**Módulo9:**

# ANILLO, SUBANILLO E IDEALES.

En este módulo abarcaremos todo lo relacionado con estructura de anillos, haciendo alusión a algunas definiciones especiales; como anillo cancelativo, con identidad. Además las condiciones pertinentes para un subanillo e ideal, finalizando con una serie de ejercicios desarrollados y de aplicación.

**Definición 1:** Dado $A$ un conjunto no vacío y $+,\cdot$ dos leyes de composición interna definidas en $A$. $(A,+,\cdot)$ es un anillo si se verifica:

1) $(A,+)$ es un grupo abeliano.
2) $(A,\cdot)$ es un semigrupo (es asociativo).
3) Distributividad de $\cdot$ con respecto a $+$, es decir que para todo $a,b,c \in A$, se cumple
   i) $a\cdot(b+c)=a\cdot b+a\cdot c$ (distributividad por la izquierda).
   ii) $(b+c)\cdot a=b\cdot a+c\cdot a$ (distributividad por la derecha).

**Ejemplo 1:**

$(\mathbb{Z},+,\cdot);(\mathbb{R},+,\cdot);(\mathbb{Q},+,\cdot);\left(\mathbb{R}[X],+,\cdot\right);(\mathbb{R}^{n\times m},+,\cdot)$ son ejemplos que verifican ser anillos



*Eduardo Cabrera de Arrizabalaga (profesor guía), Eduardo González, Pablo Ossa & Oliver Tapia (tesistas 2008)*

**Ejemplo 2:**

Sea $(A,+,\cdot)$ un anillo y $S$ un conjunto cualquiera no vacío. En el conjunto $A^s = \{f : S \to A \,/\, f \text{ es función}\}$ se definen las leyes de composición interna $\oplus$ y $\odot$ como siguen:

$$\oplus : A^s \times A^s \longrightarrow A^s$$
$$(f,g) \mapsto f \oplus g : S \longrightarrow A$$
$$s \mapsto (f \oplus g)(s) = f(s) + g(s)$$
$$(\text{donde } f(s), g(s) \in A)$$

$$\odot : A^s \times A^s \longrightarrow A^s$$
$$(f,g) \mapsto f \odot g : S \longrightarrow A$$
$$s \mapsto (f \odot g)(s) = f(s) \cdot g(s)$$
$$(\text{donde } f(s), g(s) \in A)$$

Podemos demostrar que $(A^s, \oplus, \odot)$ es un anillo.

**Demostración:**

i) Demostraremos que $(A^s, \oplus)$ es un grupo abeliano.

i.1) Conmutatividad en $(A^s, \oplus)$:

Para todo $f$, $g \in A^s$; por demostrar que $f \oplus g = g \oplus f$, es decir, debemos demostrar que para todo $s \in S$, $(f \oplus g)(s) = (g \oplus f)(s)$. En efecto, $(f \oplus g)(s) = f(s) + g(s)$, como $f(s), g(s) \in A$ y $+$ es conmutativa en $A$, se tiene que $f(s) + g(s) = g(s) + f(s) = (g \oplus f)(s)$. Luego $f \oplus g = g \oplus f$.

i.2) Asociatividad en $(A^s,\oplus)$:

Para todo $f,g,h\in A^s$, por demostrar $(f\oplus g)\oplus h=f\oplus(g\oplus h)$, es decir, debemos demostrar que para todo $s\in S$,

$$((f\oplus g)\oplus h)(s)=(f\oplus(g\oplus h))(s)$$

En efecto, se tiene que $((f\oplus g)\oplus h)(s)=(f\oplus g)(s)+h(s)$

Como $+$ es asociativo en $A$, se tiene que $=f(s)+g(s)+h(s)$

$$=f(s)+(g\oplus h)(s)$$

$$=((f\oplus g)\oplus h)(s)$$

Luego $(f\oplus g)\oplus h=f\oplus(g\oplus h)$

i.3) Elemento Neutro en $(A^s,\oplus)$:

Debe existir un $g\in A^s$, para todo $f\in A^s$ tal que $f\oplus g=g\oplus f=f$, es decir, debemos demostrar que $(f\oplus g)(s)=f(s)+g(s)=f(s)$, $\forall s\in S$.

Se tiene $(f\oplus g)(s)=f(s)+g(s)=f(s)$, como $f(s),g(s)\in A$, además sumando el inverso aditivo de $f(s)\in A$ por la izquierda, se tiene que: $-f(s)+f(s)+g(s)=-f(s)+f(s)$, lo que implica $g(s)=0_A$, $\forall s\in A$.

Por lo tanto el neutro en $(A^s,\oplus)$ es la función nula, de valor constante $0_A$, que anotaremos por $\theta$, esto es $g=\theta\in A^s$.

i.4) Elemento Inverso en $(A^s,\oplus)$:

Para todo $f\in A^s$, debe existir $h\in A^s$ tal que $f\oplus h=h\oplus f=\theta$ (neutro en $(A^s,\oplus)$).

Supongamos que para todo $s\in S$, $(f\oplus h)(s)=\theta(s)$, de lo que se deduce $f(s)+h(s)=0_A$, por ser $(A,+,\cdot)$ anillo se tiene que $h(s)=-f(s)$

De igual manera verifica ser inverso por la izquierda.

Por lo tanto, el inverso aditivo de $f$ es la función $h\in A^S$, donde $h=-f$.

Nótese que $(-f)(s)=-f(s),\forall s\in S.$

En consecuencia, de lo anterior, $(A^s,+)$ es grupo abeliano.

ii) Demostrar que $(A^s,\odot)$ es un semigrupo.

Para todo $f,g,h\in A^s$, por demostrar $(f\odot g)\odot h=f\odot(g\odot h)$, es decir, debemos demostrar que $((f\odot g)\odot h)(s)=(f\odot(g\odot h))(s)$, $\forall s\in S$.

En efecto:

$$\begin{aligned}((f\odot g)\odot h)(s)&=(f\odot g)(s)\cdot h(s)\\&=(f(s)\cdot g(s))\cdot h(s),\text{ por asociatividad en } A.\\&=f(s)\cdot(g(s)\cdot h(s))\\&=f(s)\cdot(g\odot h)(s)\\&=(f\odot(g\odot h))(s)\end{aligned}$$

Por lo tanto $(A^s,\odot)$ es un semigrupo.

iii) Distributividad de $(\odot)$ con respecto a $(\oplus)$:

Es decir para todo $f, g, h \in A^s$ se debe demostrar que verifica distributividad por la derecha y por la izquierda, la demostración se deja de ejercicio al lector.

De lo anterior, podemos decir que $(A^s, \oplus, \odot)$ es un anillo.

