

Problemas de Estructuras Algebraicas

Rafael Arquero Gimeno @_arkeros
Helena Garv Casas

16 de noviembre de 2014

ndice

1. Grupos	2
2. Anillos	11

ndice de figuras

ndice de cuadros

1. Grupos

1. Sea E un espacio vectorial sobre un cuerpo K . Determina si los siguientes conjuntos con las operaciones indicadas son grupos o no:

- (a) $(\mathbb{N}, +)$
- (b) $(\mathbb{Q}, +)$
- (c) (\mathbb{Q}, \cdot)
- (d) $(S^1 := \{z \in \mathbb{C} : |z| = 1\}, \cdot)$
- (e) $(P_n := \{p(x) \in \mathbb{R}[x] : \text{gr}(p(x)) \leq n\}, +)$
- (f) (P_n, \cdot)
- (g) $(\text{End}(E), \circ)$
- (h) $(\text{Aut}(E), \circ)$

2. Sean G un conjunto y

$$\star : G \times G \rightarrow G$$

$$(x, y) \mapsto xy$$

una operación binaria asociativa que cumple:

- 1. $\exists e \in G \forall x \in G \quad ex = x$
- 2. $\forall x \in G \exists x' \in G \mid x'x = e$

Demuestra que (G, \star) es grupo, el elemento neutro es e y el simétrico de x es x' .

3. (a)
(b)

4. Considera

$$GL(n, \mathbb{Z}) := \{M \in M_{n \times n}(\mathbb{Z}) : \det(M) \in \mathbb{Z}^*\},$$

$$SL(n, \mathbb{Z}) := \{M \in GL(n, \mathbb{Z}) : \det(M) = 1\},$$

$$O(n, \mathbb{Z}) := \{M \in GL(n, \mathbb{Z}) : M^T M = Id\},$$

$$SO(n, \mathbb{Z}) := \{M \in O(n, \mathbb{Z}) : \det(M) = 1\},$$

el grupo lineal, el grupo especial lineal, el grupo ortogonal y el grupo especial ortogonal respectivamente.

- (a) Demuestra que $GL(n, \mathbb{Z})$ es un grupo con la multiplicación de matrices.
- (b) Demuestra que $SL(n, \mathbb{Z})$ y $O(n, \mathbb{Z})$ son subgrupos del grupo $GL(n, \mathbb{Z})$.
- (c) Demuestra que $SO(n, \mathbb{Z})$ es un subgrupo de $O(n, \mathbb{Z})$.

5. Sea K un cuerpo:

- (a) Demuestra $SO(2, K)$ es abeliano.
- (b) Demuestra $\neg(SO(3, K)$ es abeliano).

6. Demuestra $\forall n \geq 2, H := \{M \in GL(n, \mathbb{Z}) : M = M^T\}$ no es subgrupo de $GL(n, \mathbb{Z})$.

7. Considera $K := \mathbb{Z}/2\mathbb{Z}$ y $G := GL(2, K)$. Escribe los elementos de G y la tabla del producto de G . ¿ G es abeliano?
8. Sea G un grupo. Demuestra $\forall x \in G : \text{ord}(x) = 2 \implies G$ es abeliano.
9. Sea G un grupo tal que $|G| = n$ y $G = \langle a \rangle$:
 - (a) Determina $\forall k \in \mathbb{Z} \quad |\langle a^k \rangle|$
 - (b) Demuestra $G = \langle a^k \rangle \iff \text{mcd}(k, n) = 1$
10. Sea G un grupo ciclico con orden n :
 - (a) Demuestra que todo subgrupo de G es ciclico.
 - (b) Demuestra $\forall d|n \exists! H \subset G : |H| = d$.
11. Sea $\mu_n := \{z \in \mathbb{C} : z^n = 1\}$. Demuestra que μ_n con el producto de \mathbb{C} es un grupo ciclico.
12. Sean p, q numeros primos distintos y $r, s \in \mathbb{N}^*$:
 - (a) Determina $\#\{x \in \mathbb{Z}/p\mathbb{Z} : \mathbb{Z}/p\mathbb{Z} = \langle x \rangle\}$.
 - (b) Determina $\#\{x \in \mathbb{Z}/p^r\mathbb{Z} : \mathbb{Z}/p^r\mathbb{Z} = \langle x \rangle\}$.
 - (c) Determina $\#\{x \in \mathbb{Z}/p^r q^s\mathbb{Z} : \mathbb{Z}/p^r q^s\mathbb{Z} = \langle x \rangle\}$.
13. Sean $\sigma, \tau \in S_9$ las permutaciones siguientes:

$$\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 9 & 1 & 8 & 7 & 6 & 3 & 4 & 5 \end{bmatrix} \quad (1)$$

$$\tau = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 1 & 3 & 5 & 8 & 2 & 9 & 6 & 4 \end{bmatrix} \quad (2)$$

- (a) Calcula $\sigma\tau$ y $\tau\sigma$.
- (b) Descompon σ y τ como producto de ciclos disjuntos, como producto de transposiciones y calcula $\varepsilon(\sigma)$.
- (c) Calcula σ^{2012} .

