Ejercicios y Soluciones de Anillos y Campos

Camila Contreras (Código: 20182167055)
Wilson Jerez (Código: 201181167034)

Universidad Distrital Francisco José de Caldas
Facultad de Ciencias Matemáticas y Naturales
Programa Académico de Matemáticas

Ejercicios y Soluciones

1. **Sea R un anillo y a un elemento fijo de R. Sea R_a el subanillo de R que es la intersección de todos los subanillos de R que contienen a a (ver Ejercicio 49). El anillo R_a es el subanillo de R generado por a. Demuestra que el grupo abeliano $\langle R_a, +\rangle$ está generado (en el sentido de la Sección 7) por $\{a^n \mid n \in \mathbb{Z}^+\}$.**

   Solución:
   Por definición, cada subanillo de R que contiene a a debe contener también a todas las potencias a^n (para $n \in \mathbb{Z}^+$), así como sus inversos aditivos. Por ende, el subanillo R_a (intersección de todos esos subanillos) contiene $\{a^n \mid n \in \mathbb{Z}^+\}$. Sea G el subgrupo aditivo generado por $S = \{a^n \mid n \in \mathbb{Z}^+\}$. Claramente, $G \subseteq \langle R_a, +\rangle$.

   Para mostrar que $G = R_a$, vemos que G es cerrado bajo la multiplicación (gracias a la conmutatividad y la distributividad en R): el producto de dos sumas finitas de potencias de a (incluyendo potencias negativas si uno considera los inversos aditivos) sigue siendo suma finita de potencias de a. De este modo, G resulta ser un subanillo que contiene a a y está contenido en R_a, así que $G = R_a$.

2. **Resuelve la ecuación $3x = 2$ en el campo $\mathbb{Z}_7$ y en el campo $\mathbb{Z}_{23}$.**

   Solución:
   En $\mathbb{Z}_7$, necesitamos x tal que $3x \equiv 2 \pmod 7$. Se puede comprobar que $x = 3$ funciona: $3 \cdot 3 = 9 \equiv 2 \pmod 7$. Por lo tanto, la solución en $\mathbb{Z}_7$ es $x = 3$.

   En $\mathbb{Z}_{23}$, se desea $3x \equiv 2 \pmod{23}$. Podemos tantear o usar la inversa de 3 en $\mathbb{Z}_{23}$: $3 \cdot 16 = 48 \equiv 2 \pmod{23}$. Así que $x = 16$ es la solución en $\mathbb{Z}_{23}$.

3. **Muestra que si D es un dominio integral, entonces $\{n \cdot 1 \mid n \in \mathbb{Z}\}$ es un subdominio de D contenido en cada subdominio de D.**

   Solución:
   Sea $R = \{n \cdot 1 \mid n \in \mathbb{Z}\}$. Observamos que si $n, m \in \mathbb{Z}$,

   $$n \cdot 1 + m \cdot 1 = (n + m) \cdot 1 \quad \text{y} \quad (n \cdot 1)(m \cdot 1) = (nm) \cdot 1.$$

Por lo tanto, R está cerrado bajo la suma y el producto, y contiene el 1. Asimismo, $0 = 0 \cdot 1$ está en R. Dado que D no tiene divisores de 0 y R hereda esa propiedad, R tampoco tiene divisores de 0.

En consecuencia, R es un subdominio de D. Además, todo subdominio de D que contenga 1 debe contener a todos los enteros $n \cdot 1$, de manera que R está contenido en cualquier otro subdominio.

4. **Dése la tabla de la multiplicación de grupo para los elementos de $\mathbb{Z}_{12}$ primos relativos con 12. ¿A qué grupo de orden 4 es isomorfo?**

Comentario / Sugerencia: Los elementos unidades en $\mathbb{Z}_{12}$ (es decir, los que son primos relativos con 12) son:

$$U(\mathbb{Z}_{12}) \; = \; \{1, 5, 7, 11\}.$$

Su orden es 4. Al construir la tabla de multiplicación (módulo 12), se observa que cada elemento es de orden 2 salvo la identidad, de modo que el grupo resultante es isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_2$ (el grupo de Klein).

