ESTRUCTURAS ALGEBRAICAS
TEORIA DE ANILLOS

NELSON ARAVENA CASTILLO

DEPARTAMENTO DE MATEMATICA
UNIVERSIDAD METROPOLITANA
DE CIENCIAS DE LA EDUCACION

UNIVERSIDAD METROPOLITANA
DE CIENCIAS DE LA EDUCACION
DEPARTAMENTO DE MATEMATICA
Prof.: Nelson Aravena Castillo

TEORIA DE ANILLOS

En álgebra, dos estructuras importantes son la de grupo y la de anillo. En general, el algebrista opera con grupos y anillos como herramientas básicas, los teoremas se tratan de formular en términos de estas estructuras.

Esto se contrapone al punto de vista clásico de trabajar casi exclusivamente con los números naturales, racionales, reales y complejos. El punto de vista más general de trabajar con estructuras algebraicas generales, ha sido de inestimable importancia; no sólo en álgebra, sino en otras ramas de la matemática como son: el análisis y la geometría. Es así como **Félix Klein** (1849 – 1925) realiza una jerarquización de las geometrías mediante grupos y subgrupos, en su famoso "Programa de Erlangen" en 1878 señala que: El objeto de cada geometría es el descubrimiento de invariantes respecto de ciertos grupos de transformaciones y cada geometría puede considerarse como subgeometría de otra a la que se adjuntan ciertas figuras básicas que deben quedar invariantes. Así, la geometría afín estudia las propiedades proyectivas que conversan el paralelismo, es decir, los puntos y rectas impropias y dentro de la afín las propiedades métricas son las que conservan la perpendicularidad.

El concepto de anillo surge en el siglo XIX y viene a generalizar las propiedades de los números enteros. La

palabra **“anillo”** parece haber sido introducida por **David Hilbert** (1862 -1943).

El concepto de cuerpo estaba ya implícito en la obra de **Abel** (1802 - 1829) y de **Galois** (1811 – 1832) pero es **Dedekind** (1831 – 1910) el primero que da explícitamente en 1879 la definición de un cuerpo de números: un conjunto de números que forman un grupo abeliano con respecto a la suma y con respecto a la multiplicación (excepto en lo referente al inverso del cero) tal que la multiplicación es distributiva con respecto a la suma. Los ejemplos más sencillos son los sistemas de los números racionales, de los números reales y de los números complejos. **Kronecker** (1823 – 1891) dio otros ejemplos en 1881 basado en sus **“dominios de racionalidad”.** El conjunto $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ es un cuerpo en la adición y multiplicación usual de los números reales, es cuerpo de infinitos elementos; un cuerpo con un número finito de elementos se conoce como un **“cuerpo de Galois”** y un ejemplo sencillo es $\mathbb{Z}_3$ (o cualquier otro número primo).

El interés en la idea abstracta de estructura y la aparición de nuevas algebras, especialmente durante la segunda mitad del siglo XIX, condujo también a amplias generaciones en el campo de los números y su aritmética. **Gauss** (1777 – 1855) extendió la idea de un número entero ordinario a los llamados enteros de **Gauss** $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$. Dedekind la generalizó a su vez en su teoría de los **“enteros algebraicos”**, es decir, números que son raíces de ecuaciones polinómicas con coeficientes enteros y tales que el coeficiente supremo del polinomio es 1.

Tales sistemas de **“enteros”** no constituyen estructura de cuerpo, sino que son anillos íntegros. Tales generalizaciones de la idea de entero tuvo un costo que fue la perdida de la propiedad de factorización única. Debido a ello, Dedekind y otro matemático y otro matemático contemporáneo, **Ernest**

Eduard Kummer (1810 – 1893), introdujeron en la aritmética el concepto de “ideal”, basado en la idea del anillo.

Recordemos algunos conductos estudiados anteriormente con las operaciones que se indican.

1) $\mathbb{Z}$ números enteros con la adición y multiplicación ordinaria.
   $\mathbb{Z}$ números pares con la adición y multiplicación ordinaria.

2) $\mathbb{Z}_5 = \{\overline{0}, \overline{1}, \ldots \overline{4}\}$ con la adición y multiplicación de clases.

   $\mathbb{Z}_6 = \{\overline{0}, \overline{1}, \ldots \overline{5}\}$ con la adición y multiplicación de clases.

3) $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ con la adición y multiplicación.

4) $M_n(\mathbb{R})$ con la adición y multiplicación ordinaria de matrices.

5) $C[0,1] = \{ f \mid f : [0,1] \to \mathbb{R}, f$ función continua$\}$ con las operaciones que se indican.

$(f + g)(x) = f(x) + g(x)$

Para todo $x \in [0, 1]$

$(f + g)(x) = f(x) \cdot g(x)$

6) Sea $\mathbb{V}$ un espacio vectorial sobre un cuerpo K.

