Estructuras Algebraicas para la Computación

Mariam Cobalea

Universidad de Málaga
Dpto. de Matemática Aplicada

Tema 3: Grupos, anillos y cuerpos

- Grupos y subgrupos. Clases laterales y teorema de Lagrange.
- Introducción a la teoría de la codificación.
- Anillos. Elementos inversibles y divisores de cero. Cuerpos.

Anillos

Introducción

Para resolver en $\mathbb{Z}$ una ecuación tal como

$$2(x+3)+4(x-5)=28$$

procedemos de la siguiente manera:

- Se aplica la propiedad distributiva del producto respecto a la suma
$$(2x+2\cdot 3)+(4x+4(-5))=28$$
- Se aplican las propiedades asociativa y conmutativa de la suma
$$(2x+4x)+(6-20)=28$$
- Se aplica la propiedad distributiva del producto respecto a la suma y se suma 14 en ambos miembros
$$((2+4)x+(-14))+14=28+14$$
- Se aplica la propiedad asociativa de la suma
$$6x+((-14)+14)=42$$

Anillos

Introducción

- Se aplica la propiedad del opuesto
$$6x+(0)=42$$
- Se usa la propiedad de identidad del neutro de la suma
$$6x=42$$
- Se aplica la propiedad de simplificación del producto
$$6x=6\cdot 7 \implies x=7$$

Anillos

En este ejemplo, además de usar que la suma y el producto son operaciones binarias en el conjunto de los enteros, se aplican otras propiedades.
Estas propiedades se usan para definir la estructura algebraica de **anillo**.

Definición

Sean $+$ *y* $\cdot$ *dos operaciones binarias definidas en un conjunto* A. *Se dice que* $(A,+,\cdot)$ *es un* **anillo** *si se verifica:*

1. $(A,+)$ *es grupo abeliano.*
2. *La operación* $\cdot$ *es asociativa:* $(a\cdot b)\cdot c = a\cdot(b\cdot c)$
3. *La operación* $\cdot$ *es distributiva respecto de* $+$

$$\begin{cases} a\cdot(b+c) &= a\cdot b + a\cdot c \\ (b+c)\cdot a &= b\cdot a + c\cdot a \end{cases}$$

Ejemplos Son anillos:

1. $(\mathbb{Z},+,\cdot)$, $(m\mathbb{Z},+,\cdot)$, $(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$, $(\mathbb{C},+,\cdot)$

Anillos

Ejemplos Son anillos:

2. $(\mathbb{Z}_m,+_m,\cdot_m)$, $1 < m \in \mathbb{N}$
3. $(\mathcal{M}_{2\times 2}(\mathbb{R}),+,\cdot)$

Ejercicio

1. En el conjunto $\mathcal{F}(\mathbb{R}) = \{f : D \subseteq \mathbb{R} \to \mathbb{R}\}$ se definen la suma y el producto usuales

$$\forall x \in D,\quad \begin{aligned}(f+g)(x) &= f(x)+g(x)\\ (f\cdot g)(x) &= f(x)\cdot g(x)\end{aligned}$$

   Demuestra que $(\mathcal{F}(\mathbb{R}),+,\cdot)$ es anillo.
2. Sea el conjunto $\mathcal{A}_{2\times 2}(\mathbb{Z}_3)$ de las matrices dos por dos antisimétricas

$$\mathcal{A}_{2\times 2}(\mathbb{Z}_3) = \left\{A = \begin{pmatrix} x & y \\ -y & x \end{pmatrix},\ x,y \in \mathbb{Z}_3\right\}$$

   Demuestra que $(\mathcal{A}_{2\times 2}(\mathbb{Z}_3),+,\cdot)$ es anillo.

Anillos

Propiedades de los Anillos

En todo anillo $(A,+,\cdot)$ se verifican todas las propiedades estudiadas anteriormente para los grupos, (por ser $(A,+)$ grupo abeliano). Y además

Teorema

Sea $(A,+,\cdot)$ *un anillo. Para todo* $a,b \in A$ *se verifica:*

1. $a\cdot 0 = 0\cdot a = 0$
2. $(-a)\cdot b = a\cdot(-b) = -(a\cdot b)$
3. $(-a)\cdot(-b) = a\cdot b$

Las dos últimas propiedades se conocen como ***reglas de los signos***.

