Anillos

Definición 1. *Un anillo $(R, +, \cdot)$ es un conjunto, junto con dos operaciones binarias que llamaremos suma y producto y denotamos por $+$ y $\cdot$ respectivamente, que satifacen las siguientes propiedades para cualesquiera $x, y, z \in R$*

1. $(x + y) + z = x + (y + z)$; *asociatividad de la suma*
2. $x + y = y + x$; *conmutatividad de la suma*
3. *Existe un elemento en R, denotado por 0, tal que $x + 0 = 0 + x = x$ existencia de neutro aditivo*
4. *Para todo $x \in R$, exite $w \in R$ tal que $w + x = x + w = 0$ existencia de inverso aditivo*
5. $(xy)z = x(yz)$ *asociatividad del producto*
6. *Existe un elemento, denotado por 1, tal que $x \cdot 1 = 1 \cdot x = x$ existencia del neutro multiplicativo*
7. $x(y + z) = xy + xz$ *distributividad del producto respecto a la suma*
8. $(x + y) \cdot z = xz + yz$ *distributividad del producto respecto a la suma*

Ejemplo El conjunto de las matrices cuadradas $M_{n\times n}$ satisface las propiedades que definen un anillo

Si el producto en un anillo es conmutativo diremos que el anillo es un anillo conmutativo

Ejemplo El conjunto $(\mathbb{Z}, +, \cdot)$ es un anillo conmutativo.

Ejemplo Consideramos el conjunto

$$F = \{f : \mathbb{Z} \to \mathbb{Z} \mid f \text{ es función}\}$$

donde la suma $(f + g)(n)$ se define $f(n) + g(n)$ y el producto se define $(f \cdot g)(n) = f(n) \cdot g(n)$. Por lo tanto $(F, +, \cdot)$ es un anillo conmutativo.

Proposición 1. *Sea $(R, +, \cdot)$ un anillo y sean $x, y, z \in R$.*

1. *Si $x + y = x + z$ o $y + x = z + x$, entonces $y = z$*
2. *El neutro aditivo es único*
3. *El inverso aditivo es único*
4. *El neutro multiplicativo es único*
5. $x \cdot 0 = 0 \cdot x = 0$.

Demostración. 1. Supongamos que $x+y = x+z$ y sea w un inverso aditivo de x. Sumando w a ambos lados de la igualdad obtenemos

$$\begin{aligned} w + (x + y) &= w + (x + z) \\ (w + x) + y &= (w + x) + z \quad (\textit{ por la asociatividad de la suma }) \\ 0 + y &= 0 + z \quad (\textit{ debido a que } w + x = 0 \textit{ por ser } w \textit{ inverso aditivo de } x) \\ y &= z \quad (\textit{ debido que } 0 \textit{ es neutro aditivo }) \end{aligned}$$

Como la suma es conmutativa, automáticamente se cumple el otro caso.

2. Supongamos que 0 y $0'$ son neutros aditivos en R. Entonces

$$0 \underbrace{=}_{0' \text{ es neutro aditivo}} 0+0' \underbrace{=}_{0 \text{ es neutro aditivo}} 0'$$

3. Supongamos que w y w' son inversos aditivos de x.

$$\begin{aligned} w &= w+0 \quad (\textit{propiedas del neutro aditivo}) \\ &= w+(x+w') \quad (w' \textit{ es inverso multiplicativo de } x) \\ &= (w+x)+w' \quad (\textit{asociatividad de la suma}) \\ &= 0+w' \quad (w \textit{ es inverso aditivo de } x) \\ &= w' \quad (\textit{propiedad del neutro aditivo}) \end{aligned}$$

4. La demostración es análoga a (2)

5. Por ser 0 el neutro en R, tenemos que $0+0=0$. Entonces

$$\begin{aligned} x\cdot(0+0) &= x\cdot 0 \\ x\cdot 0+x\cdot 0 &= x\cdot 0 \quad (\textit{Ley distributiva}) \\ x\cdot 0+x\cdot 0 &= x\cdot 0+0 \quad (\textit{propiedad del neutro aditivo}) \\ x\cdot 0 &= 0 \quad (\textit{ley de cancelacin }) \end{aligned}$$

De la misma mmanera se demuestra que $0\cdot x=0$

□

Proposición 2. *Sea $(R,+,\cdot)$ un anillo. Entonces $-a=(-1)a$ para cada $a\in R$*

Demostración. Basta demostrar que $(-1)a$ es el inverso aditivo de a

$$\begin{aligned} (-1)a+a &= (-1)a+1a \quad (\textit{propiedad del neutro multiplicativo}) \\ &= ((-1)+1)a \quad (\textit{ley distributiva}) \\ &= 0a \quad (\textit{inverso aditivo}) \\ &0 \end{aligned}$$

Por la unicidad del inverso aditivo, tenemos que $-a=(-1)a$ □

Proposición 3. *Sea $(R,+,\cdot)$ un anillo y sean $a,b\in R$. Entonces*

1. $-(-a)=a$
2. $(-a)b=a(-b)=-(ab)$. *En particular,* $(-1)b=-b$
3. $(-a)(-b)=ab$

Demostración. 1. $-(-a)$ denota el inverso de $-a$ y por otro lado a es el inverso de $-a$ ya que $(-a)+a=0$, por lo que, debido a que el inverso es único, $-(-a)=a$