$End_K(\mathbb{V}) = \{f \mid f : \mathbb{V} \to \mathbb{V}$ función lineal $\}$ con la adición y composición de funciones.

$(f + g)(x) = f(x) + g(x)$; $(f \circ g)(x) = f(g(x))$, $x \in \mathbb{V}$.

7) $\mathbb{R}[x]$ polinomios en la indeterminada x con coeficientes en $\mathbb{R}$, con la adición y
multiplicación ordinaria de polinomios.

Todos estos conjuntos tienen en común estar dotados cada uno de dos operaciones (adición y multiplicación) que tienen ciertas propiedades, por ejemplo, ambas son asociativas, la adición es muy buena (constituye estructura de grupo abeliano), la multiplicación no lo es tanto, además la adición y la multiplicación están vinculadas entre si (distributividad). Esta observación de propiedades comunes nos mueve a conversar estas propiedades comunes en un nuevo modelo de estructura algebraica, llamado **anillo** que generaliza los ejemplos anteriormente expuestos.

Definición: Sea A un conjunto no vacío dotado de dos operaciones (adición (+) y multiplicación (·). Diremos que A con dichas operaciones definen una estructura algebraica de **anillo** si:

1) $(A, +)$ es un grupo abeliano

2) La multiplicación es asociativa $(a \cdot b) \cdot c = a \cdot (b \cdot c)$; $a, b, c, \in A$.

3) La multiplicación es distributiva con respecto a la adición.

- $a \cdot (b + c) = a \cdot b + a \cdot c$ (distributividad a mano izquierda)
- $(a + b) \cdot c = a \cdot c + b \cdot c$ (distributividad a mano derecha)

para todo $a, b, c, \in A$.

Definición: Sea *A* un anillo

i) Diremos que *A* es un **anillo conmutativo** ó **anillo abeliano si**

$a \cdot b = b \cdot a$; para todo $a, b \in A$

ii) Diremos que A es un **anillo con unidad o identidad o elemento neutro**, si A posee un elemento $1 \neq 0$ tal que $a \cdot 1 = 1 \cdot a = a$; $a \in A$.

iii) Diremos que es ***A* un anillo de división**, si *A* es un anillo con identidad tal que todo elemento no nulo tiene inverso multiplicativo en *A*.

iv) Diremos que ***A* es un cuerpo**, si *A* es un anillo de división conmutativo (cuerpo o campo).

Ejemplos:

1) $\mathbb{Z}[i] = \{a + b_i \mid a, b \in \mathbb{Z}\}$

Con la adición y multiplicación ordinaria de complejos es un anillo
conmutativo con unidad.

2) $\mathbb{Z}[\sqrt{-5}] = \{a + b[\sqrt{-5} \mid a, b, \mathbb{Z}\}$

Dotado de la adición y multiplicación definidas del modo siguiente:

$(a + b \sqrt{-5}) + (c + d \sqrt{-5}) = (a + c) + (b + d) \sqrt{-5}$

$(a + b \sqrt{-5}) \cdot (c + d \sqrt{-5}) = (ac - 5\, bd) + (ad + bc) \sqrt{-5}$

Es un anillo con unidad conmutativa.

3) Sea A un anillo, I conjunto no vacío. Consideremos el conjunto

$A^I = \{f \mid f : I \rightarrow$ función$\}$ con las operaciones

$(f + g)(x) = f(x) + g(x)$; $(f \cdot g)(x) = f(x) \cdot g(x), x \in I$ es un anillo.

Si A es un anillo conmutativo, A^I es un anillo conmutativo.

4) Cuaterniones, reales de Hamilton (su interés original es el de ser un ejemplo importante, pues juega un papel fundamental en la geometría y la teoría de los números).
Sea $C_H = \{a_1 + a_2 i + a_3 j + a_4 k \mid a_1, a_2, a_3, a_4 \in \mathbb{R}\}$

Se definen las operaciones de edición y multiplicación,

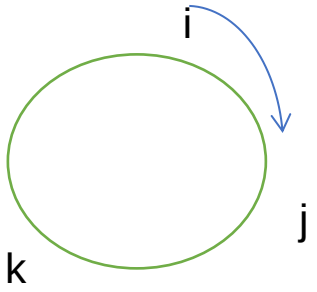
Adición:

$$(a_1 + a_2 i + a_3 j + a_4 k) + (b_1 + b_2 i + b_3 j + b_4 k)$$

$= (a_1 + b_1) + (a_2 + b_2)\,i + (a_3 + b_3)\,j + (a_4 + b_4)k.$

Multiplicación :