**Definición 2:** Sea $(A,+,\cdot)$ un anillo. Diremos que $(A,+,\cdot)$ es un anillo con identidad, si existe $1 \in A$ tal que $a \cdot 1 = 1 \cdot a = a, \forall a \in A$.

**Definición 3:** Sea $(A,+,\cdot)$ un anillo. Diremos que $(A,+,\cdot)$ es un anillo conmutativo, si con respecto a la segunda operación $(\cdot)$ se verifica conmutatividad.

**Definición 4:** Sea $(A,+,\cdot)$ un anillo. Diremos que $(A,+,\cdot)$ es un anillo sin divisores de cero, si $a \cdot b = 0$ entonces $a = 0$ ó $b = 0$ con $a, b \in A$

**Definición 5:** Sea $(A,+,\cdot)$ un anillo; $a \in A - \{0\}$ es un divisor de cero izquierdo (o derecha) si existe $b \in A - \{0\}$ tal que $a \cdot b = 0$ (ó $b \cdot a = 0$)

**Definición 6:** Un anillo $(A,+,\cdot)$ conmutativo con identidad y sin divisores de cero se llama Dominio de Integridad.

**Definición 7:** Sea $(A,+,\cdot)$ un anillo con identidad. Un elemento $u \in A$ es una unidad o es un elemento invertible si existe $v \in A$ tal que $u \cdot v = v \cdot u = 1$ .

El conjunto de las unidades de $A$ está denotado por $U(A) = \{u \in A / \, u \text{ es unidad}\}$.

**Ejemplos:**

**3.-** $(\mathbb{Z},+,\cdot)$ es un anillo sin divisores de cero, $U(\mathbb{Z})=\{-1,1\}$.

**4.-** $(\mathbb{Z}_3,+,\cdot)$ es anillo sin divisores de cero y $U(\mathbb{Z}_3)=\mathbb{Z}_3-\{\bar{0}\}$.

**5.-** $(\mathbb{Z}_6,+,\cdot)$ es con divisores de cero, pues existen $\bar{2},\bar{3}\in\mathbb{Z}_6$ tal que $\bar{2}\cdot\bar{3}=\bar{0}$ con $\bar{0}\in\mathbb{Z}_6$, pero $\bar{2}\neq\bar{0}$ y $\bar{3}\neq\bar{0}$; las $U(\mathbb{Z}_6)=\{\bar{1},\bar{5}\}$.

**Proposición**: Sea $(A,+,\cdot)$ un anillo con identidad $1_A$, si $1_A=0_A$ entonces $A=\{0_A\}$.

**Demostración:**

Sea $(A,+,\cdot)$ un anillo con identidad $1_A$, por demostrar que: i) $\{0_A\}\subseteq A$ y ii) $A\subseteq\{0_A\}$.

i) Se sabe que $\{0_A\}\subseteq A$, pues $(A,+,\cdot)$ es anillo.

ii) Para todo $a\in A, a\cdot 1_A=a$, como $1_A=0_A$ se tiene que $a=a\cdot 1_A=a\cdot 0_A=0_A$, luego $a=0_A$, por lo tanto $A\subseteq\{0_A\}$

Luego, de i) y ii) tenemos que $A=\{0_A\}$.

Évariste Galois

(1811-1832)

Matemático francés. Educado en el Collège Royal de Louis-le-Grand, mostró unas extraordinarias aptitudes para las matemáticas. Interesado en hallar las condiciones necesarias para definir si una ecuación algebraica es posible de ser resuelta por el método de los radicales, empezó a esbozar lo que más adelante se conocería como la Teoría de Galois. A pesar de sus revolucionarios descubrimientos, todas las memorias que publicó con sus resultados fueron rechazadas por la Academia de las Ciencias. Intentos de entrar en la Escuela Politécnica se saldaron con fracasos, lo cual le sumió en una profunda crisis personal, agravada por el suicidio de su padre. Se vio implicado en un permanecen confusas. Previendo su posible muerte, trabajó en una especie de testamento científico que dirigió a su amigo Auguste Chevalier. A los pocos días tuvo lugar el duelo y el matemático, herido en el vientre, murió unas horas después, apenas cumplidos los veintiún años.

**Proposición**: Dado $(A,+,\cdot)$ un anillo, para todo $a,b\in A$ se verifica que:

i) $a\cdot 0=0\cdot a=0$

ii) $a\cdot(-b)=(-a)\cdot(b)=-(a\cdot b)$

iii) $(-a)\cdot(-b)=a\cdot b$

**Demostración**:

i) Para todo $a,b\in A$, por demostrar (i.1) $a\cdot 0=0$ y (i.2) $0\cdot a=0$

(i.1) Sabemos que $0=0+0$, luego:

$a\cdot 0=a\cdot(0+0)=a\cdot 0+a\cdot 0$, así

$a\cdot 0=a\cdot 0+a\cdot 0$, aplicando el inverso aditivo de $a\cdot 0$, se tiene

$0=a\cdot 0+0$

Por lo tanto $0=a\cdot 0$, $\forall a\in A$.

(i.2) La demostración queda de ejercicio para el lector

De lo anterior, es claro que $a\cdot 0=0\cdot a=0$

ii) Para todo $a,b\in A$, por demostrar (ii.1) $a\cdot(-b)=-(a\cdot b)$ y

(ii.2) $(-a)\cdot b=-(a\cdot b)$.

(ii.1) Sabemos que $0=b+-b$, con $b\in A$ y que $0=a\cdot 0$, para todo $a\in A$.

Luego $0=a\cdot(b+-b)=a\cdot b+a\cdot(-b)$, es decir

$0=a\cdot b+a\cdot(-b)$, sumando el inverso de $a\cdot b$ por la izquierda,

$-(a\cdot b)=0+a\cdot(-b)$

Por lo tanto $-(a\cdot b)=a\cdot(-b)$.

(ii.2) La demostración queda de ejercicio al lector

Por lo tanto, podemos decir que $a\cdot(-b)=(-a)\cdot b=-(a\cdot b)$.

iii) Para todo $a, b \in A$, por demostrar $(-a)\cdot(-b) = a \cdot b$.

Sabemos que $0 = b + -b$, con $b \in A$, tenemos que $a \cdot 0 = 0$, para todo $a \in A$.

En efecto, $(-a)\cdot 0 = 0$, luego

$$(-a)\cdot(b + -b) = 0$$

$(-a)\cdot b + (-a)\cdot(-b) = 0$, por propiedad anterior se verifica:

$-(a \cdot b) + (-a)\cdot(-b) = 0$, sumando $a \cdot b$ por la izquierda se tiene que:

$$0 + (-a)\cdot(-b) = (a \cdot b)$$

Por lo tanto $(-a)\cdot(-b) = (a \cdot b)$.

