Universidad Técnica Federico Santa María
Departamento de matemáticas

Pauta Ayudantía 1 MAT214

19 de marzo 2024

Mateo Hidalgo

1. Repaso Capítulo 1

1. Sea $f : A \to B$. Probar que f es inyectiva (respectivamente sobreyectiva) si y solo si tiene inversa por la izquierda (respectivamente derecha). Para probar que la sobreyectividad implica la existencia de inversa por la derecha es necesario el axioma de elección.
   Solución: Si f tiene una inversa g por la izquierda, $f(x) = f(y) \implies g(f(x)) = g(f(y)) = x = y$. Si f es inyectiva, basta definir $g(x) := f^{-1}(x)$ para todo $x \in \mathrm{Im}(f) \subset B$.
   Si f tiene una inversa h por la derecha, dado $y \in B$ entonces $f(h(y)) = y$ (así que es sobreyectiva). Si f es sobreyectiva, los conjuntos de la forma $f^{-1}(b) := A_b \neq \emptyset$, es decir los A_b forman una partición de B, el axioma de elección dice que existe una función $h : B \to \bigcup A_b = A$ tal que $h(b) \in A_b = f^{-1}(b)$.

2. Calcule los últimos dos dígitos de 9^{1500}.
   Solución: El truco es que $[ab]_{100} = [a]_{100} \cdot [b]_{100}$. Denotaremos la imagen de a en el cociente como $\overline{a}$ así tenemos

$$\overline{9^2} = \overline{9}^2 = \overline{81} = \overline{-19} \tag{1}$$
$$\implies \overline{9^4} = \overline{9^2}^2 = \overline{-19}^2 = \overline{361} = \overline{61} \tag{2}$$
$$\implies \overline{9^5} = \overline{9 \cdot 61} = \overline{49} \tag{3}$$
$$\implies \overline{9^{10}} = \overline{9^5}^2 = \overline{49}^2 = \overline{1} \tag{4}$$
$$\implies \overline{9^{1500}} = \overline{01} \tag{5}$$

3. Pruebe que para cualquier par de enteros $a, b \in \mathbb{Z}$, la expresión $a^2 + b^2$ nunca tiene resto 3 al dividir por 4.
   Solución: Tenemos en $\mathbb{Z}/4\mathbb{Z}$: $\overline{0}^2 = \overline{0}$, $\overline{1}^2 = \overline{1}$, $\overline{2}^2 = \overline{0}$, $\overline{3}^2 = \overline{1}$. Así las posibles sumas de cuadrados de elementos en $\mathbb{Z}/4\mathbb{Z}$ son $0 + 0 = 1, 1 + 1 = 2, 1 + 0 = 1$ pero nunca 3.

   Para ejercicios más difíciles de aritmética modular pueden revisar https://aryansh-s.github.io/The_Art_of_Modular_Arithmetic.pdf

4. Probar que $(\mathbb{Q}, +)$ es un grupo que no es finitamente generado.
   Solución: Notemos que los elementos de $\langle a_1/b_1, \ldots, a_n/b_n \rangle$ son combinaciones lineales de los a_i/b_i a coeficientes enteros. Por simplicidad trabajamos siempre con las fracciones en su expresión irreducible. Como la multiplicación de un entero con una fracción no aumenta (el valor absoluto) del denominador (por ejemplo $2 \cdot \frac{5}{6} = \frac{5}{3}$), tenemos que el denominador más grande que aparece en un elemento de $\langle a_1/b_1, \ldots, a_n/b_n \rangle$ es el denominador de $a_1/b_1 + \cdots + a_n/b_n$, que sabemos es el mínimo común denominador, es decir $\mathrm{mcm}(b_1, \ldots, b_n) < +\infty$, pero los denominadores de elementos en $\mathbb{Q}$ tienen valores arbitrariamente grandes.

5. Sea k un cuerpo, demuestre que la siguiente es una relación de equivalencia en $k^n \setminus \{0\}$:

$$x \sim y \iff \exists \lambda \in k \setminus \{0\}, x = \lambda y$$

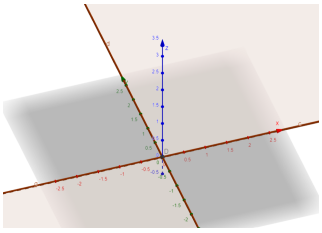

Figura 1: Solución Item c) en Geogebra

Al espacio cociente le llamamos proyectivización de k^n y lo denotamos por $\mathbb{P}(k^n)$ y a la clase de equivalencia de $x = (x_1, \ldots, x_n)$ la denotamos por $[x_1 : \cdots : x_n]$. Considere la aplicación $\pi : k^n \setminus \{0\} \to \mathbb{P}(k^n), v \mapsto [v]$ o en cordenadas, $(v_1, \ldots, v_n) \mapsto [v_1 : \cdots : v_n]$. Fijando $k = \mathbb{R}$, $n = 3$. Describa la preimagen a través de π de los siguientes conjuntos

a) Un punto $[x_1 : \cdots : x_n]$.
Solución: Una recta en $\mathbb{R}^3$ que pasa por $(x_1, \ldots, x_n)$

b) El conjunto $\{[\lambda' + \lambda x_1 : \lambda x_2 : \lambda x_3]$ con $\lambda, \lambda' \in \mathbb{R}\}$.
Solución: El plano generado por $(1, 0, 0)$ y (x_1, x_2, x_3)

c) El conjunto $\{[t : 1 - t : 0]$ con $t \in [0, 1]\}$.
Solución: La unión de todas las rectas generaadas por los vectores de la forma $(v_1, v_2, 0)$ con $v_1, v_2 \geq 0$