Anillos

Propiedades de los Anillos

Demostración:

1. $a\cdot 0 = a(0+0) = a\cdot 0 + a\cdot 0 \implies a\cdot 0 = 0$

   Análogamente, $0\cdot a = 0$

2. Veamos que $(-a)\cdot b = a\cdot(-b) = -(a\cdot b)$
   - $a\cdot b + (-a)\cdot b = (a+(-a))\cdot b = 0\cdot b = 0 \implies (-a)\cdot b = -(a\cdot b)$
   - $a\cdot + a\cdot(-b) = a\cdot(b+(-b)) = a\cdot 0 = 0 \implies a\cdot(-b) = -(a\cdot b)$
3. $(-a)\cdot(-b) = a\cdot b$

   Ejercicio

Anillos
Definiciones adicionales

$(A,+,\cdot)$ es un ***anillo unitario*** si tiene elemento unidad para el producto.

Ejemplos Son anillos unitarios

1. $(\mathbb{Z},+,\cdot)$, $(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$, $(\mathbb{C},+,\cdot)$, $(\mathbb{Z}_m,+_m,\cdot_m)$, $1<m\in\mathbb{N}$
2. $(\mathcal{F}(\mathbb{R}),+,\cdot)$, con elemento unidad la función constante 1.
3. $(\mathcal{M}_{2\times 2}(\mathbb{R}),+,\cdot)$, con elemento unidad la matriz identidad

$$\mathtt{I}=\begin{pmatrix}1&0\\0&1\end{pmatrix}$$

4. $(\mathcal{A}_{2\times 2}(\mathbb{Z}_3),+,\cdot)$, $\mathcal{A}_{2\times 2}(\mathbb{Z}_3)=\left\{A=\begin{pmatrix}x&y\\-y&x\end{pmatrix},\ x,y\in\mathbb{Z}_3\right\}$,

con elemento unidad la matriz identidad $\mathtt{I}$.

Anillos
Definiciones adicionales

Ejemplos

- No son unitarios los anillos
  1. $(n\mathbb{Z},+,\cdot)$, $1<n\in\mathbb{N}$
  2. $(\mathcal{N}_{2\times 2}(\mathbb{R}),+,\cdot)$,

$$\mathcal{N}_{2\times 2}(\mathbb{R})=\left\{N\in\mathcal{M}_{2\times 2}(\mathbb{R})\middle| N=\begin{pmatrix}x&0\\y&0\end{pmatrix},x,y\in\mathbb{R}\right\}$$

Ejercicio

- En el anillo $(\mathbb{Z}_{15},+_{15},\cdot_{15})$ se considera el subconjunto

$$S=\{[0]_{15},[3]_{15},[6]_{15},[9]_{15},[12]_{15}\}$$

  Estudia si $(S,+_{15},\cdot_{15})$ es un anillo unitario.
- En caso afirmativo, señala el elemento unidad.

Anillos
Definiciones adicionales

$(A,+,\cdot)$ es ***anillo conmutativo*** si la operación $\cdot$ verifica la propiedad conmutativa:

$$a\cdot b=b\cdot a,\qquad \text{para todo } a,b\in A$$

Ejemplos

- Son anillos conmutativos
  $(\mathbb{Z},+,\cdot)$, $(\mathbb{Z}_m,+,\cdot)$, $(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$, $(\mathbb{C},+,\cdot)$
- $(\mathcal{M}_{2\times 2}(\mathbb{R}),+,\cdot)$ es un anillo no conmutativo, ya que

$$\begin{pmatrix}0&1\\2&3\end{pmatrix}\begin{pmatrix}1&2\\3&4\end{pmatrix}=\begin{pmatrix}3&4\\11&16\end{pmatrix}\neq\begin{pmatrix}4&7\\8&15\end{pmatrix}=\begin{pmatrix}1&2\\3&4\end{pmatrix}\begin{pmatrix}0&1\\2&3\end{pmatrix}$$

☛ En los anillos no conmutativos, en general

$$(a+b)^2=a^2+ab+ba+b^2\neq a^2+2ab+b^2$$

Anillos
Definiciones adicionales

Los elementos del anillo $(A,+,\cdot)$ que verifiquen ciertas propiedades se llamarán:

Elementos permutables de un anillo $(A,+,\cdot)$ son aquellos elementos $a,b\in A$, tales que $a\cdot b=b\cdot a$