Solución:

1. Calculamos de la forma $\sigma(\tau(i))$ y viceversa $\forall i \ 1 \leq i \leq 9$

$$\sigma\tau = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 3 & 1 & 7 & 4 & 9 & 5 & 6 & 8 \end{bmatrix} \quad \tau\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 4 & 7 & 6 & 9 & 2 & 3 & 5 & 8 \end{bmatrix}$$

2. Ciclos:

$$\sigma = (129573)(48)$$

$$\tau = (17945862)$$

Transposiciones:

$$\sigma = (12)(29)(95)(57)(73)(48)$$

$$\tau = (17)(79)(94)(45)(58)(86)(62)$$

$\Sigma :$

$$\Sigma(\sigma) : (-1)^6 = 1$$

$$\sigma(\tau) : (-1)^7 = -1$$

3. $\sigma = (129573)(48) = S_6 \cup S_2$. Por lo que: $S_6^6 = Id, S_2^2 = Id$.

Entonces:

$$2012 \equiv 2(mod 6) \rightarrow 335 * 6 + 2$$

$$2012 \equiv 0(mod 6) \rightarrow 1006 * 2$$

Por lo que:

$$\sigma^{2012} = S_6^2$$

14. Determina $\varepsilon(\sigma) \quad \forall \sigma \in S_3$. Determina todos los subgrupos de S_3 .

Solución:

$$S_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right\} \quad (3)$$

$$S_3 = \{Id, t_1, c_2, c_1, t_2, t_3\} \quad (4)$$

(5)

$$\varepsilon(Id) = (-1)^0 = +1 \quad (6)$$

$$\varepsilon(t_1) = (-1)^1 = -1 \quad (7)$$

$$\varepsilon(c_2) = (-1)^2 = +1 \quad (8)$$

$$\varepsilon(c_1) = (-1)^2 = +1 \quad (9)$$

$$\varepsilon(t_2) = (-1)^1 = -1 \quad (10)$$

$$\varepsilon(t_3) = (-1)^1 = -1 \quad (11)$$

Subgrupos:

1. $\{Id\}$

2. $\{S_3\}$

3. $\{Id, t_1\}$

4. $\{Id, t_2\}$

5. $\{Id, t_3\}$

6. $\{Id, c_1, c_2\}$

Esto es así ya que $t_i^2 = Id \quad \forall i, 1 \leq i \leq 3$ mientras que por ejemplo $c_2^2 = c_1$.

15. Demuestra $\forall n \geq 2, |A_n| = |S_n/A_n|$.

Solución:

Toda permutación descompone en producto de transposiciones. Esta descomposición no es única, más su ε se mantiene. Es decir, son o pares o impares.

Sea la aplicación:

$$f : P \rightarrow I \quad (12)$$

$$\sigma \mapsto \tau\sigma \quad (13)$$

Que envia las permutaciones pares a las impares, solo queda ver que esta es biyectiva.

1. inyectiva:

$$f(\sigma) = f(\xi) \implies \sigma = \xi? \quad (14)$$

$$\tau\sigma = \tau\xi \implies \sigma = \xi \quad (15)$$

2. exhaustiva:

Si, pues $f(\tau\sigma) = \tau\tau\sigma = \sigma$.

Como f es biyectiva, entonces tendrá siempre la misma cantidad de permutaciones pares que impares; ergo la mitad de S_n .