Para más información pueden revisar https://en.wikipedia.org/wiki/Real_projective_plane# especialmente la parte de cordenadas homogeneas. La construcción del plano proyectivo es muy usada, pueden encontrarla fácilmente en la literatura.

6. (Recuerdo: un m-ciclo (o simplemente un ciclo) es una permutación $(a_1, \ldots, a_m)$ (con todos los a_i distintos) que envía $a_i \mapsto a_{i+1}$ para $i < m$ y $a_m \mapsto 1$. Dos ciclos $(a_1, \ldots, a_m)$ y $(b_1, \ldots, b_k)$ se dicen disjuntos si $a_i \neq b_i$ para todo i.

   Sea σ la permutación dada por

   $$1 \mapsto 3, 2 \mapsto 4, 3 \mapsto 5, 4 \mapsto 2, 5 \mapsto 1$$

   y sea τ la permutación dada por

   $$1 \mapsto 5, 2 \mapsto 3, 3 \mapsto 2, 4 \mapsto 4, 5 \mapsto 1$$

   Escriba $\sigma, \tau, \sigma^2, \sigma\tau$ y $\tau\sigma$ como producto de ciclos disjuntos disjuntos (más adelante en el curso probarán que esto siempre es posible y la descomposición es única).

Solución:

$$\begin{aligned}
\sigma &= (1\ 3\ 5)(2\ 4)\\
\tau &= (1\ 5)(2\ 3)\\
\sigma^2 &= (1\ 3\ 5)(2\ 4)(1\ 3\ 5)(2\ 4)\\
&= (1\ 5\ 3)\\
\sigma\tau &= (1\ 3\ 5)(2\ 4)(1\ 5)(2\ 3)\\
&= (2\ 5\ 3\ 4)\\
\tau\sigma &= (1\ 5)(2\ 3)(1\ 3\ 5)(2\ 4)\\
&= (1\ 2\ 4\ 3)\\
\tau^2\sigma &= \tau(\tau\sigma) = (1\ 5)(2\ 3)((1\ 5)(2\ 3)(1\ 3\ 5)(2\ 4))\\
&= (1\ 5)(2\ 3)(1\ 2\ 4\ 3)\\
&= (1\ 3\ 5)(2\ 4)
\end{aligned}$$

7. Definimos el orden de una permutación σ como el entero positivo n más pequeño tal que $\sigma^n = \sigma\circ\cdots\circ\sigma = \mathrm{id}$. A el orden de σ lo denotamos $\mathrm{ord}(\sigma)$. (si no existe tal entero decimos que la permutación tiene orden infinito y anotamos $\mathrm{ord}(\sigma) = +\infty$). El soporte de una permutación σ es el conjunto $\mathrm{Supp}(\sigma)$ de elementos en el dominio de la permutación tal que $\sigma(x) \neq x$, así cuando decimos que dos permutaciones son disjuntas, nos referimos a que tienen soportes disjuntos.

   a) Pruebe que si una permutación es un m-ciclo entonces no es un n-ciclo para $m \neq n$.
   Solución: Si $\sigma = (a_1 \ldots, a_n) = (b_1, \ldots, b_m)$ entonces $\mathrm{Supp}\,\sigma = \{a_1, \ldots, a_n\} = \{b_1, \ldots, b_m\}$, como asumimos que los elementos no se repiten dentro de la escritura de un ciclo, esto solo es posible si $m = n$.

   b) Pruebe que un n-ciclo tiene orden n.
   Solución: Es fácil notar que $\sigma^n = \mathrm{id}$ así que $\mathrm{ord}(x) \leq n$ y además como $\sigma^i(a_1) = a_i$ (para $i < n$) tenemos $\mathrm{ord}(\sigma) \geq n$

   c) Pruebe que los ciclos disjuntos conmutan.
   Solución: Sean σ, τ permutaciones disjuntas, si x no está en ninguno de los dos soportes, $\sigma\tau x = x = \tau\sigma x$, si x está en el soporte de τ entonces **no** está en el soporte de σ y $\tau x \neq x$, por biyectividad $\tau\tau x \neq \tau x$ así que τx también está en el soporte de τ y por tanto **no** está en el soporte de σ. Así $\sigma\tau x = \tau x$ y $\tau\sigma x = \tau x$. En caso de que x esté en el soporte de σ el desarrollo es análogo.

