ESTRUCTURAS ALGEBRAICAS.

En matemáticas aparecen distintos conjuntos cuyos elementos podemos operar de alguna manera. Los conjuntos de números usuales: $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$, y $\mathbb{R}$ son unos ejemplos claros. Otros ejemplos pueden ser el conjunto de matrices o de polinomios; en estos casos podemos sumar y multiplicar sus respectivos elementos. Las biyecciones de un conjunto sobre si mismo son suceptibles de ser compuestas unas con otras, lo que es otro ejemplo de operación entre los elementos de un conjunto, en este caso el conjunto de biyecciones.

Por otro lado es fácil observar que operaciones distintas sobre conjuntos distintos tienen propiedades análogas. Estas analogías permiten englobar en una misma "**categoría**" a distintos conjuntos con operaciones diversas. Estas categorías es lo que llamaremos **estructuras algebraicas** (en concreto, estructura de **Grupo**, **Anillo** o **Cuerpo**). Se pueden estudiar de forma abstracta y después sacar conclusiones sobre ellas. Con esta información se pueden buscar aplicaciones. Lo anterior es lo que vamos a desarrollar en los siguientes temas.

Introducción al Álgebra.

Definición 1. *Dado un conjunto C una aplicación $*$ definida por*

$$\begin{array}{rccc} * & : & C \times C & \to & C \\ & & (a,b) & \to & a*b \in C. \end{array}$$

*que relaciona a un par de elementos $a, b \in C$ con otro elemento de C (que notamos $a*b$) es lo que llamamos una **operación**.*

Nos vamos a fijar en algunas propiedades usuales que suelen tener las operaciones. **No siempre una operación tendrá todas las propiedades**. Según se cumplan unas u otras estaremos delante de distintos tipos de estructuras.

Propiedades *Sea $(C, *)$ un conjunto sobre el que hay definida una operación $*$.*

- *Si $a*b = b*a$ para todo par $a, b \in C$, se dice que la operación es **conmutativa**.*
- *Si $(a*b)*c = a*(b*c)$ para todo $a, b, c \in C$, se dice que la operación es **asociativa*** (aquí los paréntesis indican prioridad en la operación).

- *Si existe un elemento* $e \in C$ *de modo que* $e * a = a * e = a$ *para todo* $a \in C$, *se dice que* e *es el* ***elemento neutro*** *de la operación.*
- *Dado* $a \in C$, *se dice que tiene un* ***elemento inverso****, si existe* $b \in C$ *de modo que* $a * b = b * a = e$ *(se suele notar* $b = a^{-1}$ *o* $b = -a$*).*

Ejemplos 1.

- $(\mathbb{N} = \{0, 1, 2, ..., n, n+1, ...\}, +)$ *los números naturales con la suma. Esta es una operación asociativa, conmutativa y* 0 *es el elemento neutro. Ahora para todo par* $n, m \in \mathbb{N}$ *con* $n \neq 0$ *se tiene que* $n + m > 0$*, luego ningún elemento no nulo de* $\mathbb{N}$ *tiene inverso (o* ***elemento opuesto****, en el caso de las sumas se dice de esta manera al inverso).*
- $(\mathbb{Z}, +)$ *La suma de enteros es asociativa, conmutativa,* 0 *es el elemento neutro y cada* $m \in \mathbb{Z}$ *tiene a* $-m$ *como elemento opuesto.*
- $(\mathbb{Z}, \times)$ *El producto de enteros es asociativo, conmutativo y* 1 *es el elemento neutro. Ahora para todo par* $n, m \in \mathbb{Z}$ *con* $n \neq 1$ *se tiene que* $n \times m \neq 1$*, luego ningún elemento distinto de* 1 *tiene inverso.*

Definición 2. *Un conjunto* $(\mathbb{G}, *)$ *con una operación* $*$*, definida sobre él, se dice que es un:*

- ***Grupo*** *si* $(\mathbb{G}, *)$ *tiene las propiedades asociativa, existe un elemento neutro y cada elemento de* $\mathbb{G}$ *tiene un opuesto o inverso.*
- ***Grupo Conmutativo o Abeliano*** *si* $(\mathbb{G}, *)$ *es un grupo y además la operación* $*$ *es* ***conmutativa****.*

Ejemplos 2.

- $(\mathbb{Z}, +)$ *los números enteros con su suma habitual forman un grupo conmutativo.*
- $(\overline{M_{n\times n}}(\mathbb{R}), \times)$ *el conjunto de la matrices cuadradas* $n \times n$ *con entradas reales y determinante no nulo (es decir que existe la inversa) junto con el producto de matrices es un grupo. En este caso no es conmutativo ya que no es conmutativo el producto de matrices.*

Si sobre un conjunto consideramos dos operaciones (la suma y el producto como ocurre en los conjutos de números por ejemplo) esto nos permite definir nuevas estructuras.

