# ANILLLOS

Carolina Gáspero y Agustina Torres

# Indroducción

En  las unidades trabajamos con algúnos grupos como por ejemplo (Z,+) ,pero vimos que con '·' este conjunto no era grupo , sin embargo está operación cumple algunas de las propiedades de grupo
Y esto de un conjunto con dos operaciones con propiedades paralelas, nos introducen a una nueva estructura:

# ¿Qué es un Anillo?

Dado $(A,+,\cdot)$ un conjunto con sus dos operaciones lo llamaremos anillo si se cumplen las siguientes propiedades:

(i) $(A,+)$es un grupo abeliano.

(ii) El producto · es asociativo.

(iii) Se cumplen las propiedades distributivas, es decir

1. $(a \cdot (b+c)=a \cdot b+a \cdot c$  2. $(b+c) \cdot a=b \cdot a+c \cdot a$

para cualquier $a \in A, b \in A, c \in A$

# Clasificación:

1) Si el producto es conmutativo, A se dice que es un anillo conmutativo.

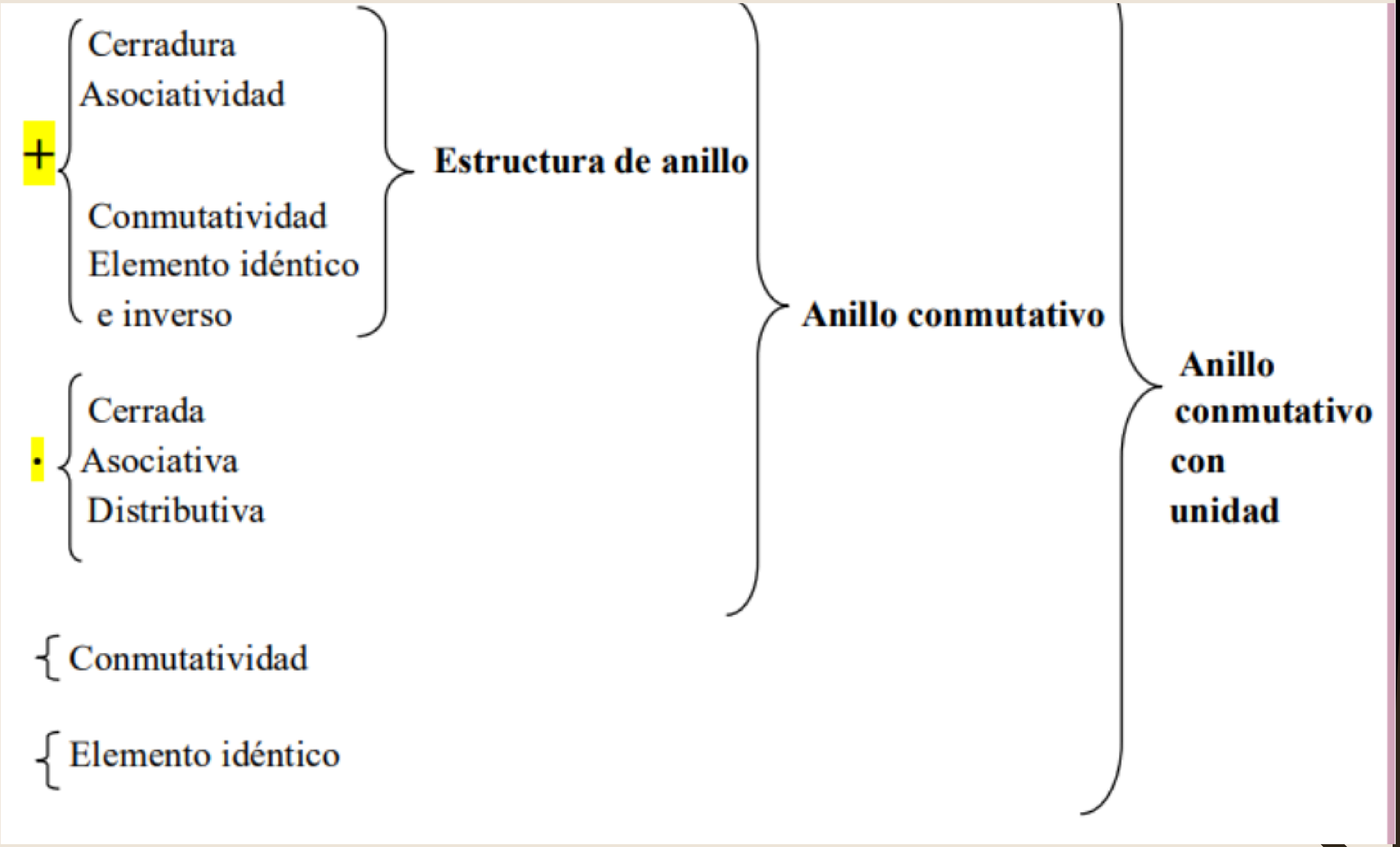
Si existe un elemento, que simbolizaremos mediante 1, tal que para todo a ∈ A

