Ejercicios Álgebra - Relación 6
Dominios de Integridad

6.1. Determinar las unidades y los divisores de cero de los anillos $\mathbb{Z}_5$ y $\mathbb{Z}_6$.

Ser unidad $\Rightarrow$ Ser regular

Unidades de $\mathbb{Z}_5 = \{1, 2, 3, 4\}$

Unidades de $\mathbb{Z}_6 = \{1, 5\}$

Divisores de cero de $\mathbb{Z}_5$ = Ninguno

Divisores de cero de $\mathbb{Z}_6 = \{2, 3, 4\}$

6.2. ¿Es el anillo definido por el conjunto $\mathbb{Z}\times\mathbb{Z}$ con las operaciones $(a,a')+(b,b')=(a+b,a'+b')$ y $(a,a')(b,b')=(ab,ab'+a'b)$ un Dominio de Integridad?

Supongamos que existen divisores de cero y que, por lo tanto, no es O.I.:

$$(a,a')(b,b')=(0,0) \Leftrightarrow (ab, ab'+a'b)$$

$$\hookrightarrow \begin{cases} ab=0 \\ ab'+a'b=0 \end{cases} \xrightarrow{\text{Como } \mathbb{Z} \text{ es O.I.}} \begin{array}{|l} a=0 \\ b=0 \end{array}$$

$a=0 \rightarrow a'b=0 \rightarrow b=0$ pues si $a'=0$, entonces $(a,a')=(0,0)$ y no nos sirve.

Tomamos (a,a') como $(0,1)$ y (b,b') como $(0,1)$:

$$(0,1)\cdot(0,1)=(0\cdot 0, 0\cdot 1+1\cdot 0)=(0,0)$$

Hemos encontrado divisores de 0, y por la proposición 4.1.1., concluimos que $\mathbb{Z}\times\mathbb{Z}$ no es O.I.

6.3. Estudiar si los siguientes anillos son, o no, Dominios de Integridad:

a) $\mathbb{Z}_8$ No es D.I. ya que hay productos de elementos no nulos que dan 0, como $4\cdot 2=0$.

b) $\mathbb{Z}[\sqrt{2}]$ Sí es D.I. ya que está contenido en $\mathbb{C}$ y sabemos que:

$\mathbb{C}$ es un cuerpo y por tanto un D.I.

Como $\mathbb{Z}[\sqrt{2}] \subseteq \mathbb{C}$ y $\mathbb{C}$ es D.I., $\mathbb{Z}[\sqrt{2}]$ también lo es.

c) $\mathbb{Z}_3$ Sí es D.I. ya que es un cuerpo.

d) $\mathbb{Z}_6[x]$ No es D.I. ya que existen divisores de 0:

$3x^2 \cdot 2x = 0$

e) $\mathbb{Z}[i]$ Sí es D.I. ya que $\mathbb{Z}[i] \subseteq \mathbb{C}$ y $\mathbb{C}$ es cuerpo.

f) $\mathbb{Z}_5[x]$ Sí es D.I. ya que si cogemos dos polinomios de grado n y m, eso significa que los coeficientes a_n y b_m son no nulos, y al multiplicarlos y tener $a_n b_m$, como $a_n, b_m \in \mathbb{Z}_5$ y $\mathbb{Z}_5$ es D.I., $a_n b_m \neq 0$ y por lo tanto no tendremos divisores de cero en $\mathbb{Z}_5$.

6.4. En un anillo R un elemento a es idempotente si $a^2 = a$. Demuestra que en un dominio de integridad los únicos idempotentes son 0 y 1. Dar un ejemplo de un anillo que tenga otros idempotentes.

Supongamos que a es idempotente en A y A es D.I.:

$$a^2 = a \Rightarrow a^2 - a = 0 \Rightarrow a(a-1) = 0$$

Como A es D.I., o $a = 0$ o $a - 1 = 0$, por lo que $a = 0$ ó $a = 1$

Un ejemplo de un anillo que tenga otros idempotentes es $\mathbb{Z}_6$ pues, por ejemplo, $3 \cdot 3 = 3$.

6.5. ¿Es $3-2i$ un divisor de $8-i$ en el anillo $\mathbb{Z}[i]$? ¿Es 5 ... ¿Cuáles son los divisores de 5 en $\mathbb{Z}[i]$?

¿$3-2i \mid 8-i$?

