TEMA 11: CONCEPTOS BÁSICOS DE LA TEORÍA DE CONJUNTOS. ESTRUCTURAS ALGEBRAICAS

TIEMPO: XX — XX

Esquema

1) Introducción
   1.1) Cantor y la Teoría de Conjuntos
   1.2) Escuelas históricos
2 Álgebras de Boole
   2.1) Definición: unión, intersección, retículo algebraico
   2.2) Definición: inclusión, orden + propiedades
   2.3) Definición: retículo algebraico
   2.4) Definición: complementario, retículo complementario
   2.5) Definición: Álgebra de Boole
3) Otras operaciones
   3.1) Diferencia de conjuntos
      3.1.1) Propiedades
   3.2) Diferencia simétrica
      3.2.1) Propiedades
   3.3) Producto cartesiano
      3.3.1) Propiedades
4) Relaciones. Aplicaciones
   4.1) Definición: relación binaria + propiedades
   4.2) Definición: relación de equivalencia + propiedades
   4.3) Definición: relación de orden + propiedades
   4.4) Definición: correspondencia + tipos de correspondencia
5) Estructuras algebraicas
   5.1) Estructuras con una operación interna
      5.1.1) Grupoide, monoide, semigrupo, grupo + propiedades
   5.2) Estructuras con dos operaciones internas
      5.2.1) Definición: Anillo + propiedades
      5.2.2) Definición: Cuerpo + propiedades
   5.3) Estructuras con una operación interna y otra externa
      5.3.1) Módulo, espacio vectorial, álgebra

1) Introducción:

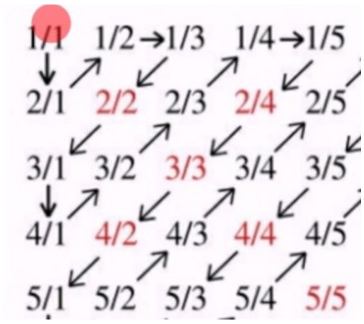
▷ El nacimiento de la Teoría de Conjuntos en el s.XIX es fruto de los trabajos del matemático alemán George Cantor y se produjo paralelamente al desarrollo de las bases de la lógica matemática en la obra de Frege.

Según Cantor un conjunto es una colección de objetos definidos y separados para la que podemos decidir si un objeto dado pertenece o no a la colección. Cantor afirma la existencia de conjuntos infinitos y muestra que un conjunto es infinito si existe una correspondencia biunívoca entre él mismo y una de sus partes.

Esta idea de la correspondencia biunívoca le sirve para definir la equivalencia entre dos conjuntos: si dos conjuntos pueden ser puestos en correspondencia biunívoca, entonces decimos que son equivalentes o equipotentes o que tienen la misma potencia.

▷ Cantor ilustró sus conceptos de equivalencia y de potencia mediante conjuntos de números. Introduce el término numerable para designar a todo conjunto que pueda ponerse en correspondencia biunívoca con los naturales (o una parte suya).

Para demostrar que $\mathbb{Q}$ es numerable ideó el siguiente esquema de conteo donde cada $(a,\, b)$ se relaciona con $\frac{a}{b}$ y después se introduce $\mathbb{N}$ en los enteros haciendo $f : \mathbb{N} \mapsto \mathbb{Z}$ definida por
$\{$ pares $\mapsto$ positivos; impares $\mapsto 0 +$ negativos $\}$



▷ Pero no todos los conjuntos infinitos tienen la misma potencia y, por consiguiente, no todos son numerable. $\mathbb{R}$ no lo es y asociada a su potencia tenemos la Hipótesis del Continuo, que pregunta sobre si hay algún cardinal entre el card($\mathbb{N}$) y el card($\mathbb{R}$) (que será verdadera o falsa según los axiomas con los que se trabaje).

▷ En la época que se difundía la Teoría de Conjuntos algunos matemáticos atacaron duramente esta concepción de las Matemáticas. En esta época surgieron tres grandes corrientes filosóficas en cuanto a la concepción y los fundamentos de las Matemáticas y, aunque no todos los matemáticos se pueden englobar en una de ellas, si hubo/hay muchos partidarios de cada una. Cada una de las corrientes se asocia a una escuela de pensamiento:

a) La escuela logística

b) La escuela formalista

c) La escuela intuicionista

▷ Su importancia radica no tanto en saber cómo son sino que las contribuciones que han aportado a las Matemáticas, tanto a nivel conceptual como en el de contenido, han sido muy numerosas e importantes.