-a1=1a=a.

-a1=1a=a.

2)A se dice que es un anillo con unidad; en este caso, el elemento 1, que recibe el nombre de elemento unidad, es único.

3)Un anillo conmutativo con unidad (A, +, ·) se dice que es un cuerpo si el conjunto $A^*$, formado por todos los elementos de A excepto el neutro de la suma, es un grupo con respecto a la segunda operación.



# Cuerpos vs Dominios de Integridad

- Un **campo** es un anillo conmutativo con unidad, cuyos elementos distintos de cero tienen un inverso para la operación producto.

Ejemplos

- Q (cuerpo)
- R (cuerpo)
- C (cuerpo)
- Zp (cuerpo, cuando p es primo)

- Si $(A, +, \cdot)$ es un anillo, un elemento $a \in A$, con $a \neq 0$, se dice que es un divisor de cero si existe un elemento $b \in A$, $b \neq 0$, tal que $ab = 0$ o $ba = 0$.

Proposición 6.1.4. En un anillo $(A, +, \cdot)$, sea $a$ un elemento de $A$ que no es un divisor de 0. Entonces:

i) Si $ab = ac$ con $b \in A$ y $c \in A$, se tiene $b = c$.

ii) Si $ba = ca$ con $b \in A$ y $c \in A$, se tiene $b = c$.

- Un anillo A sin divisores de cero se llama un <u>dominio de integridad</u> (DI).

- Sea A un anillo con unidad 1 y $1 \neq 0$. Un elemento u de A se dice que es <u>invertible</u> si existe un elemento v, también de A, tal que $uv = vu = 1$

<u>Proposición 6.1.7</u>. Sea A un anillo con unidad. Si U(A) es el conjunto de los elementos invertibles de A, $(U(A), \cdot)$ es un grupo.

- Un anillo unitario A, con $1 \neq 0$, se dice un <u>anillo de división</u> si $U(A) = A^* = A - \{0\}$.

Q, R y C son ejemplos de anillos de división y, de hecho, un cuerpo puede definirse como un anillo de división conmutativo. Existen anillos de división no conmutativos; un ejemplo es el anillo de los cuaterniones

# SUBANILLOS

- Un subconjunto S de un anillo (A, +, ·) se dice que es un subanillo de A si (S, +) es un subgrupo de (A, +) y el producto · restringido a S es cerrado; de forma equivalente, la suma y el producto son operaciones cerradas sobre S y (S, +, ·) es un anillo.

- Un subconjunto S de un cuerpo (C, +, ·) se dice que es un subcuerpo de C si (S, +) es un subgrupo de (C, +) y (S, ·) es un subgrupo de (C, ·); de manera equivalente, la suma y el producto son operaciones cerradas en S y (S, +, ·) es un cuerpo.

- Un subanillo I de un anillo A se dice que es un ideal de A si para todo i ∈ I y para todo a ∈ A, ai e ia pertenecen a I.

## Proposición 6.2.4. Sea I un ideal de un anillo A; la suma y el producto de clases en el cociente A/I están bien definidas y, con estas, A/I posee una estructura de anillo.

