CAPÍTULO 1. FUNDAMENTOS DE LÓGICA Y TEORÍA DE CONJUNTOS

1. Lógica

1.1 Definición. *Una* **proposición** *es una oración declarativa de la cual se puede decir sin ambigüedad si es verdadera o falsa.*

1.2 Definición. *Sea p y q proposiciones. Vamos a definir nuevas proposiciones a partir de éstas:*

i) *Definimos la proposición $\neg p$ como "no p". Esta es verdadera si p es falsa y falsa si p es verdadera.*

ii) *Definimos la proposición $p \vee q$ como "p o q". Esta será verdadera cuando p, q o ambas son verdaderas y falsa cuando p y q lo son.*

iii) *Definimos $p \wedge q$ como "p y q". Esta es verdadera cuando p y q lo son y falsa en otro caso.*

iv) *Definimos $p \Rightarrow q$ como "si p entonces q". Esta es verdadera excepto cuando p es verdadera y q es falsa.*

v) *Definimos $p \Leftrightarrow q$ como "p si y sólo si q". Esta es verdadera cuando ambas son verdaderas o ambas falsas y falsa en otro caso. Si $p \Leftrightarrow q$ es verdadera diremos que p y q son* **equivalentes**. *La proposición $p \Leftrightarrow q$ coincide con $(p \Rightarrow q) \wedge (q \Rightarrow p)$.*

Si 1 representa verdadero y 0 falso, lo anterior se puede resumir en la siguiente tabla:

p	q	$p \vee q$	$p \wedge q$	$p \Rightarrow q$	$p \Leftrightarrow q$
1	1	1	1	1	1
1	0	1	0	0	0
0	1	1	0	1	0
0	0	0	0	1	1

Notas.

Sean p y q proposiciones:

i) $p \Rightarrow q$ es verdadera $\Leftrightarrow \neg q \Rightarrow \neg p$ es verdadera. La proposición $\neg q \Rightarrow \neg p$ recibe el nombre de contrarecíproco de $p \Rightarrow q$.

ii) $p \Rightarrow q$ es verdadera $\Leftrightarrow p \wedge \neg q \Rightarrow \neg p$ es verdadera. También $p \Rightarrow q$ es verdadera $\Leftrightarrow p \wedge \neg q \Rightarrow q$ es verdadera. Cuando para demostrar que $p \Rightarrow q$ es verdadera se prueba la veracidad de una de las proposiciones anteriores, se dice que que se demuestra $p \Rightarrow q$ por reducción al absurdo y cuando se logra, se dice que hemos llegado a contradicción.

Demostración. i)

($\Rightarrow$) Si $p \Rightarrow q$ es verdadera entonces:

p es verdadera y q es verdadera. Entonces $\neg q$ es falsa luego $\neg q \Rightarrow \neg p$ es verdadera.

p es falsa y q es verdadera. Entonces $\neg q$ es falsa luego $\neg q \Rightarrow \neg p$ es verdadera.

p es falsa y q es falsa. Entonces $\neg q$ es verdadera y $\neg p$ es verdadera luego $\neg q \Rightarrow \neg p$ es verdadera.

($\Leftarrow$) ejercicio.

ii)

($\Rightarrow$) Si $p \Rightarrow q$ es verdadera veamos en primer lugar que $p \wedge \neg q \Rightarrow \neg p$ es verdadera.

Si p es verdadera y q es verdadera entonces $\neg q$ es falsa luego $p \wedge \neg q$ es falsa y entonces $p \wedge \neg q \Rightarrow \neg p$ es verdadera.

Si p es falsa y q es verdadera entonces $p \wedge \neg q$ es falsa luego $p \wedge \neg q \Rightarrow \neg p$ es verdadera.

Si p es falsa y q es falsa entonces $p \wedge \neg q$ es falsa luego $p \wedge \neg q \Rightarrow \neg p$ es verdadera.

($\Leftarrow$) y lo demás, ejercicio.

1.3 Definición. *Un* **teorema** *es una proposición de uno de los tipos siguientes:*

(I) $p \Rightarrow q$ *verificando:*

a) $p \Rightarrow q$ *es verdadera.*

b) p *es verdadera.*

c) *Existe una relación de causa y efecto entre* p *y* q*.*

(II) $(p \Rightarrow q) \wedge (q \Rightarrow p)$ *cuando* $p \Rightarrow q$ *y* $q \Rightarrow p$ *son teoremas. Se denota por* $p \Leftrightarrow q$*.*

El teorema $p \Rightarrow q$ se lee p **implica** q o p **es condición suficiente para** q o q **es condición necesaria para** p.

Si $p \Rightarrow q$ es un teorema, a la proposición p se le llama **hipótesis** y a la proposición q se le llama **tesis**.

Así, una proposición $p \Rightarrow q$ es teorema si se deduce la veracidad de q de que p es verdadera.

El teorema $p \Leftrightarrow q$ se lee p **si y sólo si** q o p **es condición necesaria y suficiente para** q.