Tabla de multiplicación resumida (mod 12):

$\cdot$	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

Se ve que cada elemento es su propio inverso (excepto la identidad 1), lo que coincide con la estructura de Klein, $V_4 \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

5. **Describe el campo F de cocientes del subdominio integral $D = \{n + mi \mid n, m \in \mathbb{Z}\}$ de $\mathbb{C}$.**

Solución:
El anillo D consiste en todos los *enteros gaussianos* $n + mi$, con $n, m \in \mathbb{Z}$. Su campo de cocientes (análogo a cómo $\mathbb{Q}$ se obtiene de $\mathbb{Z}$) es

$$F \; = \; \left\{ q_1 + q_2\, i \;\middle|\; q_1, q_2 \in \mathbb{Q} \right\}.$$

Este campo se puede ver como tomar todos los elementos de D y permitir divisiones por cualquier entero gaussiano no nulo. Al simplificar, se llega a números con partes real e imaginaria en $\mathbb{Q}$.

6. **Muéstrese, mediante un ejemplo, que un campo F de cocientes de un subdominio propio D' de un dominio entero D también puede ser campo de cocientes de D.**

Solución:
Consideremos $D = \mathbb{Z}\left[\frac{1}{2}\right] = \left\{\frac{m}{2^n} : m \in \mathbb{Z}, n \in \mathbb{Z}_{\geq 0}\right\}$, que es un subanillo de $\mathbb{Q}$ (y por tanto un dominio entero). Sea $D' = \mathbb{Z}$, que claramente está contenido en D, pero $D' \subsetneq D$.

El campo de fracciones de D' es $\mathbb{Q}$. Sin embargo, el campo de fracciones de D también es $\mathbb{Q}$, porque al tomar cualquier cociente

$$\frac{\frac{m_1}{2^{n_1}}}{\frac{m_2}{2^{n_2}}} \; = \; \frac{m_1}{2^{n_1}} \cdot \frac{2^{n_2}}{m_2} \; = \; \frac{m_1\, 2^{n_2}}{m_2\, 2^{n_1}} \; = \; \frac{m_1}{m_2} \cdot 2^{(n_2 - n_1)},$$

eso es todavía un número racional. Por lo tanto, $K(D) = K(D') = \mathbb{Q}$, ilustrando que un subdominio propio puede compartir el mismo campo de fracciones que su superdominio.

7. (Falso o Verdadero) sobre campos de cocientes de un dominio entero D:

(a) $\mathbb{Q}$ es un campo de cocientes de $\mathbb{Z}$. **Verdadero.** Ejemplo canónico.

(b) $\mathbb{R}$ es un campo de cocientes de $\mathbb{Z}$. **Falso.** $\mathbb{Q}$ es el único (salvo isomorfismo) campo de fracciones de $\mathbb{Z}$, y $\mathbb{R}$ contiene números irracionales.

(c) $\mathbb{R}$ es un campo de cocientes de $\mathbb{R}$. **Verdadero.** Si D es un campo, su propio campo de cocientes es isomorfo a él mismo.

(d) $\mathbb{C}$ es un campo de cocientes de $\mathbb{R}$. **Falso.** $\mathbb{R}$ ya es campo, su campo de fracciones se identifica con él mismo. No se "gana" nada pasando a $\mathbb{C}$.

(e) Si D es un campo, entonces cualquier campo de cocientes de D es isomorfo a D. **Verdadero.**

(f) El hecho de que D no tenga divisores de 0 se usó muchas veces en la construcción del campo de cocientes. **Verdadero.** Se requiere que $b \neq 0$ no se anule con ningún otro factor para que $\frac{a}{b}$ tenga sentido unívoco.

(g) Todo elemento de un dominio entero D es una unidad en un campo F de cocientes de D. **Falso.** El 0 no puede invertirse. Solo los no ceros de D se vuelven unidades en F.

(h) Todo elemento distinto de cero de un dominio entero D es una unidad en un campo F de cocientes de D. **Verdadero.**

(i) Un campo de cocientes F' de un subdominio D' de un dominio entero D puede considerarse subcampo de algún campo de cocientes de D. **Verdadero.** Existen monomorfismos naturales entre los campos de fracciones.

(j) Todo campo de cocientes de $\mathbb{Z}$ es isomorfo a $\mathbb{Q}$. **Verdadero.**

8. Sea R un anillo conmutativo no nulo, y sea T un subconjunto no vacío de R cerrado bajo la multiplicación y que no contiene ni 0 ni divisores de 0. Partiendo de $R \times T$ y siguiendo la construcción análoga a la de fracciones, se obtiene un anillo parcial de cocientes $Q(R, T)$.

