

Problemas de Álgebra Abstracta

Roberto Hernando Velasco

8 de abril de 2005

1. Teoría de Grupos

1.1. Generalidades

Ejercicio 1.1. Dada una recta r en el plano \mathbb{R}^2 se llama simetría respecto de r a la aplicación

$$\sigma_r : \mathbb{R}^2 \rightarrow \mathbb{R}^2$$

que deja fijos los puntos de r y transforma todo punto $P \notin r$ en el único punto Q , situado en la perpendicular a r que pasa por P , que cumple

$$\text{dist}(P, r) = \text{dist}(Q, r).$$

Si O es un punto de \mathbb{R}^2 , la simetría respecto de O es la aplicación

$$\sigma_o^2 : \mathbb{R}^2 \rightarrow \mathbb{R}^2$$

que deja fijo O y transforma $P \neq O$ en el único punto Q que cumple

$$\overrightarrow{OP} = -\overrightarrow{OQ}.$$

Si

$$1 : \mathbb{R}^2 \rightarrow \mathbb{R}^2$$

es la aplicación identidad, demuestre que dadas dos rectas perpendiculares r y s , que se cortan en O , el conjunto $V = \{1, \sigma_r, \sigma_s, \sigma_o\}$ es un grupo abeliano con la operación composición de aplicaciones.¹

Ejercicio 1.2. Pruebe que todo grupo con cuatro elementos es abeliano.

Solución. Sea G un grupo de orden 4. Distinguiamos dos posibilidades:

CASO 1. $a^2 = 1$ para cada $a \in G$.

Entonces G es abeliano.

CASO 2. Existe $a \in G$ tal que $a^2 \neq 1$.

Entonces el orden de a , $\text{ord}(a)$, que divide a 4 por el teorema de Lagrange, no es ni 1 ni 2. Se concluye que $\text{ord}(a) = 4 = \text{ord}(G)$, luego $G = \langle a \rangle$ es cíclico y, en particular, abeliano.

¹Éste es el llamado grupo de Klein.

Ejercicio 1.3. Supongamos que en el grupo G se tiene

$$(ab)^n = a^n b^n$$

para cada $a, b \in G$ y tres naturales consecutivos n . Demuestre que G es abeliano.

Solución. Sean $m, m + 1, m + 2$ dichos naturales consecutivos. Dados $a, b \in G$, probemos que $ab = ba$.

Por la hipótesis

$$(ab)^m = a^m b^m$$

y también

$$(ab)^{m+1} = a^{m+1} b^{m+1}.$$

Sustituyendo,

$$a^{m+1} b^{m+1} = (ab)^{m+1} = (ab)^m ab = a^m b^m ab$$

y simplificando

$$ab^m = b^m a \tag{1}$$

Como

$$(ab)^{m+2} = a^{m+2} b^{m+2}, \tag{2}$$

se tiene

$$a^{m+2} b^{m+2} = (ab)^{m+2} = (ab)^{m+1} ab = a^{m+1} b^{m+1} ab$$

luego simplificando

$$ab^{m+1} = b^{m+1} a.$$

Podemos ahora escribir

$$ab^m b = b^{m+1} a$$

y, utilizando (1),

$$b^m ab = b^{m+1} a.$$

Simplificando una vez más,

$$ab = ba.$$

Ejercicio 1.4. Encuentre un grupo G y elementos a, b de G tales que $\text{ord}(a)$ y $\text{ord}(b)$ sean primos entre sí, pero $\text{ord}(ab) \neq \text{ord}(a) \text{ord}(b)$.

Solución. Basta tomar $G = D_3$, a el giro de ángulo $\frac{2\pi}{3}$ y b la simetría respecto de la recta que une el centro y un vértice del triángulo regular.

Ejercicio 1.5. Sean G un grupo, H un subgrupo de G y $x \in G$. Sea m un número natural que no tiene ningún factor² con $\text{ord}(x)$. Demuestre que si $x^m \in H$ entonces $x \in H$.

²Es decir, es primo

Solución. Sea $n = \text{ord}(x)$. Como m y n son primos entre sí, se tiene que $am + bn = 1$ para ciertos enteros a y b .

Entonces

$$x = x^{am+bn} = (x^m)^a (x^n)^b = (x^m)^a \in H,$$

pues $x^m \in H$.

Ejercicio 1.6. *¿Es cierto que el producto directo de dos grupos cíclicos también es cíclico?*

Solución. No; basta tomar $G_1 = \mathbb{Z} = G_2$ con la operación suma.