Ejemplo En el anillo $(\mathcal{M}_{2\times 2}(\mathbb{R}),+,\cdot)$ son elementos permutables

$$\begin{pmatrix}0&1\\2&3\end{pmatrix}\text{ y }\begin{pmatrix}-3&1\\2&0\end{pmatrix}$$

ya que

$$\begin{pmatrix}0&1\\2&3\end{pmatrix}\cdot\begin{pmatrix}-3&1\\2&0\end{pmatrix}=\begin{pmatrix}2&0\\0&2\end{pmatrix}=\begin{pmatrix}-3&1\\2&0\end{pmatrix}\cdot\begin{pmatrix}0&1\\2&3\end{pmatrix}$$

Anillos

Definiciones adicionales

Elementos inversibles de un anillo unitario $(A, +, \cdot)$ son aquellos elementos $a \in A$ que tienen simétrico respecto a la segunda operación. Este elemento se llama ***inverso*** de a y se denota a^{-1}.

Ejemplos

- En el anillo unitario $(\mathbb{Z}_9, +_9, \cdot_9)$, algunos elementos son inversibles:

$$[1]_9^{-1} = [1]_9; \quad [2]_9^{-1} = [5]_9; \quad [4]_9^{-1} = [7]_9; \quad [8]_9^{-1} = [8]_9$$

- En el anillo unitario $(\mathcal{M}_2(\mathbb{Z}_2), +, \cdot)$, algunos elementos son inversibles:

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}; \quad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^{-1} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}; \quad \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix};$$

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}; \quad \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^{-1} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$$

Anillos

Grupo multiplicativo de un anillo unitario

Teorema

*Sea $(A, +, \cdot)$ un anillo unitario y sea A^* el subconjunto de todos los elementos inversibles de A. Entonces $(A^*, \cdot)$ es grupo, (llamado **grupo multiplicativo** del anillo unitario $(A, +, \cdot)$).*

Demostración: En el subconjunto A^* de los elementos inversibles de A tenemos que:

$$\left.\begin{array}{l} 1 \in A^* \\ \forall a \in A^*,\ a^{-1} \in A^* \\ \forall a, b \in A^*,\ a \cdot b \in A^* \end{array}\right\}$$

Por lo tanto, $(A^*, \cdot)$ es grupo. Y se llama **grupo multiplicativo** del anillo unitario $(A, +, \cdot)$.

Anillos

Grupo multiplicativo de un anillo unitario

Ejemplos

- El grupo multiplicativo del anillo unitario $(\mathbb{Z}_9, +_9, \cdot_9)$ es

$$\mathbb{Z}_9^* = \{[1]_9, [2]_9, [4]_9, [5]_9, [7]_9, [8]_9\}$$

- El grupo multiplicativo del anillo unitario $(\mathcal{M}_2(\mathbb{Z}_2), +, \cdot)$, es

$$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \right\}$$

Anillos

Ejercicio

- Determina el grupo multiplicativo $(U_{36}, \cdot_{36})$ del anillo $(\mathbb{Z}_{36}, +_{36}, \cdot_{36})$

Anillos
Definiciones adicionales

Divisor de cero en un anillo $(A,+,\cdot)$ es un elemento $0 \neq a \in A$ tal que $a \cdot b = 0$ ó bien $b \cdot a = 0$, con $0 \neq b \in A$.

Ejemplos

- En el anillo $(\mathbb{Z}_9,+_9,\cdot_9)$ la clase $[3]_9$ es un divisor de cero ya que existe la clase $[6]_9 \neq [0]_9$ tal que $[3]_9 \cdot_9 [6]_9 = [18]_9 = [0]_9$
- En el anillo $(\mathcal{M}_2(\mathbb{Z}_2),+,\cdot)$ son divisores de cero las matrices

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \text{ y } \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \text{ ya que } \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

¿Es divisor de cero la matriz $\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$?

