Universidad Nacional de Rosario

Facultad de Ciencias Exactas, Ingeniería y Agrimensura

Resúmen

Complementos de Matemática II

Autor:
Arroyo, Joaquín

September 18, 2023

Contents

1 Unidad 1: Relaciones

Definición 1. Relación.
Definición 2. Relación funcional.
Definición 3. Sobreyectividad, inyectividad y biyectividad de relación funcional.
Definición 4. Matriz de una relación.
Definición 5. Relación inversa.
Lema 1. Si R relación y R^{-1} su inversa, entonces $Dom(R^{-1}) = Im(R)$ y $Dom(R) = Im(R^{-1})$.
Lema 2. Si R relación y R^{-1} su inversa, entonces $M(R^{-1}) = M(R)^t$
Lema 3. Si R relación funcional, entonces R^{-1} es una relación funcional sii R es biyectiva
Definición 6. Composición de relaciones.
Definición 7. Restricción de una relación. Sea R una relación de A en B, y sean $C \subset A$ y $D \subset B$, entonces la restricción de R en $C \times D$ es:

$$R|_{C\times D} = \{(a,b) \in C \times D \mid aRb\} = R \cap (C \times D)$$

Definición 8. Definición de reflexividad, simetría, transitividad y antisimetría.
Definición 9. Una relación R en A se denomina:

1. **Preorden** si R es reflexiva y transitiva
2. De **Equivalencia** si R es reflexiva, transitiva y simétrica.
3. De **Order parcial** si R es reflexiva, transitiva y antisimétrica.

Definición 10. Una relación $\sim$ una relación de equivalencia en A. Para cada $x \in A$ se define la *clase de equivalencia* de x como el conjunto:

$$[x] = \{y \in A \ : \ x \sim y\}$$

Teorema 1. Una relación $\sim$ una relación de equivalencia en un conjunto no vacío A. Entonces:

1. $[x] \neq \emptyset$ para cada $x \in A$
2. $x \sim y$ sii $[x] = [y]$
3. si $x \nsim y$ entonces $[x] \cap [y] = \emptyset$
4. La unión de todas las clases de equivalencia es el conjunto A

Definición 11. Partición de un conjunto.
Teorema 2. Sea $P = \{B_i\}_{i\in I}$ una partición del conjunto $A \neq \emptyset$. Entonces la relación $\sim$ en A dada por $x \sim y$ si $x, y \in B_i$ para algún $i \in I$ es una relación de equivalencia en A. Más aún, si $x \in B_i$ entonces, $[x] = B_i$.
Teorema 3. Existe una correspondencia biunívoca entre el conjunto de relaciones de equivalencia en un conjunto no vacío A y el conjunto de particiones de A.
Definición 12. Definición de conjunto cociente. Sea A un conjunto no vacío y $\sim$ una relación de equivalencia en A. El conjunto cociente $A/\sim$ se define como:

$$A/\sim = \{[x] : x \in A\}$$

2 Unidad 2: Conjuntos ordenados

Definición 1. Grafo dirigido.
Definición 2. Grafo dirigido asociado a una relación.
Definición 3. Camino simple.
Definición 4. Jerarquías Sea R un preorden en un conjunto no vacío A. Decimos que un elemento $a \in A$ es un elemento:

- **maximal** si para cada $x \in A$ tal que aRx se verifica xRa.

- **minimal** si para cada $x \in A$ tal que xRa se verifica aRx.
- **máximo** si para cada $x \in A$ tal que xRa.
- **mínimo** si para cada $x \in A$ tal que aRx.

Claramante, todo elemento máximo es maximal y todo mínimo minimal.

Definición 5. Sea R un preoden en $A, B \subseteq A$ y $a \in A$. Decimos que

- a es **cota superior** de B si bRa para cada $b \in B$. Si existe una cota superior de B decimos que B esta **acotado superiormente**.
- a es **cota inferior** de B si aRb para cada $b \in B$. Si existe una cota inferior de B decimos que B esta **acotado inferiormente**.
- a es **supremo** de B si a es un mínimo de

$$\{c \in A : c \; es \; cota \; superior \; de \; B\}$$

- a es **ínfimo** de B si a es un máximo de

$$\{c \in A : c \; es \; cota \; inferior \; de \; B\}$$

Definición 6. Si R es un orden parcial en A decimos que A es un poset.
Definición 7. Sea $\preceq$ una relación de orden en un conjunto A. Dados $x, y \in A$, decimos que x e y son elementos **comparables** si se verifica $x \preceq y$ o $y \preceq$ x (Como $\preceq$ es antisimétrica, estas dos condiciones se verifican simultáneamente ólo cuando $x = y$).
Definición 8. La relación $\preceq$ se denomina un **orden total** si todo par de elementos de A son comparables.
Lema 1. Sea $\preceq$ una relación de orden en un conjunto A y sea $B \subseteq A$, entonces:

1. $\preceq_{|B}$ es un orden en B. Si $\preceq$ es un orden total, entonces $\preceq_{|B}$ también lo es.
2. $\preceq^{-1}$ es un orden en A denominada el **orden inverso**. Si $\preceq$ es un orden total, entonces su orden inverso también lo es.

Definición 9. Orden lexicográfico y Orden producto.
Teorema 1. Sea $(A, \preceq)$ un conjunto parcialmente ordenado y sea $a \in A$. Entonces

1. a es un elemento minimal si para cada $x \in A$ se verifica que: $x \preceq a \implies x = a$
2. a es un elemento maximal si para cada $x \in A$ se verifica que: $a \preceq x \implies x = a$

Teorema 2. Si un conjunto parcialmente ordenado tiene un elemento máximo (mínimo) entonces este es único.
Corolario 1. Todo subconjunto de un conjunto parcialmente ordenado tiene a lo sumo un ínfimo y/o un supremo.
Teorema 3. Sea $(A, \preceq)$ un conjunto parcialmente ordenado. Si $B \neq \emptyset$ es un subconjunto finito de A, entonces $(B, \preceq_{|B})$ tiene al menos un elemento minimal y al menos un elemento maximal.
Corolario 2. Todo conjunto finito totalmente ordenado tiene un máximo y un mínimo.
Definición 10. Sea $(A, \preceq)$ un poset. Un subconjunto $X \subseteq A$ se dice una **cadena** si $(X, \preceq_{|X})$ es un conjunto totalmente ordenado.
Teorema 4. Lema de Zorn. Sea $(A, \preceq)$ un poset no vacío. Si toda cadena en A tiene cota superior, entonces A tiene al menos un elemento maximal.
Definición 11. Principio de dualidad. Consiste en que cualquier proposición que involucre cotas inferiores, elementos minimales, mínimos o ínfimos en $(A, \preceq)$ sigue siendo válida en $(A, \preceq^{-1})$ cambiando estos elementos por cotas superiores, elementos maximales, máximos o supremos respectivamente (y también cambiando cotas superiores en $(A, \preceq)$ por cotas inferiores en $(A, \preceq^{-1})$ etc.)

Teorema 5. Sea $(A, \preceq)$ un conjunto parcialmente ordenado y sea $\preceq^{-1}$ el orden inverso de $\preceq$. Entonces

1. Si a es un elemento minimal (resp. maximal) de $(A, \preceq)$, entonces a es un elemento maximal (resp. minimal) de $(A, \preceq^{-1})$.
2. Si a es un mínimo (resp. máximo) de $(A, \preceq)$, entonces a es un máximo (resp. mínimo) de $\preceq^{-1}$
3. Sea $B \subseteq A$. Si a es una cota inferior de B (resp. cota superior) en $(A, \preceq)$, entonces a es una cota superior de B (resp. cota inferior) en $\preceq^{-1}$.
4. Sea $B \subseteq A$. Si a es el ínfimo de B (resp. supremo) en $(A, \preceq)$, entonces a es el supremo de B (resp. ínfimo) en $\preceq^{-1}$.

Definición 12. Morfismos Sean $(A, \preceq_A)$ y $(B, \preceq_B)$ dos posets y sea $f : (A, \preceq_A) \to (B, \preceq_B)$ decimos que:

- f es un **morfismo de orden** (o **morfismo de posets**) si para cada $x, y \in A$ se verifica

$$x \preceq_A y \implies f(x) \preceq_B f(y)$$

- f es un **isomorfismo** de $(A, \preceq_A)$ en $(B, \preceq_B)$ si f es un morfismo de orden biyectivo tal que $f^{-1} : (B, \preceq_B) \to (A, \preceq_A)$ es un morfismo de orden.

