AMPLIACIÓN DE MATEMÁTICAS

DEFINICIÓN DE ANILLOS.

En la Introducción a las Estructuras Algebraicas definimos las estructuras de Grupo, **Anillo** y Cuerpo. Repasemos la definición de Anillo antes de argumentar sobre la necesidad de estudiarlos en abstractos.

Definición 1. $(\mathbb{A}, *_1, *_2)$ *un conjunto* $\mathbb{A}$ *con dos operaciones* $*_1$ *y* $*_2$.

a: *Se llama* ***Anillo*** *si se verifican estas tres condiciones*

- $(\mathbb{A}, *_1)$ *es un grupo conmutativo*
- $(\mathbb{A}, *_2)$ *tiene las propiedades asociativa.*
- *La propiedad* ***distributiva*** *de la segunda operación respecto de la primera, es decir si para todo* $a, b, c \in \mathbb{A}$ *se cumple que*

$$a *_2 (b *_1 c) = (a *_2 b) *_1 (a *_2 c).$$

b: *Se llama* ***anillo con unidad*** *si es un anillo y además* $(\mathbb{A}, *_2)$ *tiene elemento neutro.*

c: *Se llama* ***anillo conmutativo*** *si es un anillo y además* $(\mathbb{A}, *_2)$ *tiene la propiedad* ***conmutativa****.*

Ejemplos 1.

- *El ejemplo típico de anillo (conmutativo) es* $(\mathbb{Z}, +, \times)$ *el conjunto de los enteros con la suma y el producto. Notemos que los enteros no tiene inversos respecto del producto.*
- $(M_{n\times n}(\mathbb{R})+, \times)$ *las matrices cuadradas* $(n \times n)$ *con su suma y producto habitual es un ejemplo de anillo esta vez* ***no*** *conmutatico.*
- *Otro de los ejemplos importantes de anillo es él de los polinomios sobre un cuerpo, pero antes de verlos hay que definir lo que es un* ***cuerpo****.*
- *Los anillos de polinomios se pueden montar sobre coeficientes en un anillo. Así por ejemplo, se puede contruir el anillos de polinomios cuyos coeficientes son los polinomios con coeficientes*

reales

$$\mathbb{R}[x][y] = \mathbb{R}[x, y]$$

que forman el anillos de polinomios en dos variables y coeficientes reales. Ésto es importante para la Geomatía, pero nosotros no lo vamos estudiar.

Nuestro objetivo es estudiar anillos de polinomios con coeficientes en un cuerpo (finito). Veremos, un poco más adelante, que se puede dar una teoría de **divisibilidad** para polinomios análoga a la que tenemos para enteros (incluidos un Teorema del Resto, un Algoritmo de Euclides y un Teorema Chino del Resto para polinomios). Si descomponer números no es "fácil", hacer lo mismo para polinomios es más complejo. Como en el caso de números, esta dificultad de "descomponer" polinomios la hace preciosa en **Criptografía**.

Para descomponer polinomios es importante la estructura de **Anillo Cociente**. Y a esto es lo que vamos a dedicar un tiempo.

El modelo del que partimos es el de los enteros $\mathbb{Z}$ y la relación de congruencia habitual

$$(\mathbb{Z}/n\mathbb{Z}, +, \times) = (\mathbb{Z}_n, +\times).$$

Vimos que este cociente $\mathbb{Z}_n$ era un anillo con la suma y el producto en congruencias (ver Congruencias de Enteros).

Esta construcción de **Anillos Cocientes** se puede hacer en abstacto. Y es lo que vamos a ver con la **Teoría de Anillos**. Veremos que al emplearla sobre anillos de polimonios podemos encontrar **Cuerpos de Descomposición** donde los polinomios tienen raíces y por tanto pueden ser descompuestos (**Teorema de Kronecker**).

Volviendo a nuestro modelo $(\mathbb{Z}_n, +, \times)$ veíamos al estudiar congruencias que

- si n no es primo, existen $k_1, k_2 \in \mathbb{Z}_n \backslash \{0\}$ de modo que $k_1 \times k_2 = 0$.
- Lo anterior no pasa en $\mathbb{Z}$ ni en $\mathbb{Z}_p$ con p primo. Ni en $\mathbb{F}[x]$, como veremos.
- En $\mathbb{Z}_n$,

$$1 + 1 + 1 + ...{}_{n-\text{veces}}.. + 1 = 0.$$

- Lo anterior no ocurre en $\mathbb{Z}$ (ni en $\mathbb{R}[x]$, pero si en $\mathbb{Z}_p[x]$, p primo, como veremos).

Los ejemplos anteriores nos sugieren que hay **muchos tipos de anillos**. No pretendemos estudiarlos todos. Para el lector interesado está preparado el apéndice que sigue: **Tipos de Anillos.**

Para nosotros los anillos serán de un solo tipo.

