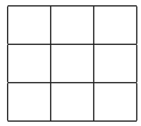
Estructuras Algebraicas
Prof. Giancarlo Lucchini
Ay. Claudio Bravo, Juan Pablo Llerena

UNIVERSIDAD DE CHILE
Facultad de Ciencias
Licenciatura en Ciencias Matemáticas

Prueba 2

Viernes 22 de octubre de 2021

Ejercicio 1. Considere un tablero cuadrado de 3×3 como el siguiente:



Encuentre la cantidad de maneras esencialmente distintas (es decir, salvo rotaciones) en las que se puede colorear las casillas de dicho tablero usando 3 colores. Justifique su respuesta. Puede usar calculadora para obtener el número final.

Demostración. Aplicaremos el Teorema de conteo de Burnside para encontrar el número buscado. El grupo que actúa es el grupo de *rotaciones* del cuadrado, es decir $G = \langle r \rangle = \{1, r, r^2, r^3\}$, donde r es la rotación en 90 grados (nótese que r tiene efectivamente orden 4).

Para contar las coloraciones esencialmente distintas, debemos contar las órbitas de la acción de G sobre el conjunto de coloraciones. Por el Teorema de conteo de Burnside (Teorema 9.19), el número de órbitas de esta acción es

$$k = \frac{1}{|G|} \sum_{g \in G} |C_g| = \frac{1}{4}(|C_1| + |C_r| + |C_{r^2}| + |C_{r^3}|),$$

donde C es el conjunto de coloraciones posibles y C_g el conjunto de coloraciones fijas por el elemento $g \in G$. Calculemos pues los conjuntos C_g para $g \in G$:

- Para $g = 1$, vemos que toda coloración queda fija, por lo que $|C_g| = |C| = 3^9$.
- Para $g = r$, vemos que una coloración fija por r tiene un color arbitrario al centro, pero debe tener las cuatro esquinas iguales y las cuatro casillas restantes iguales también. Esto deja 3 elecciones de colores en total, por lo que $|C_r| = 3^3$.
- Para $g = r^3 = r^{-1}$ el análisis es el mismo, puesto que se trata de una rotación en 90 grados en el sentido opuesto. Por lo tanto $|C_{r^3}| = 3^3$.
- Para $g = r^2$, vemos que una coloración queda fija si cada casilla tiene el mismo color que la casilla diametralmente opuesta. Esto deja una elección de 5 colores (la casilla central y las cuatro parejas de casillas opuestas), por lo que $|C_{r^2}| = 3^5$.

Luego de este análisis, tenemos entonces que el número total de coloraciones esencialmente distintas del tablero es

$$k = \frac{1}{4}(3^9 + 3^3 + 3^5 + 3^3) = 4995.$$

Nótese que este resultado también se puede obtener usando la Proposición 9.21 y el hecho que, si numeramos las casillas del tablero de la forma usual, entonces r corresponde a la permutación $(1\,7\,9\,3)(2\,4\,8\,6)$. $\square$

Ejercicio 2. Sea G un grupo actuando sobre un conjunto X y sea $\mathcal{O}$ una órbita de la acción. Para $x \in \mathcal{O}$, sea G_x el estabilizador de x en G.

1. Demuestre que si no existe otra órbita para esta acción, entonces $|X| \leq |G|$.
2. Sea $x \in \mathcal{O}$. Demuestre que $G_x = G_y$ para todo $y \in \mathcal{O}$ si y sólo si G_x es normal en G.
3. Sea $x \in \mathcal{O}$ tal que $G_x \lhd G$. Demuestre que el grupo cociente G/G_x actúa sobre $\mathcal{O}$ vía la fórmula $(gG_x)y := gy$ para $gG_x \in G/G_x$ e $y \in \mathcal{O}$.

Demostración. Vamos por orden.

1. Si no hay más órbitas, entonces $|X| = |\mathcal{O}|$ y, por la fórmula órbita-estabilizador (Teorema 9.11) tenemos que $|\mathcal{O}| = [G : G_x]$ para algún $x \in \mathcal{O}$. En particular, como $[G : G_x] = |G|/|G_x|$ por el Teorema de Lagrange, vemos que $|\mathcal{O}|$ debe dividir a $|G|$ y por lo tanto $|X| \leq |G|$.

2. Sea $y \in \mathcal{O}$ y sea $g \in G$ un elemento tal que $gx = y$ (que existe por la mera definición de órbita). Entonces, por la demostración del Lema 9.18, tenemos que $G_y = gG_xg^{-1}$.