**Definición 8:** Un anillo $(A,+,\cdot)$ es un anillo cancelativo si lo es cancelativo izquierdo $\left(a \cdot b = a \cdot c, \text{ con } a \neq 0, \text{ entonces } b = c\right)$; y cancelativo derecho $\left(b \cdot a = c \cdot a, \text{ con } a \neq 0, \text{ entonces } b = c\right)$

**Proposición:** $(A,+,\cdot)$ es un anillo cancelativo si solo si $(A,+,\cdot)$ es un anillo sin divisores de cero.

**Demostración:**

$\Rightarrow$ Asumiendo $a \cdot b = 0$, con $a \neq 0$, debemos demostrar que $b = 0$.

Como $0 = a \cdot 0$, para todo $a \in A$, y $a \cdot b = 0$, se tiene que $a \cdot b = a \cdot 0$, pero $a \neq 0$, luego por hipótesis se concluye que $b = 0$.

$\Leftarrow$ Asumiendo $a \cdot b = a \cdot c$, con $a \neq 0$, debemos demostrar que $b = c$.

De $a \cdot b = a \cdot c$, sumando el inverso aditivo de $a \cdot c$ por la derecha se tiene $a \cdot b - a \cdot c = 0$, luego $a \cdot (b - c) = 0$, pero $A$ es sin divisores de cero izquierdo, entonces $b - c = 0$. Por lo tanto $b = c$.

De manera similar, asumiendo el anillo cancelativo derecho se prueba que es sin divisores de cero derecho.

**Proposición:** Sea $(A,+,\cdot)$ un anillo con identidad $1_A$. Si $u \in U(A)$, entonces $u$ no es un divisor de cero.

**Demostración:**

Supongamos, por el contrario, que $u$ es divisor de cero (izquierdo), entonces existe $r \neq 0$ en $A$ tal que $u \cdot r = 0$. Como $u \in U(A)$, $\exists v \in A$ tal que $v \cdot u = u \cdot v = 1_A$, luego multiplicando $u \cdot r = 0$ por $v$ por la izquierda se tiene $(v \cdot u) \cdot r = 0$, es decir $1_A \cdot r = 0$, lo que implica $r = 0$, ¡Contradicción! , pues $r \neq 0$.

Por lo tanto no es un divisor de cero.

**Definición 9:** Sea $(A,+,\cdot)$ un anillo con identidad, diremos que $(A,+,\cdot)$ es un anillo con división si $U(A) = A - \{0\}$.

**Definición 10:** Sea $(A,+,\cdot)$ es un anillo con división conmutativo, llamaremos a $(A,+,\cdot)$ un cuerpo.

**Ejemplo 6:**

$(\mathbb{Z}_5,+,\cdot)$ es cuerpo.

**Definición 11:** Sea $(A,+_A,\cdot_A)$ un anillo y $B$ un subconjunto no vacío de $A\,(\varnothing \neq B \subset A)$, diremos que $(B,+_A,\cdot_A)$ es un subanillo de $(A,+_A,\cdot_A)$ si $(B,+_A,\cdot_A)$ es un anillo respecto de las operaciones definidas en $A$..

**Criterio para Subanillos.**

**Proposición:** Sea $(A,+_A,\cdot_A)$ un anillo. Diremos que $(B,+_A,\cdot_A)$, con $B$ un subconjunto no vacío de $A\,(\varnothing \neq B \subset A)$, es un subanillo de $A$ si y solo si:

**1.-** Dados $a,b \in B$ entonces $a-b \in B$, y

**2.-** Dados $a,b \in B$ entonces $a \cdot b \in B$

**Demostración:**

$\Rightarrow$ ]] Como $(B,+_A,\cdot_A)$ es un anillo, es evidente que dados $a,b \in B$ , se verifica que $a-b \in B$ y $a \cdot b \in B$, por hipótesis.

$\Leftarrow$ ]] Asumiendo las condiciones (1) y (2); debemos demostrar que $(B,+_A,\cdot_A)$ es un anillo.

Para probar que es grupo abeliano, sólo basta probar la existencia de elemento neutro y elemento inverso porque $(B,+_A)$ hereda las propiedades de conmutatividad y asociatividad de $(A,+_A,\cdot_A)$ anillo.

Existe elemento neutro, pues si $x \in B$, por hipótesis, $x-x \in B$, es decir $0_A \in B$.

También se verifica la existencia de elemento inverso ya que si $x \in B$ y $0 \in B$, entonces $0 - x \in B$, luego $-x \in B$. Por lo tanto $(B,+)$ es grupo abeliano.

Por otro lado, es evidente que $(B,\cdot_A)$ es un semigrupo y se cumple la distributividad, ya que ambas propiedades se heredan del anillo $(A,+_A,\cdot_A)$.

Luego, de las condiciones anteriores, $(B,+_A,\cdot_A)$ es un anillo.

Por lo tanto $(B,+_A,\cdot_A)$ es un subanillo de $(A,+_A,\cdot_A)$.

**Ejemplo 7:**

Sea $B=\{\bar{0},\bar{2},\bar{4},\bar{6},\bar{8}\} \subset \mathbb{Z}_{10}$. Afirmamos que $(B,+_{\text{mod}10},\cdot_{\text{mod}10})$ es un subanillo de $\mathbb{Z}_{10}$.

En efecto, considerando las siguientes tablas para cada operación, notamos que $(B,+_{\text{mod}10})$ es grupo abeliano, $(B,\cdot_{\text{mod}10})$ es un semigrupo y además se cumple distributividad.

| $+$ | $\bar{0}$ | $\bar{2}$ | $\bar{4}$ | $\bar{6}$ | $\bar{8}$ |
|---|---|---|---|---|---|
| $\bar{0}$ | $\bar{0}$ | $\bar{2}$ | $\bar{4}$ | $\bar{6}$ | $\bar{8}$ |
| $\bar{2}$ | $\bar{2}$ | $\bar{4}$ | $\bar{6}$ | $\bar{8}$ | $\bar{0}$ |
| $\bar{4}$ | $\bar{4}$ | $\bar{6}$ | $\bar{8}$ | $\bar{0}$ | $\bar{2}$ |
| $\bar{6}$ | $\bar{6}$ | $\bar{8}$ | $\bar{0}$ | $\bar{2}$ | $\bar{4}$ |
| $\bar{8}$ | $\bar{8}$ | $\bar{0}$ | $\bar{2}$ | $\bar{4}$ | $\bar{6}$ |

| $\cdot$ | $\bar{0}$ | $\bar{2}$ | $\bar{4}$ | $\bar{6}$ | $\bar{8}$ |
|---|---|---|---|---|---|
| $\bar{0}$ | $\bar{0}$ | $\bar{0}$ | $\bar{0}$ | $\bar{0}$ | $\bar{0}$ |
| $\bar{2}$ | $\bar{0}$ | $\bar{4}$ | $\bar{8}$ | $\bar{2}$ | $\bar{6}$ |
| $\bar{4}$ | $\bar{0}$ | $\bar{8}$ | $\bar{6}$ | $\bar{4}$ | $\bar{2}$ |
| $\bar{6}$ | $\bar{0}$ | $\bar{2}$ | $\bar{4}$ | $\bar{6}$ | $\bar{8}$ |
| $\bar{8}$ | $\bar{0}$ | $\bar{6}$ | $\bar{2}$ | $\bar{8}$ | $\bar{4}$ |