1.4 Ejemplos.

1. Sean $p =$ "$2 + 2 = 5$" y $q =$ "$2 + 3 = 5$".

Aunque la proposición $p \Rightarrow q$ es verdadera, $p \Rightarrow q$ no es teorema dado que p no es verdadera.

2. Supongamos que la proposición $p =$ "Yo tengo un perro" es verdadera y $q =$ "$2 + 2 = 4$". Entonces $p \Rightarrow q$ es verdadera, p es verdadera pero no es un teorema dado que no existe una relación de causa y efecto entre p y q.

3. Supongamos que la pasada noche estuve en el cine de las 10:00 a las 12:00. Sea $p =$" Estuve en el cine de 10:00 a 12:00" y $q =$"No estuve en el bar a las 10:30 de la noche". Entonces $p \Rightarrow q$ es un teorema.

2. Conjuntos

Damos la definición de conjunto dada por G. Cantor:

2.1 Definición. *Un* **conjunto** *es la reunión en un todo de determinados objetos bien definidos y diferenciables los unos de los otros.*

2.2 Ejemplos. $A = \{a, b, c\}$, $\mathbb{R}$, $\mathbb{N}^*$, $\mathbb{C}$, etc...

Adoptaremos esta definición de conjunto aunque no sea del todo rigurosa.

2.3 Definición. *Si A es un conjunto, a los objetos que lo forman se les llaman* **elementos**. *Si un conjunto A es finito, al número de elementos se le llama cardinal de A y se denota $|A|$. Si a es un elemento de A escribiremos $a \in A$. Se define* **el conjunto vacio** *como el conjunto que no tiene ningún elemento. El conjunto vacio se denota $\emptyset$.*

2.4 Definición. *Dos conjuntos A y B son iguales si tienen los mismos elementos y se denota $A = B$.*

Hay dos formas de describir un conjunto:

1) Enumerando sus elementos:

$$A = \{1, 2, 3, 4, 5\}.$$

2) Definiéndolo por las propiedades que verifican sus elementos:

$$A = \{x \in \mathbb{N}^* \mid x \leq 5\}.$$

2.5 Definición. *Un conjunto B se dice que es* **subconjunto** *de un conjunto A si cada elemento de B es elemento de A. Lo denotaremos $B \subseteq A$. Así:*

$$B \subseteq A \Leftrightarrow (x \in B \Rightarrow x \in A).$$

Claramente $\emptyset \subseteq A$ para todo conjunto A.

Además, si $A \subseteq B$ y $B \subseteq C$ entonces $A \subseteq C$.

También claramente $A = B \Leftrightarrow (A \subseteq B \wedge B \subseteq A)$.

2.6 Definición. *Si $A \subseteq X$ definimos el complementario de A en X y se denota $\overline{A}^X = \{x \in X \mid x \notin A\}$.*

2.7 Definición. *Dado X es un conjunto se define el conjunto de las partes de X como el conjunto formado por todos los subconjuntos de X y se denota $\mathbb{P}(X)$. Así:*

$$\mathbb{P}(X) = \{A \mid A \subseteq X\}.$$

Volviendo a la lógica, damos las siguientes definiciones:

2.8 Definición. *Sea X un conjunto no vacio y $\{p(x)\}_{x\in X}$ un conjunto donde para cada $x \in X$, $p(x)$ es una proposición.*

i) *Definimos la proposición " $\forall x \in X, p(x)$" como la proposición "para todo $x \in X$ se satisface $p(x)$" la cual es verdadera si siempre $p(x)$ es verdadera para cualquier $x \in X$ y falsa en otro caso.*

ii) *Definimos la proposición " $\exists\ x \in X, p(x)$" como "existe al menos un $x \in X$ para el que se satisface $p(x)$". Esta proposición es verdadera si para algún $x \in X$ $p(x)$ es verdadera y falsa en otro caso.*

iii) *Se define la proposición " $\exists\ !x \in X, p(x)$" como "existe un único $x \in X$ para el que se satisface $p(x)$".*

La negación de " $\forall x \in X, p(x)$" es " $\exists\ x \in X, \neg p(x)$".

La negación de " $\exists\ x \in X, p(x)$" es " $\forall x \in X, \neg p(x)$".

3. Operaciones con conjuntos

3.1 Definición. *Sean A, B conjuntos.*

i) *Se define A* **unión** *B y se denota $A \cup B$ a :*

$$A \cup B = \{x \mid x \in A \vee x \in B\}.$$

ii) *Se define A* **intersección** *B y se denota $A \cap B$ a:*

$$A \cap B = \{x \mid x \in A \wedge x \in B\}.$$

iii) *Se define* $A \setminus B = \{x \mid x \in A \wedge x \notin B\}$.

3.2 Ejemplo.

Sea $A = \{1, 2, 3, 4, 5\}$, $B = \{2, 4, 6\}$.