   Así, si G_x es normal en G, entonces $G_x = gG_xg^{-1}$ para todo $g \in G$ (Teorema 6.3), por lo que en particular tenemos que $G_x = G_y$ para todo $y \in \mathcal{O}$.

   Por otra parte, supongamos que $G_x = G_y$ para todo $y \in \mathcal{O}$. Sea $g \in G$ y sea $y = gx$. Como $y \in \mathcal{O}$ por la definición de órbita, entonces $G_x = G_y = gG_xg^{-1}$. Como esto vale para un $g \in G$ arbitrario, tenemos que G_x es normal en G por el Teorema 6.3.

3. Probemos ante todo que la función

$$(G/G_x) \times \mathcal{O} \to \mathcal{O} \,:\, (gG_x, y) \mapsto (gG_x)y = gy,$$

   está bien definida. Supongamos que $gG_x = hG_x$. Entonces $h^{-1}g \in G_x$. Como además sabemos que $G_y = G_x$ por la pregunta anterior, tenemos que $h^{-1}g \in G_y$. Así $h^{-1}gy = y$ y por lo tanto, multiplicando ambos lados por h a la izquierda, vemos que $gy = hy$.

   Para verificar que la función es una acción, basta ver que $(eG_x)y = ey = y$ para todo $y \in \mathcal{O}$ y que

$$(gG_x)[(hG_x)y] = (gG_x)(hy) = g(hy) = (gh)y = (ghG_x)y = [(gG_x)(hG_x)]y,$$

   para todo $g, h \in G$ y todo $y \in \mathcal{O}$.

$\square$

Ejercicio 3. Sea $\mathbb{H} = \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{R}\}$ el anillo de cuaterniones.

1. Encuentre subanillos de $\mathbb{H}$ isomorfos a $\mathbb{R}$ y $\mathbb{C}$ respectivamente.
2. Encuentre todos los ideales de $\mathbb{H}$.
3. Pruebe que el anillo $\mathbb{R}[x]/\langle x^2 + 1\rangle$ es isomorfo a $\mathbb{C}$.
4. ¿Existe un ideal I de $\mathbb{R}[x]$ tal que $\mathbb{R}[x]/I$ sea isomorfo a $\mathbb{H}$?

Demostración. Vamos por orden:

1. Consideremos los homomorfismos de anillos
$$\varphi_1 : \mathbb{R} \to \mathbb{H} : a \mapsto a \qquad \text{y} \qquad \varphi_2 : \mathbb{C} \to \mathbb{H} : a + bi \mapsto a + bi.$$
Dadas las fórmulas de suma y multiplicación en $\mathbb{H}$ (en particular, $i^2 = -1$), vemos claramente que φ_1y φ_2 son homomorfismos de anillos (de hecho, φ_1 es la restricción de φ_2 al subanillo $\mathbb{R} \subset \mathbb{C}$). Como además el núcleo es claramente $\{0\}$ para ambos, las imágenes respectivas son subanillos de $\mathbb{H}$ isomorfos a $\mathbb{R}$ y $\mathbb{C}$ respectivamente por el primer teorema de isomorfía.

2. Evidentemente, tenemos el ideal trivial $\{0\}$. Sea entonces $I \subset \mathbb{H}$ un ideal distinto de $\{0\}$ y sea $x \in I$ no nulo. Sabemos que $\mathbb{H}$ es un álgebra de división, por lo que existe un elemento $x^{-1} \in \mathbb{H}$ tal que $x^{-1}x = 1$. Como I es un ideal, vemos que $1 = x^{-1}x \in I$ y por lo tanto $I = \mathbb{H}$ ya que para todo $h \in \mathbb{H}$ tenemos que $h = h1$ y $1 \in I$. Esto prueba que los únicos ideales de $\mathbb{H}$ son los triviales: $\{0\}$ y $\mathbb{H}$.