Por lo tanto $(B,+_{\text{mod}10},\cdot_{\text{mod}10})$ es un subanillo de $(\mathbb{Z}_{10},+,\cdot)$.

**Ejemplo 8:**

Sea $(A,+,\cdot)$ un anillo. Entonces $Z(A)=\{c\in A/\, a\cdot c=c\cdot a,\forall a\in A\}$, llamado el centro del anillo $(A,+,\cdot)$,es un subanillo de $(A.+,\cdot)$.

En efecto, es claro que $Z(A)\subset A$ y $Z(A)\neq\varnothing$ (pues $0\cdot a=a\cdot 0=0$, con $0\in Z(A)$), además:

**(i)** Dados $x,y\in Z(A)$, implica que $a\cdot x=x\cdot a$ y $a\cdot y=y\cdot a$, $\forall\, a\in A$. Luego, $(x-y)\cdot a=x\cdot a-y\cdot a=a\cdot x-a\cdot y=a\cdot(x-y)$. Por lo tanto $x-y\in Z(A)$.

**(ii)** Del hecho que $x,y\in Z(A)$ y por la asociatividad del producto, se tiene $(x\cdot y)\cdot a=x\cdot(y\cdot a)=x\cdot(a\cdot y)=(x\cdot a)\cdot y=(a\cdot x)\cdot y=a\cdot(x\cdot y)$. Por lo tanto $x\cdot y\in Z(A)$.

En consecuencia de lo anterior, $Z(A)$ es un subanillo de $(A.+,\cdot)$.

**Ejemplo 9:**

Sea $(A,+,\cdot)$ un anillo y $H=\{B:B\leq A\}$ una familia de subanillos de $A$. Entonces $\bigcap_{B\in H} B$ es un subanillo de $(A,+,\cdot)$.

i) Es claro que $\bigcap_{B\in H} B\neq\varnothing$; como $0_A\in B$ para cada $B\in H$, se tiene que $0_A\in\bigcap_{B\in H} B$.

ii) Si $x, y \in \bigcap_{B\in H} B$, por demostrar que $x-y \in \bigcap_{B\in H} B$ y $x\cdot y \in \bigcap_{B\in H} B$ .

(ii.1) Si $x, y \in \bigcap_{B\in H} B$, entonces $x, y \in B$, para cada $B \in H$. Pero $H$ es una familia de subanillos de $A$, luego $x-y \in B$, para cada $B \in H$. Por lo tanto, $x-y \in \bigcap_{B\in H} B$.

(ii.2) Si $x, y \in \bigcap_{B\in H} B$, es claro que $x, y \in B$, para cada $B \in H$, y como $H$ es una familia de subanillos de $A$, se tiene que $x\cdot y \in B$. Luego $x\cdot y \in \bigcap_{B\in H} B$.

En consecuencia, podemos decir que $\bigcap_{B\in H} B$ es un subanillo de $(A,+,\cdot)$.

**Definición 12:** Sea $(A,+,\cdot)$ un anillo y $S \subset A$ , con $S$ no vacío. El conjunto, anotado por $H(S)=\{B : B \le A \wedge S \subset B\}$, es la familia de subanillos de $(A,+,\cdot)$ que contienen a $S$. El subanillo generado por $S$, anotado por $A[S]$ se define por $A[S]=\bigcap B$, tal que $B \in H(S)$.

**Proposición:** Sea $(A,+,\cdot)$ un anillo con identidad, $S=\{s\}\subset A$, tal que $s\in Z(A)$. Entonces $A[S]=\left\{\sum_{i=0}^{n}a_i s^i : a_i\in A, i\in\mathbb{N}\right\}$.

**Demostración:**

Llamaremos a $\left\{\sum_{i=0}^{n}a_i s^i : a_i\in A, i\in\mathbb{N}\right\}=B$

Primero debemos verificar que $B$ es un subanillo de $(A,+,\cdot)$, para luego demostrar la igualdad con $A[S]$.

Se tiene que $(B,+,\cdot)$ es un subanillo de $(A,+,\cdot)$ pues:

i) Afirmamos que $B\neq\varnothing$, ya que basta considerar $a_i\in A$, con $a_i=0_A$ de tal manera que $\sum_{i=0}^{n}a_i s^i=\sum_{i=0}^{n}0_A s^i=0_B$, tal que $0_B\in B$

ii) Dados $x,y\in B$ por demostrar $x-y\in B$.

Sean $x=\sum_{i=0}^{n}a_i s^i$ , $y=\sum_{i=0}^{n}b_i s^i$ en $B$, entonces

$x-y=\sum_{i=0}^{n}a_i s^i-\sum_{i=0}^{n}b_i s^i=\sum_{i=0}^{n}(a_i-b_i)s^i$, con $a_i-b_i=c_i\in A$ para todo i,

entonces $x-y=\sum_{i=0}^{n}c_i s^i$. Por lo tanto $x-y\in B$.