$i^2 = j^2 = k^2 = -1$



$i_j = j_i = k$
$j_k = -\,k\;j = i$

$k_i = -\,i\;k = j$

$(a_1 + a_2 i + a_3 j + a_4 k) \cdot (b_1 + b_2 i + b_3 j + b_4 k) =$

$= (a_1\,b_1 - a_2\,b_2 - a_3\,b_3 - a_4\,b_4) + (a_1\,b_2 + a_2\,b_1 + a_3\,b_4 - a_4\,b_3)\,i$

$+ (a_1\,b_3 - a_3\,b_1 - a_4\,b_2 - a_1\,b_4)\,j + (a_1\,b_4 + a_4\,b_1 + a_2\,b_3 - a_3\,b_2)\,k$

Sir Williams Rowson Hamilton (1805 – 1865)

$z = a + bi + cj + dk \quad , \quad z^{-1} = x + yi + zj + wk$

$z\,z^{-1} = 1$ cuaternios o cuaterniones

$$\begin{aligned} ax + by - cz - dw &= 1 \\ bx + ay - dz + cw &= 0 \\ cx + dy + az - bw &= 0 \\ dx - cy + bz + aw &= 0 \end{aligned}$$

$$D = \begin{vmatrix} a & b & -c & -d \\ b & a & -d & c \\ c & d & a & -b \\ d & -c & b & a \end{vmatrix} = (a^2 + b^2 + c^2 + d^2)^2$$

El conjugado de z denotado por $\bar{z}$ es

$\bar{z} = 2a - z = a - bi - cj - dk$

es $\bar{z}\, z = a^2 + b^2 + c^2 + d^2$

$|z|^2 = \bar{z}\, z \quad \Leftrightarrow |z|^2 = a^2 + b^2 + c^2 + d^2$

Luego $|z| = \sqrt{a^2 + b^2 + c^2 + d^2}$

Si $z \neq 0$

$$z^{-1} = \frac{1}{z} = \frac{\bar{z}}{z\,\bar{z}} = \frac{a - bi - cj - dk}{a^2 + b^2 + c^2 + d^2}$$

Los cuaterniones con las operaciones definidas es un anillo de división.

5) Sea

$\mathbb{Q}[\sqrt{2}] = \{a + \sqrt{2}\, b \mid a, b \in \mathbb{Q}\}$

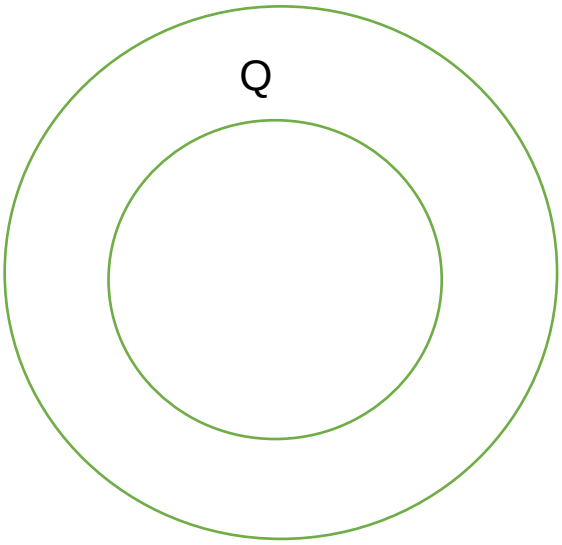
Con las operaciones de adición y multiplicación definidas por :

$(a + b \sqrt{2}) + (c + d \sqrt{2}) = (a + c) + (b + d) \sqrt{2}.$

$(a + b \sqrt{2}) + (c + d \sqrt{2}) = (ac + bd) + (ad + b c) \sqrt{2}$

Es un cuerpo campo.

$Q[\sqrt{2}]$



6) Sean A y A' , $A \times A = \{(a, a') \; a \in A, a' \in A'\}$

Con las operaciones de adición y multiplicación definidas por:

$(a, a') + (b, b') = (a + b, a' + b')$

$(a, a') \cdot (b , b') = (a \cdot a', b \cdot b')$

$(A \times A + \cdot)$ es un anillo, llamado **anillo producto.**

Caso particular $\mathbb{Z} \times \mathbb{Z}$.

7) Sea E conjunto, Δ diferencia simétrica $(P(E), \Delta, \cap)$ es un anillo conmutativo llamado, **Anillo Booleano**.

8) Sea (A, +) grupo abeliano. Si definimos la multiplicación de la siguiente forma:
$A \cdot b = 0$, para todo $a, b \in A$.
Entonces $(A, +, \cdot)$ es un anillo conmutativo
(Llamado **Anillo Trivial**).

