ALGEBRA LINEAL

David Delepine, Mauro Napsuciale, Simón Rodríguez

29 de agosto de 2005

Índice general

Capítulo 1

Repaso: Lógica, Conjuntos y Estructuras Algebraicas.

1.1. Introducción.

En este capítulo daremos un repaso de lógica y teoría de conjuntos, así como una breve descripción de las estructuras algebraicas básicas, poniendo énfasis en la estructura de **campo**, que será necesaria después en la formulación de la teoría de los espacios vectoriales, el Algebra Lineal.

1.2. Elementos de Lógica formal.

Definición 1 *Una proposición es un enunciado respecto del cual se disponga de un criterio que nos permite afirmar que su contenido es falso o verdadero.*

Ejemplo 1 *"Todos los profesores de tiempo completo del IFUG son investigadores activos.*^{es} *una proposición ya que existen criterios bien claros para determinar si el contenido es falso o verdadero: los productos de su investigación, por ejemplo artículos publicados, conferencias etc.. En este caso la proposición es verdadera.*

Ejemplo 2 *"Levanten todos su mano izquierda"no es una proposición.*

Usualmente las proposiciones son enunciados largos por lo que es conveniente usar un lenguaje simbólico. En lo sucesivo denotaremos a las proposiciones por letras mayúsculas (P, Q, R etc.).

Definición 2 *Dada una proposición P se define la **negación** de P que denotaremos por $\widetilde{P}$ como aquella proposición que tiene el valor opuesto a P. Si P es verdadera, entonces $\widetilde{P}$ es falsa y si P es falsa entonces $\widetilde{P}$ es verdadera.*

Ejemplo 3 *"No todos los profesores de tiempo completo del IFUG son investigadores activos.^{es} la negación de la proposición en el ejemplo 1.*

Además de proposiciones, existen "*conectores*"lógicos, que en la lógica formal definen operaciones binarias de las proposiciones.Un *conector* lógico o *conjuntor* es un elemento que enlaza o relaciona dos proposiciones para formar una nueva proposición. Los conectores lógicos elementales son "o.$^{\text{e}}$ "y". A las proposiciones que no tienen conectores lógicos las llamaremos proposiciones simples mientras que a las proposiciones que contengan conectores lógicos las llamaremos composiciones compuestas o simplemente proposiciones. Ejemplos de proposiciones compuestas son:

Ejemplo 4 *.^{El} León pasará a primera división este año o despedirán al director técnico"*

Ejemplo 5 *"Ayer estuvo nublado y llovió"*

Definición 3 *Dadas dos proposiciones P , Q, el conector "o"define una operacion entre proposiciones que llamaremos la **disyunción** de P con Q y denotaremos por $P \vee Q$. Por definición, si al menos una de las proposiciones P, Q es verdadera, entonces $P \vee Q$ es verdadera. En caso contrario $P \vee Q$ es falsa.*

Es conveniente ilustrar gráficamente esta definición en una tabla de valores, usualmente llamada "tabla de verdad"

P	Q	$P \vee Q$
V	V	V
V	F	V
F	V	V
F	F	F

(1.1)

A la proposición $\widetilde{P} \vee Q$ se le llama la **implicación** de Q por P y se denota por $P \Rightarrow Q$. Dada la importancia de esta operación en la extracción

de las consecuencias de una proposición, daremos explícitamente su tabla de valores, que puede deducirse de la anterior

P	Q	$P \Rightarrow Q$
V	V	V
V	F	F
F	V	V
F	F	V

(1.2)

Claramente, esta proposición no es conmutativa, es decir, $P \Rightarrow Q$, toma valores distintos de la implicación $Q \Rightarrow P$.

De estas definiciones obtenemos que las siguientes propiedades se satisfacen, esto es, las siguientes proposiciones son siempre verdaderas

1. $P \Rightarrow P$
2. $P \vee P \Rightarrow P$
3. $P \Rightarrow P \vee Q$
4. $P \vee Q \Rightarrow Q \vee P$
5. $(P \Rightarrow Q) \Rightarrow (R \vee P \Rightarrow R \vee Q)$
6. $(P \Rightarrow Q) \Rightarrow (P \vee R \Rightarrow Q \vee R)$
7. $(P \Rightarrow Q) \Rightarrow (\widetilde{Q} \Rightarrow \widetilde{P})$
8. $P \Rightarrow \widetilde{\widetilde{P}}$.