(a) Muestra que $Q(R, T)$ tiene unidad aunque R no la tenga.

(b) En $Q(R, T)$, cada elemento no nulo de T es una unidad.

Solución:

(a) Dado que T es no vacío, elige $a \in T$. Entonces, el elemento $[(a, a)]$ en $Q(R, T)$ actúa como el 1: para todo $[(b, c)] \in Q(R, T)$,

$$[(a, a)] \cdot [(b, c)] = [(ab, ac)] \ \sim \ [(b, c)],$$

pues $abc = acb$ en un anillo conmutativo. Por lo tanto, $[(a, a)]$ es la unidad en $Q(R, T)$.

(b) Si $a \in T$ y $a \neq 0$, entonces $[(a,a)]$ está en $Q(R,T)$. Para su inverso, se toma $[(a,aa)]$ o $[(aa,a)]$, según convenga. Se verifica que

$$[(a,a)] \cdot [(aa,a)] = [(aaa,aaa)] = [(a,a)],$$

y esto muestra que cada $a \neq 0$ en T se vuelve una unidad en $Q(R,T)$.

9. Encuentra todos los ideales N de $\mathbb{Z}_{12}$. En cada caso, calcula $\mathbb{Z}_{12}/N$.

Solución:
En $\mathbb{Z}_{12}$, los ideales (subgrupos aditivos estables por la multiplicación por elementos de $\mathbb{Z}_{12}$) son exactamente los generados por divisores de 12. Por notación cíclica:

$$\begin{aligned}
\langle 0 \rangle &= \{0\}, \\
\langle 1 \rangle &= \{0,1,2,\dots,11\} = \mathbb{Z}_{12}, \\
\langle 2 \rangle &= \{0,2,4,6,8,10\}, \\
\langle 3 \rangle &= \{0,3,6,9\}, \\
\langle 4 \rangle &= \{0,4,8\}, \\
\langle 6 \rangle &= \{0,6\}.
\end{aligned}$$

- $N = \langle 0 \rangle$: $\mathbb{Z}_{12}/N \cong \mathbb{Z}_{12}$. - $N = \langle 1 \rangle$: $\mathbb{Z}_{12}/N \cong \{0\}$ (el anillo trivial). - $N = \langle 2 \rangle$: $\mathbb{Z}_{12}/N \cong \mathbb{Z}_2$. - $N = \langle 3 \rangle$: $\mathbb{Z}_{12}/N \cong \mathbb{Z}_3$. - $N = \langle 4 \rangle$: $\mathbb{Z}_{12}/N \cong \mathbb{Z}_4$. - $N = \langle 6 \rangle$: $\mathbb{Z}_{12}/N \cong \mathbb{Z}_2$.

10. Determínense todos los ideales de $\mathbb{Z} \times \mathbb{Z}$.

Solución:
Los ideales de $\mathbb{Z} \times \mathbb{Z}$ son exactamente de la forma

$$n\mathbb{Z} \times m\mathbb{Z}, \quad \text{con } n, m \in \mathbb{Z}_{\geq 0}.$$

Esbozo de demostración:

- Cada $n\mathbb{Z} \times m\mathbb{Z}$ es un ideal: está cerrado bajo suma y la multiplicación por cualquier elemento de $\mathbb{Z} \times \mathbb{Z}$.
- Si I es un ideal de $\mathbb{Z} \times \mathbb{Z}$, sus proyecciones sobre cada coordenada,

  $$I_1 = \{\, x \mid (x,y) \in I \}, \quad I_2 = \{\, y \mid (x,y) \in I \},$$

  son ideales en $\mathbb{Z}$. Pero en $\mathbb{Z}$, los únicos ideales son de la forma $n\mathbb{Z}$. Así pues $I_1 = n\mathbb{Z}$ e $I_2 = m\mathbb{Z}$ para algunos $n, m \geq 0$. Se ve luego que $I \subseteq n\mathbb{Z} \times m\mathbb{Z}$ y, por la posibilidad de generar con $(n,0)$ y $(0,m)$, en realidad $I = n\mathbb{Z} \times m\mathbb{Z}$.

11. Si A y B son ideales de un anillo R, se define

$$A + B = \{\, a + b \mid a \in A,\, b \in B \}.$$

(a) Demuestra que $A + B$ es un ideal.