16. (a) Demuestra $\forall \sigma \in S_n \quad \sigma \circ (a_1, \dots, a_r) \circ \sigma^{-1} = (\sigma(a_1), \dots, \sigma(a_r))$.
 (b) Demuestra $\forall \sigma_1, \sigma_2 \in S_n \quad (\text{ord}(\sigma_1) = \text{ord}(\sigma_2) \implies \exists \sigma \in S_n | \sigma \circ \sigma_1 \circ \sigma^{-1} = \sigma_2)$.
 (c) Sean $\sigma_1, \dots, \sigma_k \in S_n$ ciclos disjuntos dos a dos y también $\tau_1, \dots, \tau_k \in S_n$ ciclos disjuntos dos a dos. Pongamos $\sigma := \sigma_1 \circ \dots \circ \sigma_k$ y $\tau := \tau_1 \circ \dots \circ \tau_k$. Demuestra $\forall i \ 1 \leq i \leq k$, si la longitud del ciclo σ_i coincide con la del ciclo $\tau_i \implies \exists \rho \in S_n | \rho \circ \sigma \circ \rho^{-1} = \tau$
17. Demuestra
- (a) $S_n = \langle (1, 2), (1, 3), \dots, (1, n) \rangle$.
 - (b) $S_n = \langle (1, 2), (2, 3), \dots, (n-1, n) \rangle$.
 - (c) $S_n = \langle (1, 2, \dots, n), (1, 2) \rangle$.
18. Sea $A_n := \{\sigma \in S_n : \varepsilon(\sigma) = 1\}$ el subgrupo alternado de S_n . Demuestra que A_n es subgrupo de S_n , $[S_n : A_n] = 2$ y $A_n = \langle 3 - \text{ciclos} \rangle$.
19. El grupo diedral $D_{2,n}$ es el grupo de los desplazamientos en el plano que dejan invariante un poligono regular de n lados. Esto es, $D_{2,n} = \langle \rho, \sigma \rangle$, donde ρ es una rotación de angulo $\frac{2\pi}{n}$ centrada en el centro de simetria del poligono y σ es una simetria axial respecto a auno de los radios del poligono.
- (a) Demuestra $\rho^n = \sigma^2 = Id \wedge \rho\sigma = \sigma\rho^{-1}$.
 - (b) Escribe todos los elementos de $D_{2,n}$ ¿Cuántos son?
 - (c) Define un monomorfismo $f : D_{2,n} \rightarrow S_n$.
 - (d) Demuestra $\neg(D_{2,4} \simeq \mathbb{Z}/8\mathbb{Z})$.

20. (El grupo de los cuaterniones) Sea H_8 el subgrupo de $GL(2, \mathbb{C})$ generado por las matrices

$$Id := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, I := \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, J := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, K := \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

- (a) Demuestra que H_8 es un grupo tal que Id es el elemento neutro, $I^4 = Id$, $I^2 = J^2$ y $IJ = JI^3$.
 - (b) Calcula el orden de cada elemento de H_8 .
 - (c) Demuestra $\langle a, b | a^4 = e, a^2 = b^2, ab = ba^3 \rangle \simeq H_8$.
21. Sea G un grupo. Demuestra $\forall H \subset G \quad [G : H] = 2 \implies H \triangleleft G$.
22. Sea G un grupo y $Z(G) := \{g \in G : gh = hg, \forall h \in G\}$ su centro. Demuestra $Z(G) \triangleleft G$.
23. Sea K un cuerpo. Demuestra $Z(GL(n, K)) = \{M \in GL(n, K) : M = \lambda Id \quad \lambda \in K^*\}$.
24. Demuestra $\forall n \geq 3 \quad Z(S_n) = \{Id\}$.
25. Sean $f : G_1 \rightarrow G_2$ un morfismo de grupos, $H_1 \subseteq G_1$ y $H_2 \subseteq G_2$ subgrupos.
- (a) Demuestra que $f(H_1)$ es subgrupo de G_2 y $f^{-1}(H_2)$ de G_1 .
 - (b) Demuestra $H_1 \triangleleft G_2 \implies f^{-1}(H_2) \triangleleft G_1$.
 - (c) Demuestra $H_2 \triangleleft G_1 \implies f(H_1) \triangleleft f(G_1)$; pero no necesariamente $f(H_1) \triangleleft G_2$.
26. Teoremas de isomorfía de grupos.
- (a) Sean G un grupo, $H \triangleleft G$ y F un subgrupo cualquiera. Demuestra que HF es subgrupo de G , $F \cap H \triangleleft F$, $H \triangleleft HF$ y que $HF/H \simeq F/(F \cap H)$.
 - (b) Sean $\varphi : G \rightarrow G'$ un epimorfismo de grupos, $H' \triangleleft G'$ y $H = \varphi^{-1}(H')$. Demuestra que $G/H \simeq G'/H'$.
 - (c) Sean G un grupo y $F \subset H$ dos subgrupos normales en G . Demuestra que $H/F \triangleleft G/F$ y $(G/F)/(H/F) \simeq G/H$.
27. Considera $T \subset GL(2, \mathbb{C})$ el subgrupo de matrices diagonales y $D = \langle T, TODO \rangle$.
- (a) Demuestra $T \triangleleft D$.
 - (b) Describe un isomorfismo entre D/T y $\mathbb{Z}/2\mathbb{Z}$.
 - (c) Estudia si $D \triangleleft GL(2, \mathbb{C})$.
28. Considera el grupo diedral $D_{2,n}$.
- (a) Explicita todos los subgrupos de $D_{2,n}$ e indica cuales son normales.
 - (b) Demuestra $\exists H \subset D_{2,n} : H \triangleleft D_{2,n} \wedge |H| = n \wedge H$ es ciclico.
 - (c) Demuestra $D_{2,3} \simeq S_3$.
29. Calcula todos los subgrupos del grupo de cuaterniones H_8 e indica cuales son normales.
30. (a) Demuestra que A_4 es el unico subgrupo con indice 2 de S_4 . Es cierto que A_n es el unico subgrupo con indice 2 de $S_n, \forall n$?
- (b) Demuestra que A_4 no tiene subgrupos con indice 2. Tiene A_n cuando $n \geq 5$?
31. Determina, salvo isomorfismo, todos los grupos de orden menor o igual que 8.

