

ANILLOS

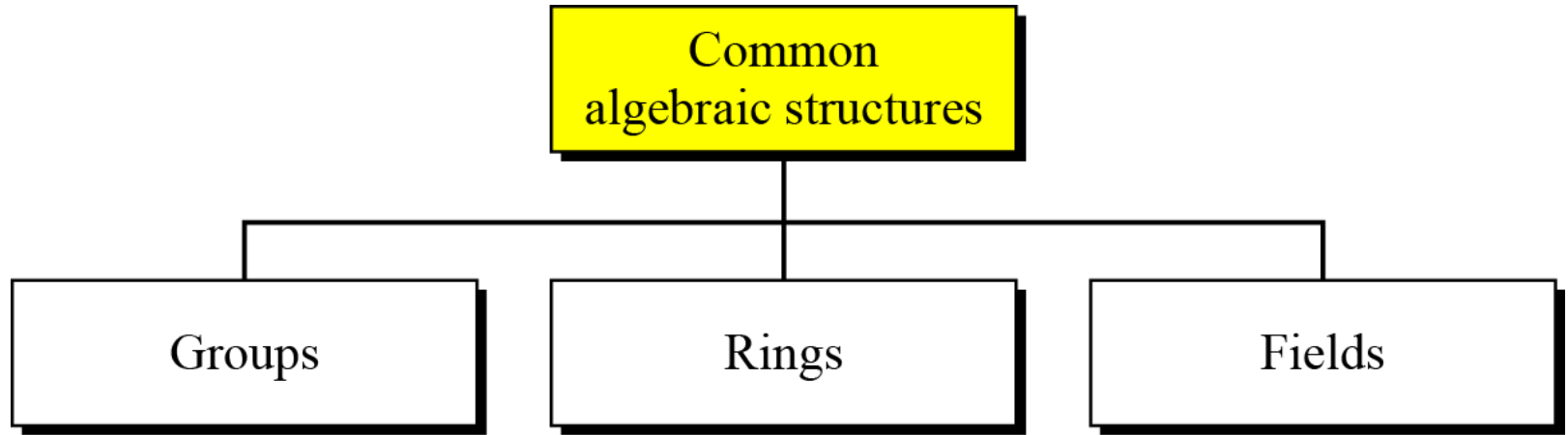
CAP 14 – Grimaldi

Cryptography and Network Security (CAP 4)

Estructuras Algebraicas

- **Concepto:** Combinación del conjunto de enteros y las operaciones sobre los elementos del conjunto.
- Criptografía requiere conjuntos de enteros y determinadas operaciones que son definidas para aquellos conjuntos.

Estructuras Algebraicas



Anillo: Concepto

- Un anillo, $R = \langle \{...\}, \bullet, \square \rangle$, es una estructura algebraica con dos operaciones. $R(\bullet, \square)$


Distribution of \square over \bullet

1. Cerradura
2. Asociativa
3. Conmutativa
4. Existencia de identidad
5. Existencia de inversa

1. Cerradura
2. Asociativa
3. Conmutativa

Nota:
La tercera propiedad es
solo satisfecha para un
anillo conmutativo

$\{a, b, c, \dots\}$
Set


Operations

Ring

Anillo: Propiedades

1. Cerrado con respecto a la operación:

- Si a y b están en el conjunto, entonces el elemento $a \cdot b = c$ está también en el conjunto

2. Asociativa:

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

3. Conmutativa:

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

4. Existencia de identidad:

Existe $z \in R$ tal que $a \cdot z = z \cdot a = a$ para todo $a \in R$

5. Existencia de inversa:

Para cada $a \in R$ existe un elemento $b \in R$ tal que

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

6. Distributiva de \square sobre \cdot

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

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

Anillo: Ejemplo 1

- $R(\mathbb{Z}_5, +, \cdot)$

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

.	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Es cerrado?

Asociativo?

Conmutativo?

Existencia de Identidad?

Existencia de Inverso?

Distributiva de \cdot Sobre $+$?

Es cerrado?

Asociativo?

Conmutativo?

Anillo: Ejemplo

- El conjunto \mathbb{Z} con dos operaciones, suma y multiplicación, es un anillo conmutativo. Para $(\mathbb{Z}, +, \cdot)$ satisface las 5 propiedades para la suma, y las 3 propiedades para la multiplicación.