Teorema 6. Sean $(A, \preceq_A)$ y $(B, \preceq_B)$ dos conjuntos parcialmente ordenados y sea $f : (A, \preceq_A) \to (B, \preceq_B)$ un morfismo de orden, entonces:

1. f es un isomorfisco de $(A, \preceq_A)$ en $(B, \preceq_B)$ sii f es sobreyectiva y se verifica que para cada $x, y \in A$

$$x \preceq_A y \Leftrightarrow f(x) \preceq_B f(y)$$

2. f es un isomorfisco de $(A, \preceq_A)$ en $(B, \preceq_B)$ sii f^{-1} es un isomorfisco de $(B, \preceq_B)$ en $(A, \preceq_A)$
3. Si $f : (A, \preceq_A) \to (B, \preceq_B)$ y $g : (B, \preceq_B) \to (C, \preceq_C)$ son morfismos de orden, entonces:

$$g \circ f : (A, \preceq_A) \to (C, \preceq_C)$$

es un morfismo de orden. Si f y g son isomorfismos, entonces $g \circ f$ es un isomorfismo.

Corolario 3. Sea *Poset* el conjunto de todos los conjuntos parcialmente ordenados. Entonces la relación $\sim$ en *Poset* dada por $(A, \preceq_A) \sim (B, \preceq_B)$ es una relación de equivalencia si existe un isomorfismo f de $(A, \preceq_A)$ en $(B, \preceq_B)$.
Teorema 7. Sean $(A, \preceq_A)$, $(B, \preceq_B)$ posets y sea $f : (A, \preceq_A) \to (B, \preceq_B)$ un isomorfismo. Entonces.

1. A y B tienen el mismo cardinal.
2. A es totalmente ordenado sii B es totalmente ordenado.
3. $a \in A$ es un elemento maximal (resp. minimal) de A sii $f(a)$ es un elemento maximal (resp. minimal) de B.
4. $a \in A$ es un máximo (resp. mínimo) de A sii $f(a)$ es un mínimo (resp. máximo) de B.
5. Sea $X \subseteq A$. $a \in A$ es una cota superior (resp. inferior) de X sii $f(a)$ es una cota inferior (resp. superior) de $f(X)$.
6. Sea $X \subseteq A$. $a \in A$ es el supremo (resp. ínfimo) de X sii $f(a)$ es el supremo (resp. ínfimo) de $f(X)$.

Definición 13. Un poset $(A, \preceq)$ se dice un **conjunto bien ordenado** si para cualquier subconjunto no vacío B de A, $(B, \preceq_B)$ tiene un mínimo (denominado **primer elemento**). La relación $\preceq$ se dice en este caso un **buen orden**.
Lema 2. Si $(A, \preceq)$ es un conjunto bien ordenado, entonces $\preceq$ es un orden total.
Lema 3. Si $(A, \preceq_A)$ y $(B, \preceq_B)$ son conjuntos ordenados isomorfos, entonces $(A, \preceq_A)$ es un conjunto bien ordenado sii $(B, \preceq_B)$ es bien ordenado.
Teorema 8. Principio del Buen Orden. $(\mathbb{N}, \leq)$ es un conjunto bien ordenado.
Teorema 9. Algoritmo de la división. Sean a y b números enteros con a ¿ 0. Entonces existen únicos números enteros q y r tales que $b = qa + r$ y $0 \leq r < a$
Teorema 10. Cualesquiera sean $a, b \in \mathbb{N}$, existe el máximo común divisor de a y b.
Corolario 4. El máximo común divisor entre a y b es la única combinación entera positiva de a y b que divide a a y b.
Definición 14. Un número entero k se dice **primo** si tiene exactamente dos divisores positivos: 1 y k. Si k tiene más de dos divisores positivos, k se dice **compuesto** (en consecuencia 1 no es primo ni compuesto).

Dos enteros a y b se denominan **coprimos** o **primos relativos** si $mcd(a, b) = 1$ (mcd denota el máximo común divisor)
Teorema 11. Sea $n \in \mathbb{N}$ un número compuesto. Entonces existe un número primo p tal que $p \mid n$.
Teorema 12. Euclides. Existen infinitos números primos.
Teorema 13. Teorema Fundamental de la Aritmética. Cada entero $n > 1$ puede escribirse de manera única como un producto de factores primos, excepto por el orden de los mismos.
Corolario 5. Sean $x, y \in \mathbb{N}$. Entonces el máximo común divisor de x e y es el producto de los factores primos comunes de x e y elevados al mínimo exponente en el que aparecen y el mínimo común múltiplo de x e y es el producto de los factores comunes y no comunes elevados al máximo exponente en el que aparecen.
Teorema 14. Principio del Buen Orden. Todo conjunto no vacío X admite una relación de orden $\preceq$ tal que $(X, \preceq)$ es un conjunto bien ordenado.