2) Álgebras de Boole:

▷ Sea un conjunto A y consideremos un conjunto cuyos elementos son todos los subconjuntos de A y lo llamaremos "partes de A": $\mathscr{P}(A)$. En $\mathscr{P}(A)$ definimos dos operaciones, la unión y al intersección de subconjuntos de A.

▷ **Definición**: llamamos unión de B y C, $B \cup C$, al siguiente conjunto:

$$B \cup C = \{x \in A : x \in B \text{ o } x \in C\}$$

▷ **Definición**: llamamos intersección de B y C, $B \cap C$, al siguiente conjunto:

$$B \cup C = \{x \in A : x \in B \text{ y } x \in C\}$$

▷ **Propiedades**:

1) Idempotencia: $\forall B \in \mathscr{P}(A)$, $B \cup B = B = B \cap B$

2) Asociativa: $\forall B, C, D \in \mathscr{P}(A)$, $B \cup (C \cup D) = (B \cup C) \cup D$ y $B \cap (C \cap D) = (B \cap C) \cap D$

3) Conmutativa: $\forall B, C \in \mathscr{P}(A)$, $B \cup C = C \cup B$ y $B \cap C = C \cap B$

4) De simplificación: $\forall B, C \in \mathscr{P}(A)$, $B \cup (B \cap C) = B$ y $B \cap (B \cup C) = B$

▷ **Definición**: llamamos retículo algebraico a un conjunto con dos operaciones cumpliendo las cuatro propiedades anteriores.

▷ Así pues, $(\mathscr{P}(A), \cup, \cap)$ es un retículo. La unión tiene elemento neutro pues $\forall B \in \mathscr{P}(A)$, $B \cup \emptyset = B$ y tiene un elemento máximo: $B \cup A = A$. La intersección tiene como elemento neutro a A pues $A \cap B = B$ y un elemento mínimo: $A \cap \emptyset = \emptyset$.

▷ **Definición**: diremos que B está incluido en C, $B \subset C$, si se cumple que $\forall x \in B$, $x \in C$.

▷ **Definición**: una relación binaria R, definida en un conjunto A se dice que es de orden si es:

a) Reflexiva: $\forall B \in A$, $B \mathrm{R} B$

b) Antisimétrica: $\forall B, C \in A$, si $B \mathrm{R} C$ y $C \mathrm{R} B \to B = C$

c) Transitiva: $\forall B, C, D \in A$, si $B \mathrm{R} C$ y $C \mathrm{R} D \to B \mathrm{R} D$

▷ Si R es una relación de orden en A, diremos que A está ordenado.

▷ **<u>Definición</u>**: diremos que le orden de A es <u>total</u> si $\forall a, b \in A$ o $a\text{R}b$ o $b\text{R}a$.

La relación de inclusión en $\mathscr{P}(A)$ es una relación de orden, pero no es un orden total en general.

▷ **<u>Teorema</u>**: un orden en $\mathscr{P}(A)$ es total $\iff$ A tiene menos de dos elementos.

▷ Dado el conjunto $\mathscr{P}(A)$ con el orden "inclusión", se verifican las siguientes propiedades:

1) $B \subset B \cup C$, $C \subset B \cup C$, $B \cap C \subset B, C$
2) Si $B \subset D$ y $C \subset D \Rightarrow B \cup C \subset D$. Si $D \subset B$ y $D \subset C \Rightarrow D \subset B \cap C$
3) Se cumple la llamada propiedad distributiva de la unión respecto de la intersección (y viceversa):
   - $B \cup (C \cap D) = (B \cup C) \cap (B \cup D)$
   - $B \cap (C \cup D) = (B \cap C) \cup (B \cap D)$

▷ **<u>Definición</u>**: dado el conjunto A retículo algebraico donde se cumplen las dos distributivas, diremos que A es un <u>retículo algebraico</u>.