Adjunción de unidad

Definición : Sea A un anillo.

$$n\,a = \begin{cases} a + a + \ldots + a & \text{si } n > 0 \quad (n \text{ veces}) \\ \text{ó si } n = 0 & \\ -(a + a + \ldots + a) & \text{si } n < 0 \end{cases}$$

En $\overline{A} = A \times \mathbb{Z}$ definimos las operaciones de adición y multiplicación de la siguiente manera:

$(a, n) + (b, m) = (a + b, n + m)$

$(a, n) \cdot (b, m) = (ab + ma + nb, nm)$

La forma de obtener este producto es desarrollando

$(a + n)(b + m) = ab + ma + nb + nm)$

$(\overline{A}, +)$ es un grupo abeliano. $(\overline{A}, +, \cdot)$ es un anillo.

Observación

1) Sea $f : A \to \overline{A}$ función definida por $f(a) = (a, 0)$

$f(a) = f(b) \to (a, 0) = (b, 0) \to a = b$ luego f es inyectiva

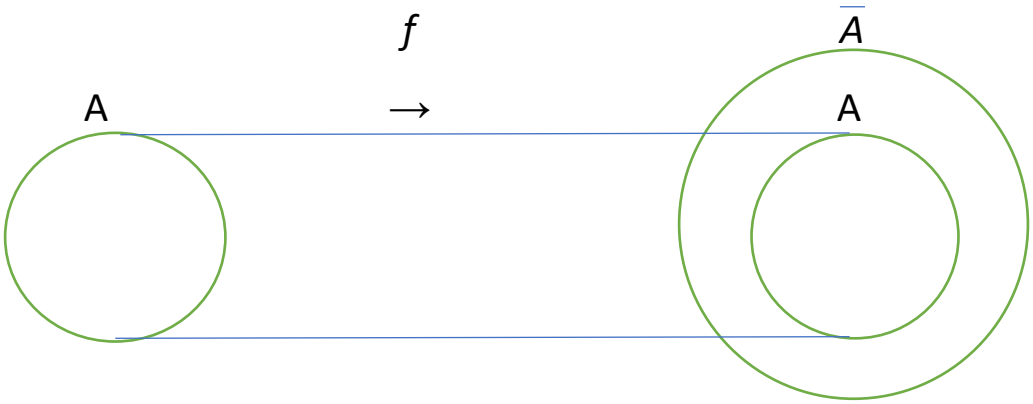
Además $f(a + b) = f(a) + f(b)$

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

$f(ab) = (ab, 0) = (ab + 0 \cdot a + 0\, b, 0 \cdot 0) = (a, 0)(b, 0)$

$= f$ a) f (b)

Luego



Por lo tanto f es una inmersión

identificamos $a = f(a, 0)$

2) Para todo $(a, n) \in \overline{A}$ existe $(0, 1) \in \overline{A}$ tal que

$(a, n)(0, 1) = (a \cdot 0 + a \cdot 1 + n \cdot 0,\ n \cdot 1) = (a, n)$

$(0, 1)(a, n) = 0 \cdot a + n \cdot 0 + 1 \cdot a,\ 1 \cdot n) = (a, n)$

Luego (0, 1) es unidad de $\overline{A}$.

Por tanto $\overline{A}$ es un anillo con unidad

Teorema:

Sea A un anillo, $a, b, c \in A$ entonces:

1) $a \cdot 0 = 0 \cdot a = 0$

2) $(-a) \cdot b = a \cdot (-b) = -(ab)$

3) $(-a) \cdot (-b) = a \cdot b$

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

Demostración:

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

$a \cdot 0 + 0 = a \cdot 0 + a \cdot 0$ por cancelación aditiva tenemos $0 = a \cdot 0$

2) Sabemos que $ab + (-ab) = 0$

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

$a\,b + (-a)\cdot b = a\,b + (ab)$

$(-a)\cdot b = -ab$

análogamente $a\cdot(-b) = -ab$

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

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

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

$-ab + (-a)(-b) = 0$

$(-a)(-b) = ab$

4) $a - b = a + (-b)$ por definición

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

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

$= a\cdot b + (-ac)$

$= ab - ac$

Observación:

Las relaciones siguientes no son válidas en un anillo cualquiera, sino solo en anillos conmutativos.

$(a + b)^2 = a^2 + 2ab + b2$

$(a + b)(a - b) = a^2 - b^2$

Definición :

Sea A un anillo conmutativo. Diremos que un elemento $a \in A \quad a \neq 0$ es un **divisor de cero** si existe un elemento $b \in A \quad b \neq 0$ tal que $a \cdot b = 0$.

Ejemplos:

1) Sea $A = \mathbb{Z}_6$

$\overline{3} \in \mathbb{Z}_6$ un divisor de cero pues existe $\overline{2} \neq 0$ en $\mathbb{Z}_6$ tal que $\overline{2} \cdot \overline{3} = \overline{0}$.

(divisor de cero a mano derecha, también lo es a la izquierda).