3 Unidad 3: Lattices

Definición 1. Retículo.
Definición 2. join y meet. Sea $(L, \preceq)$ un retículo. Para cada par $x, y \in L$ podemos definir las siguientes operaciones:

1. **join.** $x \vee y = sup\{x, y\}$
2. **meet.** $x \wedge y = inf\{x, y\}$

Teorema 1. Sea $(L, \preceq)$ un retículo. Entonces para cada $x, y, z \in L$ se verifica:

1. $x \preceq x \vee y$
2. $x \wedge y \preceq y$
3. $x \preceq y \Leftrightarrow x = x \wedge y \Leftrightarrow y = x \vee y$
4. $\vee$ y $\wedge$ son asociativas.
5. $\vee$ y $\wedge$ son conmutativas.
6. $\vee$ y $\wedge$ son idempotentes.
7. $x \vee (x \wedge y) = x = x \wedge (x \vee y)$ (absorción)
8. $\vee$ y $\wedge$ son compatibles con el orden, esto es,

$$x \preceq y \ \&\& \ w \preceq z \implies x \vee w \preceq y \vee z$$

$$x \preceq y \ \&\& \ w \preceq z \implies x \wedge w \preceq y \wedge z$$

(Uso && para denotar el AND lógico para diferenciar de join y meet)

Teorema 2. Sea L un conjunto no vacío con dos operaciones $\vee^{\sim}$ y $\wedge^{\sim}$ tales que:

1. $\vee^{\sim}$ y $\wedge^{\sim}$ son asociativas.
2. $\vee^{\sim}$ y $\wedge^{\sim}$ son conmutativas.
3. $\vee^{\sim}$ y $\wedge^{\sim}$ son idempotentes.
4. Valen las propiedades de absorción.

Entonces la relación $\preceq$ en L definida por

$$x \preceq y \Leftrightarrow x \vee^{\sim} y = y$$

es un orden parcial en L tal que $(L, \preceq)$ es un retículo para el cual $\vee = \vee^{\sim}$ y $\wedge = \wedge^{\sim}$.

Definición 3. Si $(L, \preceq)$ es un retículo, entonces $(L, \preceq^{-1})$ se denomina **retículo dual** de $(L, \preceq)$. Cuando la relación es conocida y denotamos al retículo por L, su dual suele denotarse por L^*. Además si $\wedge^*$ y $\vee^*$ son operaciones asociadas a L^*, es inmediato que $\vee = \wedge^*$ y $\wedge = \vee^*$

Definición 4. Subretículos. Sea $(L, \preceq) = (L, \vee, \wedge)$ un retículo. Un subconjunto $L' \subseteq L$ es un subretículo de L si para cada $x, y \in L'$, $x \vee y \in L'$ y $x \wedge y \in L'$, es decir, $(L', \vee', \wedge')$ es un retículo definido algebraicamente, donde $\vee' = \vee_{L' \times L'}$ y $\wedge' = \wedge_{L' \times L'}$.

Definición 5. Sean $(L, \preceq)$ y $(L', \preceq')$ dos retículos. Una función $f : L \to L'$ es un **morfismo de retículos** si f es un morfismo de orden tal que para cada $x, y \in L$

$$f(sup\{x, y\}_L) = sup\{f(x), f(y)\}_{L'} \text{ y}$$

$$f(inf\{x, y\}_L) = inf\{f(x), f(y)\}_{L'}$$

o equivalentemente,

$$f(x \vee y) = f(x) \vee' f(y) \text{ y}$$

$$f(x \wedge y) = f(x) \wedge' f(y)$$

Definición 6. f es un **morfismo de retículos** si f es un isomorfismo de orden tal que f y f^{-1} son morfismos de retículos.