Anillos
Definiciones adicionales

Ejemplo En el anillo $(\mathcal{M}_2(\mathbb{R}),+,\cdot)$ la matriz $\begin{pmatrix} 1 & 2 \\ 0 & 0 \end{pmatrix}$ es un divisor de cero, ya que podemos encontrar una matriz no nula $\begin{pmatrix} 2 & 0 \\ -1 & 0 \end{pmatrix}$ tal que

$$\begin{pmatrix} 1 & 2 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 2 & 0 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

Aunque

$$\begin{pmatrix} 2 & 0 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 2 & 4 \\ -1 & -2 \end{pmatrix}$$

Anillos
Simplificación

En al anillo $(\mathcal{M}_2(\mathbb{R}),+,\cdot)$ podemos encontrar elementos que no son simplificables. Por ejemplo, dadas las matrices

$$A = \begin{pmatrix} 1 & 2 \\ 0 & 0 \end{pmatrix}, B = \begin{pmatrix} 5 & 0 \\ 1 & 0 \end{pmatrix} \text{ y } C = \begin{pmatrix} 3 & -2 \\ 2 & 1 \end{pmatrix}$$

tenemos que

$$A \cdot B = \begin{pmatrix} 1 & 2 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 5 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 7 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 3 & -2 \\ 2 & 1 \end{pmatrix} = A \cdot C$$

Y sin embargo,

$$B = \begin{pmatrix} 5 & 0 \\ 1 & 0 \end{pmatrix} \neq \begin{pmatrix} 3 & -2 \\ 2 & 1 \end{pmatrix} = C$$

¿Por qué $\begin{pmatrix} 1 & 2 \\ 0 & 0 \end{pmatrix}$ no se ha podido simplificar ?

Anillos
Simplificación

A continuación, caracterizamos los elementos simplificables.

Teorema

En un anillo $(A,+,\cdot)$ un elemento $0 \neq c \in A$ es simplificable si y sólo si c no es divisor de cero.

$$0 \neq c \text{ es simplificable} \iff c \text{ no es divisor de cero}$$

Demostración:

- Sea c simplificable. Si $c \cdot b = 0$, entonces (como $0 = c \cdot 0$) tendremos que $b = 0$. Luego c no es divisor de cero.
$$c \cdot b = 0 = c \cdot 0 \implies b = 0$$
- Sea c no divisor de cero. Si $c \cdot a = c \cdot b$, entonces $c \cdot (a - b) = 0$. Y, de aquí, $a = b$. Por lo tanto, c es simplificable.

Anillos

Simplificación

Consecuencias

1. En todo anillo en el que no existan divisores de cero es válida para el producto la simplificación.
2. Todo elemento inversible es simplificable. Por tanto, ningún elemento inversible es divisor de cero.

inversible $\implies$ simplificable $\iff$ no divisor de cero

no inversible $\impliedby$ no simplificable $\iff$ divisor de cero

☛ Los divisores de cero son elementos que no se pueden simplificar.

Anillo de integridad es un anillo que no tiene divisores de cero.

Dominio de integridad es un anillo de integridad conmutativo y unitario.

Anillos

Simplificación

Ejemplo En el anillo unitario $(\mathcal{F}(\mathbb{R}),+,\cdot)$ los divisores de cero son las funciones que se anulan al menos en un punto. (Luego, una función f que no se anula en ningún punto NO es un divisor de cero.)

$$f \in \mathcal{F}(\mathbb{R}) \text{ es divisor de cero} \iff \exists x \in \mathbb{R},\ f(x)=0$$
$$f \in \mathcal{F}(\mathbb{R}) \text{ no es divisor de cero} \iff \forall x \in \mathbb{R},\ f(x)\neq 0$$

Aplicando la proposición anterior, obtenemos:

- Una función $f \in \mathcal{F}(\mathbb{R})$ será simplificable si y sólo si f no se anula en ningún punto. Esto es,

$$\Big(\forall x,\quad f(x)\cdot g(x)=f(x)\cdot h(x) \implies g(x)=h(x)\Big) \iff \Big(\forall x,\quad f(x)\neq 0\Big)$$

- Por lo tanto, los divisores de cero son las funciones que se anulan al menos en un punto.

Anillos

Ejercicio

1. En el anillo $(\mathbb{Z}_{36},+_{36},\cdot_{36})$ determina los elementos que son divisores de cero.
2. En el grupo multiplicativo $(U_{36},\cdot_{36})$ encuentra los inversos de cada uno de los elementos.

Anillos

Ejercicios

3. Halla los valores de a en el anillo $(\mathbb{Z}_8,+_8,\cdot_8)$ que hacen que la ecuación $ax=a$ tenga solución única.
4. Estudia para qué valores de $m \in \{3,4,5,6,7,8\}$, la ecuación $2x=6$ tiene solución única en el anillo $(\mathbb{Z}_m,+_m,\cdot_m)$.

