Facultad de Ciencias Exactas, Ingeniería y Agrimensura
Escuela de Ciencias Exactas y Naturales
Departamento de Matemática

Álgebra Lineal (R211 - CE9)
2024

1.1 Cuerpos

A modo de introducción veamos una estructura algebraica abstracta que nos servirá como punto de partida para la definición de Espacios Vectoriales (recordemos la definición que vimos en Álgebra y Geometría Analítica II). ¿Conocemos cuerpos? Si!! $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{C}$. Sabemos además que $\mathbb{Z}$ y $\mathbb{N}$ no lo son. ¿Cuál es la diferencia? ¿Cómo definimos *cuerpo de escalares*? Como toda estructura algebraica, la definimos de manera axiomática.

Definición: Sea F un conjunto no vacío dotado de dos operaciones: $+ : F \times F \to F$ llamada *suma* y $\cdot : F \times F \to F$ llamada multiplicación. Decimos que $(F, +, \cdot)$ es un *cuerpo* o que F *es un cuerpo con la suma* $+$ *y el producto* $\cdot$ si se verifican los siguientes axiomas

(i) la suma es asociativa: para todos $a, b, c \in F$ tenemos que $a + (b + c) = (a + b) + c$,

(ii) existe un elemento neutro para la suma: existe un elemento $0 \in F$ tal que para todo $a \in F$, $a + 0 = 0 + a = a$,

(iii) existencia de opuestos para la suma: dado $a \in F$ existe $b \in F$ tal que $a + b = b + a = 0$,

(iv) la suma es conmutativa: para todos $a, b \in F$ tenemos que $a + b = b + a$,

(v) la multiplicación es asociativa: para todos $a, b, c \in F$ tenemos que $a \cdot (b \cdot c) = (a \cdot b) \cdot c$,

(vi) existe un elemento neutro para la multiplicación: existe un elemento $1 \in F$ tal que para todo $a \in F$, $a \cdot 1 = c \cdot a = a$,

(vii) existencia de inversos para la multiplicación: dado $a \in F^*$ (donde definimos $F^* := F \backslash \{0\}$) existe $b \in F$ tal que $a \cdot b = b \cdot a = 1$,

(viii) el producto es conmutativo: para todos $a, b \in F$ tenemos que $a \cdot b = b \cdot a$,

(ix) distributiva de la multiplicación respecto de la suma: para todos $a, b, c \in F$ tenemos que $a \cdot (b + c) = a \cdot b + a \cdot c$.

A los elementos de F los llamamos *escalares*.

Ejemplos:

1. $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ con las operaciones usuales son cuerpos. EJERCICIO!
2. $\mathbb{Z}$ con las operaciones usuales no es un cuerpo. EJERCICIO!
3. Un subconjunto $\mathbb{F} \subset \mathbb{C}$ es un *subcuerpo* si con las operaciones restringidas tenemos que $(\mathbb{F}, +, \cdot)$ es un cuerpo.

   $\mathbb{Q}$ y $\mathbb{R}$ son subcuerpos de $\mathbb{C}$ y $\mathbb{Q} \subsetneq \mathbb{R} \subsetneq \mathbb{C}$. EJERCICIO!

   Puesto que la asociatividad, conmutatividad y distributivas se heredan del cuerpo, bastará con chequear:

   a) para todos $a, b \in \mathbb{F}$ tenemos que $a + b \in \mathbb{F}$, esto es que la suma sea cerrada en $\mathbb{F}$,

   b) para todos $a, b \in \mathbb{F}$ tenemos que $a \cdot b \in \mathbb{F}$, esto es que la multiplicación también sea cerrada en $\mathbb{F}$,

c) $0, 1 \in \mathbb{F}$ (es decir que ambos neutros para la suma y la multiplicación de $\mathbb{C}$ también sean elementos de $\mathbb{F}$)

d) para todo $a \in \mathbb{F}$ su opuesto $-a \in \mathbb{C}$ también sea un elemento de $\mathbb{F}$, es decir $-a \in \mathbb{F}$,

e) para todo $a \in \mathbb{F}^*$ su inverso $a^{-1} \in \mathbb{C}$ también sea un elemento de $\mathbb{F}$, es decir $a^{-1} \in \mathbb{F}$.

Observemos que aquí hemos usado la notación de opuesto e inverso puesto que estamos en $\mathbb{C}$ y sabemos de su unicidad. Para un cuerpo general, luego de probar la unicidad de opuestos e inversos podríamos dar la misma definición y caracterización de subcuerpo.

Más arriba mencionamos la cadena de contenciones estrictas $\mathbb{Q} \subsetneq \mathbb{R} \subsetneq \mathbb{C}$. Éstos no son los únicos subcuerpos de $\mathbb{C}$. Veamos un subcuerpo de $\mathbb{C}$ que contiene estrictamente a $\mathbb{Q}$ y está estrictamente contenido en $\mathbb{C}$.

