AMPLIACIÓN DE MATEMÁTICAS

TIPOS DE ANILLOS.

Un anillo $(\mathbb{A}, +, \times)$ es un grupo conmutativo con respecto a la suma; al producto solo le pedimos la propiedad asociativa y a ambas la propiedad distributiva. Dependiendo de propiedades adicionales del producto tenemos distintas clases de anillos.

Definición 1. *Sea un anillo $(\mathbb{A}, +, \times)$. Se dice que*

- $\mathbb{A}$ *es* ***conmutativo*** *si $(\mathbb{A}, \times)$ lo es.*
- $\mathbb{A}$ *tiene* ***unidad*** *si existe $1 \in \mathbb{A}$, el elemento neutro del producto.*
- *Si existen $r, s \in \mathbb{A}\backslash\{0\}$ de modo que $r \times s = 0$ se dice que r es un divisor de cero por la izquierda y que s es un divisor de cero por la derecha.*
- *Si $\mathbb{A}$ no tiene divisores de cero se le llama* ***anillo integral****.*
- *Un anillo $\mathbb{A}$ conmutativo, integral y con unidad se llama* ***DOMINIO DE INTEGRIDAD****.*
- *Si $(\mathbb{A}^*, \times)$ es un grupo, $(\mathbb{A}, +, \times)$ es un* ***cuerpo de fracciones*** *o* ***anillo división****.*
- *Si $(\mathbb{A}^*, \times)$ es un grupo conmutativo, entonces $(\mathbb{A}, +, \times)$ es un* ***CUERPO****.*

Observación 1. *Nuestro interés se centra en* ***cuerpos*** *$\mathbb{F}$ (finitos) y en* ***dominios de integridad****, como los anillos de polinomios sobre cuerpos $\mathbb{F}[x]$.*

Observación 2. *Todo anillo $\mathbb{A}$ se puede incluir en otro mayor con unidad.*

Claro, sea $\mathbb{B} = \mathbb{A} \times \mathbb{Z}$ con las operaciones:

- **suma:** para todo $(r, n), (s, m) \in \mathbb{A} \times \mathbb{Z}$

$$(r, n) + (s, m) = (r + s, n + m);$$

- **producto:** para todo $(r,n),(s,m) \in \mathbb{A} \times \mathbb{Z}$

$$(r,n) \times (s,m) = (rs + rm + sn, nm).$$

Ahora es fácil ver que $(\mathbb{B}, +, \times)$ es un anillo, donde $(0,1)$ es la unidad del producto.

Además, si a cada $r \in \mathbb{A}$ le asociamos $(r,0) \in \mathbb{B}$, vemos claramente que $\mathbb{A} \subset \mathbb{B}$.

Ejemplos 1. **A:** *$\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ y $n\mathbb{Z}$ son **anillos** conmutativos e integrales. Es más:*
- *$\mathbb{Q}, \mathbb{R}$ y $\mathbb{C}$ son **cuerpos**.*
- *$\mathbb{Z}$ tiene unidad, $1 \in \mathbb{Z}$; es un **dominio de integridad**.*
- *$n\mathbb{Z}$, $n > 1$, **no** tiene unidad.*

*Además la **característica** de todos estos anillos es cero.*

B: *$(\mathbb{Z}_n, +, \times)$ son anillos para todo $n \in \mathbb{N} \backslash \{0\}$.*
- *Si n es primo, entonces $\mathbb{Z}_n$ es un cuerpo y $Char\mathbb{Z}_n = n$.*
- *Si n **no** es primo, entonces $\mathbb{Z}_n$ **no** es un anillo integral y $Char\mathbb{Z}_n = n$.*

C: *Si $\mathbb{F}$ es un cuerpo, el conjunto de polinomios con coeficientes en $\mathbb{F}$, $(\mathbb{F}[x], +, \times)$, es un **dominio de integridad**, como vimos en la introducción a las estructuras algebraicas y en el capítulo anterior.*

Algunas relaciones entre las definiciones de arriba las da el siguiente Teorema.

Teorema 1. **a:** *Si $\mathbb{A}$ es un anillo de integridad, entonces $Char\mathbb{A}$, si no es nula, es un número primo.*

b: *Si $\mathbb{F}$ es un cuerpo, entonces $Char\mathbb{F} = Char\mathbb{F}[x]$.*

c: *Todo dominio de integridad finito es un cuerpo.*

d: *Todo cuerpo es un dominio de integridad.*

e: *Todo anillo división finito es un cuerpo.*

Demostración:

a: La prueba es la misma que vimos para dominios de integridad en el capítulo anterior.

b: La vimos en el capítulo anterior.

c: Solo hay que probar que para todo $a \in \mathbb{A}^*$, del dominio de integridad, existe a^{-1}. Sea ahora el subconjunto

$$\{a, a^2, ..., a^{Card\mathbb{A}}\}.$$

Como $\mathbb{A}$ es un domino de integridad $a^j \neq 0$ para todo j. Y por ser finito tienen que existir $j, r \in \mathbb{N}$ con

$$a^j = a^{j+r} = a^j a^r \qquad \Leftrightarrow \qquad a^j(1 - a^r) = 0$$

Por ser $\mathbb{A}$ dominio de integridad, se sigue que $a^r = 1$ y así $a^{r-1}a = 1$. Por tanto el inverso de a es a^{r-1}.

d: Es evidente. Los cuerpos no tienen divisores de cero ya que salvo el cero todo elemento tiene inverso respecto del producto.

e: Éste es el Teorema de Wedderburn. El cuál queda fuera de nuestro alcance □

Referencias

Departamento de Análisis Matemático, Facultad de Matemáticas, Universidad Complutense, 28040 Madrid, Spain
E-mail address: `Cesar_Ruiz@mat.ucm.es`