Definición 7. f es un **anti isomorfismo de retículos** de L en L' SI f es un isomorfismo de retículos de $(L, \preceq)$ en $(L', \preceq^{-1})$

Lema 1. Sean $(L, \preceq)$ y $(L', \preceq')$ dos retículos, y sea $f : L \to L'$. Entonces:

1. f es un morfismo de retículos sii para cada $x, y \in L$ se verifican

$$f(x \vee y) = f(x) \vee' f(y),\ f(x \wedge y) = f(x) \wedge' f(y)$$

2. f es un isomorfismo de retículos sii f es un morfismo de retículos biyectivo.

Corolario 1. Sean L, L' y L'' retículos y sean $f : L \to L'$, $g : L' \to L''$ isomorfismos de retículos. Entonces:

1. $f^{-1} : L' \to L$ es un isomorfismo de retículos.
2. $g \circ f : L \to L''$ es un isomorfismo de retículos.

Corolario 2. Sea Ret el conjunto de todos los retículos. Entonces la relación $\sim$ en Ret definida por $L \sim L'$ si L y L' son retículos isomorfos es una relación de equivalencia.

Teorema 3. Si $f : L \to L'$ y $g : S \to S'$ son morfismos de retículos, entonces $f \times g : L \times S \to L' \times S'$ definido por $(f \times g)(x, y) = (f(x), g(y))$ es un morfismo de retículos. Si f y g son isomorfismos, entonces $f \times g$ es un isomorfismo.

Definición 8. Un retículo L se dice **auto-dual** si L y $L*$ son isomorfos.

Teorema 4. Sean L y S dos retículos y sea $f : L \to S$ un morfismo de retículos. Entonces:

1. Si L' es un subretículo de L, entonces $f(L')$ es un subretículo de S.

2. Si S' es un subretículo de S, entonces $f(S')^{-1}$ es un subretículo de L.

Definición 9. Un retículo $(L, \preceq) = (L, \vee, \wedge)$ se dice **acotado** si como conjunto ordenado tiene máximo y mínimo. El máximo de L suele denotarse por $\top$ o por 1 (**top**) y el mínimo de L por $\perp$ o 0 (**bottom**). Denotaremos $(L, \preceq, 1, 0) = (L, \vee, \wedge, 1, 0) = (L, \vee, \wedge, \perp, \top)$ a un retículo acotado con máximo 1 o $\top$ y mínimo 0 o $\perp$.

Definición 10. Sea L un retículo acotado. Dado $a \in L$, un elemento $b \in L$ se denomina un **complemento** de a, o se dice que a está **complementado por** b, si

$$a \vee b = \top, a \wedge b = \perp$$

Denotamos por $comp(a) = \{b \in L : b \text{ } es \text{ } un \text{ } complemento \text{ } de \text{ } a\}$

Un retículo acotado se dice un **retículo complementado** si existe una función

$$(.)^c : L \to L, a \mapsto a^c$$

tal que para cada $a \in L$, a^c es un complemento de a.

Observación 1. Resulta claro (apelando al Axioma de elección) que un retículo es complementado sii todo elemento admite al menos un complemento.

En este caso, el complemento de a no necesariamente es único, y por lo tanto, pueden existir distintas funciones que hagan de L un retículo complementado.

Observación 3. Es inmediato de la conmutatividad de $\wedge$ y $\vee$ que para cada $a \in L$, b es un complemento de a sii a es un complemento de b.

Además es claro que $\top$ u $\perp$ son complementos uno del otro.

Teorema 5. Sean L y S retículos y $f : L \to S$ un isomorfismo de retículos. Entonces:

1. L es un retículo acotado sii S es un retículo acotado.

2. Para cada $x \in L$, $comp(f(x)) = f(comp(x))$

3. L es un retículo complementado sii S es un retículo complementado.

Definición 11. Sea $(L, \preceq) = (L, \wedge, \vee)$ un retículo. Decimos que L es un **retículo distributivo** si para cada $x, y, z \in L$ se verifican:

$$(1) \quad x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$$

$$(2) \quad x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$$

Teorema 6. Sean L y S retículos y sea $f : L \to S$ un isomormismo de retículos. Entonces L es un retículo dsitributivo sii S es un retículo distributivo.

Teorema 7. Si un retículo L satisface una de las propiedades (1) o (2) entonces satisface la otra, y por lo tanto es distributivo.

Teorema 8. (Teorema $M_3 - N_5$). Un retículo es distributivo sii no contiene subretículos isomorfos a M_3 o a N_5.

Teorema 8. Sea L un retículo distributivo y acotado. Entonces todo elemento de L tiene a lo sumo un elemento complementario.