3. Consideremos el homomorfismo de evaluación en i:
$$\phi : \mathbb{R}[x] \to \mathbb{C} : P \mapsto P(i).$$
Se trata claramente de un homomorfismo sobreyectivo ya que para todo $a+bi \in \mathbb{C}$ tenemos que $\phi(bx + a) = a + bi$. Por otra parte, si $P \in \ker(\phi)$, entonces $P(i) = 0$. Aplicando conjugación compleja a esta igualdad y recordando que los coeficientes de P son reales, vemos también que $P(-i) = P(\bar{i}) = \overline{P(i)} = \overline{0} = 0$. Así, vemos que tanto i como $-i$ son raíces del polinomio, o bien que $(x - i)$ y $(x + i)$ dividen a P, o bien que $(x - i)(x + i) = x^2 + 1$ divide a P. En otras palabras, tenemos que $\ker(\phi) \subset \langle x^2 + 1\rangle$. Pero como también tenemos que $\phi(x^2 + 1) = i^2 + 1 = 0$, vemos que $x^2 + 1 \in \ker(\phi)$ y por lo tanto $\langle x^2 + 1\rangle \subset \ker(\phi)$ ya que $\ker(\phi)$ es un ideal. Tenemos entonces que $\ker(\phi) = \langle x^2 + 1\rangle$ y obtenemos entonces el isomorfismo pedido por el primer teorema de isomorfía.

4. No, puesto que $\mathbb{R}[x]$ es un anillo conmutativo y por lo tanto todo anillo cociente $\mathbb{R}[x]/I$ ha de ser conmutativo también ya que hereda la multiplicación de $\mathbb{R}[x]$. Sin embargo, sabemos bien que $\mathbb{H}$ no es conmutativo puesto que $ij \neq ji$. Así, es imposible que $\mathbb{H}$ sea un cociente de $\mathbb{R}[x]$ por un ideal.

$\square$

Ejercicio 4 (Verdadero o Falso)**.** Diga si cada una de las siguientes afirmaciones es verdadera o falsa. Justifique su respuesta. Una respuesta sin justificar vale 0 puntos.

1. Sea D un dominio de integridad y sea $S \subset D$ un subanillo. Entonces S es un dominio de integridad.
2. Si R es un anillo conmutativo de característica p prima y $S \subset R$ es un subanillo distinto de $\{0\}$, entonces S tiene característica p.
3. Sean R_1, R_2 anillos conmutativos unitarios y sean $I_1 \subset R_1$, $I_2 \subset R_2$ ideales maximales respectivos. Entonces $I_1 \times I_2$ es un ideal maximal de $R_1 \times R_2$.
4. Sean $I, J \subset R$ dos ideales primos distintos de un anillo conmutativo y unitario. Entonces $I \cap J$ es un ideal primo.

Demostración. Vamos por orden:

1. **Falso.** Sea $D = \mathbb{Z}$ y $S = 2\mathbb{Z}$. Es claro que S es un subanillo ya que es un ideal de $\mathbb{Z}$. Pero $2\mathbb{Z}$ no es un anillo unitario ya que $1 \notin 2\mathbb{Z}$. Esto implica que $2\mathbb{Z}$ no es un dominio de integridad.

2. **Verdadero.** En efecto, si $s \in S$ es un elemento no nulo, su orden en el grupo aditivo $(S, +)$ es mayor que 1. Sin embargo, s es un elemento no nulo de R también, por lo que $ps = s+s+\cdots+s = 0$ ya que la característica de R es p. Esto nos dice que el orden aditivo de s es un divisor de p distinto de 1, por lo que sólo puede ser p ya que se trata de un primo. Esto prueba que la característica de S es por lo menos p ya que nos es imposible anular a s con un número más pequeño. Por otra parte, como la igualdad $ps = s + s + \cdots + s = 0$ es cierta para todo $s \in S$, vemos que la característica de S es precisamente p.

3. **Falso.** Basta considerar $R_1 = R_2 = \mathbb{Q}$, $I_1 = I_2 = \{0\}$. Nótese que $\{0\} \subset \mathbb{Q}$ es efectivamente maximal ya que el cociente es, trivialmente, un cuerpo (Teorema 10.35). Ahora, el ideal $\mathbb{Q} \times \{0\}$ es claramente más grande que $\{0\} \times \{0\}$ y no es igual a $\mathbb{Q} \times \mathbb{Q}$, por lo que $\{0\} \times \{0\}$ no es maximal.

4. **Falso.** Basta considerar $R = \mathbb{Z}$, $I = 2\mathbb{Z}$ y $J = 3\mathbb{Z}$. En ese caso, vemos que I, J son ideales primos distintos (Ejemplo 10.39). Y claramente $2\mathbb{Z} \cap 3\mathbb{Z} = 6\mathbb{Z}$ no es un ideal primo ya que $6 = 2 \cdot 3 \in 6\mathbb{Z}$ pero $2, 3 \notin 6\mathbb{Z}$.

□