Entonces $A \cap B = \{2, 4\}$, $A \cup B = \{1, 2, 3, 4, 5, 6\}$, $A \setminus B = \{1, 3, 5\}$ y $B \setminus A = \{6\}$.

3.3 Propiedades.

1. Propiedad Asociativa.

$A \cup (B \cup C) = (A \cup B) \cup C$.

$A \cap (B \cap C) = (A \cap B) \cap C$.

2. Propiedad Conmutativa.

$A \cup B = B \cup A$.

$A \cap B = B \cap A$.

3.

$A \cup \emptyset = A$.

$A \cap \emptyset = \emptyset$.

4. Propiedad Distributiva.

$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

5. Leyes de De Morgan.

Supongamos que $A, B \subseteq X$. *Entonces:*
$\overline{(A \cap B)}^X = \overline{A}^X \cup \overline{B}^X$.
$\overline{(A \cup B)}^X = \overline{A}^X \cap \overline{B}^X$.

3.4 Definición. *Dados* A, B *conjuntos se define el* **producto cartesiano** *de* A *y* B *y se denota* $A \times B$ *a:*

$$A \times B = \{(a, b) \mid a \in A \wedge b \in B\}.$$

Si $A_1, A_2, \ldots, A_n$ *son conjuntos, se define el producto cartesiano de* $A_1, A_2, \ldots, A_n$

y se denota $A_1 \times A_2 \times \ldots \times A_n$ *a:*

$$A_1 \times A_2 \times \ldots \times A_n = \{(a_1, a_2, \ldots, a_n) \mid a_i \in A_i, 1 \leq i \leq n\}.$$

Dado A *un conjunto y* $n \in \mathbb{N}^*$ *de define:*

$$A^n = \overbrace{A \times A \times \ldots \times A}^{\text{n veces}} = \{(a_1, a_2, \ldots, a_n) \mid a_i \in A, 1 \leq i \leq n\}.$$

3.5 Ejemplo.
$\mathbb{R}^3 = \{(x, y, z) \mid x, y, z \in \mathbb{R}\}$. $(1, 2, 3), (0, 0, 0), \text{etc} \ldots \in \mathbb{R}^3$.

4. Aplicaciones

4.1 Definición. *Una* **aplicación** *es una terna* $f = (A, B, F)$ *donde* A, B *son conjuntos y* $F \subseteq A \times B$ *tal que* $\forall a \in A \quad \exists!\ b \in B$ *tal que* $(a, b) \in F$. *Escribiremos* $f : A \longrightarrow B$ *y diremos que* A *es el* **conjunto inicial** *y* B *es el* **conjunto final**.

Si $(a, b) \in F$ *diremos que* b *es la* **imagen** *de* a *por* f *y escribiremos* $f(a) = b$. *También diremos que* a *es una* **antiimagen** *de* b.

4.2 Ejemplos. Sea $A = \{1, 2, 3\}$, $B = \{a, b, c\}$.

1. Si $F = \{(1, a), (2, b)\}$ entonces $f = (A, B, F)$ no es una aplicación dado que 3 no tiene imagen.

2. Si $G = \{(1, a), (1, b), (2, c), (3, c)\}$ entonces $g = (A, B, G)$ no es aplicación dado que $(1, a), (1, b) \in G$.

3. Si $H = \{(1, a), (2, a), (3, c)\}$ entonces $h = (A, B, H)$ es aplicación. Observemos que $1, 2$ son antiimagenes de a y b no tiene antiimagenes.

4. Sea $f_1 = (\mathbb{R}, \mathbb{R}, F_1)$ con $F_1 = \{(x, x^2) \mid x \in \mathbb{R}\}$. Entonces f_1 es una aplicación ya que todo número real tiene cuadrado y sólo uno.

5. $f_2 = (\mathbb{R}, \mathbb{R}, F_2)$ tal que $f_2(x) = \sqrt{x}$ no es aplicación ya que por ejemplo -1 no tiene raíz cuadrada.

Sin embargo, $\tilde{f}_2 = ((\mathbb{R}^+, \mathbb{R}, \tilde{F}_2)$ con $f_2(x) = \sqrt{x}$ es aplicación.

6. Si A es un conjunto, definimos $1_A : A \longrightarrow A$ tal que $1_A(a) = a \quad \forall a \in A$. 1_A es aplicación y recibe el nombre de aplicación identidad de A.

Observemos que dos aplicaciones $f_1 = (A_1, B_1, F_1)$ y $f_2 = (A_2, B_2, F_2)$ son iguales si $A_1 = B_1$, $A_2 = B_2$ y $F_1 = F_2$ (o sea, si $\forall x \in A_1 = A_2$, $f_1(x) = f_2(x)$).

4.3 Definición. *Sea $f : A \longrightarrow B$ una aplicación.*

i) *Si $\tilde{A} \subseteq A$ se define el* **conjunto imagen** *de $\tilde{A}$ y se denota $f(\tilde{A})$ a:*

$$f(\tilde{A}) = \{f(a) \mid a \in \tilde{A}\}.$$

Como caso particular se define $\mathrm{Im}f = f(A) = \{f(a) \mid a \in A\}$.