2) $\begin{pmatrix} -1 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & -1 \end{pmatrix} \in M_2(\mathbb{R})$

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

$\begin{pmatrix} -1 & 0 \\ 1 & 0 \end{pmatrix}$ Es un divisor de cero a derecha

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

Pero no lo es a izquierda

Definición:

Un anillo *A* se dice **dominio de integridad o anillo íntegro**, si es un anillo conmutativo con unidad y sin divisores de cero.

Ejemplo

($\mathbb{Z}$, + , ·) números enteros, ($\mathbb{R}$ [*x*], + ·) anillo de polinomios.

Teorema :

Sea *A* un anillo conmutativo con unidad.

A es anillo íntegro ⇔ para todo *a, b*, *c* ∈ *A*

(*ac* = *bc* , *c* ≠ 0 ⇒ *a* = *b*).

Definición:

Un cuerpo es un anillo íntegro en que todo de elemento no nulo posee inverso multiplicativo o bien es un anillo de división conmutativo.

Ejemplo:

1) ($\mathbb{Q}$, + , ·) es un cuerpo

($\mathbb{Q}$ [$\sqrt{2}$,] , + , ·) es un cuero con adición y multiplicación ordinaria de $\mathbb{R}$.

(
($\mathbb{Q}$ ($\sqrt{2}$)] = {a + b $\sqrt{2}$ | a, b, ∈ $\mathbb{Q}$ }

($\mathbb{Q}$ ($\sqrt{2}$) , + , ·) es un cuerpo

2) $(\mathbb{R}, +, \cdot)$ es un cuerpo

3) $(\mathbb{C}, +, \cdot)$ es un cuerpo

4) $\mathbb{Z}_3 = \{\overline{0}, \overline{1}, \overline{2}\}$ con las operaciones dadas en las tablas de doble entrada es un cuerpo.
Es decir $(\mathbb{Z}_3, +, \cdot)$ es cuerpo.

Tabla de doble entrada de la adición

+	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{1}$

Tabla de doble entrada de la ultilicación

·	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{1}$

Observemos que $\mathbb{Z}_4 \{ \overline{0}, \overline{1}, \overline{2}, \overline{3} \}$ con las operaciones que se indican en las tablas de doble entrada $(\mathbb{Z}_4, +, \cdot)$ no es un cuerpo.

Adición:

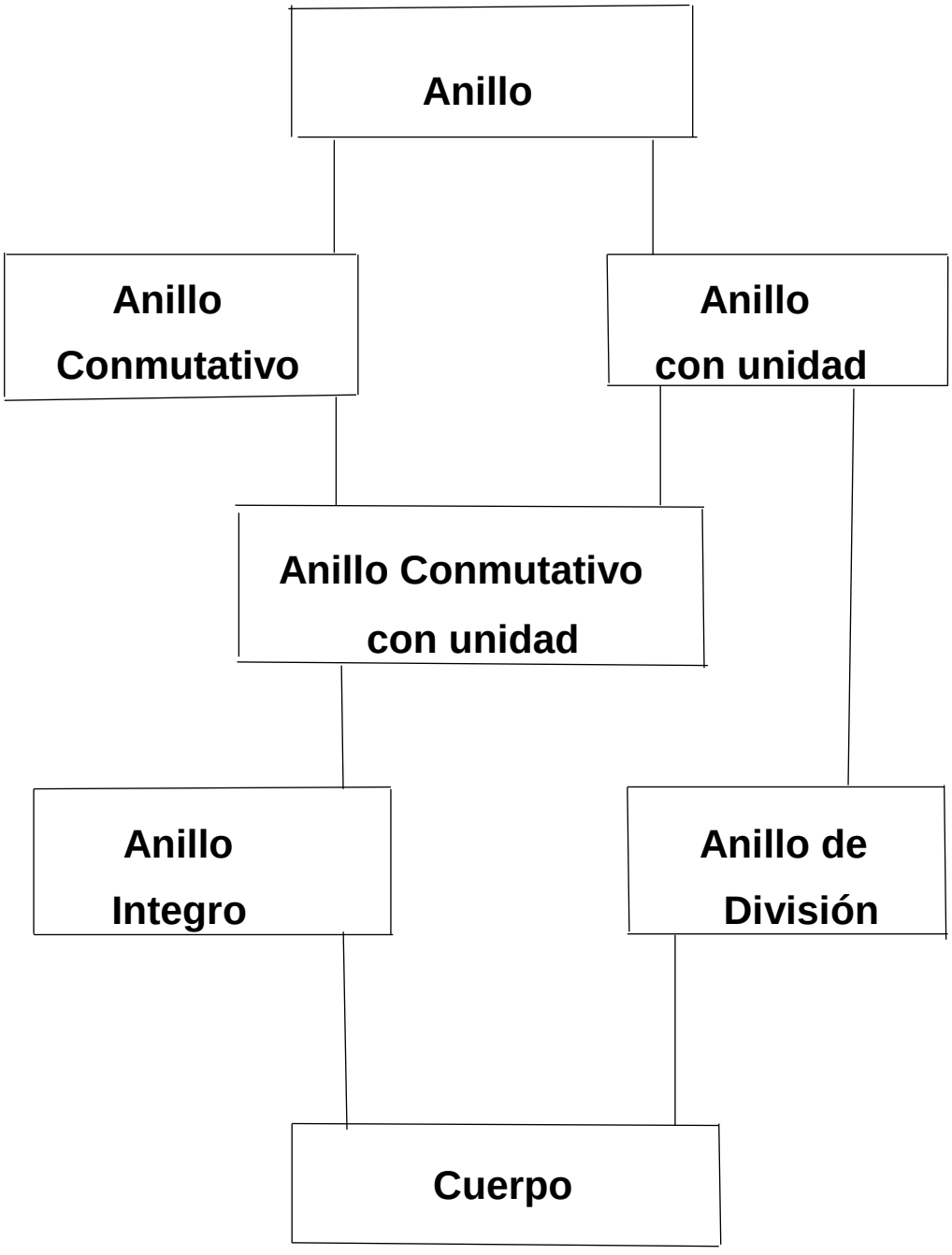
+	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{2}$