Anillo: Concepto

- Sea $(R, +, \cdot)$ un anillo.

a) **Anillo conmutativo :**

Si $a \cdot b = b \cdot a$ para todo $a, b \in R$

b) **Divisores propios de cero:** El anillo R **NO** tiene divisores propios de cero si para cualquiera

$$a, b \in R, a \cdot b = z \rightarrow a = z \text{ ó } b = z.$$

b) **Anillo con unidad:** Si un elemento $u \in R$ es tal que $u \neq z$ y $a \cdot u = u \cdot a = a$ para todo $a \in R$, decimos que **u es elemento unidad**, o identidad para el producto, de R **y es único**.

Anillo : ejemplo 2

Para $R = \{a, b, c, d, e\}$, definimos $+$ y \cdot . Como

$+$	a	b	c	d	e
a	a	b	c	d	e
b	b	c	d	e	a
c	c	d	e	a	b
d	d	e	a	b	c
e	e	a	b	c	d

\cdot	a	b	c	d	e
a	a	a	a	a	a
b	a	b	c	d	e
c	a	c	e	b	d
d	a	d	b	e	c
e	a	e	d	c	b

Identidad aditiva: $a+z=z+a=a$

Inverso aditivo : $a+b=b+a=z$

Inverso multiplicativo: $xy=yx=u$

Es conmutativa: es simétrica.

Elemento unidad: $au=ua=a$ y $u \neq z$

Divisores propios de cero $a \cdot b = z$

Anillo: Ejemplo 3

- Sea $R = \{s, t, v, w, x, y\}$, donde $+$ y \cdot , están dadas por:

+	s	t	v	w	x	y
s	s	t	v	w	x	y
t	t	v	w	x	y	s
v	v	w	x	y	s	t
w	w	x	y	s	t	v
x	x	y	s	t	v	w
y	y	s	t	v	w	x

Identidad aditiva: $a+z=z+a=a$

Inverso aditivo : $a+b=b+a=z$

Inverso multiplicativo: $xy=yx=u$

+	s	t	v	w	x	y
s	s	s	s	s	s	s
t	s	t	v	w	x	y
v	s	v	x	s	v	x
w	s	w	s	w	s	w
x	s	x	v	s	x	v
y	s	y	x	w	v	t

Es conmutativa: es simétrica.

Elemento unidad: $au=ua=a$ y $u \neq z$

Divisores propios de cero $a \cdot b = z$

Anillo: concepto

- **Unidad e inverso multiplicativo**

Sea R un anillo con elemento unidad u . Si $a, b \in R$ y $ab=ba=u$, entonces b es un inverso multiplicativo y a es una **unidad** de R . (El elemento b también es una **unidad** de R).

- Sea R un anillo conmutativo con elemento unidad. Entonces

a) R es un **dominio de integridad** si R no tiene divisores propios de cero.

b) R es un **cuerpo** (*field*) si todo elemento distinto de cero en R es una unidad.

Anillo: Ejemplo 4

- $R(\mathbb{Z}_5, +, \cdot)$

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

.	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Es cerrado?

Asociativo?

Conmutativo?

Divisores propios de cero?

Elemento Unidad?

Inversos multiplicativos?

Unidades?

Divisores propios de cero?

Cuerpo?

Inversos aditivos y multiplicativos

Z	=	0	1	2	3	4	5	6	7
8									
+									
addit. inv.	=	0	7	6	5	4	3	2	1
.									
multi. inv	=	-	1	-	3	-	5	-	7

Anillo: ejemplo 4

- Sean $\mathcal{U} = \{1,2\}$ y $R = \mathcal{P}(\mathcal{U})$. Definimos $+$ y \cdot sobre los elementos de R como:

$$A + B = A \Delta B = \{x \mid x \in A \text{ ó } x \in B, \text{ pero no ambos}\}$$

$$A \cdot B = A \cap B = \text{la intersección de los conjuntos } A, B \subseteq \mathcal{U}$$

$+$ (Δ)	0	{1}	{2}	\mathcal{U}
0				
{1}				
{2}				
\mathcal{U}				

\cdot (\cap)	0	{1}	{2}	\mathcal{U}
0				
{1}				
{2}				
\mathcal{U}				

La estructura de anillo: ejemplo 1

- Sean $\mathcal{U} = \{1,2\}$ y $R = \mathcal{P}(\mathcal{U})$. Definimos $+$ y \cdot sobre los elementos de R como:

$$A + B = A \Delta B = \{x \mid x \in A \text{ ó } x \in B, \text{ pero no ambos}\}$$

$$A \cdot B = A \cap B = \text{la intersección de los conjuntos } A, B \subseteq \mathcal{U}$$

$+$ (Δ)	0	{1}	{2}	\mathcal{U}
0	0	{1}	{2}	\mathcal{U}
{1}	{1}	0	\mathcal{U}	{2}
{2}	{2}	\mathcal{U}	0	{1}
\mathcal{U}	\mathcal{U}	{2}	{1}	0

\cdot (\cap)	0	{1}	{2}	\mathcal{U}
0	0	0	0	0
{1}	0	{1}	0	{1}
{2}	0	0	{2}	{2}
\mathcal{U}	0	{1}	{2}	\mathcal{U}

Identidad aditiva: $a+z=z+a=a=0$

Inverso aditivo : $a+b=b+a=z$

Es conmutativa: es simétrica.