(b) Demuestra que $A \subseteq A + B$ y $B \subseteq A + B$.

Solución:

(a) Sea $x = a_1 + b_1$ y $y = a_2 + b_2$, con $a_1, a_2 \in A$ y $b_1, b_2 \in B$. Entonces

$$x + y = (a_1 + b_1) + (a_2 + b_2) = (a_1 + a_2) + (b_1 + b_2) \ \in \ A + B,$$

así que está cerrado bajo suma. Si $r \in R$,

$$r \cdot (a_1 + b_1) = ra_1 + rb_1 \in A + B \quad \text{y} \quad (a_1 + b_1) \cdot r = a_1 r + b_1 r \in A + B$$

pues $ra_1, a_1 r \in A$ y $rb_1, b_1 r \in B$, al ser A, B ideales. Se verifica también que $0 \in A + B$ y los inversos aditivos están dentro. Por tanto, $A + B$ es un ideal.

(b) Claramente $a = a + 0 \in A + B$ para todo $a \in A$, y $b = 0 + b \in A + B$ para todo $b \in B$. Por ende, $A, B \subseteq A + B$.

12. Demuestra que el anillo de matrices $M_2(\mathbb{Z}_2)$ es un anillo simple (sin ideales propios no triviales).

Solución (Esbozo):
Sea $R = M_2(\mathbb{Z}_2)$. Este anillo *no* es conmutativo, pero igual consideramos sus ideales bilaterales. Observamos que si un ideal I contiene al menos una de las matrices elementales (las que tienen un 1 en una sola posición y 0 en otras), entonces mediante multiplicaciones y sumas se generan todas las demás matrices elementales, y por ende, todo R. Así que cualquier ideal no trivial debe ser todo el anillo.

En concreto, las matrices elementales

$$E_{11} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad E_{12} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad E_{21} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \quad E_{22} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix},$$

al multiplicarlas de diversas formas (a izquierda o derecha), generan el resto de matrices. Cualquier ideal que contenga una de ellas termina conteniéndolas todas. Concluimos que $M_2(\mathbb{Z}_2)$ no tiene ideales bilaterales propios no triviales y, por tanto, es simple.

13. Encuentra:

a) Un ideal maximal de $\mathbb{Z} \times \mathbb{Z}$.

b) Un ideal primo de $\mathbb{Z} \times \mathbb{Z}$ que no sea maximal.

c) Un ideal propio de $\mathbb{Z} \times \mathbb{Z}$ que no sea primo.

Solución:
Recordemos que en $\mathbb{Z} \times \mathbb{Z}$ los ideales son $n\mathbb{Z} \times m\mathbb{Z}$.

(a) **Ideal maximal:** Por ejemplo, $p\mathbb{Z} \times \mathbb{Z}$, donde p es primo. El cociente

$$(\mathbb{Z} \times \mathbb{Z})/(p\mathbb{Z} \times \mathbb{Z}) \ \cong \ \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/\mathbb{Z} \ \cong \ \mathbb{Z}/p\mathbb{Z},$$

que es un cuerpo, de modo que es maximal. Concretamente, $2\mathbb{Z} \times \mathbb{Z}$ es un ejemplo.

(b) **Ideal primo pero no maximal:** Un ejemplo es $0 \times \mathbb{Z}$. El cociente

$$(\mathbb{Z} \times \mathbb{Z})/(0 \times \mathbb{Z}) \;\cong\; \mathbb{Z},$$

y $\mathbb{Z}$ es un dominio entero (sin ser un cuerpo). Por lo tanto, $0 \times \mathbb{Z}$ es primo sin ser maximal.

(c) **Ideal propio no primo:** Ejemplo: $2\mathbb{Z} \times 3\mathbb{Z}$. Su cociente es

$$(\mathbb{Z} \times \mathbb{Z})/(2\mathbb{Z} \times 3\mathbb{Z}) \;\cong\; \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z},$$

un anillo con divisores de cero. Por ende no es un dominio, así que el ideal no es primo.

14. Sea R un anillo conmutativo con unidad de característica prima p. Demuestra que el mapa $\varphi_p : R \to R$ dado por $\varphi_p(a) = a^p$ es un homomorfismo (el homomorfismo de Frobenius).