Definición

Sea el anillo $(A,+,\cdot)$ *y sea* $\varnothing \neq B \subseteq A$. *Se dice que* B *es* ***subanillo*** *de* A *si* B *es anillo con las mismas operaciones que* A.

Se deduce que B es subanillo de A si y sólo si

$$\begin{cases} (B,+) \text{ es subgrupo de } A \\ \cdot \text{ es operación cerrada en } B \end{cases}$$

Aplicando lo estudiado en grupos, podemos afirmar que:

En un anillo $(A,+,\cdot)$, un subconjunto no vacío B es un subanillo de A si y sólo si para todo $a,b \in B$

1. $a-b \in B$
2. $a \cdot b \in B$

Ejemplos

- Para todo anillo A son subanillos $\{0\}$ y A.
- $\mathbb{Z}$ es subanillo de $\mathbb{Q}$; $\mathbb{Q}$ es subanillo de $\mathbb{R}$; $\mathbb{R}$ es subanillo de $\mathbb{C}$.
- Para todo entero $m>1$, $m\mathbb{Z}$ es subanillo de $\mathbb{Z}$. Además, $\mathbb{Z}$ sólo admite subanillos del tipo $m\mathbb{Z}$.
- $\{[0]_{12},[3]_{12},[6]_{12},[9]_{12}\}$ es subanillo de $(\mathbb{Z}_{12},+_{12},\cdot_{12})$.
- $\mathcal{J}(i)=\left\{a+bi\in\mathbb{C} \;\middle|\; a,b\in\mathbb{Z}\right\}$ (Enteros de Gauss) es subanillo de $\mathbb{C}$.

Observaciones:

- Si un anillo es conmutativo, lo son todos sus subanillos.
- Sin embargo, las propiedades que verifican sólo algunos elementos de A puede que no las verifiquen los elementos de un subanillo.

Concretamente:

- Si un anillo es unitario, puede ocurrir que un subanillo suyo no sea unitario o que aún siendo unitario, tenga unidad distinta. Por ejemplo, en el anillo unitario $\mathbb{Z}$ ninguno de los subanillos $m\mathbb{Z}$ son unitarios. Y el anillo $\mathbb{Z}^3$ es unitario con unidad $(1,1,1)$, pero el elemento unidad del subanillo $\left\{(n,0,0)\middle| n\in\mathbb{Z}\right\}$ es $(1,0,0)$.
- Los divisores de cero del subanillo lo son del anillo. Sin embargo, puede ocurrir que un elemento sea divisor de cero en el anillo y no lo sea en el subanillo. Por ejemplo, $(2,0,0)$ es divisor de cero en el anillo $\mathbb{Z}^3$, pero no lo es en el subanillo $\left\{(n,0,0)\middle| n\in\mathbb{Z}\right\}$.

Definición (Ideales de un anillo)

Dado un anillo $(A,+,\cdot)$ *decimos que una parte no vacía* $J\subset A$ *es un* ***ideal*** *siempre que*

- $\forall i,j\in J,\ i-j\in J$.
- $\forall i\in J,\forall x\in A,\ i\cdot x, x\cdot i\in J$.

Ejemplo Para todo entero $m>1$, $m\mathbb{Z}$ es un ideal del anillo $\mathbb{Z}$.

- Todo ideal es subanillo (pero no se verifia el recíproco).
- Los ideales de un anillo hacen el mismo papel que los subgrupos normales, nos permiten definir la estructura de anillo cociente.

Definición

Dados dos anillos $(A,+,\cdot)$ *y* $(B,*,\perp)$, *un* ***homomorfismo de anillos*** *es toda aplicación* $\varphi\colon A\to B$ *tal que para cualesquiera* $a_1,a_2\in A$

$$\varphi(a_1+a_2)=\varphi(a_1)*\varphi(a_2)$$

$$\varphi(a_1\cdot a_2)=\varphi(a_1)\perp\varphi(a_2)$$

- La composición de dos homomorfismos de anillos es otro homomorfismo de anillos.
- Un homomorfismo de anillos se llamará **isomorfismo** cuando φ sea biyectiva.
- Dos anillos isomorfos pueden considerarse idénticos.