32. Sea G un grupo. Considera la aplicación

$$\begin{aligned} f : G &\rightarrow G \times G \\ x &\mapsto (x, x) \end{aligned}$$

Demuestra $(f \text{ es un monomorfismo}) \wedge (f(G) \triangleleft G \times G \iff G \text{ es abeliano})$.

33. Determina todos los subgrupos de:

- (a) $\mathbb{Z}/4\mathbb{Z}$
- (b) $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
- (c) $\mathbb{Z}/6\mathbb{Z}$

34. Sea G un grupo finito ciclico. Calcula $\text{Aut}(G)$, el grupo de los automorfismos de G .

35. Dado un grupo G , denotamos por $\text{Aut}(G)$ el grupo de los automorfismos de G . Denotamos por $\text{Int}(G)$ el conjunto de los automorfismos internos de G , o sea, de los automorfismos φ_g definidos por $\varphi_g(h) := ghg^{-1}$, para $h \in G$ y $g \in G$ dado.

- (a) Demuestra que $\text{Int}(G)$ es un subgrupo de $\text{Aut}(G)$.
- (b) Demuestra $\forall \sigma \in \text{Aut}(G) \forall \varphi_g \in \text{Int}(G) \quad \sigma \varphi_g \sigma^{-1} = \varphi_{\sigma(g)}$.
- (c) Demuestra $\text{Int}(G) \triangleleft \text{Aut}(G)$.

36. Demuestra que G es un grupo $\Rightarrow G/Z(G) \simeq \text{Int}(G)$. En particular, si $Z(G) = \{1\}$, entonces $\text{Int}(G) \simeq G$. Determina $\text{Int}(G)$ cuando G es abeliano.

- 37. (a) Calcula las clases de conjugación del grupo S_3 .
- (b) Calcula las clases de conjugación del grupo S_4 .

38. Demuestra que las matrices $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ son elementos conjugados en el grupo $GL(2, \mathbb{R})$, pero que no lo son en $SL(2, \mathbb{R})$.

39. Calcula todas las clases de conjugación del grupo diedral $D_{2,n}$.

40. Demuestra $\forall n \in \mathbb{N} \forall d|n \quad \langle p^d \rangle \triangleleft D_{2,n} \wedge D_{2,n}/\langle p^d \rangle \simeq D_{2,d}$.

- 41. (a) Escribe la definición de grupo (finito) resoluble.
- (b) Demuestra que A_2 , A_3 y A_4 son resolubles.
- (c) Demuestra $\forall n \geq 5 \neg(A_n \text{ es resoluble})$.

- 42. (a) Escribe la definición de grupo finito simple.
- (b) Demuestra $\forall n \geq 5 A_n$ es simple.

43. Considera el grupo simétrico S_4 .

- (a) Calcula los 3-subgrupos de Sylow de S_4 ¿De que orden son?
- (b) Describe los elementos de S_4 con orden 2^n y recuerda que estos elementos están contenidos en un 2-subgrupo de Sylow. Deduce que un 2-subgrupo de Sylow contiene un subgrupo ciclico de orden 4. Explicita los 2-subgrupos de Sylow de S_4 .

44. Sea G un grupo finito. Demuestra $(|G| = 96) \implies \neg(G \text{ es simple})$.

45. Sea G un grupo. Demuestra $(|G| = 15) \implies (G \text{ es ciclico})$.

Solución: Factorizamos $15 = 3 \cdot 5$ y aplicamos el 3r y 2º Teoremas de Sylow:

$$\left. \begin{array}{l} |S_3| = 3 \\ n_3 \equiv 1(\text{mod } 3) \\ n_3 \mid [G : S_3] = 5 \end{array} \right\} \implies n_3 = 1 \iff S_3 \triangleleft G \quad (16)$$

$$\left. \begin{array}{l} |S_5| = 5 \\ n_5 \equiv 1(\text{mod } 5) \\ n_5 \mid [G : S_5] = 3 \end{array} \right\} \implies n_5 = 1 \iff S_5 \triangleleft G \quad (17)$$

Donde S_p es un p -subgrupo de Sylow de G y n_p la cantidad de estos.