En caso de que $n \neq m$ debemos considerar que si $x = \sum_{i=0}^{n} a_i s^i$ e $y = \sum_{i=0}^{m} b_i s^i$ , basta con igualar el número de sumandos agregando en el menor cuantos ceros sean necesarios para su demostración.

iii) Dados $x, y \in B$ por demostrar $x \cdot y \in B$

Si $x = \sum_{i=0}^{n} a_i s^i$ e $y = \sum_{j=0}^{m} b_j s^j$ entonces;

$$x = a_o + a_1 s + \cdots\cdots\cdots + a_n s^n$$

$$y = b_0 + b_1 s + \cdots\cdots\cdots + b_m s^m \text{ , luego } x \cdot y \text{ será}$$

$$x \cdot y = (a_o + a_1 s + \cdots\cdots\cdots + a_n s^n) \cdot (b_0 + b_1 s + \cdots\cdots\cdots + b_m s^m)$$

$$= a_0 b_0 + a_0 b_1 s + \cdots + a_0 b_m s^m + a_1 b_0 s + a_1 b_1 s^2 + \cdots + a_1 b_m s^{n+1} + \cdots +$$

$$+ a_n b_0 s^n + \cdots + a_n b_1 s^{n+1} + \cdots + a_n b_n s^{m+n}$$

$$= a_0 b_0 + \underbrace{(a_0 b_1 + a_1 b_0)}_{\in A} s + \cdots\cdots + a_n b_n s^{m+n}$$

$$x \cdot y = \sum_{k=0}^{m+n} c_k s^k \in B$$

Por lo tanto $(B, +, \cdot)$ es un subanillo de $(A, +, \cdot)$.contiene a $S = \{s\}$, ya que si $1_A \in A$, entonces $\sum_{i=0}^{n} a_i s^i = \sum_{i=0}^{n} 1_A s^i = \sum_{i=0}^{n} s^i$, considerando $i = 1$ se tiene que $\sum_{i=1}^{1} s^i = s$.

Ahora que ya hemos demostrado que $(B,+,\cdot)$ es un subanillo de $(A,+,\cdot)$, demostraremos la igualdad $A[S]=B$, pero demostrar esta igualdad implica verificar

(i) $A[S]\subseteq B$. y (ii) $B\subseteq A[S]$

(i) Si $x\in A[S]$, entonces $x\in \bigcap_{B\in H(S)} B$. Como $x\in \bigcap_{B\in H(S)} B$ eso implica que $x\in B$ tal que $B\in H(S)$(familia de subanillos de $(A,+,\cdot)$ que contienen a $S$). Ahora bien, como $(B,+,\cdot)$ es un subanillo de $(A,+,\cdot)$ que contiene a $S=\{s\}$, resulta evidente que $x\in B$. Por lo tanto $A[S]\subset B$

(ii) Probar que $B\subseteq A[S]$ resulta evidente al considerar lo anterior, en efecto, si $x\in B$ entonces $x=\sum_{i=0}^{n} a_i s^i$ y considerando que $A[S]$ es un anillo que contiene a $S$ por definición, luego están los productos de elementos de $A$ por "$s$" (y potencias de "$s$") y la suma de estos elementos. Entonces $x\in A[S]$. Por lo tanto $B\subseteq A[S]$.

Luego de (i) y (ii) se tiene que $A[S]=\left\{\sum_{i=0}^{n} a_i s^i : a_i\in A, i\in\mathbb{N}\right\}$.

**Definición13:** Sea $(A,+,\cdot)$ un anillo e $I$ un subconjunto no vacío de $A$. Diremos que $I$ es un ideal de $(A,+,\cdot)$ si:

**1.-** Dados $x, y \in I$ entonces $x - y \in I$

**2.-** $a \in A, x \in I$ entonces $\begin{cases} i)\ a \cdot x \in I \\ ii)\ x \cdot a \in I \end{cases}$

**Nota:** Si en la definición 13 se verifica (1) y (2.i) se dice que $I$ es ideal izquierdo de $(A,+,\cdot)$; en cambio, si se verifica (1) y (2.ii) diremos que $I$ ideal derecho de $(A,+,\cdot)$.

**Notación**: $I$ ideal de $A$: $I \lhd A$.

**Ejemplos**:

**10.-** Dado $A$ un anillo, ¿$Z(A) \lhd A$?.

i) Si $x,\ y\ \in Z(A)$ es fácil ver que $x - y \in Z(A)$, es decir $(x-y)\cdot a = a\cdot(x-y)$, $\forall\, a \in A$.

Se tiene que $(x-y)\cdot a = x\cdot a - y\cdot a$, $\forall\, x, y \in Z(A)$

$$= a\cdot x - a\cdot y$$

$$= a\cdot(x-y).$$

Por lo tanto $x - y \in Z(A)$.

Emil Artin

(1921-1931) un período de productividad investigativa difícil de igualar en la vida de un matemático.
En los diez años de vida de Artin que transcurren entre 1921 y 1931, sus aportes al desarrollo de las matemáticas son más que significativos. Se destaca su contribución a las teorías de campo y trenzas y, alrededor de 1928, elabora el modelo de anillos llamado «anillos de Artinian». En 1927, Artin halla la solución para uno de los 23 famosos problemas que presentó en 1900 David Hilbert. También en ese mimo año de 1927, desarrolló una ley general de reciprocidad que incluyó todos los leyes de la reciprocidad conocidas previamente y que habían sido descubiertas a partir de la primera que formuló Carl Gauss.

ii) Por otro lado, si $b \in A,\ x \in Z(A)$ notamos que (ii.1) $b \cdot x \notin Z(A)$ y (ii.2) $x \cdot b \notin Z(A)$. En efecto,

$$(b \cdot x) \cdot a = b \cdot (x \cdot a), \forall x \in Z(A)$$
$$= b \cdot (a \cdot x)$$
$$= (b \cdot a) \cdot x$$
$$\neq (a \cdot b) \cdot x,$$ ya que $(A,+,\cdot)$ es un anillo no conmutativo. Por lo tanto $Z(A)$ no es ideal de $(A,+,\cdot)$

**Nota:** En general $Z(A)$ es un ideal de $(A,+,\cdot)$, siempre que $(A,+,\cdot)$ sea un anillo conmutativo.

**11.-** $(2\mathbb{Z},+,\cdot)$ es un ideal de $(\mathbb{Z},+,\cdot)$, $\left(2\mathbb{Z} = \{2 \cdot k / k \in \mathbb{Z}\}\right)$

i) Si $x, y \in 2\mathbb{Z}$, por demostrar que $x - y \in 2\mathbb{Z}$. En efecto, $x = 2 \cdot k$ e $y = 2 \cdot k_1$, con $k, k_1 \in \mathbb{Z}$. Luego $x - y = 2 \cdot k - 2 \cdot k_1 = 2 \cdot (k - k_1)$, tal que $k - k_1 \in \mathbb{Z}$. Por lo tanto $x - y \in 2\mathbb{Z}$

ii) Si $a \in \mathbb{Z}$, $x \in 2\mathbb{Z}$ por demostrar: (ii.1) $a \cdot x \in 2\mathbb{Z}$ y (ii.2) $x \cdot a \in 2\mathbb{Z}$

(ii.1) Se tiene que $a \cdot x = a \cdot 2 \cdot k = 2 \cdot (a \cdot k) \in 2\mathbb{Z}$, tal que $a \cdot k \in \mathbb{Z}$.