Multiplicación

·	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{0}$	$\overline{2}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

$\overline{2} \in \mathbb{Z}_4$ no tiene inverso multiplicativo.

TIPOS DE ANILLOS



Definición:

Un anillo A se dice **anillo íntegro** ó **anillo de integridad**, si A es un anillo conmutativo con unidad sin divisores de cero.

Ejemplos:

1) $(\mathbb{Z}, +, \cdot)$ es un anillo íntegro.

2) $(\mathbb{R}, [x]+, \cdot)$ es un anillo íntegro.

3) Sea $A = \mathbb{R}$, $I = [0, 1]$

$\mathbb{R}^I = \{ f \mid f : [0, 1] \to \mathbb{R}, f$ función $\}$

Con las operaciones: $(f + g)(x) = f(x) + g(x)$ (adición)

(multiplicación) $(f \cdot g)(x) = f(x) \cdot g(x)$, $x \in [0, 1]$

$(\mathbb{R}^I, +, \cdot)$ es un anillo conmutativo con unidad o identidad.

Además

i) $f \in \mathbb{R}^I$ es inversible $\Leftrightarrow$ $f(x) \neq 0$, para todo $x \in [0,1]$.

ii) f es divisor de cero en $\mathbb{R}^I \Leftrightarrow f(x) = 0$ para algún $x \in [0, 1]$

Demostración

i) $\Rightarrow$) f $\in \mathbb{R}^I$ inversible $\Leftrightarrow$ g $\in \mathbb{R}^I$ tal que $f \cdot g = 1_R$

(donde $1_R(x) = 1$, $x \in [0, 1]$).

($f \cdot g(x) = 1_R(x)$, para todo $x \in [0, 1] \Leftrightarrow f(x) \cdot g(x) = 1_R(x) = 1$

para todo $x \in [0, 1]$.

Luego $f(x) \cdot g(x) \neq 0$ para todo $x \in [0, 1] \Rightarrow f(x) \neq 0$

para todo $x \in [0,1]$.

$\Leftarrow$) Si $f(x) \neq 0$, para todo $x \in [0, 1] \Rightarrow$ existe $(f(x)^{-1} \in \mathbb{R}$

Por lo tanto tomando $g(x) = f(x)^{-1}$ para todo $x \in [0, 1]$ tenemos que

$f(x) \cdot g(x) = 1$

$(f \cdot g)(x) = 1_R(x)$, para todo $x \in [0, 1]$

luego existe g $\in \mathbb{R}^I$ tal que $f \cdot g = 1_R$.

por lo tanto f es inversible.

ii)

Como $g \neq \hat{o}$ existe y $\in [0, 1]$ tal que $(y) \neq 0$.

Por lo tanto $(f \cdot g)(y) = \hat{o}(y)$

$f(y) \cdot g(y) = 0 \Rightarrow f(y) = 0$, cierto y $\in [0, 1]$

$g(y) \neq 0$

$\Leftarrow$) Sea $f(x_0) = 0$ para cierto $x_0 \in [0, 1]$

Sea $g : [0, 1] \to \mathbb{R}$ relación definida por

$$g(x) = \begin{cases} 1 \text{ si } x = x_0 \\ 0 \text{ si } x \neq x_0 \end{cases}$$

Claramente g es no nula , $g \in \mathbb{R}^I$ y es tal que

$$(g \cdot f)(x) = g(x) \cdot f(x) = 0 = \hat{0}(x)$$

luego $g \cdot f = \hat{0}$. Por lo tanto existe A^I tal que $g \cdot f = \hat{0}$

luego f es un divisor de cero.