S_3 y S_5 son ciclicos por ser de orden primo. Tomemos $S_3 = \langle a \rangle$ y $S_5 = \langle b \rangle$.

Observemos que todos los elementos de S_3 y S_5 , exceptuando el neutro, son generadores de estos. De lo que se deduce inmediatamente que $S_3 \cap S_5 = \{e\}$.

Veamos que a y b conmutan:

$$ab = ba \iff aba^{-1}b^{-1} = e \quad (18)$$

$$\left. \begin{array}{l} \underbrace{aba^{-1}}_{\in S_5 \triangleleft S_5 \triangleleft G} b^{-1} \in S_5 \\ a \underbrace{ba^{-1}b^{-1}}_{\in S_3 \triangleleft S_3 \triangleleft G} \in S_3 \end{array} \right\} \implies aba^{-1}b^{-1} \in S_3 \cap S_5 = \{e\} \quad (19)$$

$$\text{ord}(ab) = \text{mcm}(\text{ord}(a), \text{ord}(b)) = \text{mcm}(3, 5) = 15 \quad (20)$$

$$\text{ord}(ab) = |G| \implies G = \langle ab \rangle \quad (21)$$

$$\square \quad (22)$$

46. Sea G un grupo. Demuestra $(|G| = 255) \implies (G \text{ es ciclico})$.

47. Sea G un grup y p un numero primo mayor que 2. Demuestra $|G| = 2p \implies (G \text{ es ciclico}) \vee (G \simeq D_{2,p})$.

48. Sea G un grupo, p, q numeros primos. Demuestra $|G| = pq \implies G$ es resoluble.

Solución: Supongamos $p = q$

$$|Z(G)| \equiv |G| \equiv p^2 \equiv 0(\text{mod } p) \implies p \mid |Z(G)| \quad (23)$$

$$|G/Z(G)| = \begin{cases} 1 & \text{si } |Z(G)| = p^2 \\ p & \text{si } |Z(G)| = p \end{cases} \implies G/Z(G) \text{ es abeliano} \implies G/Z(G) \text{ es resoluble} \quad (24)$$

$$\left. \begin{array}{l} Z(G) \triangleleft G \\ Z(G) \text{ resoluble} \\ G/Z(G) \text{ resoluble} \end{array} \right\} \implies G \text{ es resoluble} \quad (25)$$

Supongamos ahora que $p \neq q$. Sin perdida de generalidad, $p < q$. Sean S_q un q -subgrupo de Sylow y n_q la cantidad de estos:

$$\left. \begin{array}{l} n_q \equiv 1(\text{mod } q) \\ n_q \mid [G : S_q] = p \end{array} \right\} \implies n_q = 1 \iff S_q \triangleleft G \quad (26)$$

$$|S_q| = q \implies S_q \text{ es ciclico} \implies S_q \text{ es abeliano} \implies S_q \text{ es resoluble} \quad (27)$$

$$|G/S_q| = p \implies G/S_q \text{ es ciclico} \implies G/S_q \text{ es abeliano} \implies G/S_q \text{ es resoluble} \quad (28)$$

$$\left. \begin{array}{l} S_q \triangleleft G \\ S_q \text{ resoluble} \\ G/S_q \text{ resoluble} \end{array} \right\} \implies G \text{ es resoluble} \quad (29)$$

$$\square \quad (30)$$

49. Sea G un grupo, p, q, r numeros primos. Demuestra $|G| = pqr \implies G$ es resoluble.

50. Sean p, q dos numeros primos tal que $0 < p < q$. Considera un grupo G :

(a) Demuestra $|G| = p^2 \implies G$ es resoluble.

(b) Demuestra $|G| = p^2q \implies (\exists! H \triangleleft G : |H| = p^2) \vee (\exists! H \triangleleft G : |H| = q)$.

(c) Demuestra $|G| = p^2q \implies G$ es resoluble.