De igual manera sucederá para $x \cdot a \in 2\mathbb{Z}$.

Por lo tanto, tenemos que $(2\mathbb{Z},+,\cdot) \lhd (\mathbb{Z},+,\cdot)$

**12.-** ¿$(\mathbb{Q},+,\cdot)$ es un ideal de $(\mathbb{R},+,\cdot)$?

i) Si $x, y \in \mathbb{Q}$ , debemos demostrar que $x - y \in \mathbb{Q}$. Si $x = \frac{q}{r}$ y $y = \frac{m}{n}$ entonces $x - y = \frac{q}{r} - \frac{m}{n} = \frac{nq - mr}{rn} \in \mathbb{Q}$. Por lo tanto $x - y \in \mathbb{Q}$

ii) Dado un $a \in \mathbb{R}, x \in \mathbb{Q}$ por demostrar: (ii.1) $x \cdot a \in \mathbb{Q}$ y (ii.2) $a \cdot x \in \mathbb{Q}$.

(ii.1) Consideremos $x = \frac{m}{n} = 1 \in \mathbb{Q}$, $a = \sqrt{3} \in \mathbb{R}$ tal que

$$x \cdot a = \frac{m}{n} \cdot \sqrt{3} = 1 \cdot \sqrt{3} = \sqrt{3} \notin \mathbb{Q}. \text{ Luego } a \cdot x \notin \mathbb{Q}.$$

Por lo tanto $(\mathbb{Q}, +, \cdot)$ no es un ideal de $(\mathbb{R}, +, \cdot)$.

**Observación:** Todo ideal es un anillo es subanillo del anillo.

Todo subanillo de un anillo no necesariamente es un ideal del anillo.

**Proposición:** Sea $(A, +, \cdot)$ un anillo con identidad $1_A$ e $I$ ideal de $A$. Si $1_A \in I$ entonces $I = A$.

**Demostración**:

Si $1_A \in I$, por demostrar que $I = A$, es decir verificar: $I \subset A$ y $A \subset I$. Pero $I \subset A$, por condición de $I \lhd A$. Por otro lado, dado $a \in A$, por demostrar que $a \in I$, luego si $1_A \in I$, tenemos que $1_A \cdot a = a \in I$. Por lo tanto $A \subset I$, en consecuencia $I = A$.

**Proposición:** Sea $(A,+,\cdot)$ un anillo con identidad e $I$ ideal de $A$. Si $u \in U(A)$ tal que $u \in I$, entonces $I = A$.

**Demostración:**

Debemos demostrar que $I = A$, es decir que: $I \subset A$ y $A \subset I$. Pero $I \subset A$ por condición de $I \lhd A$, sólo bastaría verificar que $A \subset I$.

En efecto, dado $u \in U(A)$, entonces existe $v \in A$ tal que $u \cdot v = v \cdot u = 1$, ahora considerando que $u \in I$, tenemos que $u \cdot v \in I$, lo que implica $1_A \in I$. Por lo tanto $I = A$.

## Ejercicios

**1.-** Establezca cuales de los siguientes sistemas algebraicos tienen estructura de anillo.

a) $(\mathbb{Z}\times\mathbb{Z},+,\cdot)$.

b) $(B,+,\cdot)$, tal que $B=\{ri / r\in\mathbb{R}\wedge i=\sqrt{-1}\}$

**2.-** Encuentre las unidades de:

a) $\mathbb{Z}$ ; b) $\mathbb{Z}_5$ ; c) $\mathbb{Q}$ ; d) $\mathbb{Z}_6$

**3.-** $(A,+,\cdot)$ anillo $a\in A$ fijo. Demuestre que $I_a=\{x\in A: a\cdot x=0\}$ es un subanillo de $A$.

## Desarrollo:

**1.-** Establezca cuales de los siguientes sistemas algebraicos tienen estructura de anillo.

a) $(\mathbb{Z}\times\mathbb{Z},+,\cdot)$.

Probar que $(\mathbb{Z}\times\mathbb{Z},+,\cdot)$ tiene estructura de anillo, significa verificar:

(1) $(\mathbb{Z}\times\mathbb{Z},+)$ es grupo abeliano.

(2) $(\mathbb{Z}\times\mathbb{Z},+)$ es semigrupo.

(3) Existe distributividad de $(\cdot)$ con respecto a $(+)$ en la estructura en $(\mathbb{Z}\times\mathbb{Z},+,\cdot)$

(1) Definimos $(+)$ en el conjunto $\mathbb{Z}\times\mathbb{Z}$ y luego verificamos que es grupo abeliano.

$$+ : (\mathbb{Z}\times\mathbb{Z})\times(\mathbb{Z}\times\mathbb{Z})\longrightarrow(\mathbb{Z}\times\mathbb{Z})$$

$$\left[(a_1,b_1),(a_2,b_2)\right]\mapsto(a_1,b_1)+(a_2,b_2)=(a_1+a_2,b_1+b_2)$$

i) Conmutatividad:

Para todo $(a,b),(c,d)\in\mathbb{Z}\times\mathbb{Z}$, por demostrar: $(a,b)+(c,d)=(c,d)+(a,b)$

Es evidente pues $(a,b)+(c,d) = (a+c,b+d)$, por conmutatividad en $\mathbb{Z}$

$$=(c+a,d+b)$$

$$=(c,d)+(a,b)$$

Por lo tanto $(\mathbb{Z}\times\mathbb{Z},+,\cdot)$ es conmutativo.

ii) Asociatividad:

Para todo $(a_1,b_1),(a_2,b_2),(a_3,b_3)\in\mathbb{Z}\times\mathbb{Z}$, por demostrar:

$$(a_1,b_1)+\left[(a_2,b_2)+(a_3,b_3)\right]=\left[(a_1,b_1)+(a_2,b_2)\right]+(a_3,b_3)$$

En efecto:

$$(a_1,b_1)+\left[(a_2,b_2)+(a_3,b_3)\right]=(a_1,b_1)+(a_2+a_3,b_2+b_3)$$

$$=\left(a_1+\left[a_2+a_3\right],b_1+\left[b_2+b_3\right]\right)$$

$$=\left(\left[a_1+a_2\right]+a_3,\left[b_1+b_2\right]+b_3\right), \text{ por asoc. en } \mathbb{Z}$$

$$=\left[(a_1+a_2),(b_1+b_2)\right]+(a_3,b_3)$$

$$=\left[(a_1,b_1)+(a_2,b_2)\right]+(a_3,b_3)$$

Por lo tanto $(\mathbb{Z}\times\mathbb{Z},+)$ es asociativo.

ii) Elemento neutro:

Debe existir un $(a,b)\in\mathbb{Z}\times\mathbb{Z}$, para todo $(x,y)\in\mathbb{Z}\times\mathbb{Z}$ tal que $(x,y)+(a,b)=(a,b)+(x,y)=(a,b)$, para todo $(a,b)\in\mathbb{Z}\times\mathbb{Z}$).