Definición 3. *Sea* $(\mathbb{A}, *_1, *_2)$ *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 3.

- *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 el de los polinomios sobre un cuerpo, pero antes de verlos hay que definir lo que es un* ***cuerpo****.*

Cuando en un conjunto con dos operaciones (anillo) sus elementos tienen inversos respecto de la primera como de la segunda operación estamos delante de lo que llamamos un **cuerpo**.

Definición 4. $(\mathbb{F}, *_1, *_2)$ *un conjunto* $\mathbb{F}$ *con dos operaciones* $*_1$ *y* $*_2$. *Se dice que es un* ***cuerpo*** *si verifica las tres condiciones siguientes:*

- $(\mathbb{F}, *_1)$ *es un grupo conmutativo*
- $(\mathbb{F}\backslash\{e\}, *_2)$ *es un grupo conmutativo, donde* $\{e\}$ *es el elemento neutro de la primera operación* $*_1$.
- *La propiedad* ***distributiva*** *de la segunda operación respecto de la primera, es decir si para todo* $a, b, c \in \mathbb{F}$ *se cumple que*

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

Notación: *sobre un cuerpo las operaciones se llaman siempre* ***suma*** $(+ = *_1)$ *y* ***producto*** $(\times = *_2)$.

Observación 1. *En $(\mathbb{F}, +, \times)$ un cuerpo, si e es el elemento neutro de la suma $(+)$ y para todo elemento $x \in \mathbb{F}$, entonces se tiene que $e \times x = e$. Claro, $x \times (e + e) = (x \times e) + (x \times e)$, pero por otro dado como $e + e = e$, se tiene que $(x \times e) + (x \times e) = (x \times e)$. Ahora sumando a un lado y otro de la igualdad el opuesto de $(x \times e)$ llegamos a que $e \times x = x \times e = e$.*
Notación: *sobre un cuerpo el elemento neutro respecto de la suma $e = 0$ y el neutro respecto de la multiplicación se denota por* 1.

Ejemplos 4. *Ejemplos de cuerpos son los números racionales $\mathbb{Q}$, los reales $\mathbb{R}$ o los complejos $\mathbb{C}$. También lo son $(\mathbb{Z}_p+, \times)$ con p primo y las operaciones suma y producto en* ***congruencias****. Estos últimos ejemplos, estudiados en un curso de* ***Matemática Discreta****, los vamos a repasar en el primer tema ya que son los ejemplos más importantes de* ***Cuerpos Finitos****.*

Ahora ya estamos en condiciones de definir el conjunto de los polinomios sobre un cuerpo.

Definición 5. *(**Informal**) Sea $(\mathbb{F}, +, \times)$ un anillo conmutativo ccon unidad o un cuerpo.*

- *Se llama (anillo) de* ***polinomios con coeficientes*** *en $\mathbb{F}$ al conjunto de las expresiones*

$$\mathbb{F}[x] = \{a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \,:\, a_0, a_1, ..., a_n \in \mathbb{F} \text{ y } n \in \mathbb{N}\}$$

- *En el cuál se define una* ***suma****:*

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

si $n \geq m$ y $e = 0$

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

igual por definición a

$$= (a_n + e)x^n + ... + (a_{m+1} + e)x^{m+1} + (a_m + b_m)x^m + \cdots + (a_1 + b_1)x + (a_0 + b_0).$$

- *Y en el cuál se define también un* ***producto****:*

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

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

Teorema 1. *Sea* $(\mathbb{F}, +, \times)$ *un anillo conmutativo o un cuerpo. Entonces el conjunto de los* ***polinomios con coeficientes en*** $\mathbb{F}$*,* $(\mathbb{F}[x], +, \times)$*, es un anillo conmutativo.*

Demostración: Obervemos que el elemento neutro de la suma será el polinomio $a_0 = 0$. Él del producto $a_0 = 1$, donde 0 y 1 son los respectivos elementos neutro de la suma y el producto de $\mathbb{F}$. El resto de propiedades se comprueban de la forma trivial (es decir haciendo cuentas) teniendo en cuenta las respectivas propiedades que ya se dan en $\mathbb{F}\square$

En los temas que siguen nuestros objetivos serán primero repasar las operaciones en **congruencias** sobre $(\mathbb{Z}_p, +, \times)$, como primer ejemplo de cuerpos finitos. Después estudiar Teoría de Grupos, de Anillos y de Cuerpos. En particular de Cuerpos Finitos. Y así terminar trabajando en polinomios con coeficientes en cuerpos finitos. Todo ello lo veremos de forma abstracta (algebraica), aunque alcanzaremos a deducir importantes aplicaciones para la computación: **Criptografía** (y también aunque no está entre nuestro objetivos **Teoría de Códigos**).

Referencias

Departamento de Análisis Matemático, Facultad de Matemáticas, Universidad Complutense, 28040 Madrid, Spain

Email address: Cesar_Ruiz@mat.ucm.es