51. Determina los factores invariantes y los divisores elementales de los grupos abelianos definidos por los siguientes generadores y relaciones:

(a) Generadores a, b, c, d . Relaciones
$$\begin{cases} 2a + 3b = 0 \\ 4a = 0 \\ 5c + 11d = 0 \end{cases}.$$

(b) Generadores a, b, c, d, e . Relaciones
$$\begin{cases} a - 7b + 14c - 21d = 0 \\ 5a - 7b - 2c + 10d - 15e = 0 \\ 3a - 3b - 2c + 6d - 9e = 0 \\ a - b + 2d - 3e = 0 \end{cases}.$$

52. Determina los factores invariantes y los divisores elementales de los grupos abelianos definidos por los siguientes generadores y relaciones:

(a) Generadores a, b, c, d . Relaciones
$$\begin{cases} 2a + 4b = 0 \\ 3b = 0 \end{cases}.$$

(b) Generadores a, b, c, d, e . Relaciones
$$\begin{cases} a - 7b - 21c + 14d = 0 \\ 5a - 7b - 2c + 10d - 15e = 0 \\ 3a - 3b - 2c + 6d - 9e = 0 \\ a - b + 2d - 3e = 0 \end{cases}.$$

53. Sea G el grupo abeliano $\langle a, b, c \mid 2a = 5b, 2b = 5c, 2c = 5a \rangle$. Demuestra que G es finito y haya $|G|$. Escribe todos los divisores elementales y los factores invariantes de los grupos abelianos del mismo orden que G y no isomorfos a G .

54. Sean G_1 y G_2 los grupos abelianos dados por los generadores a, b, c y las relaciones.

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 6 & 8 \\ 0 & 3 & 6 \end{pmatrix} \begin{pmatrix} a \\ b \\ c \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \quad (31)$$

$$\begin{pmatrix} 1 & 0 & -3 \\ 3 & 12 & 3 \end{pmatrix} \begin{pmatrix} a \\ b \\ c \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix} \quad (32)$$

- (a) Determina los factores invariantes y los divisores elementales de G_1 y de G_2 .
 - (b) Determina un monomorfismo $G_1 \rightarrow G_2$
55. (a) Encuentra todos los divisores elementales y los factores invariantes de todos los grupos abelianos de orden 200.
- (b) Clasifica el grupo abeliano $\mathbb{Z}/(2) \oplus \mathbb{Z}/(5) \oplus \mathbb{Z}/(20)$.
56. Determina todos los grupos abelianos con $|G| = 24$ tal que $\forall x \in G \quad \text{ord}(x) \leq 12$.
57. Sea G un grupo abeliano finito, demuestra G es ciclico $\iff \forall S_p$ subgrupo de Sylow de G , S_p es ciclico.
58. Sea G un grupo abeliano finito, $\neg(G \text{ es ciclico}) \implies \exists p | \exists H \subset G | h \simeq C_p \times C_p$.
59. Sea G un grupo abeliano finito, demuestra $\neg(G \text{ es ciclico}) \implies \exists p \text{ primo} \mid \exists H \subset G \mid G/H \simeq C_p \times C_p$.
60. Demuestra que un sistema de ecuaciones lineales $\forall M \in M_{m \times n}(\mathbb{Z}) \forall b \in M_{m \times 1}(\mathbb{Z}) \exists X \in M_{n \times 1}(\mathbb{Z}) \mid MX = b \iff \forall 0 < r \leq \min(m, n)$, el maximo comun divisor de los r -menores de M y el maximo comun divisor de los r -menores de la matriz ampliada $(M : b)$ coinciden.
61. (a) Demuestra que el grupo (\mathbb{Q}^+, \cdot) no es finitamente generado.
- (b) Escribe un conjunto de generadores.
62. (a) Demuestra que el grupo $(\mathbb{Q} \setminus \{0\}, \cdot)$ no es finitamente generado.
- (b) Escribe un conjunto de generadores.
63. Sea p un numero primo ≤ 20 , clasifica los grupos abelianos dados por los grupos multiplicativos $(\mathbb{Z}/p\mathbb{Z})^*$.
64. $\forall 2 \leq n \leq 15$, clasifica los grupos abelianos dados por los grupos multiplicativos $(\mathbb{Z}/n\mathbb{Z})^*$.
65. Explicita la estructura de los grupos abelianos dados por los grupos multiplicativos $(\mathbb{Z}/n\mathbb{Z})^*$.

2. Anillos

1. Sea A un anillo. Demuestra las siguientes propiedades:

- (a) $a \in A^* \implies a$ no es un divisor de cero.
- (b) Sea $I \subset A$ un ideal. $\exists u \in I \cap A^* \implies I = A$.
- (c) $(a \in A) \wedge (u \in A^*) \implies (ua) = (a)$.
- (d) Sea A un dominio de integridad y $a, b \in A$. $(a) = (b) \iff \exists u \in A^* \mid b = au$.