Definición 2. *En un anillo* $(\mathbb{A}, +, \times)$ *donde* 0 *es el elemento neutro de la suma, se llaman* ***divisor de cero*** *a todo elemento* $a \in \mathbb{A}\backslash\{0\}$ *de modo que existe otro elemento* $b \in \mathbb{A}\backslash\{0\}$ *para los cuáles*

$$a \times b = 0.$$

Un anillo conmutativo $(\mathbb{A}, +, \times)$ *se llama* ***dominio de integridad*** *si* ***no*** *tiene divisores de cero.*

Nosotros solo vamos a fijarnos en **dominio de integridad**.

Ejemplos 2.

- $(\mathbb{Z}, +, \times)$ *es un dominio de integridad.*
- $(\mathbb{Z}_p, +, \times)$*, p primo, es un dominio de integridad. De hecho es más, es un* ***cuerpo*** *(finito).*
- *El conjunto de polinomios sobe un cuerpo,* $\mathbb{F}[x]$*, es un dominio de integridad.*

Claro, dados dos polinomios, $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, con $a_n \neq 0$ y $q(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0$, con $b_m \neq 0$, su producto

$$(a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0) \times (b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0)$$

$$= \sum_{j=0}^{n} a_j x^j (b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0) = \sum_{j=0}^{n}\sum_{k=0}^{m} a_j b_k x^{j+k}.$$

no puede ser cero ya que $a_n \times b_m \neq 0$ (en un cuerpo, donde cada elemento no nulo tiene inverso, no hay divisores de cero).

Notación: En un anillo $(\mathbb{A}, +, \times)$

- en un anillo a las operaciones las llamamos **suma** $(+)$ y **producto** $(\times)$,
- al **elemento neutro de la suma** lo notamos por 0,
- al **elemento opuesto de** de t lo denotamos por $-t$
- al **elemento neutro del producto** lo notamos por 1,
- notamos $\mathbb{A}^* = \mathbb{A}\backslash\{0\}$.

Definición 3. *Sea $(\mathbb{A}, +, \times)$ un anillo (o un cuerpo). Se llama* ***característica*** *de $\mathbb{A}$ al menor entero k de modo que*

$$ka = a(1 + 1 + ...{}_{k_{veces}}.. + 1) = a + a + ...{}_{k_{veces}}.. + a = 0,$$

para todo $a \in \mathbb{A}$. Escribimos que

$$Char\mathbb{A} = \begin{cases} k \in \mathbb{N} \\ o \\ 0 \qquad (si\ no\ existe\ tal\ k). \end{cases}$$

Ejemplos 3.
- $Char\mathbb{Z} = 0$.
- $Char\mathbb{Z}_n = n$.
- $Char\mathbb{R}[x] = 0$
- $Char\mathbb{Z}_p[x] = p$, *p primo.*

Veamos este último ejemplo. $(\mathbb{Z}_p, +\times)$, con p primo, es un cuerpo como sabemos. Pero para todo $n \in \mathbb{Z}_p$

$$n + n + ...{}_{p-\text{veces}}.. + n = p \times n = 0.$$

Y claramente p es el menor entero con esta propiedad. Luego $Char\mathbb{Z}_p = p$.

Ahora si $q(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0 \in \mathbb{Z}_p[x]$, entonces

$$p \times q(x) = pb_m x^m + ... + pb_1 x + pb_0 = 0$$

ya que $pb_i = 0$ para todo $i = 0, 1, ..., m$. De hecho, este resultado es general.

Teorema 1. **A:** *Si $\mathbb{F}$ es un cuerpo, entonces*

$$Char\mathbb{F} = Char\mathbb{F}[x].$$

B: *En un* ***dominio de integridad*** *$\mathbb{A}$, en particular en un cuerpo, si $Char\mathbb{A}$ no es nula, entonces es un número primo.*

Demostración:

A: Como en el ejemplo de arriba.

B: Sea $n = Char\mathbb{A}$. Si n no es primo, entonces $n = k_1 \times k_2$, con $k_1, k_2 > 1$. Ahora, por la propiedad distributiva,

$$0 = 1+1+....{}_{n-\text{veces}}..+1 = (1+1+....{}_{k_1-\text{veces}}..+1)(1+1+....{}_{k_2-\text{veces}}..+1).$$

Como $1 + 1 + ...{}_{k_1-\text{veces}}.. + 1 \neq 0$ y $1 + 1 + ...{}_{k_2-\text{veces}}.. + 1 \neq 0$, ya que k_1 y k_2 son menores que $n = Char\mathbb{A}$, su producto no puede

ser cero ya que estamos en un dominio de integridad. Luego la suposición de que n no es primo no es correcta $\square$

Referencias

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