▷ **<u>Definición</u>**: llamamos <u>complementario</u> de B, $\overline{B}$, al conjunto: $\overline{B} = \{x \in A : x \notin B\}$

▷ **<u>Propiedades</u>**:

1) $B \cup \overline{B} = A$, $B \cap \overline{B} = \emptyset$, $\overline{\overline{B}} = B$
2) $\overline{A} = \emptyset$ y $\overline{\emptyset} = A$
3) $B \subset D \Longrightarrow \overline{D} \subset \overline{B}$
4) Leyes de Morgan:
   - $\overline{B \cup C} = \overline{B} \cap \overline{C}$
   - $\overline{B \cap C} = \overline{B} \cup \overline{C}$

▷ **<u>Definición</u>**: si existe una función $f : A \mapsto A$ de manera que $\forall B \in A$, $f(B) = \overline{B}$, hablaremos de un retículo complementario.

▷ **<u>Definición</u>**: llamamos <u>Álgebra de Boole</u> a un retículo distributivo y complementario.
Por ejemplo, $(\mathscr{P}(A), \cup, \cap, f)$ es un Álgebra de Boole.

3) Otras Operaciones:

▷ <u>**Diferencia de conjuntos**</u>:

▷ <u>**Definición**</u>: llamaremos <u>diferencia de A y B</u> al conjunto:

$$A - B = \{x \in A \text{ y } x \notin B\}$$

▷ <u>**Propiedades**</u>:

1) $A - B = A \cap \overline{B}$

2) $A - B = \overline{B} - \overline{A}$

3) $\overline{A - B} = \overline{A} \cup B$

4) $A - (B \cup C) = (A - B) \cap (A - C)$

5) $A - (B \cap C) = (A - B) \cup (A - C)$

▷ <u>**Diferencia simétrica**</u>:

▷ <u>**Definición**</u>: llamaremos <u>diferencia simétrica (o suma booleana) de A y B</u> al conjunto

$$A \triangle B = A + B = (A - B) \cup (B - A)$$

▷ <u>**Propiedades**</u>:

1) Asociativa: $A + (B + C) = (A + B) + C$

2) Conmutativa: $A + B = B + A$

3) Elemento neutro: $\emptyset$ pues $B + \emptyset = B$

4) Elemento simétrico: B pues $B + B = \emptyset$

▷ <u>**Producto de conjuntos**</u>:

▷ <u>**Definición**</u>: dados "n" objetos matemáticos $x_j / j = 1, \ldots, n$, llamamos <u>n-upla</u> a un nuevo objeto de la forma $(x_1, \ldots, x_n)$ donde dos objetos serán distintos si algún elemento está cambiado de orden. Para $n = 2$ son pares, $= 3$ ternas, etc.

▷ <u>**Definición**</u>: sean A y B dos conjuntos cualesquiera, llamaremos <u>producto cartesiano</u> de ambos al conjunto de los pares de elementos de la forma:

$$A \times B = \{(A, b) : a \in A \text{ y } b \in B\}$$

▷ <u>**Propiedades**</u>:

1) Sean $A' \subset A$ y $B' \subset B$, entonces $A' \times B' \subset A \times B$ y el recíproco es cierto si A', $B' \neq \emptyset$

2) Dado $(x,\, y) \in A \times B$, x es la "primera proyección" o "proyección sobre A". Análogo para y y B.

3) El producto cartesiano es distributivo respecto a la unión, intersección y la diferencia de conjuntos.

4) Relaciones. Aplicaciones:

▷ **Definición**: sean A y B conjuntos. Llamaremos relación entre elementos de A y B a un subconjunto de su producto cartesiano. Al elemento (a, b) lo notaremos por aRb o $a \sim b$ y lo leemos "a está relacionado con b".

▷ **Definición**: decimos que la relación R es binaria si es un subconjunto de $A \times A$.

▷ **Definición**: llamamos grafo de la relación binaria a: $G = \{(x, y) \in A \times A : xRy\}$

▷ **Definición**: en el caso de $G = A \times A$ se hablará de relación total.