Solución:

Tenemos que $a \in A$ es unidad.

$$\exists b \in A \mid ab = 0 \implies 0 = a^{-1}0 = a^{-1}(ab) = 1b = b \implies \quad (33)$$

$$b = 0 \iff a \text{ no es un divisor de cero} \quad (34)$$

$$\square \quad (35)$$

Tenemos que $I \subset A$ es un ideal.

$$\exists u \in I \mid u \in A^* \implies u^{-1}u = 1 \in I \quad (36)$$

$$a \in A \implies a = a \cdot 1 \in I \implies I = A \quad (37)$$

$$\square \quad (38)$$

Tenemos $a \in A$ y $u \in A^*$.

$$u \in A \wedge a \in (a) \implies ua \in (a) \implies (ua) \subset (a) \quad (39)$$

$$u^{-1} \in A \wedge ua \in (ua) \implies u^{-1}ua = a \in (ua) \implies (a) \subset (ua) \quad (40)$$

$$(ua) \subset (a) \wedge (a) \subset (ua) \iff (ua) = (a) \quad (41)$$

$$\square \quad (42)$$

Tenemos que A es un dominio de integridad y $a, b \in A$.

Ya hemos demostrado en 1.c $\exists u \in A^* \mid b = au \implies (a) = (b)$.

Solo queda demostrar $(a) = (b) \implies \exists u \in A^* \mid b = au$:

$$(a) = (b) \implies a \in (b) \implies \exists c \in A \mid a = bc \quad (43)$$

$$(a) = (b) \implies b \in (a) \implies \exists d \in A \mid b = ad \quad (44)$$

$$b = ad = bcd \implies b(1 - cd) = 0 \xrightarrow[\text{de integridad}]{A \text{ es dominio}} \begin{cases} b = 0 \implies a = bc = 0 & u := 1 \\ \vee \\ 1 = cd \implies d \in A^* & u := d \end{cases} \quad (45)$$

$$\square \quad (46)$$

2. Caracteriza, en función del numero entero $m > 1$, los elementos invertibles y los divisores de cero del anillo $\mathbb{Z}/m\mathbb{Z}$. Deduce, $\mathbb{Z}/m\mathbb{Z}$ es un dominio de integridad $\iff \mathbb{Z}/m\mathbb{Z}$ es un cuerpo $\iff m$ es un numero primo.

Solución:

$$(\mathbb{Z}/m\mathbb{Z})^* := \{[x] \in \mathbb{Z}/m\mathbb{Z} : \exists [y] \in \mathbb{Z}/m\mathbb{Z} \mid [x][y] = [1]\} \quad (47)$$

$$[x][y] = [1] \iff [xy] = [1] \iff xy \equiv 1 \pmod{m} \iff \exists k \in \mathbb{Z} \mid xy = km + 1 \quad (48)$$

$$(49)$$

3. Demuestra que el ideal $(2, X)$ de $\mathbb{Z}[X]$ no es principal.

4. Sea A un anillo $a, b, d \in A$. Recuerda:

$$d \in \text{mcd}(a, b) \iff \begin{cases} d|a \\ d|b \\ \exists c \in A \mid (c|a \wedge c|b) \implies c|d \end{cases} \quad (50)$$

(a) Demuestra $d \in \text{mcd}(a, b) \implies (a, b) \subseteq (d)$. Escribe un ejemplo en $\mathbb{Z}[X]$ donde no se cumpla la igualdad.

(b) Sean $d, d' \in \text{mcd}(a, b)$. Demuestra A es un dominio $\implies \exists u \in A^* \mid d = ud'$

(c) Sea A un dominio de ideales principales. Demuestra $d \in \text{mcd}(a, b) \iff (a, b) = (d)$. Deduce que en un dominio de ideales principales, siempre existe el $\text{mcd}(a, b)$

Solución:

Tenemos $d \in \text{mcd}(a, b)$.

$$x \in (a, b) \implies \exists m, n \in A \mid x = ma + nb \quad (51)$$

$$\left. \begin{array}{l} d|a \implies a = a'd \\ d|b \implies b = b'd \end{array} \right\} \implies x = ma + nb = ma'd + nb'd = (ma' + nb')d \implies d|x \quad (52)$$

$$d|x \implies x \in (d) \implies (a, b) \subseteq (d) \quad (53)$$

$$\square \quad (54)$$

Tenemos A dominio de integridad, $d \in \text{mcd}(a, b)$ y $d' \in \text{mcd}(a, b)$.

$$\left. \begin{array}{l} \exists c \in A \mid (c|a \wedge c|b) \implies c|d \\ d'|a \\ d'|b \end{array} \right\} \implies d'|d \implies d \in (d') \implies (d) \subset (d') \quad (55)$$

$$\left. \begin{array}{l} \exists c \in A \mid (c|a \wedge c|b) \implies c|d' \\ d|a \\ d|b \end{array} \right\} \implies d|d' \implies d' \in (d) \implies (d') \subset (d) \quad (56)$$

$$(d') \subset (d) \wedge (d) \subset (d') \iff (d) = (d') \xleftrightarrow[1.d]{\text{Ejercicio}} \exists u \in A^* \mid d = ud' \quad (57)$$

$$\square \quad (58)$$

Tenemos que A es *DIP*.