Observemos que por definición de aplicación, si $a \in A$ el conjunto imagen de $\{a\}$ tiene un elemento que es $f(a)$.

ii) *Si $\tilde{B} \subseteq B$ se define el* **conjunto antiimagen** *de $\tilde{B}$ y se denota $f^{-1}(\tilde{B})$ a:*

$$f^{-1}(\tilde{B}) = \{a \in A \mid f(a) \in \tilde{B}\}$$

o sea, los elementos de A cuyas imagenes son elementos de $\tilde{B}$.

Como caso particular, si $b \in B$ se define el **conjunto antiimagen** *de b y se denota $f^{-1}(b)$ a:*

$$f^{-1}(b) = f^{-1}(\{b\}).$$

Observemos que de la definición de aplicación se deduce que $f^{-1}(B) = A$ y $f^{-1}(\mathrm{Im}f) = A$.

4.4 Definición. *Sea $f : A \longrightarrow B$ una aplicación.*

i) *Diremos que f es* **inyectiva** *si se verifica:*

$$\text{Si } a_1, a_2 \in A \mid f(a_1) = f(a_2) \Rightarrow a_1 = a_2$$

o equivalentemente:

$$\text{Si } a_1, a_2 \in A \mid a_1 \neq a_2 \Rightarrow f(a_1) \neq f(a_2).$$

ii) *Diremos que f es* **suprayectiva** *si* $\mathrm{Im}f = B$. *Dado que siempre* $\mathrm{Im}f \subseteq B$ *lo anterior es equivalente a que* $B \subseteq \mathrm{Im}f$ *o sea, si* $\forall b \in B \quad \exists \ a \in A \mid f(a) = b$.

iii) *Diremos que f es* **biyectiva** *si es inyectiva y suprayectiva.*

Ejemplos.

1. $f_1 : \mathbb{R} \longrightarrow \mathbb{R}$ tal que $f_1(x) = 2x + 1$ es una aplicación biyectiva.

2. $f_2 : \mathbb{R} \longrightarrow \mathbb{R}$ tal que $f_2(x) = x^2$ es una aplicación que no es inyectiva ni suprayectiva.

3. $f_3 : \mathbb{R} \longrightarrow \mathbb{R}^+ \cup \{0\}$ tal que $f_3(x) = x^2$ es una aplicación suprayectiva pero no inyectiva.

4. $f_4 : \mathbb{R}^+ \longrightarrow \mathbb{R}$ tal que $f_4(x) = x^2$ es una aplicación inyectiva pero no suprayectiva.

4.5 Definición. *Sea $f : A \longrightarrow B$ una aplicación biyectiva. Entonces es trivial que $f^{-1} : B \longrightarrow A \mid f^{-1}(b) = a$ donde $a \in A$ con $f(a) = b$ es un aplicación biyectiva. A f^{-1} se le llama* **aplicación inversa** *de f.*

No hay que confundir la aplicación inversa de una aplicación biyectiva con el conjunto antiimagen que está definido para cualquier subconjunto del codominio de una aplicación.

4.6 Definición. *Sea $f : A \longrightarrow B$ una aplicación y $A_1 \subseteq A$.*

Entonces $f_{|_{A_1}} : A_1 \longrightarrow B$ tal que $f_{|_{A_1}}(a_1) = f(a_1) \quad \forall a_1 \in A_1$ es una aplicación que se denomina aplicación f restringida a A_1.

4.7 Notas. i) Si $f : A \longrightarrow B$ es una aplicación, $\tilde{f} : A \longrightarrow \mathrm{Im}f$ tal que $\tilde{f}(a) = f(a)$ $\forall a \in A$ es una aplicación suprayectiva.

ii) Si $f : A \longrightarrow B$ es una aplicación inyectiva, $\tilde{f} : A \longrightarrow \mathrm{Im}f \mid \tilde{f}(a) = f(a) \ \ \forall a \in A$ es una aplicación biyectiva.

4.8 Definición. *Sea $f : A \longrightarrow B$, $g : B \longrightarrow C$ aplicaciones (observemos que el codominio de f coincide con el dominio de g). Entonces si*

$$g \circ f : A \longrightarrow C \mid (g \circ f)(a) = g(f(a)) \ \ \forall a \in A,$$

$g \circ f$ es una aplicación que recibe el nombre de **aplicación composición** *de g con f.*

4.9 Ejemplo.

Sea $f : \mathbb{R} \longrightarrow \mathbb{R} \mid f(x) = x^2$ y $g : \mathbb{R} \longrightarrow \mathbb{R} \mid g(x) = x + 2$. Entonces:

$f \circ g : \mathbb{R} \longrightarrow \mathbb{R} \mid (f \circ g)(x) = f(g(x)) = f(x + 2) = (x + 2)^2 = x^2 + 4x + 4$.