En efecto, calculemos, a partir de las definiciones 1-3 los valores de estas proposiciones.

Propiedad1. Reemplazando Q por P en la tabla de la Ec.(1.2) obtenemos los valores

P	P	$P \Rightarrow P$
V	V	V
F	F	V

Propiedad 2. Reemplazando Q por P en la tabla de la Ec.(1.1)y usando la Ec.(1.2) obtenemos los valores

P	P	$P \vee P$	$P \vee P \Rightarrow P$
V	V	V	V
F	F	F	V

Propiedad 3. Usando los valores en las Ecs.(1.1,1.2) obtenemos

P	Q	$P \vee Q$	$P \Rightarrow P \vee Q$
V	V	V	V
V	F	V	V
F	V	V	V
F	F	F	V

Proposición 4.

P	Q	$P \vee Q$	$Q \vee P$	$P \vee Q \Rightarrow P \vee Q$
V	V	V	V	V
V	F	V	V	V
F	V	V	V	V
F	F	F	F	V

Propiedad 7.

P	Q	$P \Rightarrow Q$	$\widetilde{Q}$	$\widetilde{P}$	$\widetilde{Q} \Rightarrow \widetilde{P}$	$(P \Rightarrow Q) \Rightarrow (\widetilde{Q} \Rightarrow \widetilde{P})$
V	V	V	F	F	V	V
V	F	F	V	F	F	V
F	V	V	F	V	V	V
F	F	V	V	V	V	V

.

Ejercicio 1 *Muestre que las propiedades 5,6 y 8 se satisfacen.*

A las implicaciones $P \Rightarrow Q$ y $Q \Rightarrow P$ se les llama *implicaciones recíprocas.* A la implicación $\widetilde{Q} \Rightarrow \widetilde{P}$ se le llama *contrarrecíproca* de $P \Rightarrow Q$.

Si se satisfacen ambas (esto es, si ambas proposiciones son verdaderas), $P \Rightarrow Q$ y $Q \Rightarrow P$, decimos que P y Q son **equivalentes** y escribimos entonces $P \Leftrightarrow Q$. Es posible mostrar que las recíprocas de 7) y 8) se satisfacen, esto es: $i)(\widetilde{Q} \Rightarrow \widetilde{P}) \Rightarrow (P \Rightarrow Q)$, $ii)\widetilde{(\widetilde{P})} \Rightarrow P$ son siempre verdaderas por lo que se tienen las siguientes equivalencias

9. $P \Leftrightarrow \widetilde{(\widetilde{P})}$

10. $(P \Rightarrow Q) \Leftrightarrow (\widetilde{Q} \Rightarrow \widetilde{P})$

1. **Ejercicio 2** *Muestre que las proposiciones* $i)(\widetilde{Q} \Rightarrow \widetilde{P}) \Rightarrow (P \Rightarrow Q)$, $ii)\widetilde{(\widetilde{P})} \Rightarrow P$ *son verdaderas.*

A la proposición.$\widetilde{(\widetilde{P} \vee \widetilde{Q})}$ se le llama la **conjunción** de Q con P y se denota por $P \wedge Q$. Esta es la operación asociada al conector lógico "y" y su tabla de valores puede deducirse de la Eq.(1.1) y de la definición 2 como

P	Q	$P \wedge Q$
V	V	V
V	F	F
F	V	F
F	F	F

Las siguientes propiedades se satisfacen:

11 $(P \Rightarrow Q) \wedge (Q \Rightarrow R) \Rightarrow (P \Rightarrow R)$: transitividad de la implicación.

12. $\widetilde{(P \wedge Q)} \Leftrightarrow \widetilde{P} \vee \widetilde{Q}$

13. $\widetilde{(P \vee Q)} \Leftrightarrow \widetilde{P} \wedge \widetilde{Q}$

14. $(P \vee Q) \vee R \Leftrightarrow P \vee (Q \vee R)$: asociatividad de $\vee$.

15 $(P \wedge Q) \wedge R \Leftrightarrow P \wedge (Q \wedge R)$: asociatividad de $\wedge$.

