MATEMÁTICA DISCRETA
Estructuras Algebraicas

Prof. Sergio Salinas

Facultad de Ingeniería
Universidad Nacional de Cuyo

Segundo semestre 2024

Contenido

Anillos y Campos

Definición

Sea R (Ring) un conjunto no vacío con dos operaciones binarias cerradas, denotadas con $+$ y $\cdot$, que pueden ser diferentes de la suma y producto usuales. Entonces $< R, \oplus, \odot >$ es un anillo si para todos $a, b, c \in R$ se satisface que:

1) $< R, \oplus >$ **es un grupo aditivo Abeliano :**

1. *Ley asociativa de la suma:* $a \oplus (b \oplus c) = (a \oplus b) \oplus c$
2. *Existencia de la identidad en la suma:* $a \oplus e = e \oplus a = a$
3. *Existencia de inversos para la suma:* $a \oplus b = b \oplus a = e$
4. *Ley conmutativa de la suma:* $a \oplus b = b \oplus a$

2) $< R, \odot >$ **con el producto debe cumplir:**

1. *Ley asociativa del producto:* $a \odot (b \odot c) = (a \odot b) \odot c$

3) Leyes distributivas del producto sobre la suma:

1. $a \odot (b \oplus c) = a \odot b \oplus a \odot c$
2. $(b \oplus c) \odot a = b \odot a \oplus c \odot a$

Definición

Sea F (Field) un conjunto no vacío con dos operaciones binarias cerradas, denotadas con $\oplus$ y $\odot$, que pueden ser diferentes de la suma y producto usuales. Entonces $< F, \oplus, \odot >$ es un campo si para todos $a, b, c \in F$ se satisfacen las siguientes condiciones:

1. $< F, \oplus >$ **con la suma $\oplus$ es un grupo aditivo Abeliano.**
2. $< F - \{0\}, \odot >$ **con el producto $\odot$ es un grupo multiplicativo Abeliano.**
3. **La multiplicación es distributiva respecto a la adición:**
   1) $a \odot (b \oplus c) = (a \odot b) \oplus (a \odot c)$
   2) $(b \oplus c) \odot a = (b \odot a) \oplus (c \odot a)$

Definición

Sea $< R, \oplus, \odot >$ un anillo, entonces

1. *Si un elemento $u \in R$ es tal que $u \neq e$ y $au = ua = a$ para toda $a \in R$, decimos que u es el elemento unidad, o identidad del producto de R. Entonces se dice que R es un* **anillo con unidad**.
2. *Si $ab = ba$ para todos los $a, b \in R$ entonces R es un* **anillo conmutativo**.
3. *El anillo R* **no** *tiene divisores propios de cero si para cualesquiera $a, b \in R$ se cumple que $ab = e \Rightarrow a = e$ o $b = e$.*

Definición

Un **divisor propio de cero** *en un anillo es un elemento a distinto de cero tal que existe un elemento b también distinto de cero en el anillo que satisface:*

$$a \odot b = e$$

Esto significa que a y b son elementos que anulan el producto, llevando el resultado a cero. En un anillo con divisores de cero, puede haber múltiples divisores propios de cero.

Ejemplo:

$A = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}, B = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$

$A \odot B = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 \cdot 0 + 0 \cdot 1 & 1 \cdot 0 + 0 \cdot 0 \\ 1 \cdot 0 + 0 \cdot 1 & 1 \cdot 0 + 0 \cdot 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

Ejemplos de Anillo

Ejemplos básicos:

- En las operaciones binarias de la suma y producto usuales, $\mathbb{Z}$,$\mathbb{Q}$,$\mathbb{R}$ y $\mathbb{C}$ son anillos.

- El conjunto de matrices 2×2 con elementos enteros es un anillo.

- Demostrar que el conjunto $\mathbb{Z}$ con las operaciones binarias $\oplus$ y $\odot$ es un anillo, donde:
  - $x \oplus y = x + y - 1$
  - $x \odot y = x + y - xy$

Demostrar que el conjunto $\mathbb{Z}$ con las operaciones binarias $\oplus$ y $\odot$ es un anillo, donde: $x \oplus y = x + y - 1$ y $x \odot y = x + y - xy$

1. Ley conmutativa de la suma: $x \oplus y = x + y - 1 = y + x - 1 = y \oplus x$

2. Ley asociativa de la suma: $x \oplus (y \oplus z) = x \oplus (y + z - 1) = x + y + z - 1 - 1$ y $(x \oplus y) \oplus z = (x + y - 1) \oplus z = x + y - 1 + z - 1$

3. Existencia de la identidad en la suma: $a \oplus e = e \oplus a = a$ entonces $a + e - 1 = a$ donde $e = 1$

4. Existencia de inversos para la suma: $a + b = b + a = e$ donde $b = 2 - a$

5. Ley asociativa del producto: $a \odot (b \odot c) = (a \odot b) \odot c$ entonces $x \odot (y \odot z) = x \odot (x + z - xz) = x + (x + z - xz) + x(x + z - xz)$ y $(x \odot y) \odot z = (x + y - xy) \odot z = (x + y - xy) + z - (x + y - xy)z$

Ejemplos de Anillo

Leyes distributivas del producto sobre la suma:

1. $a \cdot (b + c) = a \cdot b + a \cdot c$ entonces $x \odot (y \oplus z) = x \odot (y + z - 1) = x + (y + z - 1) - x(y + z - 1) = x + y + z - 1 - xy - xz + x$

2. $(b \oplus c) \odot a = b \odot a \oplus c \odot a$ entonces $(x \odot y) \oplus (x \odot z) = (x + y - xy) \oplus (x + z - xz) = (x + y - xy) + (x + z - xz) - 1 = x + y + z - 1 - xy - xz + x$

Ejercicios de Anillo

1. Demostrar que $< Z_4, +_4, \cdot_4 >$ es un anillo.

2. Demostrar que el conjunto S de todos los pares ordenados (a, b) de números reales es un anillo conmutativo con divisores cero bajo las operaciones binarias $\oplus$ y $\odot$ definidas por:

   1) $(a, b) \oplus (c, d) = (a + c, b + d)$

   2) $(a, b) \odot (c, d) = (ac, bd)$

3. Demuestrar que $< \mathbb{Q}, \oplus, \odot >$ es un anillo, donde:

   1) $a \oplus b = a + b + 7$

   2) $a \odot b = a + b + \frac{ab}{7}$

Ejercicios de Campo

1. Demostrar que $< \mathbb{R}, +, \cdot >$ es un campo.

2. Demostrar que el conjunto S de pares ordenados (a, b) de números reales y las siguientes operaciones binarias es un campo.

   1) $(a, b) \oplus (c, d) = (a + c, b + d)$

   2) $(a, b) \odot (c, d) = (ac - bd, bc + ad)$

Fin