Ejercicio 1.7. *Sea G un grupo finito de orden impar, y sea $x \in G$. Demuestre que existe $y \in G$ tal que $x = y^2$.*

Solución. Como $n = \text{ord}(G)$ es impar, m. c. d. $(2, n) = 1$. Luego, $1 = 2a + nb$ para ciertos enteros a y b . En consecuencia,

$$x = x^{2a+nb} = (x^a)^2 (x^n)^b.$$

Como $\text{ord}(x) = m$ divide a $\text{ord}(G) = n$ por el teorema de Lagrange, se deduce que $x^n = 1$, luego $(x^n)^b = 1$.

Por tanto, el elemento $y = x^a$ cumple $x = y^2$.

Ejercicio 1.8. *Sea G un grupo no finito. ¿Posee G una cantidad no finita de subgrupos?*

Solución. Distinguimos dos casos:

CASO 1. Existe $a \in G$ que no es de torsión. Entonces los subgrupos $H_k = \langle a^k \rangle$, $k \in \mathbb{N} \setminus \{0\}$, son todos distintos ya que si $H_k = H_l$ para algunos k y l distintos, se tendría

$$a^k \in \langle a^l \rangle \text{ y } a^l \in \langle a^k \rangle,$$

y, por lo tanto, $a^k = (a^l)^n$, $a^l = (a^k)^m$ para ciertos enteros m y n .

Esto implica que $a^{ln-k} = a^{km-l} = 1$, y como a no es de torsión, se deduce que $ln - k = 0 = km - l$, y de aquí

$$kmn = ln = k,$$

luego $mn = 1$. De donde $m = n = 1$, con lo que $l = k$, que es falso, o $m = n = -1$ y $l = -k$, que también es falso, ya que $l, k \in \mathbb{N} \setminus \{0\}$.

En conclusión, hemos encontrado una familia no finita $\{H_k : k \in \mathbb{N} \setminus \{0\}\}$.

CASO 2. Supongamos ahora que cada $x \in G$ es de torsión. Evidentemente

$$G = \bigcup_{x \in G} \langle x \rangle.$$

Como x es de torsión, cada $\langle x \rangle$ es finito. Al ser G no finito, debe existir una cantidad no finita de miembros distintos en dicha unión.

Por ello, también en este caso G posee una cantidad no finita de subgrupos.

(De hecho, en ambos casos hemos probado que G posee una cantidad no finita de subgrupos cíclicos)

1.2. Subgrupos normales. Homomorfismos.

Ejercicio 1.9. Sean G un grupo y H un subgrupo propio de G tal que $H^a = H^b$ para cada $a, b \in G \setminus H$. Demuestre que G no es simple³.

Solución. Vamos a calcular el número de subgrupos de G conjugados de H . Es evidente que $H^x = H$ para cada x de H . En consecuencia, eligiendo $a \in G \setminus H$ y $x \in H$, la familia de conjugados distintos del subgrupo H es

$$\{H^a, H^x = H\}.$$

- Si $H^a = H$ todos los conjugados de H coinciden y H es subgrupo normal propio de G .
- Si $H^a \neq H$, entonces

$$[G : N_G(H)] = 2,$$

siendo $N_G(H) = \{a \in G : H^a = H\}$ el normalizador de H en G . En consecuencia, $N_G(H)$ es un subgrupo normal de G . Además, es propio pues

$$\{1\} \subset H \subset N_G(H) \subset G,$$

siendo todas las contenciones estrictas.

Por tanto, en ambos casos, G es simple.

Ejercicio 1.10. Conteste las siguientes cuestiones:

1. ¿Existen enteros positivos distintos m y n tales que \mathbb{Z}_m^* y \mathbb{Z}_n^* sean isomorfos?
2. ¿Existe algún entero positivo m tal que el número de homomorfismos inyectivos $\mathbb{Z}/m\mathbb{Z} \rightarrow \mathbb{Z}/100\mathbb{Z}$ coincida con el número de homomorfismos sobreyectivos $\mathbb{Z}/30\mathbb{Z} \rightarrow \mathbb{Z}/15\mathbb{Z}$? Calcúlese m si existe.
3. Calcule el número de homomorfismos $\mathbb{Z}/36\mathbb{Z} \rightarrow \mathbb{Z}/48\mathbb{Z}$. ¿Hay alguno inyectivo? ¿Y sobreyectivo?

Solución. 1. Considérese $m = 4$ y $n = 3$. Así

$$\text{ord}(\mathbb{Z}_4^*) = \phi(4) = \phi(2^2) = 2(2-1) = 2,$$

mientras que

$$\text{ord}(\mathbb{Z}_3^*) = \phi(3) = 3-1 = 2,$$

donde ϕ es la función de Euler.

Como 2 es primo, tanto \mathbb{Z}_4^* como \mathbb{Z}_3^* son cíclicos de orden 2, luego isomorfos a $\mathbb{Z}/2\mathbb{Z}$ y por lo tanto isomorfos entre sí.