Observación:

En cálculo es de gran importancia la situación considerada en el ejemplo 3, con la condición que las funciones sean continuas.

Teorema : Sea A un anillo conmutativo con unidad.

A no tiene divisiones de cero $\Leftrightarrow$ se cumple la ley de cancelación multiplicativa para elementos no nulos.

Teorema : (**teorema de Wedderburn**) Todo anillo íntegro finito es un cuerpo.

Demostración:

Sea A un anillo íntegro finito.

Para que A sea cuerpo solo resta demostrar que todo elemento no nulo de A

tiene inverso.

Sea $a \in A$, $a \neq 0$, consideremos la función $f : A \to A$ definido por $f(x) = ax$

Como por hipótesis A es finito $\Rightarrow f$ es epiyectiva

f es inyectiva: $f(x) = f(y) \Rightarrow ax = ay \Rightarrow x = y$ (por ser A anillo íntegro).

luego si $1 \in A \Rightarrow$ existe $b \in A$ tal que $f(b) = 1 \Rightarrow ab = 1$.

Por lo tanto b es elemento inverso de a luego A es cuerpo.

Observación:

Es importante recordar el siguiente resultado sobre funciones

(*) "Sea X conjunto finito. $f : X \to X$ función son equivalentes:

i) f es inyectiva ii) es epiyectiva iii) es biyectiva" .

Corolario:

Si p es un número primo, entonces $\mathbb{Z}_p$ es un cuerpo.

Demostración: $\mathbb{Z}_p$ es anillo conmutativo con unidad. Veamos que no tiene divisores de cero.

Sean $a, b, \in \mathbb{Z}$ y $\bar{a}\,\bar{b} = \bar{0} \Rightarrow \overline{ab} = 0 \Rightarrow$

$ab \equiv 0 \pmod{p} \Rightarrow p \mid ab \Rightarrow p|a \vee p|b \Rightarrow$

$a \equiv 0 \pmod{p} \vee b \equiv 0 \pmod{p} \Rightarrow a = 0 \vee b = 0$

Luego $\mathbb{Z}_p$ es anillo íntegro, como $\mathbb{Z}_p$ es finito por proposición anterior $\mathbb{Z}_p$ es cuerpo.

Observación : Vale el recíproco, es decir

si $\mathbb{Z}_p$ es cuerpo $\Rightarrow p$ es primo.

La característica

Definición : Sea *A* un anillo. Se llama **característica de un anillo *A***, al menor entero positivo *n* tal que:

$\underbrace{a + a + \ldots + a}_{n \text{ veces}} = 0$, para todo $a \in A$.

es decir $n\,a = 0$, para todo $a \in A$.

Si tal entero no existe decimos entonces que *A* tiene característica cero.

La característica del anillo *A* se denota por caract. (*A*).

Nota : Característica (0) = 1.

Si tal entero positivo *n* no existe, entonces la caract. (*A*) = 0.

Ejemplo: Sea $\mathbb{Z}_6$ anillo.

Caract. $(\overline{0}) = 1$, caract. $(\overline{1}) = 6$

caract. $(\overline{2}) = 3$

Caract. $(\overline{3})n= 2$ caract. $(\overline{4}) = 3$

caract. $(\overline{5}) = 6$

Luego caract. $(\mathbb{Z}_6) = 6$.

Este ejemplo ilustra el siguiente teorema.

Teorema:

Si A es un anillo de unidad 1. Entonces caract. (A) = caract. (1)

Ejemplo :

1) $\mathbb{Z}_3$

$\overline{1} + \overline{1} + \overline{1} = \overline{0}$ luego $\mathbb{Z}_3$ tiene característica 3

$\overline{2} + \overline{2} + \overline{2} = \overline{0}$

2) $\mathbb{Z}$ tiene característica cero. $\mathbb{Q}$ tiene característica cero.

Teorema:

Sea A un anillo con unidad, entonces A tiene característica $n > 0 \Leftrightarrow n$

Es el menor entero positivo tal que $n \cdot 1 = 0$.

Demostración:

$\Rightarrow$) Evidente pues ni A tiene característica $n > 0$ luego

$n \cdot a = 0$, para todo $a \in A$ en especial cuando a = 1 luego $n \cdot 1 = 0$.

$\Leftarrow$) Supongamos que n es el menor entero positivo tal que n $\cdot$ 1 = 0 luego para cada $a \in A$.

$a + a + \ldots + a = a(1 + 1 + \ldots + 1) = a \cdot (n \cdot 1) = a \cdot 0 = 0$

n veces

Por lo tanto n es la característica del anillo A.