$g \circ f : \mathbb{R} \longrightarrow \mathbb{R} \mid (g \circ f)(x) = g(f(x)) = g(x^2) = x^2 + 2$.

4.10 Propiedades. *Sean $f : A \longrightarrow B$, $g : B \longrightarrow C$, $h : C \longrightarrow D$ aplicaciones.*

1. *Si f es biyectiva entonces $f \circ f^{-1} = 1_B$ y $f^{-1} \circ f = 1_A$.*

2. $(h \circ g) \circ f = h \circ (g \circ f)$.

3. *Si f y g son inyectivas entonces $g \circ f$ es inyectiva.*

4. *Si f y g son suprayectivas entonces $g \circ f$ es suprayectiva.*

5. *Si f y g son biyectivas entonces $g \circ f$ es biyectiva.*

6. *Si f y g son biyectivas entonces $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.*

4.11 Nota. En general la composición de aplicaciones no es conmutativa.

Sean $f, g : \mathbb{R} \longrightarrow \mathbb{R}$ tales que $f(x) = x^2$ y $g(x) = 2x$.

Entonces $f \circ g, g \circ f : \mathbb{R} \longrightarrow \mathbb{R}$, $(f \circ g)(x) = f(g(x)) = f(2x) = (2x)^2 = 4x^2$ y $(g \circ f)(x) = g(f(x)) = g(x^2) = 2x^2$ luego $f \circ g \neq g \circ f$.

5. Relaciones binarias de orden

5.1 Definición. *Si A es un conjunto, una* **relación binaria** *en A es un subconjunto $\mathfrak{R}$ de $A \times A$. Si $(a, b) \in \mathfrak{R}$ escribiremos $a\mathfrak{R}b$.*

5.2 Definición. *Dado A un conjunto, una relación binaria $\leq$ en A se dice que es una* **relación binaria de orden** *(RBO) si verifica:*

i) $a \leq a \quad \forall a \in A$. *(***Propiedad Reflexiva***).*

ii) *Si* $a, b \in A \mid a \leq b \wedge b \leq a \Rightarrow a = b$. *(***Propiedad Antisimétrica***).*

iii) *Si* $a, b, c \in A \mid a \leq b \wedge b \leq c \Rightarrow a \leq c$. *(***Propiedad Transitiva***).*

Un conjunto ordenado es un par $(A, \leq)$ donde A es un conjunto y $\leq$ es una RBO definida en A.

Si $(A, \leq)$ es un conjunto ordenado y $a, b \in A$ escribiremos $a \not\leq b$ si no se verifica $a \leq b$ y $a < b$ si $a \leq b$ y $a \neq b$.

5.3 Ejemplos. Damos algunos ejemplos de conjuntos ordenados.

1. $(\mathbb{N}, \leq)$, $(\mathbb{R}, \leq)$ son conjuntos ordenados donde $\leq$ es el orden habitual.

2. Si X es un conjunto, $(\mathbb{P}(X), \subseteq)$ es un conjunto ordenado.

3. $(\mathbb{N}, |\ )$ es un conjunto ordenado donde si $n, m \in \mathbb{N}$, $n|m \Leftrightarrow n$ es divisor de m.

Observemos que existen conjuntos ordenados $(A, \leq)$ tales que existen $a, b \in A$ con $a \not\leq b$ y $b \not\leq a$. Por ejemplo, en $(\mathbb{N}, |)$, $2 \not| 5$ y $5 \not| 2$.

5.4 Definición. *Sea A un conjunto ordenado, $B \subseteq A$ y $b \in B$.*

i) *Diremos que b es un* **elemento maximal** *de B si no existe $\tilde{b} \in B$ con $b \leq \tilde{b}$ y $b \neq \tilde{b}$.*

ii) *Diremos que b es un* **elemento minimal** *de B si no existe $\tilde{b} \in B$ con $\tilde{b} \leq b$ y $b \neq \tilde{b}$.*

5.5 Definición. *Sea $(A, \leq)$ un conjunto ordenado, $B \subseteq A$ y $a \in A$.*

i) *Diremos que a es una cota superior de B si $b \leq a \quad \forall b \in B$.*

ii) *Diremos que a es una cota inferior de B si $a \leq b \quad \forall b \in B$.*

iii) *Diremos que a es el supremo de B si:*

a) *a es una cota superior de B.*

b) *Si $\tilde{a}$ es otra cota superior de B entonces $a \leq \tilde{a}$.*

Si a es el supremo de B escribiremos $a = \sup B$.

iv) *Diremos que a es el ínfimo de B s:*

a) *a es una cota inferior de B.*

b) *Si $\tilde{a}$ es otra cota inferior de B entonces $a \leq \tilde{a}$.*

Si a es el ínfimo de B escribiremos $a = \inf B$.

