto de forma abreviada como $\sigma = (a_1, a_2, \cdots, a_k)$, notar que una transposición es tan solo un 2-ciclo.

P1) Sea G un grupo, diremos que el **orden** de un elemento g en G es el minimo n tal que $g^n = e$.

(a) Considere $(S_n, \circ)$ ¿Cual es el orden de una transposición τ? ¿Y de un k-ciclo σ?

Solución: Consideremos una transposición arbitraria $\tau = (i, j)$ con $i \neq j \leq n$, primero consideremos $\tau^2 =: \tau \circ \tau$ el cual es un elemento del grupo de permutaciones, note ademas que la identidad en este grupo es la permutación identidad, es decir la permutacion ι tal que $\iota(i) = i$ para todo $i \in \{1, \cdots, n\}$. Vamos a mostrar que $\tau^2 = \iota$:

- Sea $x \in \{1, \cdots, n\} - \{i, j\}$, como la transposición solo afecta a las posiciones i e j tenemos entonces que $\tau^2(x) = \tau(x) = x$.
- Si $x = i$, entonces $\tau^2(i) = \tau(\tau(i)) = \tau(j) = i$. El calculo es analogo para j, luego τ^2 se comporta igual que la identidad, por lo que $\tau^2 = \iota$.

Claramente $\tau \neq \iota$, por lo que $n = 2$ es el minimo valor tal que $\tau^n = \iota$.

Ahora, sea $\sigma = (a_1, \cdots, a_k)$ un k-ciclo con $a_1, \cdots, a_k \subseteq \{1, \cdots, n\}$, siendo que τ es generalmente un 2-ciclo, el candidato que podemos sugerir para el orden de σ es k. Por lo que de misma forma estudiamos σ^k:

- Sea $x \in \{1, \cdots, n\} - \{a_1, \cdots, a_k\} := S$, por definición si x esta fuera del conjunto del ciclo entonces la permutación deja el elemento fijo y de misma manera será evaluar la permutacion más de una vez, en corto $\sigma^k|_S = \sigma|_S = \iota_S$. (Donde este ultimo es la funcion identidad en S)
- Si $x \in \{a_1, \cdots, a_k\}$, la definición de ciclo nos dice que $\sigma(a_i) = a_{i+1}$, aplicando la defínción j veces tenemos que $\sigma^j(a_i) = a_{i+j}$ lo cual tiene sentido siempre y cuando $i+j \leq k$. Ahora sea a_i elemento del ciclo, notemos que $\sigma^{k-i}(a_i) = a_k$, $\sigma(a_k) = a_1$ y que $\sigma^{i-1}(a_1) = a_i$, componiendo tenemos que $\sigma^{k-i} \circ \sigma \circ \sigma^{i-1}(a_i) = \sigma^k(a_i) = a_i$. Como esto funciona para todo elemento en el ciclo tenemos entonces que σ^k se comporta como la identidad en S^c.

Queda como ejercicio mostrar que no puede existir $k' < k$ tal que $\sigma^{k'}$ sea la identidad (basta proceder por induccion y usar que σ es una biyeccion sobre los elementos del ciclo). Por lo que k es el orden de un k-ciclo.

(b) Sea

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 5 & 4 & 2 \end{pmatrix}$$

Escriba σ como un producto de transposiciones. *Indicación:* Si $\sigma(i) = j$, estudie la permutacion $\tau = (i, j) \circ \sigma$.

Solución: Como dice la indicación, notemos que si $\sigma(i) = j$ entonces $\tau = (i, j) \circ \sigma$ es tal que $\tau(i) = (i, j)(\sigma(i)) = (i, j)(j) = i$, de misma manera tenemos que $\tau(j) = j$, es facil ver ademas que τ no modifica ningun otro valor de σ, por lo que de esto podemos desprender que si $\sigma(i) = j$ entonces podemos modificar mediante una transposición y obtener una permutacion que deja fijos tanto al i como al j, esto es util para nuestro ejemplo pues ahora podemos hacer esto con nuestro σ:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 5 & 4 & 2 \end{pmatrix} \implies (1,3) \circ \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 5 & 4 & 2 \end{pmatrix}$$

$$(2,5) \circ (1,3) \circ \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 2 & 4 & 5 \end{pmatrix} \implies (2,3) \circ (2,5) \circ (1,3) \circ \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = \iota$$

Luego como las transposiciones son inversas de si mismas tenemos que

$$(2,3) \circ (2,5) \circ (1,3) \circ \sigma = \iota \implies \sigma = (1,3) \circ (2,5) \circ (2,3)$$

(c) Pruebe, usando induccion y apoyandose en el ejemplo concreto, que toda permutación puede ser escrita como un producto de transposiciones.

