APELLIDOS NOMBRE

Instrucciones. Escribir la respuesta a cada cuestión en hojas separadas. Entregar al final las hojas ordenadas por cuestiones. Durante la realización del examen exclusivamente se podrá disponer de material de escritura. Ningún otro objeto está permitido.

Ejercicio 1.

1) Dar justificadamente ejemplos de aplicaciones de $\mathbb{N}$ en $\mathbb{N}$ que sean:
   (a) Inyectiva pero no sobreyectiva.
   (b) Sobreyectiva pero no inyectiva.
   (c) Ni inyectiva ni sobreyectiva.
2) Sean X e Y conjuntos, $f\colon X \to Y$ una aplicación y $A, B \subset X$ subconjuntos. Probar que $f(A) \setminus f(B) \subset f(A \setminus B)$.
3) En la situación anterior, probar que si f es inyectiva entonces $f(A) \setminus f(B) = f(A \setminus B)$.
4) Dar un ejemplo de unos conjuntos X e Y, una aplicación $f\colon X \to Y$ y unos subconjuntos $A, B \subset X$ tales que $f(A) \setminus f(B) \subsetneqq f(A \setminus B)$.

Solución.

1)
   (a) La aplicación $f\colon \mathbb{N} \to \mathbb{N}$ definida por $f(x) = 3x$ es inyectiva, pues si $f(x) = f(y)$ entonces $3x = 3y$ de donde $x = y$. Pero no es sobreyectiva, pues no hay ningún $x \in \mathbb{N}$ tal que $f(x) = 1$.
   (b) La aplicación $f\colon \mathbb{N} \to \mathbb{N}$ definida por $f(x) = \lfloor x/3 \rfloor$ es sobre yectiva, pues para todo $y \in \mathbb{N}$ existe un numero, $3y \in \mathbb{N}$ tal que $f(3y) = y$. Sin embargo no es inyectiva, pues $f(0) = f(1) = 0$.
   (c) La aplicación $f\colon \mathbb{N} \to \mathbb{N}$ definida por $f(x) = 0$, es decir, la aplicación constante 0, no es inyectiva ni sobreyectiva.
2) Sea $y \in f(A) \setminus f(B)$. Entonces existe $x \in A$ tal que $f(x) = y$. Además $f(x) = y \notin f(B)$, de donde se deduce que $x \notin B$. Luego $y = f(x)$ con $x \in A \setminus B$. Es decir, $y \in f(A \setminus B)$.
3) Falta probar $f(A) \setminus f(B) \supset f(A \setminus B)$, pues la otra inclusión (más general) se ha probado en el apartado anterior.
   Sea $y \in f(A \setminus B)$, entonces existe $x \in A \setminus B$ tal que $y = f(x)$. Como $x \in A$, es claro que $y = f(x) \in f(A)$.
   Falta comprobar que $y = f(x) \notin f(B)$. Supongamos, por *reducción al absurdo*, que $y = f(x) \in f(B)$. Entonces, por la definición de imagen de un conjunto, se tiene que existe $x' \in B$ tal que $f(x') = y = f(x)$. Como f **es inyectiva**, se deduce que $x = x' \in B$. Lo cual es una contradicción, pues $x \in A \setminus B$.
   Por tanto, $y \in f(A) \setminus f(B)$.
4) Sean $X = \{a, b\}$ e $Y = \{c\}$ conjuntos. Sean $A = \{a\}$ y $B = \{b\}$ subconjuntos de X. Sea $f\colon X \to Y$ la aplicación definida por $f(a) = f(b) = c$. Es claro que $f(A) \setminus f(B) = \emptyset \subsetneqq f(A \setminus B) = f(A) = \{c\}$.

Ejercicio 2. En el conjunto $X = \{(x, y) \in \mathbb{R}^2 \mid x \neq 0\}$ se define la relación:

$$(a, b)\mathscr{R}(c, d) \Leftrightarrow \exists \lambda \in \mathbb{R} \setminus \{0\} \text{ tal que } c = \lambda a,\ d = \lambda b.$$

Se pide:

1) Probar que $\mathscr{R}$ es una relación de equivalencia en X.
2) Probar que $(a,b)\mathscr{R}(c,d)$ si y sólo si $b/a = d/c$.
3) Probar que los conjuntos $X/\mathscr{R}$ y $\mathbb{R}$ son equipotentes. (Indicación: Tomar la aplicación $f\colon X \to \mathbb{R}$ tal que $f(x,y) = y/x$ y usar la factorización canónica de f).

Solución.