Elemento unidad: $au=ua=a$ y $u \neq z$

Divisores propios de cero $a \cdot b = z$

Anillos y cuerpos finitos especiales

ENTEROS MODULO N

- Ejemplo:
- Operaciones de suma y producto en \mathbb{Z}_7
 - Formada por 7 clases de equivalencia:

$$\mathbb{Z}_7 = \{[0][1][2][3][4][5][6]\}$$

+	0	1	2	3	4	5	6
0							
1							
2							
3							
4							
5							
6							

.	0	1	2	3	4	5	6
0							
1							
2							
3							
4							
5							
6							

ENTEROS MÓDULO N

- Teorema:
 - Para $n \in \mathbb{Z}^+$, $n > 1$, \mathbb{Z}_n es un anillo conmutativo con elemento unidad igual a $[1]$ en las operaciones binarias cerradas de $+$ y \cdot .

ENTEROS MÓDULO N

- Ejemplo Z_5 es un cuerpo?

+	0	1	2	3	4
0					
1					
2					
3					
4					

Identidad aditiva: $a+z=z+a=a$

Inverso aditivo : $a+b=b+a=z$

Inverso multiplicativo: $xy=yx=u$

.	0	1	2	3	4
0					
1					
2					
3					
4					

Es conmutativa: es simétrica.

Elemento unidad: $au=ua=a$ y $u \neq z$

Divisores propios de cero $a.b=z$

ENTEROS MÓDULO N

- Ejemplo \mathbb{Z}_6 es un cuerpo?

+	0	1	2	3	4	5
0						
1						
2						
3						
4						
5						

Identidad aditiva: $a+z=z+a=a$

Inverso aditivo : $a+b=b+a=z$

Inverso multiplicativo: $xy=yx=u$

.	0	1	2	3	4	5
0						
1						
2						
3						
4						
5						

Es conmutativa: es simétrica?.

Elemento unidad: $au=ua=a$ y $u \neq z$

Divisores propios de cero $a.b=z$

ENTEROS MODULO N

- Teorema 14.13:
 - **\mathbb{Z}_n es un cuerpo si y sólo si n es primo.**
- En \mathbb{Z}_6 , $[5]$ es una unidad y $[3]$ es un divisor de cero.
 - ¿Cómo reconocer cuándo $[a]$ es una unidad en \mathbb{Z}_n , si n es compuesto?

Función Phi-Euler

- Encuentra el número de enteros (elementos) que:
 - Son más pequeños que N
 - Relativamente primos con N
- $\Phi(1) = 0$
- $\Phi(p) = p-1$
- $\Phi(n) = \Phi(p_1^{d_1} \cdot p_2^{d_2} \dots) = (n)[1-(1/p_1)][1-(1/p_2)]$

ENTEROS MODULO N

- Teorema 14.14:
 - En \mathbb{Z}_n , $[a]$ es una unidad si y sólo si $\text{mcd}(a,n) = 1$
- Encuentre $[25]^{-1}$ en \mathbb{Z}_{72}

$$\text{mcd}(25,72)$$

ENTEROS MODULO N

- $[25]$ es una unidad en \mathbb{Z}_{72} , pero
 - ¿existe una forma de saber cuántas unidades tiene este anillo?
- El número de unidades en \mathbb{Z}_{72} es el número de enteros a tales que $1 \leq a < 72$ y $\text{mcd}(a, 72) = 1$.
- Se calcula usando la función Φ Euler:
 - $\Phi(72) = \Phi(2^3 \cdot 3^2) = (72)[1 - (1/2)][1 - (1/3)] = 24$
- En general, para $n \in \mathbb{Z}^+$, $n > 1$, existen $\Phi(n)$ **unidades** y $n-1-\Phi(n)$ **divisores propios de cero** en \mathbb{Z}_n

Ejercicios:

- Encontrar las unidades en Z_{12} y encontrar sus inversas multiplicativas.
- $S = \{a, b\}$ con operaciones de suma y multiplicación definidas como:

+	a	b
a	a	b
b	b	a

.	a	b
a	a	a
b	a	b