2. Tenemos que
$$ab + (-a)b = (a + (-a))b = 0b = 0$$
$$ab + a(-b) = a(b + (-b)) = a0 = 0$$
ya que tanto $(-a)b$ y $a(-b)$ son ambos inversos de ab, debido a la unicidad del inverso aditivo, ambos deben ser iguales

3. Como ab es el inverso de $-(ab)$, para demostrar la igualdad requerida, mostraremos que $(-a)(-b)$ es el inverso de $-(ab)$ y para esto usamos (2), que es, $-(ab) = (-a)b$,
$$-(ab) + (-a)(-b) = (-a)b + (-a)(-b) = (-a)(b + (-b)) = (-a)0 = 0$$

□

Definición 2. *Sea $(R, +, \cdot)$ un anillo y $a, b \in R$. La diferencia de a y b, denotada por $a - b$, es $a - b = a + (-b)$*

Teorema 1. *Sea $(R, +, \cdot)$ un anillo y $a, b \in R$. Entonces*

1. $a - a = 0$
2. $-(a + b) = -a - b$
3. $(a - b) + (c - d) = (a + c) - (b + d)$
4. $a(b - c) = ab - ac$
5. $(a - b)(c - d) = (ac + bd) - (ad + bc)$

Demostración. 1. Tenemos que
$$a - a = a + (-a) = 0$$

2. tenemos que $-(a+b) = (-1)(a+b)$ y por ser el producto distributivo respecto de las suma, se tiene que
$$(-1)(a + b) = (-1)a + (-1)b = -a + (-b) = -a - b$$

3. Tenemos que
$$\begin{aligned}(a - b) + (c - d) &= (a + (-b)) + (c + (-d)) \\ &= (a + c) + (-b) + (-d) \\ &= (a + c) + (-1)b + (-1)d \\ &= (a + c) + (-1)(b + d) \\ &= (a + c) - (b + d)\end{aligned}$$

4. Tenemos que
$$\begin{aligned}a(b - c) &= a(b + (-c)) \\ &= ab + a(-c) \\ &= ab + (-(ac)) \\ &= ab - ac\end{aligned}$$

5. Tenemos que

$$\begin{aligned}(a-b)(c-d) &= (a+(-b))(c+(-d))\\ &= (a+(-b))c+(a+(-b))(-d)\\ &= (ac+(-b)c)+(a(-d)+(-b)(-d))\\ &= (ac-bc)+(-ad)+(-(-bd))\\ &= (ac-bc)-ad+db\\ &= ac+db-bc-ad\\ &= (ac+db)+(-1)bc+(-1)ad\\ &= (ac+db)+(-1)(ad+bc)\\ &= (ac+db)-(ad+bc)\end{aligned}$$

□

Proposición 4. *Sean $a, b \in \mathbb{Z}$. Si $ab = 0$, entonces $a = 0$ o $b = 0$*

Demostración. Supongamos que $ab = 0$. Demostraremos que $a = 0$ o $b = 0$

1. Caso 1 $a = m$, $b = n$. Como $a, b \in \mathbb{N}$ tenemos que debe ser $a = 0$ 0 $b = 0$
2. Caso 2 $a = -m$, $b = -n$

$$\begin{aligned}0 &= ab\\ &= (-m)(-n)\\ &= mn\end{aligned}$$

   Luego $m = 0$ 0 $n = 0$ y así $a = -0 = 0$ o $b = -0 = 0$
3. Caso 3 $a = m$, $b = -n$

$$\begin{aligned}0 &= -0\\ &= -(ab)\\ &= -[m(-n)]\\ &= -[-(mn)]\\ &= mn\end{aligned}$$

   Por lo tanto $m = 0$ o $n = 0$. Luego $a = 0$ o $b = -0 = 0$
4. Caso 4 $a = -m$, $b = n$. Como el producto en $\mathbb{Z}$ es conmutativo, este caso se reduce al tercer caso

□

Definición 3. *Si un anillo $(R, +, \cdot)$ tiene un elemento unitario 1 tal que $1a = a = a1$ para todo $a \in R$, entonces el anillo se denomina anillo conmutativo unitario.*

Definición 4. *Un anillo conmutativo $(R, +, \cdot)$ se llama dominio entero en el caso de que cualquiera $x, r \in R$, si $xy = 0$, entonces $x = 0$ o $y = 0$*

Un elemento x de un anillo conmutativo R se llama divisor de cero si existe $y \in R$, $y \neq 0$, tal que $xy = 0$. Según esta definición, 0 siempre será divisor de cero debido a que $0y = 0$ para toda $y \in R$, Así pues, un anillo conmutativo será dominio si no tiene divisores de cero, con excepción de 0.

Teorema 2. *Un anillo conmutativo R es un dominio entero si y sólo si valen las leyes de cancelación para el producto, es decir, para toda $x, y, z \in R$, si $xy = xz$ y $x \neq 0$, entonces $y = z$*

Demostración. ($\Rightarrow$).
Supongamos que R es un dominio entero y supongamos que $xy = xz$ con $x \neq 0$. Entonces $0 = xy - xz = x(y - z)$ y por lo tanto $x = 0$ o $y - z = 0$.
Como por hipótesis, $x \neq 0$, debe tenerse que $y - z = 0$, que es $y = z$.
($\Leftarrow$).
Supongamos que $x, y \in R$ son tales que $xy = 0$. En el caso $x = 0$ no hay nada que demostrar, así que supondremos que $x \neq 0$. Demostraremos que $y = 0$.
Se tiene entonces que $xy = 0 = x0$ con $x \neq 0$, por lo que por hipótesis, $y = 0$ □