D//

- sabemos que (I, +) es un subgrupo normal del grupo abeliano (A, +), entonces la suma está bien definida
- Si $r \equiv r'(I)$ y $s \equiv s'(I)$ tenemos que $r' = r + i$, y $s' = s + j$, con i, j en I;

entonces $r's' = (r + i)(s + j) = rs + rj + is + ij$, esto es, $r's' - rs \in I$ ya que $rj + is + ij \in I$ por ser I un ideal; por tanto
$(r+I)(s+I)=rs+I=r's'+I=(r'+I)(s'+I)$;
así pues, el producto también está bien definido.

- Ya sabemos por teoría de grupos que (A/I, +) es un grupo abeliano, y la asociatividad del producto y su distributividad frente a la suma se comprueban fácilmente al ser consecuencia inmediata de propiedades correspondientes de A; por ejemplo,
- para la asociatividad se tiene

$[(r+I)(s+I)](t+I)=(rs+I)(t+I)=(rs)t+I=r(st)+I=(r+I)(st+I)=(r+I)[(s+I)(t+I)]$,
y la distributividad se comprueba de forma análoga

+ Dado un anillo A y un subconjunto $S \subset A$, el ideal generado por S se define como el mínimo ideal que contiene a S, esto es, el ideal I tal que $S \subset I$, y si J es otro ideal tal que $S \subset J$, entonces $I \subset J$.

Sea A un anillo conmutativo con unidad y S un subconjunto de A. El ideal generado por S es:

$$\langle S\rangle=\{r_1s_1+\dots+r_ns_n : r_i\in A, s_i\in S, n\in \mathbb{N}\}.$$

Sea I el conjunto que aparece en la parte derecha de la igualdad de la proposición. Puesto que $s=1\cdot s$, está claro que $S\subset I$. Además, si J es un ideal que contiene a S, y $s\in S$, $rs\in J$ para cualquier $r\in A$, y por tanto, cualquier combinación del tipo $r_1s_1+\dots+r_ns_n$. pertenece a J; así pues, $I\subset J$, para cualquier ideal J que contiene a S.

Por lo tanto, basta demostrar que el conjunto I es un ideal de A. Dados dos elementos $p=r_1s_1+\dots+r_ns_n, p'=r_1's_1'+\dots+r_n's_n'$, tenemos que $p-p'=r_1s_1+\dots+r_ns_n+(-r_1's_1')+\dots+(-r_n's_n')$, que obviamente pertenece a I: por tanto $(I,+)$ es un subgrupo de $(A,+)$. Además, si r es un elemento cualquiera de A y $p=r_1s_1+\dots+r_ns_n$ es un elemento cualquiera de I $rp=(rr_1)s_1+\dots+(rr_n)s_n$ pertenece a I: como el anillo es conmutativo, $pr=rp$ también es un elemento de I.

Estas dos propiedades terminan la demostración del resultado deseado.

En consecuencia, $I=\langle S\rangle$.

- Un ideal I de un anillo conmutativo A es un ideal primo si dados dos elementos cualesquiera a y b de A tales que $ab \in I$ se tiene que $a \in I$ o $b \in I$.

Proposición 6.2.8. Sea A un anillo conmutativo e I un ideal de A con $I \neq A$. El anillo cociente A/I es un dominio de integridad si y sólo si I es un ideal primo de A.

Sea A/I un dominio de integridad y queremos demostrar que I es un ideal primo de A; para ello consideremos dos elementos a y b de A tales que $ab \in I$; entonces

$$(a+I)(b+I)=ab+I=I$$

y como A/I es un dominio de integridad $a + I = I$ o $b + I = I$; esto implica que $a \in I$ o $b \in I$ con lo que I es un ideal primo de A.

Para demostrar el recíproco supongamos que I es un ideal primo de A y sea

$$(a+I)(b+I)=I$$

para cualesquiera dos elementos $a + I$ y $b + I$ de A/I. Como

$$I=(a+I)(b+I)=ab+I$$

deducimos que $ab \in I$ y como I es primo $a \in I$ o $b \in I$; por tanto $a + I = I$ o $b + I = I$, lo que demuestra que A/I es un dominio de integridad.

¡Gracias por su atención!