Solución: Vamos a proceder por inducción en n, es decir el numero de elementos que estamos permutando, si $n = 2$ entonces $S_2 = (1,1), (1,2)$ donde $(1,1) = (2,2)$ es tan solo la identidad (que por convencion la trataremos como una transposición tambien). Ahora vamos a tomar como hipotesis que toda permutación de $n-1$ elementos puede ser descompuesta en transposiciones. Para usar esta hipotesis en el paso inductivo tenemos que notar lo siguiente:

Sea $S_n^* = \{\sigma \in S_n \,|\, \sigma(n) = n\}$, es facil ver que la función

$$f : S_{n-1} \to S_n^*,\ \sigma \mapsto \begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n-1) & n \end{pmatrix}$$

es una biyección y morfismo de grupos (¿por que?), en otras palabras si puedo escribir mi permutación de n elementos como una permutación con al menos un elemento fijo entonces por hipotesis puedo descomponerla como transposiciones. Tomemonos ambos casos, sea $\sigma \in S_n$:

- Si $\sigma(n) = n$, entonces existe $\rho \in S_{n-1}$ tal que $f(\rho) = \sigma$, pero ρ por induccion puede ser escrito como $\rho = \tau_1 \cdots \tau_s$ y por lo tanto $f(\rho) = f(\tau_1 \cdots \tau_s) = f(\tau_1) \cdots f(\tau_s) = \sigma$, note que transposiciones en S_{n-1} son tambien transposiciones en S_n, por lo que $\sigma = \tau_1' \cdots \tau_s'$
- Si $\sigma(n) = k \neq n$, entonces consideramos $\sigma' = (n, k) \circ \sigma$ y asi recuperamos el caso anterior! Así $(n, k)\sigma = \tau_1' \cdots \tau_s' \implies \sigma = (n, k)\tau_1' \cdots \tau_s'$.

Tareita

Usando otra demostración por inducción una puede de hecho demostrar que toda permutacion puede ser escrita como un producto de ciclos disjuntos entre si (es decir, podemos escribir $\sigma = \sigma_1 \cdots \sigma_n$ donde cada σ_i es un ciclo de manera que si $\sigma_i = (a_1, \cdots, a_k)$ y $\sigma_j = (b_1, \cdots, b_s)$ entonces $\{a_1, \cdots, a_k\} \cap \{b_1, \cdots, b_s\} = \emptyset$. Esta hipotesis es especialmente importante por el siguiente resultado:

(d) Muestre que ciclos disjuntos τ, σ son conmutativos, (es decir $\tau \circ \sigma = \sigma \circ \tau$).

Solución: Sean $\{a_1, \cdots, a_s\}$ y $\{b_1, \cdots, b_t\}$ los elementos que mueven σ y τ respectivamente (y por hipotesis, disjuntos), procedemos por casos:

- Si $x \notin \{a_1, \cdots, a_s, b_1, \cdots, b_t\}$ entonces $\sigma(x) = \tau(x) = x$, por lo que siempre $\tau\sigma = \sigma\tau$.
- Si $x \in \{a_1, \cdots, a_s\}$ pero no en $\{b_1, \cdots, b_t\}$ hemos de notar que $\sigma(x)$ tampoco esta en los elementos de τ, por lo que τ lo deja fijo, es decir que $\tau(\sigma(x)) = \sigma(x)$ y $\sigma(\tau(x)) = \sigma(x)$, por lo que conmutan tambien.
- Analogo para el caso contrario.

(e) Sea $\sigma \in S_n$ un permutación arbitraria, mostrar que $\sigma^{n!} = \mathrm{Id}$.

Solución: Por la tareita y el item anterior, sabemos que σ puede ser escrito como un productp de ciclos disjuntos, es decir $\sigma = \sigma_1 \cdots \sigma_k$ con cada σ_i siendo un ciclo de tamaño t_i, como estos son ciclos disjuntos tenemos ademas que la suma de todos los tamaños es n (incluyendo 1-ciclos, que solo son elementos fijos). En particular cada tamaño es menor a n, ahora elevemos σ a la $n!$ y usemos el hecho de que estos ciclos conmutan.

$$\sigma^{n!} = (\sigma_1 \cdots \sigma_k)^{n!} = \sigma_1^{n!} \cdots \sigma_k^{n!} = \sigma_1^{t_1 \frac{n!}{t_1}} \cdots \sigma_1^{t_k \frac{n!}{t_k}}$$

Bien definido pues t_i siempre es un divisor de $n!$, más aun sabemos que cada tamaño es el orden de su respectivo ciclo, por lo que al final todo ciclo lo podemos escribir como una potencia de la identidad, que sigue la identidad, por lo tanto $\sigma^{n!} = \iota$

(f) Calcule explicitamente el orden de un elemento $\sigma \in S_n$, construya un elemento de orden maximal en S_6.