Para ver $d \in \text{mcd}(a, b) \implies (a, b) = (d)$ solo hace falta demostrar $d \in \text{mcd}(a, b) \implies$

$(a, b) \supset (d)$ ya que \subseteq esta demostrado en el apartado a.

$$(a, b) \text{ es principal} \implies \exists c \in A \mid (a, b) = (c) \quad (59)$$

$$(a, b) = (c) \implies a \in (c) \implies c|a \quad (60)$$

$$(a, b) = (c) \implies b \in (c) \implies c|b \quad (61)$$

$$c|a \wedge c|b \xrightarrow[d \in \text{mcd}(a,b)]{} c|d \implies d \in (c) \implies (d) \subset (c) = (a, b) \quad (62)$$

Veamos $d \in \text{mcd}(a, b) \Leftarrow (a, b) = (d)$.

$$(a, b) = (d) \implies a \in (d) \implies d|a \quad (63)$$

$$(a, b) = (d) \implies b \in (d) \implies d|b \quad (64)$$

$$x \in (a, b) \implies \exists m, n \in A \mid x = ma + nb \quad (65)$$

$$\exists c \in A \mid (c|a \wedge c|b) \implies x = ma'c + nb'c = (ma' + nb')c \implies c|x \quad (66)$$

$$c|x \implies x \in (c) \implies (d) = (a, b) \subset (c) \implies d \in (c) \implies c|d \quad (67)$$

$$\left. \begin{array}{l} d|a \\ d|b \end{array} \right\} \implies d \in \text{mcd}(a, b) \quad (68)$$

$$\exists c \in A \mid (c|a \wedge c|b) \implies c|d$$

Demostradas ambas implicaciones, tenemos demostrado el si y solo si. \square

5. Sea A un anillo i $f, g \in A[X]$.

(a) Demuestra g es monico $\implies \exists! q, r \in A[X] \mid f = gq + r$ y $gr(r) < gr(g)$.

(b) Da un ejemplo de no-unicidad y otro de no-existencia en el caso de que g no sea monico.

Solución:

$$m := gr(f) \quad (69)$$

$$n := gr(g) \quad (70)$$

$$f^{(m)} := f \quad (71)$$

$$f_j^{(i)} := \text{coeficiente } j \text{ de } f^{(i)} \quad (72)$$

$$(73)$$

Empleamos el algoritmo de división tal cual:

$$i := m \quad (74)$$

$$\text{mientras } i \geq n \text{ hacer:} \quad (75)$$

$$f^{(i-1)}(x) := f^{(i)}(x) - f_i^{(i)} x^{i-n} g(x) \quad (76)$$

$$i := i - 1 \quad (77)$$

$$q := \sum_{i=n}^m f_i^{(i)} x^{i-n} \quad (78)$$

$$r := f^{(n-1)} \quad (79)$$

Encontramos q, r por lo que demostramos su existencia. q es unico porque el primer coeficiente de q y f tiene que ser el mismo, por lo que el primer coeficiente de q es unico. Aplicamos recursión y obtenemos que todos los coeficientes de q son unicos, por lo que tenemos que q es unico. Inmediatamente, $r := f - qg$ tambien es unico. Queda demostrada la unicidad de q y r . \square

Como ejemplo de no existencia tenemos $3, 2 \in \mathbb{Z}$ ya que el residuo debe de ser 0 y eso solo ocurre con el cociente perteneciente a $\mathbb{Q} \setminus \mathbb{Z}$.

Como ejemplo de existencia pero no unicidad tomemos en $\mathbb{Z}/8\mathbb{Z}$, $f := 6x^2$ y $g := 2x$. Tenemos 2 posibles soluciones:

$$q = 3x \tag{80}$$

$$r = 0 \tag{81}$$

$$2x3x + 0 = 6x^2 \tag{82}$$

$$q' = 4x^3 + 3x \tag{83}$$

$$r' = 0 \tag{84}$$

$$2x(4x^3 + 3x) + 0 = 8x^4 + 6x^2 = 0 + 6x = 6x^2 \tag{85}$$