Cuerpos finitos y aplicaciones

1. Resultados fundamentales
2. Anillos y cuerpos
3. Polinomios sobre cuerpos finitos
4. Estructura de los cuerpos finitos.
5. Aplicaciones: · Códigos correctores de errores
   · Criptografía

① Definiciones básicas

Def 1: Un grupo $(G, *)$ es un conjunto dotado por una operación binaria $*: G \times G \to G$ con las siguientes propiedades:

i) (Asociatividad) $(a*b)*c = a*(b*c)$ $\forall a,b,c \in G$

ii) (Existencia elemento neutro) $\exists\, e \in G$: $e*a = a*e = a$ $\forall a \in G$.

iii) (Existencia de inverso) Para $a \in G$ existe $b \in G$ tal que $a*b = b*a = e$

Si $(G, *)$ cumple además que $a*b = b*a$ $\forall a,b \in G$ entonces decimos que $(G, *)$ es un **grupo abeliano** o **conmutativo**.

Ejemplos:

i) $(\mathbb{Z}, +)$ → elemento neutro 0

$a \in \mathbb{Z}$ $\quad a+0 = 0+a = a$

inverso $\quad a \in \mathbb{Z} \to -a$: $\quad a+(-a) = -a+(a) = 0$.

Es un grupo abeliano.

ii) $(GL_2(\mathbb{R}), \cdot)$ $\quad GL_2(\mathbb{R})$ Conjunto de matrices 2x2 con coeficientes reales que son invertibles.

↑ el producto usual de matrices.

$Id = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ elemento neutro. $\quad A \to A^{-1}$

No es abeliano

$$\underbrace{\begin{pmatrix} 1 & 3 \\ 1 & 1 \end{pmatrix}}_{A} \cdot \underbrace{\begin{pmatrix} 2 & 0 \\ 1 & 1 \end{pmatrix}}_{B} = \begin{pmatrix} 5 & 3 \\ 3 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 2 & 0 \\ 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 3 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 6 \\ 2 & 4 \end{pmatrix}$$

$$A \cdot B = \begin{pmatrix} 5 & 3 \\ 3 & 1 \end{pmatrix} \neq \begin{pmatrix} 2 & 6 \\ 2 & 4 \end{pmatrix} = B \cdot A$$

$A = \begin{pmatrix} 1 & 3 \\ 1 & 1 \end{pmatrix}$ $|A| = -2 \neq 0$

$B = \begin{pmatrix} 2 & 0 \\ 1 & 1 \end{pmatrix}$ $|B| = 2 \neq 0$

Ejercicio: Probar $(\{e\}, *)$ $e * e = e$ es un grupo abeliano.

Def 2: Un $(R, +, \cdot)$ anillo es un conjunto no vacío R con dos operaciones binarias $+$ y $\cdot$ que cumplen

i) $(R, +)$ es un grupo abeliano (conmutativo)

ii) $\cdot$ sea asociativa

iii) $+$ y $\cdot$ estén relacionados por las propiedades distributivas

$$a \cdot (b+c) = a \cdot b + a \cdot c$$

$$(b+c) \cdot a = b \cdot a + c \cdot a$$

Def 3:

3.1) Un anillo $(R,+,\cdot)$ es un anillo con unidad (o con identidad) si existe un elemento que actúe como neutro para $\cdot$, es decir, si existe $1 \in R$ tal que

$$1 \cdot a = a \cdot 1 = a \qquad \forall a \in R$$

3.2) Un anillo $(R,+,\cdot)$ es conmutativo si $\cdot$ es conmutativa, es decir si $\forall a,b \in R$

$$a \cdot b = b \cdot a$$

3.3) Un anillo $(R,+,\cdot)$ se llama un dominio integral (o D.I) si R es un anillo con unidad $1 \neq 0$ y se cumple que cada vez que

neutro de + $a \cdot b = 0$ entonces $a = 0$ o $b = 0$.

3.4) Se dice que $(R,+,\cdot)$ es un anillo de división si los elementos no nulos (distintos del 0) forman un grupo con $\cdot$.

3.5) Un anillo que es un anillo de división conmutativo ($\cdot$ es conmutativa) se llama un cuerpo.

En resumen, un cuerpo es un conjunto no vacío dotado con dos operaciones binarias conmutativas y asociativas, con un elemento neutro o identidad cada una, tal que cumplen las propiedades distributivas de manera que para la primera operación todo elemento tiene un inverso, y con respecto a la segunda operación existen los inversos excepto para los elementos no nulos (≠ identidad de la primera operación)

Es decir $(F, +, \cdot)$ es un cuerpo si

i) $(F, +)$ es un grupo abeliano con neutro 0

ii) $(F \setminus \{0\}, \cdot)$ es un grupo abeliano con identidad 1

iii) $a \cdot (b+c) = a \cdot b + a \cdot c \quad \forall a, b, c \in F$.
$(b+c) \cdot a = b \cdot a + c \cdot a$

Ejercicio: Probar que esto es lo mismo.

Def 4: Si F tiene una cantidad finita de elementos decimos que $(F, +, \cdot)$ es un cuerpo finito, y denotamos por $|F|$ al órden del cuerpo es decir a la cantidad de elementos de F.

Ejemplos: • $(\mathbb{Z}, +, \cdot)$ forman D.I. pero no es cuerpo
• $(\{0,1\}, +, \cdot)$ es un cuerpo finito

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

- Los enteros pares forman un anillo conmutativo sin unidad, con la suma y el producto usuales en $\mathbb{Z}$.

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

$\boxed{0 = a \cdot 0}$

$0 \cdot a$

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

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

$0 = 0 \cdot a + 0$

$0 = 0 \cdot a$

c

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

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

0