5.6 Ejemplo.

Sea $A = \{1, 2, 3, 4, 5, 6, 8\}$. Consideremos en A la RBO $|$ = "ser divisor". Entonces $(A, |\ )$ es un conjunto ordenado.

Claramente 1 es el único elemento minimal y $5, 6, 8$ son los elementos maximales de A.

Si $B = \{2, 4\}$, 4 y 8 son las cotas superiores y 1 y 2 son las cotas inferiores de B.

Si $C = \{2, 5\}$, este subconjunto no tiene cotas superiores y por tanto no tiene supremo. Sin embargo, 1 es una cota inferior de B(es la única) y $\inf B = 1$.

5.7 Definición. *Un conjunto ordenado* $(A, \leq)$ *se dice que es un* **retículo** *si* $\forall a, b \in A \ \exists \ \inf\{a, b\} \wedge \ \exists \ \sup\{a, b\}$.

5.8 Ejemplos.

1. El ejemplo anterior no era un retículo.

2. Si X es un conjunto, $(\mathbb{P}(X), \subseteq)$ es un retículo. Claramente si $A, B \in \mathbb{P}(X)$, $\sup\{A, B\} = A \cup B$ e $\inf\{A, B\} = A \cap B$.

6. Principio de inducción

6.1 Teorema. *Sea* $\{p(n)\}_{n\in\mathbb{N}^*}$ *un conjunto donde para cada* $n \in \mathbb{N}^*$, $p(n)$ *es una proposición. Supongamos que:*

i) $p(1)$ *es verdadera.*

ii) *Si* $p(k)$ *es verdadera entonces* $p(k+1)$ *es verdadera* $\forall k \in \mathbb{N}^*$.

Entonces $p(n)$ *es verdadera* $\forall n \in \mathbb{N}^*$.

6.2 Ejemplo.

Demostrar que $1 + 2 + \ldots + n = \frac{n(n+1)}{2} \quad \forall n \in \mathbb{N}^*$.

n=1. Claramente $\frac{1(1+1)}{2} = \frac{1\cdot 2}{2} = 1$.

Hipótesis de inducción. Supongamos que la propiedad es cierta para un $n \in \mathbb{N}^*$ o sea, $1 + 2 + \ldots + n = \frac{n(n+1)}{2}$ es cierto.

Entonces $1 + 2 \ldots + (n+1) = (1 + 2 + \ldots + n) + (n+1) = \frac{n(n+1)}{2} + (n+1) = \frac{n(n+1)}{2} + \frac{2(n+1)}{2} = \frac{(n+1)(n+2)}{2}$. ∎

7. Estructuras Algebraicas

7.1 Definición. *Sea A un conjunto no vacio. Una* **ley de composición interna** *(LCI) en A es una aplicación $* : A \times A \longrightarrow A$. Si $(a, b) \in A \times A$, la imagen de (a, b) por $*$ se denota $a * b$.*

7.2 Ejemplos.

1. $\cdot : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$ tal que la imagen de $(a, b) \in \mathbb{N} \times \mathbb{N}$ es el producto $a \cdot b$ es una LCI en $\mathbb{N}$.

2. La suma $+ : \mathbb{R} \times \mathbb{R} \longrightarrow \mathbb{R}$ es una LCI en $\mathbb{R}$.

3. La resta de números naturales no es una LCI en $\mathbb{N}$.

7.3 Definición. *Sea $*$ una ley de composición interna en A.*

i) *Diremos que $*$ satisface la propiedad conmutativa si $a * b = b * a \quad \forall a, b \in A$.*

ii) *Diremos que $*$ satisface la propiedad asociativa en A si $(a*b)*c = a*(b*c) \quad \forall a, b, c \in A$.*

iii) *Dado $e \in A$, diremos que e es elemento neutro de $*$ si $e * a = a * e = a \quad \forall a \in A$.*

iv) *Si $*$ tiene elemento neutro e, dado $a \in A$ diremos que $b \in A$ es elemento simétrico de a si $a * b = b * a = e$.*

Si $*$ es asociativa en A entonces si $a, b, c \in A$, entenderemos $a * b * c$ como $(a * b) * c = a * (b * c)$.

7.4 Definición. *Un grupo es un par $(G, *)$ donde G es un conjunto no vacio y $*$ es una LCI en g que verifica:*

i) *$*$ es asociativa.*

ii) $\exists \quad e \in G$ *elemento neutro de $*$.*

iii) $\forall g \in G$ existe elemento simétrico de g.

Diremos que un grupo $(G, *)$ es abeliano si $*$ es conmutativa.