Ejemplo Dados a y b números reales fijos, definimos

$$\varphi\colon(\mathcal{F}(\mathbb{R}),+,\cdot)\to(\mathbb{R}^2,+,\cdot)$$

de la siguiente manera

$$\varphi(f)=(f(a),f(b))$$

Veamos que φ es homomorfismo de anillos:

- $\varphi(f+g)=((f+g)(a),(f+g)(b))=(f(a)+g(a),f(b)+g(b))$
  $=(f(a),f(b))+(g(a),g(b))$
- $\varphi(f\cdot g)=((f\cdot g)(a),(f\cdot g)(b))=(f(a)\cdot g(a),f(b)\cdot g(b))$
  $=(f(a),f(b))\cdot(g(a),g(b))$

Teorema (Propiedades de los homomorfismos de anillos)

Sea $\varphi\colon(A,+,\cdot)\to(B,+,\cdot)$ *un homomorfismo de anillos. Entonces:*

1. $\varphi(0)=0$
2. $\forall a\in A,\ \varphi(-a)=-\varphi(a)$.
3. *Si* A_1 *es subanillo de* A, *entonces* $\varphi(A_1)$ *es subanillo de* B.
4. *Si* B_1 *es subanillo de* B, *entonces* $\varphi^{-1}(B_1)$ *es subanillo de* A.
5. *Si* φ *es isomorfismo, entonces* φ^{-1} *es también isomorfismo.*

Demostración:

1. Por ser $(A.+)$ y $(B,+)$ grupos abelianos se verifica 1.
2. Por ser $(A.+)$ y $(B,+)$ grupos abelianos se verifica 2.
3. Probamos 3 demostrando que $\varphi(A_1)$ es parte estable de B para la operación $\cdot$.
4. Análogamente, probamos 4 demostrando que $\varphi^{-1}(B_1)$ es parte estable de A para la operación $\cdot$.
5. Para mostrar 5, basta probar que φ^{-1} es lineal para la operación $\cdot$.

Definición (Imagen de un homomorfismo de anillos)

Sea $\varphi\colon (A,+,\cdot)\to(B,+,\cdot)$ *un homomorfismo de anillos. Se llama* ***imagen*** *del homomorfismo* φ *al conjunto* $\varphi(A)=\{b\in B \mid \exists a\in A,\ b=\varphi(a)\}$. *También se denota* $Im\varphi$.

- Ya que A es subanillo de sí mismo, $\varphi(A)$ es subanillo de B.
- Si A es anillo unitario, entonces $Im\varphi$ es unitario. Y si 1 es el elemento unidad de A, $\varphi(1)$ es el elemento unidad de $Im\varphi$.
- Sin embargo, cuando φ no sea sobreyectiva, el elemento unidad de B generalmente no coincidirá con el elemento unidad $\varphi(1)$ de $\varphi(A)$.

Ejemplo Sea $\varphi\colon(\mathbb{Z}^3,+,\cdot)\to(\mathbb{Z}^3,+,\cdot)$, definido $\varphi(a_1,a_2,a_3)=(a_1,a_2,0)$. El elemento unidad de $(\mathbb{Z}^3,+,\cdot)$ es $(1,1,1)$ y, sin embargo, el elemento unidad de $Im\varphi$ es $(1,1,0)$.

Definición (Núcleo de un homomorfismo de anillos)

Sea $\varphi\colon (A,+,\cdot)\to(B,+,\cdot)$ *un homomorfismo de anillos. Se llama* ***núcleo*** *de* φ *al conjunto de elementos de* A *cuya imagen es el cero de* B. *Se denota* $\mathcal{K}er\varphi$.

$$\mathcal{K}er\varphi=\{a\in A \mid \varphi(a)=0\}=\varphi^{-1}(\{0\})$$

- Ya que $\{0\}$ es subanillo de B, $\varphi^{-1}(\{0\})=\mathcal{K}er\varphi$ es subanillo de A.

Lema (Caracterización de los monomorfismos)

Un homomorfismo de anillos es inyectivo si y sólo si $\mathcal{K}er\varphi=\{0\}$

- El núcleo de un homomorfismo de grupos es un subgrupo normal o invariante.
- En el caso de los homomorfismos de anillos ocurre algo similar. Su núcleo no sólo es parte cerrada para el producto sino que verifica además:

$$\forall n\in\mathcal{K}er\varphi,\ \forall a\in A,\ \ n\cdot a\in\mathcal{K}er\varphi,\ \ a\cdot n\in\mathcal{K}er\varphi$$

El núcleo de un homomorfismo de anillos es un ideal.