³ $H^a = a^{-1}Ha$

2. Como 15 divide a 30, el número de isomorfismos sobreyectivos $\mathbb{Z}/30\mathbb{Z} \rightarrow \mathbb{Z}/15\mathbb{Z}$ es $\phi(15) = \phi(3) \cdot \phi(5) = 2 \cdot 4 = 8$.

Se trata pues de estudiar si existe un divisor m de 100 tal que $\phi(m) = 8$. Como $100 = 2^2 \cdot 5^2$, el número m se escribirá

$$m = 2^a \cdot 5^b, \quad 0 \leq a \leq 2, \quad 0 \leq b \leq 2.$$

Si $ab = 0$, será $m = 2^a$ o $m = 5^b$. Como $\phi(2^a) = 2^{a-1}(2-1) = 2^{a-1}$ con $0 \leq a \leq 2$, $\phi(2^a) \neq 8$.

Como $\phi(5^b) = 5^{b-1}(5-1)$, para que fuese $\phi(5^b) = 8$ debería ser $5^{b-1} = 2$, lo que es imposible.

Así pues $ab \neq 0$, con lo que

$$8 = \phi(m) = \phi(2^a)\phi(5^b) = 2^{a-1}5^{b-1}(5-1),$$

y de aquí

$$2 = 2^{a-1}5^{b-1} \implies 2^{2-a} = 5^{b-1}.$$

Es decir

$$2 - a = 0, \quad b - 1 = 0,$$

luego $a = 2$, $b = 1$ y la única solución es $m = 20$.

3. El número de isomorfismos entre $\mathbb{Z}/36\mathbb{Z}$ y $\mathbb{Z}/48\mathbb{Z}$ es

$$\text{m. c. d.}(36, 48) = 12.$$

No hay ninguno inyectivo porque 36 no divide a 48 y tampoco los hay sobreyectivos porque 48 no divide a 36.

Ejercicio 1.11. Sean G un grupo y $c \in G$. Definimos en G otra operación mediante

$$a * b = acb.$$

Demuestre que con la nueva operación G es un grupo isomorfo al de partida.

Solución. Basta considerar $f : G \rightarrow G$, $f(x) = c^{-1}x$.

1.3. Estructura de los grupos abelianos finitos.

Ejercicio 1.12. Demuestre que en un grupo abeliano finito, el producto de dos elementos de orden mayor que dos es 1.

Solución. Sea G un grupo abeliano de orden n y sea M el conjunto de los elementos de orden mayor que dos.

Para cada $x \in M$, $x^{-1} \in M$ ya que $\text{ord}(x^{-1}) = \text{ord}(x)$. Además $x^{-1} \neq x$ pues en caso contrario $x^2 = 1$ y $\text{ord}(x) \leq 2$.

Entonces $\{A_x : x \in M\}$ constituye una partición de M , donde $A_x = \{x, x^{-1}\}$. Así M tiene un número par $2l$ de elementos y

$$M = \{x_1, x_1^{-1}, x_2, x_2^{-1}, \dots, x_l, x_l^{-1}\},$$

por lo que el producto de los elementos de M es

$$x_1 x_1^{-1} \cdots x_l x_l^{-1} = 1.$$

2. Teoría de cuerpos. Extensiones algebraicas

2.1. Generalidades. Polinomios mínimos

Ejercicio 2.1. Encontrar sobre \mathbb{Q} el polinomio mínimo de $\frac{\sqrt{3}(i-1)}{2}$.

Solución. Sea $\alpha = \frac{\sqrt{3}(i-1)}{2}$. Operando se llega a que $\alpha^4 = -\frac{9}{4}$. Veamos que el polinomio mínimo de α sobre \mathbb{Q} es $m_\alpha(X) = X^4 + \frac{9}{4}$.

Como $4X^4 + 9$ no tiene raíces enteras (se puede comprobar aplicando el algoritmo de Ruffini), tampoco las tiene en \mathbb{Q} . Por tanto $m_\alpha(X) = X^4 + \frac{9}{4}$ no tiene raíces en \mathbb{Q} ; luego $m_\alpha(X)$ no se puede descomponer como producto de un polinomio de grado 1 y otro de grado 3.

Si $m_\alpha(X)$ se pudiese descomponer como producto de dos polinomios de grado 2, se tendría

$$X^4 + \frac{9}{4} = (X^2 + aX + b)(X^2 + cX + d)$$

y operando e igualando coeficientes se ve que no existen $a, b, c, d \in \mathbb{Q}$ cumpliendo esto.

Luego $m_\alpha(X)$ es irreducible con lo que es el polinomio mínimo de α .

Ejercicio 2.2. Demostrar que $\mathbb{Q}(\sqrt{3} + \sqrt{5}) = \mathbb{Q}(\sqrt{3}, \sqrt{5})$.