16. $(P \vee Q) \wedge R \Leftrightarrow (P \wedge R) \vee (Q \wedge R)$

17. $(P \wedge Q) \vee R \Leftrightarrow (P \vee R) \wedge (Q \vee R)$

18. $((P \vee Q) \wedge (P \Rightarrow R) \wedge (Q \Rightarrow R)) \Rightarrow R$.

Propiedad 11.

P	Q	R	$P \Rightarrow Q$	$Q \Rightarrow R$	$(P \Rightarrow Q) \wedge (Q \Rightarrow R)$	$P \Rightarrow R$	11
V	V	V	V	V	V	V	V
V	V	F	V	F	F	F	V
V	F	V	F	V	F	V	V
V	F	F	F	V	F	F	V
F	V	V	V	V	V	V	V
F	V	F	V	F	F	V	V
F	F	V	V	V	V	V	V
F	F	F	V	V	V	V	V

Propiedad 12.

Usando la definicion de la conjunción tenemos que $P \wedge Q \equiv \widetilde{(\widetilde{P} \vee \widetilde{Q})}$, asi que $\widetilde{P \wedge Q} \equiv \widetilde{\widetilde{(\widetilde{P} \vee \widetilde{Q})}}$ y usando la propiedad 9 obtenemos $\widetilde{P \wedge Q} \Leftrightarrow (\widetilde{P} \vee \widetilde{Q})$ es siempre verdadera.

Ejercicio 3 *Muestre que las proposiciones 13-18 se satisfacen.*

Nótese que toda esta estructura deviene exclusivamente de las definiciones 1-3.

Debemos enfatizar que en el lenguaje coloquial existen conectores asociados a las operaciones $\Rightarrow$ y $\Leftrightarrow$, aunque el uso de los correspondientes valores asociados (Ec.(1.2)) es mas bien restringido. En efecto, la operación $\Rightarrow$ asta asociada con el conector *"si...entonces..."*, mientras que la operación $\Leftrightarrow$ esta asociada al conector *"si y solo si"*. Así, los enunciados: *"Si* el alumno hace ejercicios *entonces* aprende*"* y *"*Los alumnos aprobarán el curso de Algebra Lineal *si y solo si* estudian*"*, son proposiciones cuyos valores pueden obtenerse usando la Ec.(1.2).

La estrucutura de una teoría matemática en general contiene dos tipos de proposiciones:

1. Un conjunto mínimo de proposiciones "primitivas"que consideramos verdaderas al que denominamos **postulados** o **axiomas**.

2. Un conjunto de proposiciones cuya certeza es demostrada conforme a las leyes de la lógica formal, partiendo del valor verdadero asociado a los axiomas. A estas proposiciones se les denomina **teoremas, proposiciones,lemas,corolarios etc.** dependiendo de su relevancia.

Dado que por definición los axiomas son verdaderos, solo será necesario usar una parte de la herramienta desarrollada. Por ejemplo, en una proposición de la forma $P \Rightarrow Q$ usualmente P tiene asignado el valor V debido a que los axiomas tienen este valor. La parte de la tabla de valores en la Ec.(1.2) a usar es entonces

P	Q	$P \Rightarrow Q$
V	V	V
V	F	F

.

Así, si demostramos que la implicación $P \Rightarrow Q$ es verdadera, necesariamente Q será verdadera. Ocasionalmente es mas facil probar implicaciones equivalentes, por ejemplo, si queremos probar que la implicación $P \Rightarrow Q$ es verdadera, puede ser mas simple probar que $\widetilde{Q} \Rightarrow \widetilde{P}$ es verdadera, lo cual prueba tambien lo que queremos en virtud de la propiedad 10.

Un método de uso común para demostrar que una proposición Q es verdadera es el llamado método de **demostración por reducción al absurdo**. Este método esta basado en la siguiente

Proposición 1 *Sea P una proposición. Si existe una proposición Q (no necesariamente verdadera) tal que las relaciones : i) $\widetilde{P} \Rightarrow Q$ y ii) $\widetilde{P} \Rightarrow \widetilde{Q}$ son verdaderas, entonces P es verdadera.*

Demostración. *Calculemos en general los valores de las correspondientes proposiciones*

$\widetilde{P}$	Q	$\widetilde{Q}$	$\widetilde{P} \Rightarrow Q$	$\widetilde{P} \Rightarrow \widetilde{Q}$
V	V	F	V	F
V	F	V	F	V
F	V	F	V	V
F	F	V	V	V

.