Sea el conjunto $\mathbb{Q}[\sqrt{2}] := \{x + \sqrt{2} \cdot y : x, y \in \mathbb{Q}\}$. Este conjunto $\mathbb{Q}[\sqrt{2}]$ es un subcuerpo de $\mathbb{C}$. EJERCICIO! Aclaración: $\mathbb{Q}[\sqrt{2}]$ es sólo una notación. Decimos que $\mathbb{Q}[\sqrt{2}]$ es la extensión de $\mathbb{Q}$ por $\sqrt{2}$. Extensión de cuerpos es un tema de importancia en álgebra abstracta, y es la base para la llamada *teoría de Galois*, que tiene importantes aplicaciones por ejemplo en Ecuaciones Diferenciales. Si no conocen a Galois, googleen su historia, es muy interesante (spoiler: se batió duelo a los 20 años!).

Existen además cuerpos que no son ninguno de los cuerpos numéricos ni extensiones de los mismos, y más sorprendentemente, son *finitos*, es decir, constan de una cantidad finita de elementos. Antes de ver la construcción general, hagamos un ejemplo de precalentamiento:

Ejemplo:

Consideremos el conjunto $\mathbb{Z}$. Ya vimos que con la suma y producto usuales no es un cuerpo. Spoiler: el problema es que los enteros no nulos diferentes de cero no tienen inverso para la multiplicación (salvo ± 1). Pensemos lo siguiente: para tener un cuerpo necesitamos un neutro para la operación suma y un neutro para la operación producto, o sea debemos tener 0 y 1. Consideremos entonces el conjunto $X = \{0, 1\}$. Si consideramos la suma y producto habituales, nos queda sólo un inconveniente: $1+1 = 2$. Para que las operaciones *cierren*, deberíamos asignar a $1 + 1$ el valor 0 o el valor 1. Si le asignamos el valor 1, no tenemos opuesto para la suma: no existe ningún elemento en X que sumado a 1 de 0 (el neutro de la suma). Si asignamos el valor 0, queda bien definidas la suma, el producto, y más aún, los axiomas que las vinculan se satisfacen (EJERCICIO!!). Esto es, tenemos un cuerpo con dos elementos. Dejamos como ejercicio completar las siguientes tablas:

$+$	0	1
0		
1		

$\cdot$	0	1
0		
1		

Esta construcción es un poco artificial, veamos cómo la podemos hacer más formalmente. En primer lugar, si consideramos paridad (0 es par y 1 es impar), podemos mirar la tabla de otra forma:

$+$	par	impar
par		
impar		

$\cdot$	par	impar
par		
impar		

Esto parece menos formal que lo anterior, no? Pero la paridad si es un concepto que podemos poner en términos formales: un número entero es par si el resto de la división por 2 es 0 y es impar si el resto de la división por 2 es 1. Dado cualquier entero podemos decidir su paridad simplemente dividiendo por dos. Es decir, separamos a todos los enteros en dos bolsitas: la bolsita de los pares y la bolsita de los impares. Hemos *particionado* el conjunto $\mathbb{Z}$, lo cual define una relación de equivalencia en $\mathbb{Z}$ que tiene dos clases: la clase $\overline{0}$ y la clase $\overline{1}$. EJERCICIO: describir esta relación de equivalencia.

Formalmente diremos que dos enteros a y b son *congruentes módulo 2* y escribimos $a \equiv b \pmod 2$ sii $2|(b-a)$. Esta definición es más que sólo una equivalencia, hablamos de *congruencia* puesto que esta relación respeta las operaciones suma y producto habituales en el sentido de que si $a \equiv b \pmod 2$ y $c \equiv d \pmod 2$ para $a, b, c, d \in \mathbb{Z}$, entonces $a + c \equiv b + d \pmod 2$ y $a \cdot c \equiv b \cdot d \pmod 2$. Sigue inmediatamente que $\overline{a} + \overline{c} = \overline{a+c}$ y $\overline{a} \cdot \overline{c} = \overline{a \cdot c}$, es decir, tenemos una suma y productos de clases de equivalencia bien definidos. Más aún, las tablas confeccionadas anteriormente son exactamente las tablas que obtenemos con esta suma y producto en el conjunto cociente (recordar que el conjunto cociente es el conjunto de las clases de equivalencia), que consiste de las clases del cero y del uno.

Hemos construido formalmente nuestro cuerpo finito de dos elementos: $\mathbb{Z}_2 := \{\overline{0}, \overline{1}\}$. Copiando esta idea, obtendremos más cuerpos finitos.