Solución:
Por la expansión binomial,

$$(a+b)^p \;=\; \sum_{k=0}^{p} \binom{p}{k} a^k b^{p-k}.$$

Cuando p es primo, todos los coeficientes $\binom{p}{k}$ para $1 \leq k \leq p-1$ son múltiplos de p. En un anillo de característica p, esos coeficientes se anulan. Así,

$$(a+b)^p \;=\; a^p + b^p.$$

Además, siendo R conmutativo, $(ab)^p = a^p b^p$. Esto prueba que

$$\varphi_p(a+b) = (a+b)^p = a^p + b^p = \varphi_p(a) + \varphi_p(b), \quad \varphi_p(ab) = (ab)^p = a^p b^p = \varphi_p(a)\varphi_p(b).$$

Por tanto, φ_p es un homomorfismo de anillos (conocido como homomorfismo de Frobenius).

15. Demuestra que $\phi : \mathbb{C} \to M_2(\mathbb{R})$ dada por

$$\phi(a+bi) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$$

es un isomorfismo sobre su imagen $\phi[\mathbb{C}]$.

Solución:
Para $z_1 = a + bi$ y $z_2 = c + di$ en $\mathbb{C}$,

$$\phi(z_1+z_2) = \phi((a+c)+(b+d)i) = \begin{pmatrix} a+c & b+d \\ -(b+d) & a+c \end{pmatrix} = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} + \begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \phi(z_1)+\phi(z_2).$$

Asimismo,

$$\phi(z_1 z_2) = \phi((a+bi)(c+di)) = \phi((ac-bd)+(ad+bc)i) = \begin{pmatrix} ac-bd & ad+bc \\ -(ad+bc) & ac-bd \end{pmatrix},$$

y se comprueba que

$$\phi(z_1)\,\phi(z_2) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \begin{pmatrix} ac-bd & ad+bc \\ -(ad+bc) & ac-bd \end{pmatrix}.$$

Esto demuestra que ϕ es un homomorfismo de anillos. Resulta inyectivo (si $\phi(a+bi) = 0$, entonces $a = b = 0$), y la imagen $\phi[\mathbb{C}]$ es un subanillo de $M_2(\mathbb{R})$. Por tanto, ϕ es un isomorfismo entre $\mathbb{C}$ y el subanillo $\phi[\mathbb{C}] \subseteq M_2(\mathbb{R})$.

16. (Falso o Verdadero) sobre DFU, DIP, etc.

(a) **Todo campo es un DFU (Dominio de Factorización Única).**

Verdadero. En un campo, todo elemento no nulo es unidad y las "factorizaciones" se reducen a $a = a \cdot 1$.

(b) **Todo campo es un DIP (Dominio de Ideales Principales).**

Verdadero. En un campo K, los únicos ideales son (0) y K, ambos principales.

(c) **Todo DIP es un DFU.**

Verdadero. Es un teorema estándar de álgebra conmutativa: los dominios de ideales principales (PID) son dominios de factorización única (UFD).

(d) **Todo DFU es un DIP.**

Falso. Ejemplo: $k[x, y]$ (polinomios en dos variables sobre un campo k) es UFD pero no PID.

(e) $\mathbb{Z}[x]$ **es un DFU.**

Verdadero. Si R es UFD, entonces $R[x]$ también es UFD (caso particular: $R = \mathbb{Z}$).

(f) **Cualesquiera dos irreducibles en cualquier DFU son asociados.**

Falso. Ejemplo: en $\mathbb{Z}$, 2 y 3 son irreducibles pero no asociados.

(g) **Si D es un DIP, entonces $D[x]$ es un DIP.**

Falso. Por ejemplo, $\mathbb{Z}$ es DIP, pero $\mathbb{Z}[x]$ no lo es.

(h) **Si D es un DFU, entonces $D[x]$ es un DFU.**

Verdadero. Resultado que se demuestra usando el Lema de Gauss y propiedades de factorización.

(i) **En cualquier DFU, si $p \mid a$ para un irreducible p, entonces p aparece en toda factorización de a.**

Verdadero. En un DFU, "irreducible" coincide con "prime", y la divisibilidad de p sobre a implica que p aparezca en la factorización única de a.

(j) **Un DFU no tiene divisores de 0.**

Verdadero. Todo DFU es, de hecho, un dominio, por lo que no admite divisores de cero.