Teorema: (Pequeño teorema de Fermat) *P.T.F.*

Si $a \in \mathbb{Z}$, p primo , $p \nmid a$, entonces $a^{p-1} \equiv 1$ (mód p) para $a \equiv 0$ (mód p) .

Demostración: Como p es primo $\Rightarrow$ $\mathbb{Z}_p$ es cuerpo.

Los elementos no nulo de $\mathbb{Z}_p$ forman un grupo multiplicativo.

Luego $\{\overline{1}, \overline{2}, \ldots, \overline{p-1}\}$ es un grupo de orden $p - 1$.

Como en un grupo el orden de un elemento cualquiera divide el orden del grupo.

Sea $\overline{a} \in \mathbb{Z}_p$, $\overline{a} \neq 0$.

Luego $a^{p-1} = 1$ en $\mathbb{Z}_p$ $\Rightarrow$ $a^{p-1} = 1$ $\Rightarrow$ $\overline{a^{p-1}} \equiv 1$ (mód p).

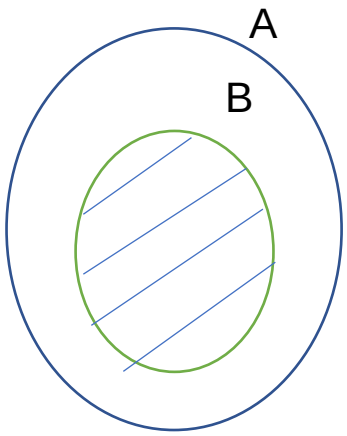
Corolario :

Si $a \in \mathbb{Z}$, entonces $a^p \equiv a \pmod{p}$ para cada primo p.

Definición: Sea $(A, +, \cdot)$ anillo.

Sea B subconjunto $\neq \emptyset$ de A. Diremos que B es un **subanillo** de A si las operaciones en A inducen en B una estructura de anillo.

Es decir $(B, +, \cdot)$ es un anillo.



Teorema :

Sea A un anillo. Sea B subconjunto de A. Entonces

B es subconjunto de $A \Leftrightarrow$ 1) $B \neq \emptyset$

2) $x, y \in B \Rightarrow x - y \in B.$

3) $x, y \in B \Rightarrow x \cdot y \in B.$

Demostración

Si B es subanillo $\Rightarrow B \neq \emptyset$ y $(B, +)$ es un grupo abeliano como $B \subset A$

Luego se cumple (2) y (3) es evidente por ser (B) anillo.

Observación:

Si A es un anillo, $B = A$ y $B = \{0\}$ son subanillos llamado subanillo triviales.

Ejemplo:

1) Sea $A = \mathbb{Z}$, $B = 2\mathbb{Z}$ (pares)

$2\mathbb{Z}$ es un subanillo.

Observar que $\mathbb{Z}$ tiene unidad $1 \in \mathbb{Z}$ pero $2\mathbb{Z}$ no tiene unidad.

2) Sea $A = \mathbb{Q}(\sqrt{2})$, $B = \mathbb{Z}(\sqrt{2})$ es subanillo de $\mathbb{Q}(\sqrt{2})$.

3) Sea $A = \mathbb{R}^{[0,1]}$

$B = \{ f \in \mathbb{R}^{[0,1]} \mid f \text{ es función constante} \}$

B es un subanillo de $\mathbb{R}^{[0,1]}$

4) Sea $A = M_2(\mathbb{R})$

$$\left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \;\middle|\; a, b \in \mathbb{R} \right\}$$

B es un subanillo de A.

(Si se identifica todo $r \in \mathbb{R}$ con $\begin{pmatrix} r & o \\ o & r \end{pmatrix}$, i con $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$,

se verifica que $i^2 = -1$ y todo elemento de B se escribe en forma única de la forma $a + bi$; $a, b \in \mathbb{R}$ obteniéndose el cuerpo de los números complejos).

.

5) Sea $C(\mathbb{R}) = \{ f \mid f : \mathbb{R} \to \mathbb{R}$, función continua$\}$ anillo de funciones contínuas

con $f + g$, $f \cdot g$.

Sea P el conjunto de las funciones polinómicas.

Luego P es subanillo de $C(\mathbb{R})$.

6) Sea $A = \mathbb{Q}(\sqrt{7})$ anillo, $B = \mathbb{Z}(\sqrt{7})$ es subanillo de $\mathbb{Q}(\sqrt{7})$.

BIBLIOGRAFÍA

1.- I. N. Herstein "Algebra Moderna" Editorial Trillas, México 1970.

2.- Garret Birkhoff Saunders Mac Lane "Algebra" Edit.Vicens-Vives, Barcelona 1963

3.- Saunders Mac Lane "Algebra" Mac-Millan, New York 1971

4.- John B. Fraleigh "A first course in abstract Algebra" Addison-Wesley 1968.