Sea $n \in \mathbb{N}$ fijo, se define la relación de *congruencia módulo n* de la siguiente manera:

$$a \equiv b \pmod n \Leftrightarrow n \,|\, (b-a).$$

1. Probar que define una relación de equivalencia en el conjunto $\mathbb{Z}$ de los enteros.

Sea $a \in \mathbb{Z}$, vamos a determinar su clase de equivalencia:

$$\begin{aligned}
\overline{a} &= \{b \in \mathbb{Z} : a \equiv b \pmod n\} \\
&= \{b \in \mathbb{Z} : n \,|\, (b-a)\} \\
&= \{b \in \mathbb{Z} : b - a = kn, \text{para algún } k \in \mathbb{Z}\} \\
&= \{b \in \mathbb{Z} : b = a + kn, \text{para algún } k \in \mathbb{Z}\}.
\end{aligned}$$

Esto es, en $\overline{a}$ se encuentran todas las sumas de a con múltiplos de n. En particular,

$$\begin{aligned}
\overline{0} &= \{\cdots, -2n, -n, 0, n, 2n, 3n, \cdots\}, \\
\overline{1} &= \{\cdots, 1-2n, 1-n, 1, 1+n, 1+2n, 1+3n, \cdots\}, \\
\overline{2} &= \{\cdots, 2-2n, 2-n, 2, 2+n, 2+2n, 2+3n, \cdots\}, \\
&\vdots \\
\overline{n-1} &= \{\cdots, -1-n, -1, -1+n, -1+2n, -1+3n, -1+4n, \cdots\}.
\end{aligned}$$

Notemos que no existen otras clases de equivalencia distintas. Por ejemplo,

$$\overline{n} = \{\cdots, -n, 0, n, 2n, 3n, 4n, \cdots\} = \overline{0}.$$

Observemos que, de acuerdo al algoritmo de la división, los representantes de las clases de equivalencia que escogimos son los posibles restos de la división de un entero por n.

Luego, el conjunto cociente resulta

$$\mathbb{Z}_n := \{\overline{0}, \overline{1}, \overline{2}, \cdots, \overline{n-1}\}.$$

Por ejemplo, si tomamos $n = 3$, el conjunto cociente es

$$\mathbb{Z}_3 = \{\overline{0}, \overline{1}, \overline{2}\},$$

donde $\overline{0}$ es el conjunto de los múltiplos de 3, o equivalentemente, el conjunto de los enteros que divididos por 3 dan resto nulo, a $\overline{1}$ pertenecen los enteros que divididos por 3 dan resto 1, y en $\overline{2}$, los enteros que divididos p or 3 dan resto 2.

Ahora, dados dos elementos $\overline{i}$ y $\overline{j}$ en $\mathbb{Z}_n$, definimos

$$\overline{i} + \overline{j} = \overline{i + j},$$
$$\overline{i} \cdot \overline{j} = \overline{i \cdot j}.$$

EJERCICIOS:

(b) Verficar que estas operaciones se encuentran bien definidas.

(c) Analizar si $\mathbb{Z}_1, \mathbb{Z}_2, \mathbb{Z}_3, \mathbb{Z}_4$ son cuerpos.

(d) Mostrar que $\mathbb{Z}_n$ es cuerpo si y sólo si n es primo.

Los cuerpos finitos tienen interés en si mismos y se estudian en áreas como aritmética modular, teoría de números, álgebra abstracta, criptografía, informática (y por supuesto interacciones entre estas áreas). Algunas aplicaciones son muy interesantes y actuales, como el cifrado RSA para comunicaciones digitales seguras. Otras son más antiguas pero no menos bellas: en la música, por ejemplo, cuando se utiliza una escala temperada, o en las artes visuales cuando se crean patrones simétricos para crear obras de arte. En el campus dejamos algunos vínculos de divulgación que les pueden interesar. Si encuentran alguna otra información de interés, siéntanse libres de compartirla.

Sea F un cuerpo. Para $n \in \mathbb{N}$ consideramos el elemento $1 + 1 + \overset{n \text{ veces}}{\ldots} + 1$ donde $n \in \mathbb{N}$ es un natural. Este elemento lo llamamos, duplicando la notación, n. Así, *identificamos* los números naturales con ciertos elementos del cuerpo. De esta forma, la expresión nx para $n \in \mathbb{N}$ y $x \in \mathbb{Z}$ la entendemos como:

$$nx = (1 + 1 + \overset{n \text{ veces}}{\ldots} + 1)x = 1x + 1x + \overset{n \text{ veces}}{\ldots} + 1x = x + x + \overset{n \text{ veces}}{\ldots} + x,$$

es decir, nx es el elemento de F que se obtiene sumando n veces el elemento x.

Un cuerpo F se dice **de característica** n si $n \in \mathbb{N}$ es el menor natural para el cual $1 + 1 + \overset{n \text{ veces}}{\ldots} + 1 = 0$. Si no existe tal $n \in \mathbb{N}$, decimos que F es **de característica 0**.

Ejercicio 1 *En un cuerpo F de característica $n \in \mathbb{N}$ se tiene que $nx = 0$ para todo $x \in F$.*