Nótese que independientemente del valor de Q, la única forma de que ambas proposiciones: $\widetilde{P} \Rightarrow Q$ y $\widetilde{P} \Rightarrow \widetilde{Q}$ sean verdaderas es cuando $\widetilde{P}$ es falsa (renglones 4 y 5). En consecuencia, bajo estas condiciones P es verdadera.

■

Demostración. *Esta proposición se puede también probarse de la siguiente forma: de la proposiciónes 9 y 10 tenemos que $(\widetilde{P} \Rightarrow Q) \Leftrightarrow (\widetilde{Q} \Rightarrow P)$ y $(\widetilde{P} \Rightarrow \widetilde{Q}) \Leftrightarrow (Q \Rightarrow P)$, así que si $\widetilde{P} \Rightarrow Q$ y $\widetilde{P} \Rightarrow \widetilde{Q}$ son verdaderas, también lo son las proposiciones $\widetilde{Q} \Rightarrow P$ y $Q \Rightarrow P$. Calculemos la tabla general de*

valores para estas implicaciones

Q	$\widetilde{Q}$	P	$Q \Rightarrow P$	$\widetilde{Q} \Rightarrow P$
V	F	V	V	V
V	F	F	F	V
F	V	V	V	V
F	V	F	V	F

.

De esta tabla de valores es claro (renglones 2 y 4) que independientemente del valor de Q, en el caso en que $Q \Rightarrow P$ y $\widetilde{Q} \Rightarrow P$ son ambas verdaderas la proposición P es necesariamente verdadera. ■

Mas adelante tendremos oportunidad de usar estos métodos de demostración en la construcción explícita de algunas teorías.

La mejor forma de iniciar la construcción de cualquier formalismo matemático es partiendo de la teoría de conjuntos cuyos principales resultados revisaremos ahora.

1.3. Conjuntos

Definición 4 *Un conjunto es una colección de objetos, que denotaremos genéricamente por letras minúsculas, llamados elementos del conjunto. Si a es un elemento del conjunto A escribimos $a \in A$; si a no es elemento de A, escribimos $a \notin A$. Por ejemplo, si A es el conjunto de alumnos de este curso, entonces yo $\in A$ y mi $profesor \notin A$.*

Se dice que dos conjuntos A y B son iguales, lo que se escribe como $A = B$, si A y B contienen exactamente los mismos elementos. Los conjuntos se pueden escribir de dos maneras:

1. Enlistando todos los elementos del conjunto entre llaves $\{\quad\}$.
2. Describiendo los elementos del conjunto en términos de alguna propiedad característica.

Por ejemplo, el conjunto que consta de los elementos $1, 2, 3$ y 4 se puede escribir como $\{1, 2, 3, 4\}$ o como

$$\{x \Uparrow \quad x \text{ es un entero positivo menor que } 5\},$$

donde el símbolo $\Uparrow$ se lee "tal que". Nótese que el orden en que se enumeran los elementos es intrascendente; por lo tanto

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

Ejemplo 6 *El conjunto de los números naturales* $\mathbf{N} = \{1,2,3,4,...\}$

Ejemplo 7 *El conjunto de los números enteros* $\mathbf{Z} = \{...-4,-3,-2,-1,0,1,2,3,4...\}$

Ejemplo 8 *El conjunto de los números racionales* $\mathbf{Q} = \{\frac{n}{m} \Uparrow n,m \in \mathbf{Z}, m \neq 0\}$

Ejemplo 9 *Sea A el conjunto de números reales comprendidos entre 1 y 2, Entonces A se puede escribir como*

$$A = \{x \Uparrow \quad x \text{ es un número real y } 1 < x < 2\}$$

o bien si $\mathbf{R}$ *es el conjunto de los números reales, como*

$$A = \{x \in \mathbf{R} \Uparrow 1 < x < 2\}$$

Definición 5 *Se dice que un conjunto B es subconjunto de un conjunto A, lo que se escribe como $B \subset A$ o $A \supset B$, si todo elemento de B es un elemento de A. Por ejemplo,* $\{1,2,6\} \subset \{2,8,7,6,1\}$.