Supongamos que: $(x,y)+(a,b)=(a,b)$ en efecto:

$$(x,y)+(a,b)=(x+a,y+b)=(a,b)$$

Luego por igualdad de pares ordenados se tiene:

$x+a=a$, entonces $x=0$, por cancelación en $\mathbb{Z}$

$y+b=b$ , entonces $y=0$, por cancelación en $\mathbb{Z}$

Por lo tanto el neutro existe y es el par $(x,y)=(0,0)$ de tal manera que $(0,0)+(a,b)=(a,b)$

iii) Elemento inverso:

Para cualquier $(a,b)\in\mathbb{Z}\times\mathbb{Z}$ por encontrar $(u,v)\in\mathbb{Z}\times\mathbb{Z}$ tal que $(a,b)+(u,v)=(u,v)+(a,b)=(0,0)$

Supongamos que: $(a,b)+(u,v)=(0,0)$

En efecto se tiene:

$(a+u,b+v)=(0,0)$, entonces $\begin{cases} a+u=0 \\ b+v=0 \end{cases}$ de tal forma que, $\begin{cases} u=-a \\ v=-b \end{cases}$

Por lo tanto el inverso de $(a,b)$ existe y es el par $(u,v)=(-a,-b)\in\mathbb{Z}$ x $\mathbb{Z}$.

En consecuencia de i), ii), iii), iv), $(\mathbb{Z}\times\mathbb{Z},+)$ es grupo abeliano.

(2) Definimos $(\cdot)$ en el conjunto $\mathbb{Z}\times\mathbb{Z}$ para luego verificar si $(\mathbb{Z}\times\mathbb{Z},\cdot)$ es semigrupo.

$$\cdot : (\mathbb{Z}\times\mathbb{Z})\times(\mathbb{Z}\times\mathbb{Z})\longrightarrow(\mathbb{Z}\times\mathbb{Z})$$

$$\big[(a,b),(a_1,b_1)\big]\mapsto(a,b)\cdot(a_1,b_1)=\underbrace{(a\cdot a_1,b\cdot b_1)}_{\in\mathbb{Z}}$$

¿$(\mathbb{Z}\times\mathbb{Z},\cdot)$ es un semigrupo?

Para todo $(a,b),(c,d),(e,f)\in\mathbb{Z}\times\mathbb{Z}$, se tiene que $(a,b)\cdot\big[(c,d)\cdot(e,f)\big]=\big[(a,b)\cdot(c,d)\big]\cdot(e,f)$.

En efecto:

$$\begin{aligned}(a,b)\cdot\big[(c,d)\cdot(e,f)\big]&=(a,b)\cdot\big[(c\cdot e,d\cdot f)\big]\text{; por definición de }(\cdot)\text{ en }\mathbb{Z}\times\mathbb{Z}\\&=\big(a\cdot[c\cdot e],b\cdot[d\cdot f]\big)\text{; por asociatividad en }\mathbb{Z}\\&=\big([a\cdot c]\cdot e,[b\cdot d]\cdot f\big)\text{; por definición de }(\cdot)\text{ en }\mathbb{Z}\times\mathbb{Z}\\&=\big[(a\cdot c,b\cdot d)\big]\cdot(e,f)\\&=\big[(a,b)\cdot(c,d)\big]\cdot(e,f)\end{aligned}$$

Por lo tanto $(\mathbb{Z}\times\mathbb{Z},\cdot)$ es asociativo.

(3) Verificar si en $(\mathbb{Z}\times\mathbb{Z},+,\cdot)$ existe distributividad de $(\cdot)$ con respecto a $(+)$

Para todo $(a,b),(c,d),(e,f)\in\mathbb{Z}\times\mathbb{Z}$, por demostrar que $(a,b)\cdot[(c,d)+(e,f)]=(a,b)\cdot(c,d)+(a,b)\cdot(e,f)$

En efecto, pues $(a,b)\cdot[(c,d)+(e,f)]=(a,b)\cdot[(c+e,d+f)]$

$=(a\cdot[c+e],b\cdot[d+f]),$

por distributividad en $\mathbb{Z}$, se tiene que

$=(a\cdot c+a\cdot e,b\cdot d+b\cdot f),$

por definición de $(+)$ en $\mathbb{Z}\times\mathbb{Z}$, se tiene

$=(a\cdot c,b\cdot d)+(a\cdot e,b\cdot f)$

por definición de $(\cdot)$ en $\mathbb{Z}\times\mathbb{Z}$, se tiene

$=(a,b)\cdot(c,d)+(a,b)\cdot(e,f)$

Por lo tanto en $(\mathbb{Z}\times\mathbb{Z},+,\cdot)$ existe distributividad de $(\cdot)$ con respecto a $(+)$.

Luego de (1),(2) y (3), $(\mathbb{Z}\times\mathbb{Z},+,\cdot)$ es un anillo

b) $(B,+,\cdot)$, tal que $B=\{ri/r\in\mathbb{R}\wedge i=\sqrt{-1}\}$

Probar que $(B,+,\cdot)$ tiene estructura de anillo significa verificar:

(1) $(B,+)$ es un grupo abeliano

(2) $(B,\cdot)$ es asociativo

(3) Existe distributividad de $(\cdot)$ con respecto a $(+)$ en la estructura en $(B,+,\cdot)$

Por definición:

$+ : \ B \times B \longrightarrow B$

$(ai, bi) \mapsto +(ai, bi) = ai + bi = (a+b)i$ tal que $a + b \in \mathbb{R}$.

i) Conmutatividad:

Dados $ai, bi \in B$ por demostrar que $ai + bi = bi + ai$.