7.5 Proposición. *Sea G un grupo. Entonces:*

a) *El elemento neutro es único.*

b) *Si $g \in G$, g tiene un único elemento simétrico.*

Demostración. a) Supongamos que $e, \tilde{e} \in G$ son elementos neutros. Entonces:

$e = e * \tilde{e} = \tilde{e}$.

b) Sea $g \in G$ y supongamos que $g_1, g_2 \in G$ son elementos simétricos de G. Entonces $g_1 = g_1 * e = g_1 * (g * g_2) = (g_1 * g) * g_2 = e * g_2 = g_2$. ∎

7.6 Notación. Normalmente si (G,*) es un grupo abeliano se suele usar + en lugar de $*$ y si $g \in G$, el inverso de g se denota $(-g)$ y el elemento neutro por 0. Si $(G, *)$ no es abeliano, se suele mantener para la LCI $*$, para el elemento neutro 1 y si $g \in G$, el simétrico de g se denota g^{-1}.

7.7 Proposición. *Sea G un grupo. Entonces:*

i) $(g^{-1})^{-1} = g \quad \forall g \in G$.

ii) $(g_1 * g_2)^{-1} = {g_2}^{-1} * {g_1}^{-1} \quad \forall g_1, g_2 \in G$.

Demostración. i) Como $g * g^{-1} = g^{-1} * g = e$ entonces $(g^{-1})^{-1} = g$.

ii) $(g_1 * g_2) * ({g_2}^{-1}) * (g_1)^{-1} = g_1 * e * {g_1}^{-1} = e$ luego $(g_1 * g_2)^{-1} = {g_2}^{-1} * {g_1}^{-1}$. ∎

7.8 Definición. *Si G es un grupo, un subconjunto no vacio H de G se dice que es un subgrupo de G si:*

i) *$\forall x, y \in H$, $x * y \in H$. (O sea, $*$ es una ley de composición interna en H.)*

ii) *$(H, *)$ es un grupo.*

7.9 Proposición. Sea $(G, *)$ un grupo con elemento neutro e y H un subgrupo de G. Entonces:

i) *$e \in H$ y por lo tanto, e es el elemento neutro en H.*

ii) *Si $g \in H$, y g^{-1} es el elemento simétrico de g en G entonces $g^{-1} \in H$ y por lo tanto, g^{-1} es el elemento simétrico de g en H.*

Demostración. i) Supongamos que $\tilde{e}$ es elemento neutro en H. Entonces $\tilde{e} * \tilde{e} = \tilde{e}$ luego $(\tilde{e} * \tilde{e}) * \tilde{e}^{-1} = \tilde{e} * \tilde{e}^{-1}$ y entonces $\tilde{e} * e = e$ y así $\tilde{e} = e$.

ii) Si $\tilde{g}$ es el elemento simétrico de g en H entonces $g * \tilde{g} = \tilde{g} * g = e$ luego $\tilde{g} = g^{-1}$ y $g^{-1} \in H$. ∎

7.10 Proposición. *Sea G un grupo y H un subconjunto no vacio de G. Las siguientes afirmaciones son equivalentes:*

i) *H es un subgrupo de G.*

ii) $x * y^{-1} \in H$, $\forall x, y \in H$.

Demostración. i) $\Rightarrow$ ii). Es obvio.

ii) $\Rightarrow$ i). Dado que H es no vacio, existe $x \in H$. Entonces por hipótesis, $1 = x * x^{-1} \in H$. Así H tiene elemento neutro.

Ahora, si $x \in H$ entonces por hipótesis $x^{-1} = 1 * x^{-1} \in H$, luego cada elemento de H tiene elemento simétrico.

Si $x, y \in H$ entonces por lo anterior $y^{-1} \in H$ y entonces por hipótesis $x * y = x * (y^{-1})^{-1} \in H$, luego $*$ en H es una LCI.

Finalmente como $*$ es asociativa en G, lo es H. Así $(H, *)$ es un grupo luego H es un subgrupo de G. ∎

7.11 Definición. *Un* **cuerpo** *es una terna $(K, +, \cdot)$ donde K es un conjunto no vacio y $+, \cdot$ son LCI en K tales que:*

(I) *$(K, +)$ es un grupo abeliano. Denotaremos por 0 el elemento neutro de K y si $a \in K$ denotaremos por $-a$ es el elemento simétrico de a.*

(II)

i) *$\cdot$ es asociativa.*

ii) *$\cdot$ es conmutativa.*

iii) *Existe $1 \in K \setminus \{0\}$ tal que $1 \cdot a = a \quad \forall a \in K \setminus \{0\}$.*

iv) *$\forall\ a \in K \setminus \{0\}$ existe $a^{-1} \in K \setminus \{0\}$ tal que $a^{-1} * a = 1$. A a^{-1} le llamaremos inverso de a.*

v) $a \cdot (b + c) = (a \cdot b) + (a \cdot c) \ \ \forall a, b, c \in K$.

7.12 Ejemplos.

1. $(\mathbb{R}, +, \cdot)$ es un cuerpo.

2. $(\mathbb{C}, +, \cdot)$ es un cuerpo.

3. $(\mathbb{Z}, +, \cdot)$ no es un cuerpo ya que por ejemplo $5 \in \mathbb{Z} \setminus \{0\}$ y no tiene inverso.