1) Veamos que $\mathscr{R}$ es relación de equivalencia.
   - Propiedad reflexiva: Es evidente que $(a,b)\mathscr{R}(a,b)$, pues $a = 1 \cdot a$ y $b = 1 \cdot b$.
   - Propiedad simétrica: Supongamos que $(a,b)\mathscr{R}(c,d)$, entones existe un número real $\lambda \neq 0$ tal que $c = \lambda a$ y $d = \lambda b$. Despejando tenemos que $a = 1/\lambda b$ y $c = 1/\lambda d$, de donde $(c,d)\mathscr{R}(a,b)$.
   - Propiedad transitiva: Supongamos que $(a,b)\mathscr{R}(c,d)$ y que $(c,d)\mathscr{R}(e,f)$. Entonces existen dos números reales $\lambda, \mu \neq 0$ tales que $c = \lambda a$, $d = \lambda b$ y $e = \mu c$, $f = \mu d$. Combinando ambas propiedades se obtiene que $e = \mu c = \mu\lambda a$ y $f = \mu d = \mu\lambda b$. Luego existe un real no nulo $\delta = \mu\lambda$ tal que $e = \delta a$ y $f = \delta b$. Es decir, $(a,b)\mathscr{R}(e,f)$,
2) Hay que probar una doble implicación:
   $\Rightarrow$ Si $(a,b)\mathscr{R}(c,d)$ entonces existe $\lambda \neq 0$ tal que $c = \lambda a$ y $d = \lambda b$. Despejando en la primera igualdad se tiene que $\lambda = c/a$. Sustituyendo en la segunda tenemos $d = (c/a)b$, de donde $d/c = b/a$.
   $\Leftarrow$ Si $b/a = d/c$ entonces $d = (c/a)b$. Como $c = (c/a)a$, tomando $\lambda = c/a \neq 0$ se tiene que $c = \lambda a$ y $d = \lambda b$. Luego $(a,b)\mathscr{R}(c,d)$.
3) Consideremos como nos indican la aplicación $f\colon X \to \mathbb{R}$ tal que $f(x,y) = y/x$. La factorización canónica nos da el diagrama

$$\begin{tikzcd} X \arrow[r, "f"] \arrow[d, "\pi"'] & Y \\ X/\mathscr{R}_f \arrow[r, "\bar{f}"] & \mathrm{Im}(f) \arrow[u, "i"'] \end{tikzcd}$$

donde $\bar{f}$ es biyectiva y $\mathscr{R}_f$ es la relación dada por

$$(a,b)\mathscr{R}_f(c,d) \Leftrightarrow f(a,b) = f(c,d).$$

Si probamos que $X/\mathscr{R} = X/\mathscr{R}_f$ y que $\mathrm{Im}(f) = \mathbb{R}$ tendremos que $\bar{f}$ es una biyección entre ambos conjuntos y, por tanto, son equipotentes.
Las relaciones $\mathscr{R}$ y $\mathscr{R}_f$ son iguales, pues usando el apartado anterior

$$(a,b)\mathscr{R}_f(c,d) \Leftrightarrow f(a,b) = f(c,d) \Leftrightarrow b/a = d/c \Leftrightarrow (a,b)\mathscr{R}(c,d).$$

Luego $X/\mathscr{R} = X/\mathscr{R}_f$.
Por otro lado f es sobreyectiva, ya que para cada $\lambda \in \mathbb{R}$ se tiene que $f(1,\lambda) = \lambda$. En consecuencia $\mathrm{Im}(f) = \mathbb{R}$.
Se concluye que los conjuntos $X/\mathscr{R}$ y $\mathbb{R}$ son equipotentes, pues la aplicación $\bar{f}\colon X/\mathscr{R} \to \mathbb{R}$ es biyectiva.

Ejercicio 3. En S_8 consideramos las permutaciones $\sigma = (1\ 2\ 3\ 4)(5\ 6\ 7\ 8)$ y $\tau = (1\ 5\ 3\ 7)(2\ 8\ 4\ 6)$. Se pide:

1) Calcular todos los elementos del subgrupo $G = \langle \sigma, \tau \rangle$. (Indicación: hay 8 elementos, obsérvese que $\sigma^2 = \tau^2$ y $\sigma\tau = \tau\sigma^3$).
2) Calcular el orden de cada elemento de G.

3) Comprobar que G sólo contiene subgrupos cíclicos (salvo el propio G).

Solución.