En efecto:

$ai + bi = (a+b)i$, por conmutatividad en $\mathbb{R}$, ya que $a, b \in \mathbb{R}$, se tiene que

$= (b+a)i$

$= bi + ai$

ii) Asociatividad:

Dados $ai, bi, ci \in B$ por demostrar que: $ai + (bi + ci) = (ai + bi) + ci$

En efecto:

$ai + (bi + ci) = ai + [(b+c)i]$

$= [a + (b+c)]i$

$= [(a+b) + c]i$, por asociatividad en $\mathbb{R}$

$= [(a+b)i + ci]$

$= (ai + bi) + ci$

Por lo tanto $(B, +)$ es asociativo

iii) Elemento Neutro:

Debe existir un $xi \in B$ para todo $ai \in B$ tal que

$ai + xi = xi + ai = ai, \ \forall ai \in B$

Supongamos $ai + xi = ai$ , en efecto:

$$(a + x)i = ai$$

Como $a + x = a$ con $(a + x) \in \mathbb{R}$ eso implica que $x = 0$

Por lo tanto $xi \in B$ existe y $xi = 0i$

Por lo tanto $(B, +)$ tiene elemento neutro, para todo elemento de $B$.

iv) Elemento Inverso:

Para todo $ai \in B$ debe existir $yi \in B$ tal que

$$ai + yi = yi + ai = 0i, \ \forall ai \in B$$

Supongamos que $ai + yi = 0i$, en efecto:

$(a + y)i = 0i$ , con $a + y \in \mathbb{R}$

Como $a + y = 0$, con $(a + y) \in \mathbb{R}$, eso implica que $y = -a$

Por lo tanto el inverso de $ai$ es $-ai$

Por lo tanto $(B, +)$ tiene elemento inverso.

De lo anterior, $(B, +)$ es grupo abeliano.

(2) Por definir $(\cdot)$ en $B$, para verificar si $(B, \cdot)$ es asociativo

Por definir $\cdot : B \times B \longrightarrow B$

$$(ai, bi) \mapsto \cdot(ai, bi) = ai \cdot bi = -a \cdot b \notin B$$

Por lo tanto no se puede tener un anillo.

**2.-** Encuentre las unidades de:

a) $U(\mathbb{Z}) = \{1, -1\}$

b) $U(\mathbb{Z}_5) = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}\} = \mathbb{Z}_5 - \{\bar{0}\}$ ; identidad de $\mathbb{Z}_5$ es $\bar{1}$

| + | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ | $\bar{4}$ |
|---|---|---|---|---|---|
| $\bar{0}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ | $\bar{4}$ |
| $\bar{1}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ | $\bar{4}$ | $\bar{0}$ |
| $\bar{2}$ | $\bar{2}$ | $\bar{3}$ | $\bar{4}$ | $\bar{0}$ | $\bar{1}$ |
| $\bar{3}$ | $\bar{3}$ | $\bar{4}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ |
| $\bar{4}$ | $\bar{4}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ |

| · | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ | $\bar{4}$ |
|---|---|---|---|---|---|
| $\bar{0}$ | $\bar{0}$ | $\bar{0}$ | $\bar{0}$ | $\bar{0}$ | $\bar{0}$ |
| $\bar{1}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ | $\bar{4}$ |
| $\bar{2}$ | $\bar{0}$ | $\bar{2}$ | $\bar{4}$ | $\bar{1}$ | $\bar{3}$ |
| $\bar{3}$ | $\bar{0}$ | $\bar{3}$ | $\bar{1}$ | $\bar{4}$ | $\bar{2}$ |
| $\bar{4}$ | $\bar{0}$ | $\bar{4}$ | $\bar{3}$ | $\bar{2}$ | $\bar{1}$ |

$\mathbb{Z}_5$ es un cuerpo, por lo que no tiene divisores de cero.

c) $U(\mathbb{Q}) = \mathbb{Q} - \{0\}$ es un cuerpo.

d) $U(\mathbb{Z}_6) = \{\bar{1}, \bar{5}\}$ y sus divisores de cero son $\bar{2}$, $\bar{3}$ y $\bar{4}$.

**Nota**: Cuando se esta en presencia de clases residuales modulo un número primo se asegura tener un "Dominio de Integridad".

**3.-** Sea $(A,+,\cdot)$ anillo con $a \in A$ fijo. Demuestre que $I_a = \{x \in A : a \cdot x = 0\}$ es un subanillo de $(A,+,\cdot)$.

**Dem.**:

i) Es claro que $I_a \neq \varnothing$, pues $0 \in I_a$.

ii) Si $x, y \in I_a$ , por demostrar (a) $x - y \in I_a$ y (b) $x \cdot y \in I_a$

a) Si $x \in I_a$ , entonces $a \cdot x = 0$, y si $y \in I_a$ , entonces $a \cdot y = 0$

Ahora bien, $a \cdot (x - y) = a \cdot x - a \cdot y = 0$. Por lo tanto $x - y \in I_a$

b) Si $x \in I_a$ , entonces $a \cdot x = 0$, y si $y \in I_a$ , entonces $a \cdot y = 0$

Ahora bien, $a \cdot (x \cdot y) = (a \cdot x) \cdot y = 0 \cdot y = 0$. Por lo tanto $x \cdot y \in I_a$

En consecuencia de (i) y (ii) $I_a$ es subanillo de $(A,+,\cdot)$.

## Autoevaluación 9

Pruebe o refute las siguientes afirmaciones. Justifique sus respuestas.

**1.-** Establezca cuales de los siguientes sistemas algebraicos tienen estructura de anillo.

a) $\left(\left\{a+b\sqrt{2}/a,b\in\mathbb{Z}\right\},+,\cdot\right)$.

b) $\left(\left\{a+b\sqrt{2}/a,b\in\mathbb{Q}\right\},+,\cdot\right)$.

c) $(P(s),\oplus,\odot)$ donde $P(s)$ es el conjunto potencia de $S$, $P(s)=\{A/A\subset S\}$ tal que se define $A\oplus B=A\cup B$ y $A\odot B=A\cap B$

**2.-** Sea $A$ un anillo conmutativo e $I\lhd A$.

Pruebe que $\sqrt{I}=\left\{a\in A:a^n\in I\ ,\forall n\in\mathbb{Z}^+\right\}$ es ideal de $A$.

**3.-**Sea $(A,+,\cdot)$un anillo cualquiera. Sea $B\subseteq A$, si $(B,+_B,\cdot_B)$es un anillo y $1_A=1_B$ decimos que el anillo $(B,+_B,\cdot_B)$ es un subanillo de $(A,+,\cdot)$.

**4.-** Sea $(A,+,\cdot)$ un anillo conmutativo e $I\lhd A$. Si existe un elemento $x\in A$ tal que $I=\langle x\rangle$, donde $\langle x\rangle=A\cdot x=\{a\cdot x/a\in A\}$ decimos que $(I,+,\cdot)$ es un ideal principal del anillo $(A,+,\cdot)$.

**5.-** Sea $(A,+,\cdot)$ un anillo tal que $a^2=a$ , $\forall a\in A$ (un anillo con esta propiedad se llama booleana) es conmutativo.

**6.-** Pruebe que $(B,+,\cdot)$ es un anillo, si $c\cdot a=c\cdot b$, implica $a=b$ con $c\in B$.