Tarea No. 1

Anillos, Dominios enteros, divisibilidad.

1. Sea R un anillo con uno. Demuestra que si $a \in R$ es invertible, entonces a no es un divisor de cero.

2. Sea R un anillo con uno, denotado por 1_R. Demuestra que el 1_R es único.

3. Sea R un anillo con uno y $u \in R$ un elemento invertible. Demuestra que $-u \in R$ también es invertible.

4. Sea R un anillo con uno y sea S un subanillo de R tal que $1_R \in S$. Demuestra que si u es invertible en S, entonces u es invertible en R.

5. Demuestra que el conjunto de los elementos invertibles de un anillo conmutativo con uno forman un grupo abeliano (con el producto).

6. Demuestra el siguiente resultado. Si R es un anillo, entonces para cualesquiera $a, b, c \in R$, se tiene.

   a) $0a = a0 = 0$;
   b) $a(-b) = (-a)b = -(ab)$;
   c) $(-a)(-b) = ab$;
   d) $a(b - c) = ab - ac$;
   e) $(b - c)a = ba - ca$.

7. Demuestra el siguiente resultado. Un anillo R es un anillo sin divisores de cero si, y solamente si, en R se satisfacen las leyes de cancelación izquierda y derecha para la multiplicación.

8. Sean R un anillo conmutativo con uno 1_R y S un subanillo con uno 1_S de R tales que $1_S \neq 1_R$.

   a) Demuestra que 1_S es un divisor de cero en R;
   b) Da un ejemplo de un anillo R y un subanillo S de R tales que $1_S \neq 1_R$.

9. Sea $(R, +, \cdot)$ un anillo distinto del anillo trivial. Denotemos por $R^n = \{(r_1, r_2, \ldots, r_n) : r_1, r_2, \ldots, r_n \in R\}$ y definamos en el conjunto R^n las operaciones de adición y multiplicación dadas por:

$$(r_1, r_2, \ldots, r_n) +_{R^n} (s_1, s_2, \ldots, s_n) = (r_1 + s_1, r_2 + s_2, \ldots, r_n + s_n)$$

   y

$$(r_1, r_2, \ldots, r_n) \cdot_{R^n} (s_1, s_2, \ldots, s_n) = (r_1 \cdot s_1, r_2 \cdot s_2, \ldots, r_n \cdot s_n).$$

   a) Demuestra que el sistema $(R^n, +_{R^n}, \cdot_{R^n})$ es un anillo.
   b) Demuestra que si R es un anillo con uno, entonces R^n es un anillo con uno.
   c) Demuestra que si R es un anillo conmutativo, entonces R^n es un anillo conmutativo.

d) Demuestra que R^n no es un dominio entero.

e) Considera el conjunto $R_1 = \{(0, r_2, \ldots, r_n) : r_2, \ldots, r_n \in R\}$. Demuestra que el sistema $(R_1, +_{R^n}, \cdot_{R^n})$ es un subanillo de R^n.

f) Verifica que si R es un anillo con uno, entonces R_1 es un anillo con uno.

10. Considera el anillo $\mathbb{Z}_4$ de los enteros módulo 4. Verifica que $\overline{2}$ es el único elemento de $\mathbb{Z}_4$ que es un divisor de cero.

11. Considera el anillo $\mathbb{Z}_5$ de los enteros módulo 5. Verifica que el anillo $\mathbb{Z}_5$ no tiene divisores de cero. Es decir, $\mathbb{Z}_5$ es un dominio entero.

12. Sean R un subanillo con uno y S un subanillo de R con uno. Denotemos por 1_R al uno de R y por 1_S al uno de S. Demuestra que si $1_R \neq 1_S$, entonces el elemento 1_S del subanillo S es un divisor de cero en el anillo R.

13. Si R es un anillo con división. Demuestra que cen$R$ es un campo.

14. Considera el anillo de los Cuaternios $(H, +, \cdot)$ donde

$$H = \{a \cdot 1 + b \cdot \hat{\imath} + c \cdot \hat{\jmath} + d \cdot \hat{k} \,:\, a, b, c, d \in \mathbb{R}\}.$$

Usando el hecho de que $(H, +)$ es un grupo abeliano.

a) Demuestra que el conjunto H es un espacio vectorial sobre el campo de los números reales, con la multiplicación por escalares definida como sigue:
Dado $r \in \mathbb{R}$, define $r(a \cdot 1 + b \cdot \hat{\imath} + c \cdot \hat{\jmath} + d \cdot \hat{k}) =$
$(r \cdot 1 + 0 \cdot \hat{\imath} + 0 \cdot \hat{\jmath} + 0 \cdot \hat{k})(a \cdot 1 + b \cdot \hat{\imath} + c \cdot \hat{\jmath}) + d \cdot \hat{k})$.

b) Demuestra que una base para el espacio vectorial H es $\{1, \hat{\imath}, \hat{\jmath}, \hat{k}\}$.

15. Describe el centro del anillo de los Cuaternios.

16. Demuestra que el conjnto $\{a \cdot 1 + b \cdot \hat{\imath} \,:\, a, b \in \mathbb{R}\}$ es un subanillo de los Cuaternios que es un campo, pero que no está contenido en el centro de los Cuaternios.

17. Dado un elemento $a \cdot 1 + b \cdot \hat{\imath} + c \cdot \hat{\jmath} + d \cdot \hat{k} \neq 0_C$, en el anillo con división de los Cuaternios, donde $0_C = 0 + 0i + 0j + 0k$. Encuentra su inverso multiplicativo.