▷ **Propiedades (posibles) de una relación binaria**:

1) Reflexiva: $\forall x \in A,\ x \sim x$
2) Antirreflexiva: $\forall x \in A,\ x \not\sim x$
3) Simétrica: $\forall x, y \in A$, si $x \sim y \Longrightarrow y \sim x$
4) Antisimétrica: $\forall x, y \in A$, si $x \sim y$ e $y \sim x \Longrightarrow x = y$
5) Transitiva: si $x \sim y$ e $y \sim z \Longrightarrow x \sim z$
6) Conexa: $\forall x, y \in A$ o bien $x \sim y$ o bien $y \sim x$

▷ **Definición**: dado $A \neq \emptyset$. una relación binaria R en A diremos que es de equivalencia si cumple las propiedades **reflexiva**, **simétrica** y **transitiva**.

▷ $\forall x \in A$ consideramos todos los elementos que están relacionados con él. Notaremos por $[x] = \{y \in A : xRy\}$ y lo llamaremos clase de equivalencia definida por x. Al elemento x lo llamaremos representante de la clase.

▷ **Definición**: llamaremos conjunto cociente $A/R = \{\ [x]\ \}$

▷ **Proposición**: A/R es una partición de A, es decir: $A = \bigcup_{x \in A} [x]$ y $[x] \cap [y] \neq \emptyset \Longrightarrow [x] = [y]$

▷ **Definición**:dado $A \neq \emptyset$. una relación binaria R en A diremos que es de orden si cumple las propiedades **reflexiva**, **antisimétrica** y **transitiva**.

▷ Si sólo cumple las propiedades reflexiva y transitiva hablaremos de preorden. Si una relación de orden cumple. además, la propiedad conexa se llama de orden total. Si en R cambia reflexiva por antirreflexiva decimos que el es un orden estricto. Si R es una relación de orden la notaremos por "$\leq$". Al par $(A, \leq)$ lo llamaremos conjunto ordenado. Para representar gráficamente una relación de orden se utilizan los diagramas de Hesse. Podemos tener un orden en A que no sea total, pero podemos encontrar un subconjunto de A donde la relación de orden inducida sí sea un orden total; a este subconjunto lo llamaremos cadena.

▷ **Definición**: dado $(A, \leq)$ decimos que está bien ordenado (o que el orden es un buen orden) si cualquier subconjunto suyo no vacío posee un primer elemento.

▷ **Teorema**: buen orden $\Longrightarrow$ orden total ($\not\Longleftarrow$)

▷ **Definición**: dados A y B llamamos correspondencia "f" entre A y B a un subconjunto de su producto cartesiano $A \times B$.

▷ **Definición**: dos elementos a y b son homólogos cuando pertenecen al subconjunto de $A \times B$. Escribiremos $f(a) = b$. Al elemento "a" lo llamaremos original de "b" y a éste imagen de "a". Al subconjunto de A formado por los originales lo llamaremos conjunto original. Para B, lo llamaremos conjunto imagen. Llamamos correspondencia inversa de "f" al subconjunto de $B \times A$ formado por los pares (b, a).

▷ Tipos de correspondencias:

a) Sobreyectiva / Suprayectiva / Exhaustiva: el conjunto imagen coincide con el conjunto final (B).

b) Correspondencia "en": el conjunto imagen es un subconjunto propio del conjunto final.

c) Aplicación: es una correspondencia cumpliendo dos condiciones:

   1) El conjunto original coincide con el conjunto inicial (A).
   2) Todo elemento tiene una sola imagen.

▷ **Definición**: dadas dos aplicaciones $f : A \mapsto B$ y $g : B \mapsto C$ de manera que el conjunto imagen de "f" es el conjunto inicial de "g", llamaremos composición de ambas aplicaciones a aquella definida como: $g \circ f : A \mapsto C$, $(g \circ f)(x) = g\big(f(x)\big)$

5) Estructuras Algebraicas:

▷ **Definición**: sea un conjunto A, llamaremos operación interna o ley de composición interna a toda aplicación de $A \times A$ en A. La notaremos por $\star$ y lo expresaremos así: $(A, \star)$. Una operación puede ser asociativa, conmutativa, tener elemento neutro, simétrico, etc.

▷ Estructuras algebraicas con una operación interna:

▷ **Definición**: un conjunto donde se ha definido (al menos) una operación interna se llama estructura algebraica.

▷ **Definición**: al par $(A, \star)$ lo llamaremos grupoide.

▷ **Definición**: si $(A, \star)$ es tal que cumple la propiedad asociativa, se llamará semigrupo.