Solución: Si bien sabemos que siempre podemos elevar a la $n!$ y obtener la identidad, esto es una (drastica) sobrestimación del orden, para eso notemos que si tenemos σ descompuesto como el item anterior entonces lo unico que necesitamos para que σ^s sea la identidad es que s sea multiplo de cada uno de los ordenes de los ciclos (pues en ese caso todos los ciclos se convierten en la identidad), como buscamos el minimo entre estos consideramos entonces el minimo común multiplo, es decir $s = mcm(t_1, \cdots, t_k)$.

Usemos esto para conseguir un elemento de orden maximo en S_6, para esto notemos que los posibles tamaños para los ciclos son todas las posibles sumas de numeros enteros positivos que suman 6 (por la hipotesis de ciclos disconjuntos).

Particion	6	5+1	4+2	4+1+1	3+3	3+2+1	$3+3\cdot 1$	$3\cdot 2$	$2\cdot 2+2\cdot 1$	$2+4\cdot 1$	$6\cdot 1$
MCM	6	5	4	4	3	6	3	2	2	2	1

Asi, las particiones 6 y $3, 2, 1$ son las que dan mayores ordenes, un elemento de orden maximo seria por ejemplo $\sigma = (2, 3, 1)(5, 6)(4)$

P2) Sea $G = \{g_1, g_2, \cdots, g_n\}$ un grupo finito, considere $g \in G$ fijo y la función $\lambda_g : G \to G,\ x \mapsto g \cdot x$. Considere tambien que hay una función biyectiva entre G y $\{1, \cdots, n\}$ dada por $g_i \mapsto i$.

(a) Muestre que para un $g \in G$ fijo podemos asociar a λ_g una permutación en S_n, especifique la identificación. ¿Es $\lambda_g \colon G \to G$ un morfismo de grupos? Haga el mismo analisis con $\kappa_g \colon G \to G,\ x \mapsto g \cdot x \cdot g^{-1}$

Solución: Mediante la correspondencia $g_i \mapsto i$ podemos imaginar que λ_g actua de una manera similar a las permutaciones:

$$\lambda_g = \begin{pmatrix} g_1 & g_2 & \cdots & g_n \\ g \cdot g_1 & g \cdot g_2 & \cdots & g \cdot g_n \end{pmatrix}$$

Más formalmente si denotamos a la correspondencia $g_i \mapsto i$ como $f : G \to \{1, \cdots, n\}$, entonces podemos asociar a λ_g la permutación $\sigma = f \circ \lambda_g \circ f^{-1}$ (!), en forma de diagrama elegante tenemos:

$$\begin{array}{ccc} G & \xrightarrow{\quad\lambda_g\quad} & G \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle f} \\ \{1, \cdots, n\} & \xrightarrow{\sigma = f \circ \lambda_g \circ f^{-1}} & \{1, \cdots, n\} \end{array}$$

Ahora, para que σ sea de verdad una permutación tenemos que probar que λ_g es biyectiva, para esto basta notar que $\lambda_{g^{-1}}$ es la inversa de esta ultima, por lo que se tiene el resultado.

Sin embargo, notemos que λ_g no es un morfismos de grupos, para esto basta notar que $\lambda_g(e) = g \neq e$, por lo que si bien tenemos una biyección util no podemos usar esta para crearnos morfismos de grupos; distinto es con κ_g definido en el ejercicio, se deja como ejercicio (muy util!!!) mostrar que κ_g es un automorfismo para cualquier $g \in G$.

(b) Considere el grupo de Klein $G = \{e, a, b, c\}$, con la operacion dada por la siguiente tabla de multiplicación:

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Calcula λ_g para todo $g \in G$ y representelo como una permutación. ¿Es G un subgrupo de S_4?

Solución: Hacemos la correspondencia del ejercicio anterior y consideramos permutaciones sobre el conjunto $\{e, a, b, c\}$. Luego podemos escribir las permutaciones asociadas a cada elemento simplemente leyendo las filas de la tabla de multiplicación, de esta manera:

$$\lambda_e = \begin{pmatrix} e & a & b & c \\ e & a & b & c \end{pmatrix} = \iota$$

$$\lambda_a = \begin{pmatrix} e & a & b & c \\ a & e & c & b \end{pmatrix} = (a, e)(c, b)$$

$$\lambda_b = \begin{pmatrix} e & a & b & c \\ b & c & e & a \end{pmatrix} = (b, e)(c, a)$$

$$\lambda_c = \begin{pmatrix} e & a & b & c \\ c & b & a & e \end{pmatrix} = (c, e)(b, a)$$