$(3-2i)(a+bi) = 8-i$

$3a + 3bi - 2ai + 2b = 8 - i \Rightarrow \begin{cases} 3a + 2b = 8 \xrightarrow{\cdot 2} 6a + 4b = 16 \\ 3b - 2a = -1 \xrightarrow{\cdot 3} -6a + 9b = -3 \end{cases}$

$13b = 13$

$\boxed{a=2}$ $\boxed{b=1}$

Concluimos que $3-2i$ sí es divisor de $8-i$

$\boxed{* \; a \mid b \Rightarrow N(a) \mid N(b)}$

Divisores de 5 en $\mathbb{Z}[i]$

$x \mid 5 \Rightarrow N(x) \mid N(5) = 25 \Rightarrow N(x) = \begin{cases} 1 \\ 5 \\ 25 \end{cases}$

1^{er} caso

$\boxed{N(x)=1} \Rightarrow 1, -1, i, -i$

2^{o} caso

$\boxed{N(x)=25} \Rightarrow 5, -5, 5i, -5i$

3^{er} caso

$\boxed{N(x)=5} \Rightarrow a^2+b^2=5 \Rightarrow \left|\begin{array}{l} \begin{cases} a=1 \text{ y } b=2 \text{ ó } a=-1 \text{ y } b=-2 \text{ ó} \\ a=1 \text{ y } b=-2 \text{ ó } a=-1 \text{ y } b=2 \end{cases} \\ \begin{cases} a=2 \text{ y } b=1 \text{ ó } a=-2 \text{ y } b=-1 \text{ ó} \\ a=2 \text{ y } b=-1 \text{ ó } a=-2 \text{ y } b=1 \end{cases} \end{array}\right.$

$\begin{cases} 1+2i, -1-2i, 1-2i, -1+2i \\ 2+i, -2-i, 2-i, -2+i \end{cases}$

Para saber cuáles son divisores podemos usar que:

$\left.\begin{array}{l} a \sim b \\ a|5 \end{array}\right\} \Rightarrow b|5$

Demostración

$a|5 \Rightarrow ax=5$

$a \sim b \Rightarrow b|a \Rightarrow by=a$

$\Rightarrow byx=5$

$b|5$

Si ahora tomamos los asociados de $1+2i$ y $1-2i$:

$1+2i \begin{cases} 1+2i \\ -1-2i \\ -2+i \\ 2-i \end{cases} \qquad 1-2i \begin{cases} -1+2i \\ 1-2i \\ 2+i \\ -2-i \end{cases}$

Si llegamos a que $1+2i|5$ y que $1-2i|5$, entonces todos serán divisores de 5:

$$5 = N(1+2i) = (1+2i)(1-2i) \Rightarrow \begin{array}{l} 1+2i|5 \\ 1-2i|5 \end{array}$$

Concluimos que todos son divisores

6.6. Argumentar la veracidad o falsedad de las siguientes proposiciones referidas a elementos de un Dominio de Integridad:

1. $a|b \wedge a\nmid c \Rightarrow a\nmid(b+c)$

$a|b \Rightarrow \exists x \in A: ax=b$

$a\nmid c \Rightarrow \nexists y \in A: ay=c$

$b+c = ax+c$

Es cierta ya que para poder decir que $a|b+c$, necesitamos tener que $b+c=a\cdot$algo, pero no podemos extraer factor común de $ax+c$ ya que $a\nmid c$.

2. $a \nmid b \wedge a \nmid c \Rightarrow a \nmid b+c$

Es falsa pues tenemos contraejemplos:

$3 \nmid 2 \wedge 3 \nmid 4$ pero $3 \mid 6$, siendo $6 = 2+4$

6.7. Denotemos por $Q(x)$ el cuerpo de fracciones de $\mathbb{Z}[x]$ y sus operaciones. Probar que $Q(x)$ es también el cuerpo de fracciones de $\mathbb{Q}[x]$

$$A = \mathbb{Z}[x] \Rightarrow Q(A) = \left\{ \frac{p(x)}{q(x)} \mid p, q \in \mathbb{Z}[x],\ q \neq 0 \right\}$$

Propiedad universal

$Q(A)$ es el menor cuerpo que contiene a A

$$\left.\begin{array}{l} A \subseteq K \\ K \text{ cuerpo} \end{array}\right\} \Rightarrow Q(A) \subseteq K$$

Prop. 2

$$A \subseteq B \Rightarrow Q(A) \subseteq Q(B)$$

Prop. 3

$$A \subseteq B \subseteq Q(A) \Rightarrow Q(A) = Q(B)$$

$$\left.\begin{array}{l} A \subseteq B \overset{②}{\Rightarrow} Q(A) \subseteq Q(B) \\ B \subseteq Q(A) \Rightarrow Q(B) \subseteq Q(A) \end{array}\right\} Q(A) = Q(B)$$

$\mathbb{Z}[x]$ ¿$Q(\mathbb{Z}[x]) = Q(\mathbb{Q}[x])$?

$$\mathbb{Z}[x] \subseteq \mathbb{Q}[x] \subseteq Q(\mathbb{Z}[x])$$

Está claro

Si cogemos $q_n x^n + q_{n-1} x^{n-1} \cdots q_0$ con $q_i \in \mathbb{Q}$

Cualquier $q(x) \in \mathbb{Q}[x]$ se puede expresar como

$$\frac{\text{Suma polinomios tras factor común}}{\text{Denom. común (Pol. const. de } \mathbb{Z}[x])}$$

y ya se aplica la propiedad 3