7.13 Definición. *Sean A, B conjuntos. Una ley de composición externa(LCE) de A sobre B es una aplicación $\nu : A \times B \longrightarrow B$.*

7.14 Ejemplo. Consideramos $\nu : \mathbb{R} \times \mathbb{R}^2 \longrightarrow \mathbb{R}^2 \mid \nu(\lambda, (x, y)) = (\lambda x, \lambda y)$. Entonces ν es un LCE de $\mathbb{R}$ sobre $\mathbb{R}^2$.

7.15 Definición. *Si $(K, +, \cdot)$ es un cuerpo, se define:*

$$K[x] = \{a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n \mid a_i \in K, 1 \leq i \leq n, n \in \mathbb{N}^*\}.$$

Si $p(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n$ con $a_n \neq 0$ diremos que el grado de $p(x)$ es n. Cuando $p(x) = a \in K$ diremos que el grado de $p(x)$ es 0. A $a_0, a_1, \ldots, a_2$ se les llama coeficientes de $p(x)$.

En $K[x]$ se pueden definir dos LCI. Sea $p(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n \in K[x]$ y $q(x) = b_0 + b_1 x + b_2 x^2 + \ldots + b_m x^m$. Supongamos que $m \leq n$.

+:

$p(x) + q(x) = (a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2 + \ldots + (a_m + b_m)x^m + a_{m+1}x^{m+1} + \ldots + a_n x^n$.

·:

$p(x) \cdot q(x) = (a_0 \cdot b_o) + (a_0 \cdot b_1 + a_1 \cdot b_0)x + \ldots + (a_0 \cdot b_n + a_1 \cdot b_{n-1} + \ldots + a_{n-1} \cdot b_1 + a_n \cdot b_0)x^n + \ldots + (a_n \cdot b_m)x^{n+m}$.

7.16 Definición. *Si K es un cuerpo, $p(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n \in K[x]$ y $\alpha \in K$, diremos que α es una raíz de $p(x)$ se define $p(\alpha) = a_0 + a_1 \cdot \alpha + a_2 \cdot \alpha^2 + \ldots + a_n \cdot \alpha^n$. Si $p(\alpha) = 0$ diremos que α es una raíz de $p(x)$.*

7.17 Definición. *Si K es un cuerpo y $p(x), q(x) \in K[x]$, diremos que $p(x)$* **divide** *a $q(x)$ y se denota $p(x) | q(x)$ si existe $r(x) \in K[x]$ tal que $p(x) \cdot r(x) = q(x)$. En otro caso escribiremos $p(x) \not| q(x)$.*

7.18 Proposición. *Sea K un cuerpo. Si $\alpha \in K$ es una raíz de $p(x)$ entonces $(x-\alpha)|p(x)$.*

7.19 Definición. *Sea K un cuerpo, $p(x) \in K[x]$ y $\alpha \in K$ es una raíz de $p(x)$, diremos que α es de mutiplicidad $r \in \mathbb{N}^*$ si $(x-\alpha)^r|p(x)$ pero $(x-\alpha)^{r+1} \not| p(x)$.*

7.20 Ejemplo.

Consideramos $p(x) = x^3 - 7x^2 + 16x - 12 \in \mathbb{R}[x]$. Entonces $x = 2$ es una raíz de $p(x)$.

Dado que $(x-2)^2|p(x)$ pero $(x-2)^3 \not| p(x)$ se tiene que 2 es una raíz de $p(x)$ de multiplicidad 2.

El siguiente resultado es conocido como Teorema Fundamental del Algebra.

7.21 Teorema. *Si $p(x) \in \mathbb{C}[x]$ y el grado de $p(x)$ es mayor que 0 entonces existen $a, z_1, z_2, \ldots, z_n \in \mathbb{C}$ tales que $p(x) = a(x-z_1)(x-z_2)\ldots(x-z_n)$.*

8. Notación

Para finalizar éste capítulo, introducimos las siguientes notaciones:

i) Si $+$ es una ley de composición interna en A y $a_1, a_2, \ldots, a_n \in A$ denotaremos por:

$$\sum_{i=1}^{n} a_i = a_1 + a_2 + \ldots + a_n.$$

ii) Si $\cdot$ es una ley de composición interna en A y $a_1, a_2, \ldots, a_n \in A$ denotaremos por:

$$\prod_{i=1}^{n} a_i = a_1 \cdot a_2 \cdot \ldots \cdot a_n.$$

iii) Si $A_1, A_2, \ldots, A_n$ son conjuntos se denota:

$$\bigcup_{i=1}^{n} A_i = A_1 \cup A_2 \cup \ldots \cup A_n = \{x \mid \exists i \in \{1, \ldots, n\} \text{ con } x \in A_i\}$$

y

$$\bigcap_{i=1}^{n} A_i = A_1 \cap A_2 \cap \ldots \cap A_n = \{x \mid x \in A_i \ \forall\ i \in \{1, \ldots, n\}\}.$$