▷ **Definición**: si $(A, \star)$ es un semigrupo con elemento neutro, se llamará monoide.

▷ **Definición**: si $(A, \star)$ es un monoide con la propiedad de elemento simétrico, se llamará grupo.

▷ **Propiedades**: sea el $(G, \star)$ grupo, entonces se cumple:

1) $G \neq \emptyset$ pues $e \in G$.
2) El neutro y el simétrico de cada elemento de G son únicos.
3) $\forall a,\, b \in G$, las ecuaciones $a \star x = b$ o bien $x \star a = b$ tienen solución única en G.
4) $\forall a,\, b,\, c \in G$, si $a \star b = a \star c \implies b = c$ o bien $b \star a = c \star a \implies b = c$ (leyes de simplificación).
5) Sea $\forall a \in G$ su simétrico $\hat{a}$, entonces: $\hat{\hat{a}} = a$; $\widehat{(a \star b)} = \hat{b} \star \hat{a}$; $\widehat{(a^n)} = (\hat{a})^n$

▷ **Definición**: decimos que $(H, \star)$ es un subgrupo de $(G, \star)$ cuando es un grupo con la restricción de $\star$ a H. $(\{e\}, \star)$ y $(G, \star)$ son los subgrupos impropios. El resto, de existir, son subgrupos propios.

▷ **Teorema**: $(H, \star)$ subgrupo de $(G, \star) \iff H \neq \emptyset$ y $\forall x$, y$\in H$, $x \star \hat{y} \in H$

$\triangleright$ Estructuras algebraicas con dos operaciones internas: sea un conjunto A con dos operaciones internas que notaremos por $(+)$ y $(\cdot)$.

$\triangleright$ **Definición**: decimos que $(A, +, \cdot)$ tiene estructura de anillo si cumple:

1) $(A, +)$ es grupo abeliano.

2) $(A, \cdot)$ es semigrupo.

3) La segunda operación es distributiva con respecto a la primera.

$\triangleright$ Decimos que el anillo es abeliano si $(A, \cdot)$ lo es. Decimos que es unitario si $(A, \cdot)$ tiene elemento neutro.

$\triangleright$ **Propiedades**: sean $(A, +, \cdot)$ un anillo, "$\mathbf{0}$" el neutro de $(A, +)$, "$\mathbf{1}$" el de $(A, \cdot)$ y "$-a$" el simétrico de a.

1) $\forall a \in A,\ a \cdot \mathbf{0} = 0 \cdot a = \mathbf{0}$

2) $\forall a \in A,\ (-\mathbf{1}) \cdot a = a \cdot (-\mathbf{1}) = -a$

3) $\forall a, b \in A,\ a \cdot (-b) = (-a) \cdot b = -(a \cdot b)$

4) $\forall a, b \in A,\ (-a) \cdot (-b) = a \cdot b$

$\triangleright$ **Definición**: sea $(A, +, \cdot)$ un anillo, decimos que $a \in A$ es un divisor de cero por la izquierda (/derecha/ambos lados) si $\exists b \in A - \{\mathbf{0}\}$ tq $a \cdot b = \mathbf{0}$ ($b \cdot a = \mathbf{0}$ / $a \cdot b = b \cdot a = \mathbf{0}$)

$\triangleright$ Llamamos anillo de integridad a todo anillo sin divisores de cero. Llamamos dominio de integridad a un anillo de integridad, unitario y abeliano.

$\triangleright$ **Definición**: sea $(A, +, \cdot)$ un anillo, decimos que $a \in A$ es nilpotente cuando $\exists n \in \mathbb{N} : a^n = \mathbf{0}$

$\triangleright$ **Definición**: decimos que $B \subset A$ es subanillo cuando B con las operaciones inducidas de A sea una anillo.

$\triangleright$ **Teorema**: $(B, +, \cdot)$ subanillo de $(A, +, \cdot) \Longleftrightarrow B \neq \emptyset$ y $\forall x, \in B,\ x - y \in B$ y $x \cdot y \in B$.

$\triangleright$ **Definición**: dado $(\mathbb{K}, +, \cdot)$, decimos que es un cuerpo si se cumple:

1) $(K, +)$ es grupo abeliano.

2) $(K - \{\mathbf{0}\}, \cdot)$ es grupo.