18. Sea R un anillo, $a, b \in R$ y $n, m \in \mathbb{Z}$. Demuestra los siguientes resultados.

a) $(n + m)a = na + ma$;

b) $(nm)a = n(ma)$;

c) $n(a + b) = na + nb$;

d) $n(ab) = (na)b = a(nb)$;

e) $(na)(mb) = (nm)(ab)$.

19. Sea R un anillo con uno y consideremos el conjunto

$$\mathbb{Z}1_R = \{n1_R \,:\, n \in Z\}$$

.

a) Demuestra que $\mathbb{Z}1_R$ es un anillo conmutativo con uno;
b) Demuestra que el orden del grupo cíclico $(\mathbb{Z}1_R, +)$ es la característica del anillo R, si $\mathrm{char}(R)$ es positiva.
c) Demuestra que el orden del grupo cíclico $(\mathbb{Z}1_R, +)$ es infinito si $\mathrm{char}(R) = 0$.
d) Si R es un dominio entero. Demuestra que $\mathbb{Z}1_R$ es un subanillo de R que es dominio entero. Es decir, $\mathbb{Z}1_R$ es un subdominio de R.
e) Si R es un dominio entero. Demuestra que $\mathbb{Z}1_R$ es el subdominio más pequeno de R.

20. Denotemos por R al anillo $(\mathbb{Z}_6, +, \cdot)$.

a) Muestra que $\mathbb{Z}1_R = \{n1_R \,:\, n \in \mathbb{Z}\} = \mathbb{Z}_6$.
b) Muestra que el subconjunto $\{2n1_R \,:\, n \in \mathbb{Z}\}$ de $\mathbb{Z}1_R$ es un subanillo de $\mathbb{Z}1_R$ que no tiene uno.
c) Encuentra otro subanillo de $\mathbb{Z}1_R$.
d) Encuentra $\mathrm{char}(R)$.
e) Encuentra $\mathrm{char}(\mathbb{Z}1_R)$.

21. Denotemos por R al anillo $(\mathbb{Z}_5, +, \cdot)$.

a) Muestra que R es un dominio entero.
b) Muestra que $\mathbb{Z}1_R = \{n1_R \,:\, n \in Z\} = \mathbb{Z}_5$.
c) Deduce que $\mathbb{Z}1_R = \{n1_R \,:\, n \in Z\}$ es el subdominio más pequeno de $\mathbb{Z}_5$.
d) Encuentra $\mathrm{char}(R)$.
e) Encuentra $\mathrm{char}(\mathbb{Z}1_R)$.

22. Denotemos por R al anillo $(\mathbb{Q}, +, \cdot)$.

a) Muestra que R es un dominio entero.
b) Encuentra $\mathrm{char}(R)$.
c) Encuentra el orden del grupo R.
d) Describe $\mathbb{Z}1_R$.
e) Muestra que $\mathbb{Z}1_R$ es el subdominio más pequeno de R.
f) Encuentra $\mathrm{char}(\mathbb{Z}1_R)$.

23. Denotemos por R al conjunto $\mathbb{Z}_2 \times \mathbb{Z}_3$.

a) Con las operaciones de adición y multiplicación en R definidas por:

$$(\overline{a},\overline{b}) +_R (\overline{a'},\overline{b'}) = (\overline{a+a'},\overline{b+b'})$$

y

$$(\overline{a},\overline{b}) \cdot_R (\overline{a'},\overline{b'}) = (\overline{aa'},\overline{bb'})$$

Demuestra que R es un anillo conmutativo con uno.

b) Muestra que $\mathbb{Z}_2$ es un dominio entero y que $\mathrm{char}(\mathbb{Z}_2) = 2$.

c) Muestra que $\mathbb{Z}_3$ es un dominio entero y que $\mathrm{char}(\mathbb{Z}_3) = 3$.

d) Muestra que R no es un dominio entero.

e) Muestra que $\mathrm{char}(R) = 6$.

f) Encuentra el orden del grupo abeliano $(R,+)$.

g) Encuentra $\mathrm{char}(\mathbb{Z}1_R)$.

24. Denotemos por R al conjunto $\mathbb{Z} \times \mathbb{Z}_3$.

a) Con las operaciones de adición y multiplicación en R definidas por:

$$(a,\overline{b}) +_R (a',\overline{b'}) = (a+a',\overline{b+b'})$$

y

$$(a,\overline{b}) \cdot_R (a',\overline{b'}) = (aa',\overline{bb'})$$

Demuestra que R es un anillo conmutativo con uno.

b) Muestra que R no es un dominio entero.

c) Muestra que $\mathrm{char}(R) = 0$.

d) Encuentra el orden del grupo abeliano $(R,+)$.

e) Encuentra $\mathrm{char}(\mathbb{Z}1_R)$.

25. Sean $a,b,c \in R$ con R un anillo conmutativo. Demuestra que:

a) Si $a \mid b$ y $b \mid c$ entonces $a \mid c$;

b) Si $a \mid b$ y $a \mid c$ entonces $a \mid (b+c)$ y $a \mid (b-c)$;

c) Si $a \mid b$ entonces $a \mid bc$.

26. Sea R un anillo conmutativo con uno.

a) Dados $a,b \in R$, considera la relación $\sim$ en $R \times R$ dada por: $a \sim b$ si a y b son asociados en R.

b) Demuestra que la relación $\sim$ es una relación de equivalencia en $R \times R$.

27. Considera el anillo $F[x]$, de los polinomios en la indeterminada x sobre un campo F, con las operaciones usuales de adición y multiplicación de polinomios. Demuestra que

a) $F[x]$ es un dominio entero;

b) Determina los elementos invertibles en $F[x]$.

c) Da un ejemplo de dos elementos asociados en $F[x]$.