Componiendo las permutaciones una obtiene que $\lambda_a \circ \lambda_b = \lambda_c$, luego notemos que cada λ_g es un producto de transposiciones disjuntas y por lo tanto tienen orden dos (i.e $\lambda_g^2 = \iota$ para todo $g \in \{e, a, b, c\}$), por lo que moviendo esta ultima igualdad podemos obtener todas las posibles multiplicaciones de elementos no triviales, luego G esta cerrado por multiplicacion de S_4, más aún tenemos que $\lambda_e = \iota$, por lo que efectivamente G es un subgrupo de S_4.

(c) Sea $(a_1, a_2, \cdots, a_t)$ un t-ciclo en S_n, sea $\sigma \in S_n$, muestre que $\kappa_\sigma((a_1, \cdots, a_t)) = (\sigma(a_1), \cdots, \sigma(a_t))$

Solución: Recordemos que $\kappa_\sigma((a_1, \cdots, a_t)) = \sigma \cdot (a_1, \cdots, a_t) \cdot \sigma^{-1}$, basta evaluar en los elementos del ciclo esperado para verificar el resultado, sea a_i elemento del ciclo $(a_1, \cdots, a_t)$, evaluaremos $\sigma(a_i)$ en $\kappa_\sigma((a_1, \cdots, a_t))$:

$$\sigma \circ (a_1, \cdots, a_t)(\sigma^{-1}(\sigma(a_i))) = \sigma \circ (a_1, \cdots, a_t)(a_i) = \sigma(a_{i+1})$$

Recuerdo

Sea $n \in \mathbb{N}^{\geq 1}$. Consideramos la relación dada en $\mathbb{Z}$ por:

$a \sim_n b \iff n$ divide $a - b \iff n$ cuando divide a a y b tiene el mismo resto. $\iff a \equiv b \mod n$

El conjunto cociente $\mathbb{Z}/n\mathbb{Z}$ es el conjunto de todas las clases de equivalencia $[a]_n = \{b \in \mathbb{Z} \,|\, a \equiv b \mod n\}$. Usando el algoritmo de division euclideana es facil mostrar que $\mathbb{Z}/n\mathbb{Z} = \{[0]_n, [1]_n, \cdots, [n-1]_n\}$ (¿por que?)

P3) Queremos darle una estructura de grupos al conjunto $\mathbb{Z}/n\mathbb{Z}$, para eso la decisión mas obvia seria usar la suma o producto en $\mathbb{Z}$, sin embargo no siempre es verdad que las operaciones de un conjunto estan bien definidas sobre un cociente de el, por ejemplo:

(a) Sea $\mathbb{Z}/3\mathbb{Z}$, definamos la operación $[x]_3 \cdot [y]_3 = [x^y]_3$. Muestre que $[2]_3 \cdot [1]_3$ no esta bien definido, pues depende del numero escogido en la clase de equivalencia.

(b) Sea $n \in \mathbb{N}^{\geq 1}$. Muestre que tanto la suma como el producto de $\mathbb{Z}$ estan bien definidos en $\mathbb{Z}/n\mathbb{Z}$, es decir que $[a+b]_n$ y $[ab]_n$ no dependen de la clase escogida para a y b. En otras palabras que si $a \equiv a' \mod n$ y $b \equiv b' \mod n$ entonces $[a+b]_n = [a'+b']_n$ y $[ab]_n = [a'b']_n$.

Observación

Ahora, para armar un grupo a partir de alguna de estas operaciones es necesario que se cumplan los axiomas de grupos, es facil mostrar que la suma cumple todos los axiomas y que $(\mathbb{Z}/n\mathbb{Z}, +)$ es un grupo, sin embargo esto no es siempre verdad para la multiplicación. Note por ejemplo que no existe un inverso para el numero 2 modulo 6, es decir que no existe $x := [2]_6^{-1}$ tal que $2x \equiv 1 \mod 6$.

Para especificar cuando tenemos inversos multiplicativos tenemos hacemos uso del siguiente lema:

Lemma 4. *Si $a, b \in \mathbb{N}$, entonces exsiten $m, n \in \mathbb{Z}$ tal que: $am + bn = mcd(a, b)$*

(c) Sea $n > 1$ entero y sea $a, b \in \mathbb{Z}$. Muestre que la ecuación $ax \equiv b \mod n$ tiene solución si y solo si $\text{mcd}(a, n) | b$. Muestre que $(\mathbb{Z}/p\mathbb{Z}, \cdot)$ es un grupo si y solo si p es primo.