3) La segunda operación es distributiva con respecto a la primera.

▷ **Propiedades**:

1) Todos los elementos del cuerpo, salvo el cero, tienen simétrico para ambas operaciones.
2) Todo cuerpo conmutativo es un dominio de integridad.

▷ **Definición**: decimos que $K' \subset \mathbb{K}$ es subcuerpo cuando K' con las operaciones inducidas de $\mathbb{K}$ sea una anillo. Todo subcuerpo de $\mathbb{K}$ distinto de "$\mathbb{K}$" se denomina propio.

▷ **Definición**: $(\mathbb{K}, +, \cdot)$ es un cuerpo primo si no contiene subcuerpos propios.

▷ **Teorema**: $(K', +, \cdot)$ es subcuerpo de $(\mathbb{K}, +, \cdot) \Longleftrightarrow (K', +)$ y $(K' - \{\mathbf{0}\}, \cdot)$ son subgrupos de $(\mathbb{K}, +, \cdot)$.

▷ Estructuras algebraicas con una operación interna y otra externa:

▷ **Definición**: dados dos conjuntos A y B, llamamos operación externa por la izquierda definida en B a toda aplicación de $A \times B$ en B. Si fuese $B \times A \mapsto B$ sería operación externa por la derecha. El conjunto A es llamado dominio de operadores.

▷ **Definición**: sean $(A, +, \cdot)$ anillo unitario, $(B, +)$ grupo abeliano y consideramos la aplicación $f : A \times B \mapsto f((\lambda, b)) = \lambda * b$ cumpliendo:

1) $\forall \lambda \in A, \forall b, d \in B, \lambda * (b + d) = \lambda * b + \lambda * d$
2) $\forall \lambda, \beta \in A, \forall b \in B, (\lambda + \beta) * b = \lambda * b + \beta * b$
3) $\forall \lambda, \beta \in A, \forall b \in B, (\lambda \cdot \beta) * b = \lambda * (\beta * b)$
4) $\forall b \in B, \mathbf{1} * b = b$

En estas condiciones, la terna $(B, +,$ operación externa$)$ es un módulo izquierda sobre A (igualmente módulo derecha y si A es conmutativo, simplemente módulo).

▷ **Definición**: un subconjunto no vacío de un módulo será un submódulo cuando con las mismas operaciones del módulo tenga dicha estructura.

▷ **Definición**: si en la estructura de módulo exigimos que el dominio de operadores sea un cuerpo, entonces la estructura algebraica resultante es un espacio vectorial.

▷ Notemos que aquí están presentes cuatro operaciones distintas: tres internas y una externa. Por un lado tenemos las dos internas del cuerpo de operadores, la propia de $(B, +)$ y la externa entre el grupo y el cuerpo. Si el cuerpo no es conmutativo operamos a izquierda y derecha para hablar de espacio vectorial por la izquierda o por la derecha. Para referirnos al cuerpo, usamos la expresión K-espacio vectorial.

▷ **Propiedades**: llamemos $(V,+)$ al grupo abeliano.

1) $\forall b \in V$, $\mathbf{0} * b = \overrightarrow{0}$ donde $\overrightarrow{0}$ es el neutro de $(V,+)$

2) $\forall \lambda \in \mathbb{K}$, $\lambda * \overrightarrow{0} = \overrightarrow{0}$

3) Si $\lambda * b = \overrightarrow{0}$ o bien $\lambda = \mathbf{0}$ o bien $b = \overrightarrow{0}$

4) $\forall \lambda \in \mathbb{K}$, $\forall b \in V$, $(-\lambda) * b = -(\lambda * b)$

5) Si $\lambda \neq \mathbf{0}$, $\forall b$, $d \in V : \lambda * b = \lambda * d$, entonces $b = d$

6) Si $\forall \lambda$, $\beta \in \mathbb{K}$, $\forall b \in V - \{\overrightarrow{0}\} : \lambda * b = \beta * b$, entonces $\lambda = \beta$

7) Como $(V, +)$ es un grupo abeliano, $a + x = b$ siempre tiene solución en $(V, +)$

▷ **Definición**: una K-álgebra es un K-espacio vectorial en el que hay definida una relación interna que es bilineal, asociativa y unitaria.