   d) Pruebe que el orden de un elemento en S_n es el mínimo común múltiplo de los largos de sus ciclos en una descomposición en ciclos disjuntos (por ejemplo si $\sigma = (15)(234)$ entonces $\mathrm{ord}(\sigma) = 2 \cdot 3 = 6$).
   Solución: Si una descomposición de σ en ciclos disjuntos es $\sigma = \sigma_1 \cdots \sigma_k$ entonces, como los ciclos disjuntos conmutan $\sigma^i = \sigma_1^i \cdots \sigma_k^i$ y es claro entonces que $\sigma^i = \mathrm{id}$ si y solo si $\sigma_j^i = \mathrm{id}$ para todo j, es decir σ_j divide a i para todo j.

   e) Encuentre todos los enteros n tal que S_5 contiene un elemento de orden n. (Repetir para S_7).
   Solución: Usar el ejercicio anterior y notar que no S_n no puede tener elementos de ordenes mayores a n. Así, por inspección, los ordenes posibles en S_5 son 1,2,3,4,5 y 6 y en S_7 son 1,2,3,4,5,6,7,10 y 12.

8. Pruebe que un m-ciclo puede escribirse como producto de $m-1$ traspociones y deduzca que un m-ciclo es una permutación impar si y solo si m es par.
   Solución: En efecto
   $$(a_1 \ldots a_n) = (a_n a_1) \cdots (a_3\ a_1)(a_2\ a_1)$$

2. Propuestos

1. El algoritmo euclidiano es un procedimiento importante el cual produce el máximo común divisor de dos entero a y b iterando el algoritmo de la división: si $a, b \in \mathbb{Z} \setminus \{0\}$, entonces obtenemos una secuencia de cociente y restos:

$$a = q_0 b + r_0 \tag{6}$$
$$b = q_1 r_0 + r_1 \tag{7}$$
$$r_0 = q_2 r_1 + r_2 \tag{8}$$
$$\vdots \tag{9}$$
$$r_{n-2} = q_n r_{n-1} + r_n \tag{10}$$
$$r_{n-1} = q_{n+1} r_n \tag{11}$$

donde r_n es el último resto no nulo. Tal r_n existe dado que $|b| > |r_0| > |r_1| > \cdots > |r_n|$ es una secuencia estrictamente decreciente de enteros positivos, así que no puede disminuir indefinidamente. Una inducción y mantener un buen registro de las divisibilidades permite demostrar que r_n es el máximo común divisor (a, b) de a y b. (No se le pide probar esto)

Use este algoritmo para lo siguiente:

a) Pruebe usando lo anterior, que existen enteros x, y no necesariamente únicos tales que $(a, b) = ax + by$.

b) Calcule el máximo común divisor y determine explícitamente posibles valores de x e y del ítem anterior en los siguientes casos

1) $a = 20, b = 13$
2) $a = 69, b = 372$
3) $a = 792, b = 275$

c) Usando lo anterior, calcule el inverso de k en $\mathbb{Z}/n\mathbb{Z}$ en los siguientes casos:

1) $k = 13, n = 20$
2) $k = 69, n = 89$
3) $k = 1891, n = 3797$
4) $k = 6003722857, n = 77695236973$

2. La construcción de $\mathbb{Q}$ a partir de $\mathbb{Z}$ se generaliza a un procedimiento más general. Considere la siguiente construcción.

Sea A un anillo conmutativo. Un subconjunto $S \subset A$ es multiplicativo si $1 \in S$ y $ab \in S$ para todo $a, b \in S$.

En tal caso, definimos en $A \times S$ la relación $(a, s) \sim (a', s') \iff \exists t \in S, t(as' - a's) = 0$.

a) Demostrar que $\sim$ es una relación de equivalencia (Cuidado: S puede contener elementos no-nulos x, y tal que $xy = 0$). A la clase de equivalencia $[(a, s)]$ de (a, s) la denotaremos $\frac{a}{s}$ y al conjunto de clases de equivalencia lo denotaremos $A_S := (A \times S)/\sim$ y lo llamaremos la localización de A por S.

b) Demostrar que la función $f : A_S \times A_S \to A_S, (\frac{a}{s}, \frac{a'}{s'}) \mapsto \frac{aa'}{ss'}$ está bien definida (es decir, no depende del representante en la clase de equivalencia). Probar lo mismo para $f : A_S \times A_S \to A_S, (\frac{a}{s}, \frac{a'}{s'}) \mapsto \frac{as'+a's}{ss'}$.

c) Demostrar que usar f como producto y g como suma en A_S vuelven a A_S un anillo conmutativo en que los elementos de la forma $\frac{s}{1}$ son invertibles.

d) Demostrar que si S no contiene elementos x, y tal que $xy = 0$ entonces la función $i_S : A \hookrightarrow A_S, a \mapsto \frac{a}{1}$ es inyectiva. Demostrar además que siempre respeta $i_S(a \cdot b) = f(a, b),\ i_S(a + b) = g(a, b)$.

Cuando A es un dominio integral y $S = A \setminus \{0\}$ llamamos a A_S el cuerpo de fracciones de A y lo denotamos $\mathrm{Fr}(A)$.