Anillos y Cuerpos

Anillos

Sea un conjunto R con dos operaciones internas que llamaremos suma ($+$) y producto ($\cdot$). Diremos que $(R, +, \cdot)$ es un anillo si verifica:

- $(R, +)$ es un grupo abeliano.
- $(R, \cdot)$ es un semigrupo.
- Para cualesquiera $a, b, c \in R$ se cumplen:

$$a(b + c) = ab + ac$$
$$(a + b)c = ac + bc$$

Cuando $(R, \cdot)$ es un monoide se dice que R es un *anillo unitario o anillo con unidad* que representaremos por 1 (elemento nuetro del producto).

Cuando $(R, \cdot)$ es un semigrupo conmutativo, se dice que R es *anillo conmutativo*.

Ejemplos: Los conjuntos numéricos con las operaciones habituales $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ y $(\mathbb{C}, +, \cdot)$ son anillos conmutativos unitarios. $(\mathbb{N}, +, \cdot)$ no es un anillo por no ser $(\mathbb{N}, +)$ un grupo.

Ejemplos: Para cada entero positivo n, el conjunto de enteros modulares $\mathbb{Z}_n$ junto con la suma y el producto es anillo (conmutativo y unitario).

Teorema 1 *Si R es un anillo, con elemento neutro aditivo* 0*, entonces para cualesquiera elementos $a, b \in R$ se tiene:*

1) $0a = a0 = 0$
2) $a(-b) = (-a)b = -(ab)$
3) $(-a)(-b) = ab$

Muchas de las propiedades de los anillos son reformulaciones de las propiedades correspondientes a los grupos, por ejemplo

- Si $m, n \in \mathbb{Z}$, $a \in R$ $\begin{cases} ma + na = (m+n)a \\ m(na) = (mn)a \end{cases}$
- Si $m, n \in \mathbb{N}$, $a \in R$ $\begin{cases} a^m a^n = a^{m+n} \\ (a^m)^n = a^{mn} \end{cases}$

Al ser una estructura más rica que la de grupo, se tienen expresiones completamente nuevas basadas en la propiedad distributiva

Teorema 2 *Para cualquier entero n, dados a, b en un anillo R, se verifican las siguientes propiedades:*

1) $n(ab) = (na)b = a(nb)$
2) la fórmula binomial (también conocida como binomio de Newton)

$$(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i}$$

Subanillos

S es un *subanillo* de R si es anillo con las operaciones definidas en R, es decir:

Dados $x, y \in S \Rightarrow x - y \in S$ y $xy \in S$

Ejemplo: *enteros gaussianos* $\mathbb{Z}(i) = \{a + ib \mid a, b \in \mathbb{Z}\}$ es un subanillo de $\mathbb{C}$.

La intersección de subanillos de un anillo R sigue siendo subanillo, por tanto dado un subconjunto A de un anillo tiene perfecto sentido definir $\langle A \rangle$ como el menor subanillo que contiene al conjunto A, es decir la intersección de todos los subanillos que contiene a A.

Morfismos de anillos

Dada $f\colon R \to R'$ entre dos anillos $(R, +, \cdot)$ y $(R', \oplus, \odot)$, diremos que es un homomorfismo de anillos si

$$f(a+b) = f(a) \oplus f(b)$$
$$f(a \cdot b) = f(a) \odot f(b)$$

Teorema 3 *Si f es morfismo de anillos se tiene:*

1) $f(0) = f(0')$
2) $f(na) = nf(a)$, $n \in \mathbb{Z}$.

Teorema 4 *Sea $f\colon R \to R'$ un homomorfismo de anillos. Entonces se verifica:*

1) Si A es subanillo de R, entonces $f(A)$ es subanillo de R'.
2) Si B es subanillo de R', entonces $f^{-1}(B)$ es subanillo de R.
3) Si R es unitario y $f(1) \neq 0$, entonces $f(1)$ es un elemento neutro para el producto en el anillo $f(R)$.

Dominios de Integridad

Definición 1 *Si a y b son elementos distintos de cero de un anillo R tal que $ab = 0$, entonces se dice que a y b son divisores de cero.*

Ejemplos:

• Los elementos [2] y [3] de $\mathbb{Z}_6$ son dos divisores de cero.

• Los divisores de cero de un anillo $\mathbb{Z}_n$ son aquellas clases cuyos elementos no son primos relativos con n.

Teorema 5 *Sea R es un anillo. Entonces es válida la ley de cancelación del producto si y solo si no tiene divisores de cero.*

Llamaremos *Dominio de Integridad* a un anillo conmutativo unitario que no contiene divisores de cero.

Ejemplos:

• Los anillos numéricos $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$ son dominios de integridad.

• Los anillos $\mathcal{M}_n$ de matrices cuadradas de orden n no son dominios de integridad.

Cuerpos

Llamaremos *cuerpo* a un anillo conmutativo unitario K donde cada elemento distinto de cero es inversible, es decir: si $a \in K$, $a \neq 0$, existe a^{-1} tal que $a \cdot a^{-1} = a^{-1} \cdot a = 1$. En otras palabras, un cuerpo es un anillo conmutativo con división.

Ejemplos:

• $\mathbb{Z}$ no es un cuerpo, puesto que los únicos elementos inversibles son 1 y -1. En cambio sí son cuerpos los restantes conjuntos numéricos $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$.

• Los enteros gaussianos $\mathbb{Z}(i)$ no forman un cuerpo (¿por-qué?) aunque sí es un dominio de integridad. El cuerpo más parecido a $\mathbb{Z}(i)$ es el subcuerpo de los números complejos $\mathbb{Q}(i)$ definido de manera obvia como los elementos de la forma $a + bi$ siendo a y b racionales.

Teorema 6 *Todo cuerpo es un dominio de integridad.*

El inverso de este teorema no es cierto, en general, tenemos dominios de integridad que no son cuerpos y $\mathbb{Z}$ es un ejemplo de ello. En cambio si es cierto en el caso finito.

Teorema 7 *Todo dominio de integridad finito es un cuerpo.*

Este teorema nos identificar los cuerpos finitos

Corolario 8 *Si p es un entero positivo primo, $\mathbb{Z}_p$ es un cuerpo.*

Se puede probar (aunque no lo haremos) que todo cuerpo finito contiene un subcuerpo que es isomorfo a un cierto $\mathbb{Z}_p$, es más, se prueba también que todos los cuerpos infinitos contiene un subcuerpo isomorfo a $\mathbb{Q}$.