1) En efecto comprobamos que

$$\sigma^2 = (1\ 3)(2\ 4)(5\ 7)(6/8) = \tau^2 \text{ y}$$

$$\sigma\tau = (1\ 6\ 3\ 8)(2\ 5\ 4\ 7) = \tau^3\sigma.$$

De la segunda igualdad deducimos que cada elemento del grupo G puede escribirse en la forma $\sigma^n\tau^m$. Es más, como $\sigma^4 = \tau^4 = ()$, podemos reducir la expresión anterior a los valores de m y n entre 0 y 3. Es decir, al conjunto

$$\{\sigma^n\tau^m \mid 0 \leq m, n \leq 3\}$$

que en principio parece tener 16 elementos.
Sin embargo, la primera igualdad $\sigma^2 = \tau^2$ iguala los elementos del conjunto anterior dos a dos: $() = \sigma^2\tau^2$, $\sigma = \sigma^3\tau^2$, $\sigma^2 = \tau^2$, $sigma^3 = \sigma\tau^2$, $\tau = \sigma^2\tau^3$, $\sigma\tau = \sigma^3\tau^3$, $\sigma^2\tau = \tau^3$ y $\sigma^3\tau = \sigma\tau^3$.
Lo cual reduce el conjunto G a 8 elementos:

$$G = \{\sigma^n\tau^m \mid 0 \leq n \leq 3,\ 0 \leq m \leq 1\}.$$

Calculándolos comprobamos que son todos distintos (dejamos ese cálculo como ejercicio).

2) Una vez calculados todos los elementos del grupo no es difícil calcular el orden de cada uno de ellos.
De hecho todos los elementos del grupo, salvo $()$ y σ^2, tienen orden cuatro, pues son producto de dos ciclos disjuntos de longitud 4. Además $o(()) = 1$ y $o(\sigma^2) = 2$.

3) Por el teorema de Lagrange, los subgrupos de G distintos de G tienen orden 1, 2 o 4. El grupo de orden 1, $\{()\} = \langle()\rangle$, es cíclico. También lo son los grupos de orden 2, que sólo hay uno al haber un único elemento de orden 2: $\{(), \sigma^2\} = \langle\sigma^2\rangle$.
Quedan estudiar los subgrupos de orden 4. Un grupo de orden 4 tiene elementos de orden 1, 2 o 4, también por el teorema de Lagrange. De hecho, un grupo de orden 4 es cícclico si y sólo si contiene algún elemeto de orden 4.
Por tanto, si un grupo de orden 4 no es cíclico está formado por un elemento de orden 1 (el elemento neutro) y tres de orden 2. Dado que en G sólo hay un elemento de orden 2, no puede conteer ningún subgrupo no cíclico de orden 4.
Luego se concluye que G sólo contiene subgrupos cíclicos (salvo el propio G).

Ejercicio 4.

1) Enunciar el teorema de Lagrange. Probar que el orden de un elemento de un grupo finito divide al orden del grupo.
2) Probar que todo grupo de orden primo es cíclico.
3) Probar que todo grupo de orden 4 es abeliano.
4) Probar que el menor orden posible de un grupo **no abeliano** es 6.

Solución.

1) Teorema de Lagrange: Si G es un grupo finito y $H \subset G$ es un subgrupo, entonces $|H|$ divide a $|G|$.
Sean G un grupo finito y $x \in G$. El grupo cíclico $\langle x\rangle$ es un subgrupo de G del mismo orden que $o(x)$. Por el teorema de Lagrange, el orden de $\langle x\rangle$ divide al orden de G. Luego $o(x)$ divide a $|G|$.

2) Sea G un grupo de orden p primo, entonces G tiene al menos dos elementos, es decir, al menos uno es distinto del elemento neutro.
   Sea entonces $x \in G$ un elemento distinto del elemento neutro. Por el apartado anterior, $o(x)$ divide a $|G| = p$. Por ser p primo, $o(x)$ debe ser 1 o p. Como x no es el elemento neutro su orden es p. Luego $\langle x \rangle$ es un subgrupo de G de orden p. Por tanto $G = \langle x \rangle$ es cíclico.
3) Todo grupo cíclico es abeliano.
   Si un grupo G de orden 4 no es cíclico entonces está compuesto por un elemento de orden 1 y tres de orden 2. Es decir, si $x \in G$ es un elemento del grupo entonces $x^2 = e$ (siendo e el elemento neutro). Entonces si $x, y \in G$ se verifica que

$$x^2y^2 = e = (xy)^2.$$

   De donde $xxyy = xyxy$, multiplicando por x^{-1} a la izquierda e y^{-1} a la derecha, se tiene que $xy = yx$. Luego el grupo es abeliano.
4) El grupo de un elemento es cíclico, luego abeliano. Por el apartado 2 sabemos que los grupos de orden 2, 3 y 5 son también cíclicos, luego son abelianos. Por el apartado 3, los grupos de orden 4 son abelianos.
   Luego si un grupo no es abeliano debe tener al menos orden 6. El grupo S_3 de las permutaciones de 3 elementos no es abeliano y tiene orden 6. Luego efectivamente el menor orden **posible** de un grupo **no abeliano** es 6.

"Los métodos que he establecido no requieren construcciones ni razonamientos geométricos o mecánicos: sólo operaciones algebraicas, sujetas a una regla de procedimiento regular y uniforme."
Joseph-Louis de Lagrange