Solución. Como $\sqrt{3} + \sqrt{5} \in \mathbb{Q}(\sqrt{3}, \sqrt{5})$ se tiene que $\mathbb{Q}(\sqrt{3} + \sqrt{5}) \subseteq \mathbb{Q}(\sqrt{3}, \sqrt{5})$.

La otra contención es difícil de ver, por lo que se utilizan los grados.

$\sqrt{5} \notin \mathbb{Q}[\sqrt{3}] = \mathbb{Q}(\sqrt{3}) \Rightarrow \mathbb{Q}(\sqrt{3}) \subsetneq \mathbb{Q}(\sqrt{3}, \sqrt{5}) = \mathbb{Q}(\sqrt{3})(\sqrt{5})$.

$[\mathbb{Q}(\sqrt{3}, \sqrt{5}) : \mathbb{Q}(\sqrt{3})] = 2$, ya que $x^2 - 5$ es el polinomio mínimo de $\sqrt{5}$ sobre $\mathbb{Q}(\sqrt{3})$.

$[\mathbb{Q}(\sqrt{3}, \sqrt{5}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{3}, \sqrt{5}) : \mathbb{Q}(\sqrt{3})] \cdot [\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2 \cdot 2 = 4$

$[\mathbb{Q}(\sqrt{3} + \sqrt{5}) : \mathbb{Q}] > 2$, ya que si fuese 2, existiría $P(X) = X^2 + aX + b \in \mathbb{Q}[X]$ tal que $P(\sqrt{3} + \sqrt{5}) = 0$, lo que es absurdo.

$4 = [\mathbb{Q}(\sqrt{3}, \sqrt{5}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{3}, \sqrt{5}) : \mathbb{Q}(\sqrt{3} + \sqrt{5})] \cdot \overbrace{[\mathbb{Q}(\sqrt{3} + \sqrt{5}) : \mathbb{Q}]}^{>2}$ luego $[\mathbb{Q}(\sqrt{3}, \sqrt{5}) : \mathbb{Q}(\sqrt{3} + \sqrt{5})] = 1$.

Por lo cual $\mathbb{Q}(\sqrt{3}, \sqrt{5}) = \mathbb{Q}(\sqrt{3} + \sqrt{5})$.

2.2. Órbitas

Ejercicio 2.3. Se tienen bolas de dos colores. ¿Cuántos collares distintos se pueden hacer con ocho bolas?

2.3. Grupo de Galois

Ejercicio 2.4. Obténgase el cuerpo de descomposición en \mathbb{C} del polinomio $X^4 - 4X^2 - 1 \in \mathbb{Q}[X]$. Obténgase el grupo de Galois y muéstrense las biyecciones entre los subgrupos del grupo de Galois y los cuerpos intermedios de la extensión $\Sigma_f|_{\mathbb{Q}}$.

Solución. Sea $f(x) = x^4 - 4x^2 - 1$. Las soluciones de $f(x) = 0$ son $x = \pm\sqrt{2 \pm \sqrt{5}}$. Se tiene que $\mathcal{K} = \mathbb{Q}(\sqrt{2 + \sqrt{5}}, \sqrt{2 - \sqrt{5}}) = \mathbb{Q}(\sqrt{2 + \sqrt{5}}, i)$, y que $[\mathcal{K} : \mathbb{Q}(\sqrt{2 + \sqrt{5}})] = 2$, $[\mathbb{Q}(\sqrt{2 + \sqrt{5}}) : \mathbb{Q}] = 4$. Entonces $[\mathcal{K} : \mathbb{Q}] = 8$, luego $\sharp G(\Sigma_{f|Q}) = 8$.

Sea $\alpha = \sqrt{2 + \sqrt{5}}$. Se tienen los siguientes automorfismos:

$$\sigma_0 : \alpha \rightarrow \alpha, i \rightarrow i$$

$$\sigma_1 : \alpha \rightarrow -\alpha, i \rightarrow i$$

$$\sigma_2 : \alpha \rightarrow i\alpha^{-1}, i \rightarrow i$$

$$\sigma_3 : \alpha \rightarrow -i\alpha^{-1}, i \rightarrow i$$

$$\tau : \alpha \rightarrow \alpha, i \rightarrow -i$$

$$\sigma_1\tau : \alpha \rightarrow -\alpha, i \rightarrow -i$$

$$\sigma_2\tau : \alpha \rightarrow i\alpha^{-1}, i \rightarrow -i$$

$$-i$$

$$\sigma_3\tau : \alpha \rightarrow -i\alpha^{-1}, i \rightarrow -i$$

$$-i$$

$$\sigma_0 : \alpha \rightarrow \alpha, i \rightarrow i$$