Ejemplo Dados a y b números reales fijos, sea el homomorfismo

$$\varphi\colon(\mathcal{F}(\mathbb{R}),+,\cdot)\to(\mathbb{R}^2,+,\cdot)$$

definido

$$\varphi(f)=(f(a),f(b))$$

El núcleo de este homomorfismo es

$$\mathcal{K}er\varphi=\{f\in\mathcal{F}(\mathbb{R}) \mid f(a)=f(b)=0\}$$

el conjunto de funciones que se anulan simultáneamente en a y b.

Cuerpos

Definición

Un anillo $(K,+,\cdot)$ *se dice que es un* ***cuerpo*** *si*

1. *es conmutativo.*
2. *es unitario y su elemento unidad es distinto del cero.*
3. *todos sus elementos (excepto el cero) son inversibles.*

Definido así, un cuerpo es un conjunto K en el que se han definido dos operaciones $+$ y $\cdot$, respecto a las cuales

- $(K,+)$ es grupo abeliano.
- $(K-\{0\},\cdot)$ es grupo abeliano.
- La operación $\cdot$ es distributiva respecto a $+$.

Ejemplos

- $\mathbb{Q},\mathbb{R},\mathbb{C}$ con la suma y el producto usuales son cuerpos.
- $K=\{a+b\sqrt{2} \mid a,b\in\mathbb{Q}\}$ es cuerpo con la suma y el producto usuales.

Cuerpos

Subcuerpos

Definición (Subcuerpo)

Sea el cuerpo $(K,+,\cdot)$ *y sea* $\varnothing\neq H\subseteq K$. *Se dice que* H *es un* ***subcuerpo*** *de* K *si y solo si* H *es cuerpo con las mismas operaciones que* K.

Ejemplos

1. $\mathbb{Q}$ es subcuerpo de $\mathbb{R}$
2. $\mathbb{R}$ es subcuerpo de $\mathbb{C}$

Aplicando lo estudiado anteriormente, podemos afirmar que:

H es subcuerpo de $(K,+,\cdot)$ si y sólo si

1. H es subanillo de $(K,+,\cdot)$
2. el inverso de todo elemento de H pertenece a H

Ejercicio Demuestra que $K=\{a+b\sqrt{2} \mid a,b\in\mathbb{Q}\}$ es subcuerpo de $\mathbb{R}$.

Cuerpos

Propiedades de los cuerpos

Los cuerpos verifican las propiedades de los anillos y además:

Teorema

1. *Todo cuerpo es dominio de integridad.*
2. *Todo dominio de integridad finito es un cuerpo.*
3. *Los únicos ideales que existen en un cuerpo* K *son* $\{0\}$ *y* K.
4. *En todo cuerpo* $(K,+,\cdot)$ *tiene siempre solución única la ecuación* $a\cdot x=b,\ b\neq 0$.

Cuerpos

Cuerpos finitos

- $\mathbb{Z}$ no es un cuerpo, ya que sólo 1 y -1 tienen inverso en $\mathbb{Z}$.
- En general, el anillo $(\mathbb{Z}_m,+,\cdot)$ no es un cuerpo. Sin embargo, aplicando lo estudiado en Matemática discreta, se demuestra que:

Si p es primo, $(\mathbb{Z}_p,+,\cdot)$ es cuerpo.

Existen otros cuerpos finitos además de los cuerpos $\mathbb{Z}_p$.

Ejercicio Sea K un cuerpo y $\mathcal{A}_2(K)$ el conjunto de las matrices 2×2 antisimétricas sobre K

Demuestra que $$\mathcal{A}_2(K)=\{A=\begin{pmatrix} x & y\\ -y & x\end{pmatrix},\quad x,y\in K\}$$

1. $\mathcal{A}_2(K)$ es un anillo con las operaciones de suma y producto de matrices.
2. el producto es conmutativo en $\mathcal{A}_2(K)$.
3. $\mathcal{A}_2(K)$ es un cuerpo si $K=\mathbb{Z}_3$, pero no lo es si $K=\mathbb{Z}_5$.