Obsérvese que $A = B$ si y sólo si $B \subset A$ y $A \subset B$, un hecho que se utiliza frecuentemente para demostrar que dos conjuntos son iguales.

El conjunto vacío denotado por $\emptyset$, es el conjunto que no tiene ningún elemento. El conjunto vacío es por defnición un subconjunto de todo conjunto.

Existen tres dos operaciones básicas entre conjuntos

Definición 6 *La unión de dos conjuntos A y B que se escribe $A \cup B$ se define como el conjunto de todos los elementos que están en A, o en B, o en ambos; esto es*

$$A \cup B = \{x \Uparrow x \in A \text{ o } x \in B\}\,.$$

La intersección de dos conjuntos A y B, que se escribe como $A \cap B$ es el conjunto de todos los elementos que están en A y en B; esto es,

$$A \cap B = \{x \Uparrow x \in A \text{ y } x \in B\}\,.$$

Dos conjuntos se llaman ***disjuntos*** *si su intersección es el conjunto vacío.*

Ejemplo 10 *Sea* $A = \{1, 3, 5\}$ *y* $B = \{1, 5, 7, 8\}$ *. Entonces*

$$A \cup B = \{1, 3, 5, 7, 8\} \quad y \quad A \cap B = \{1, 5\}.$$

De manera semejante si $X = \{1, 2, 8\}$ *y* $Y = \{3, 4, 5\}$ *. Entonces*

$$X \cup Y = \{1, 2, 3, 4, 5, 8\} \quad y \quad X \cap Y = \emptyset.$$

Por lo tanto X *y* Y *son conjuntos disjuntos.*

La unión e intersección de más de dos conjuntos puede definirse de manera análoga. Especificamente si A_1, A_2, ..., A_n son conjuntos, entonces la unión y la interseción de estos conjuntos se define por

$$\bigcup_{i=1}^{n} A_i = \{x \nmid x \in A_i \text{ para alguna } i = 1, 2, \ldots, n\}$$

y

$$\bigcap_{i=1}^{n} A_i = \{x \nmid x \in A_i \text{ para toda } i = 1, 2, \ldots, n\}.$$

De manera semejante, si Λ es un conjunto de índices y $\{A_\alpha \nmid \alpha \in \Lambda\}$ es una colección de conjuntos, la unión e intersección de estos conjuntos de define como

$$\bigcup_{\alpha \in \Lambda} A_\alpha = \{x \nmid x \in A_\alpha \text{ para alguna } \alpha \in \Lambda\}$$

y

$$\bigcap_{\alpha \in \Lambda} A_\alpha = \{x \nmid x \in A_\alpha \text{ para toda } \alpha \in \Lambda\}$$

Ejemplo 11 *Sea* $\Lambda = \{\alpha \in \mathbf{R} \nmid \alpha > 1\}$ *donde* $\mathbf{R}$ *es el conjunto de los números reales y sea*

$$A_\alpha = \left\{ x \in \mathbf{R} \nmid \frac{-1}{\alpha} \leq x \leq 1 + \alpha \right\}$$

para toda $\alpha \in \Lambda$ *. Entonces*

$$\bigcup_{\alpha \in \Lambda} A_\alpha = \{x \in \mathbf{R} \nmid x > -1\} \quad y \quad \bigcap_{\alpha \in \Lambda} A_\alpha = \{x \in \mathbf{R} \nmid 0 \leq x \leq 2\}$$

Proposición 2 *Sean* A, B, C, D *conjuntos, entonces*

1. $A \cup A = A$
2. $A \cap A = A$

3. $A \subset (A \cup B)$
4. Si $B \subset A \Rightarrow A \cup B = A$ y $A \cap B = B$ y $C \cap B \subset C \cap A$
5. Si $B \subset A$ y $D \subset C \Rightarrow (B \cup D) \subset (A \cup C)$
6. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

Demostración. 6.) Probaremos.primero que $[(A \cap B) \cup (A \cap C)] \subset [A \cap (B \cup C)]$ y después que $[A \cap (B \cup C)] \subset [(A \cap B) \cup (A \cap C)]$, lo cual probará la igualdad.

En virtud de 3) tenemos que $B \subset (B \cup C)$ entonces por la propiedad 4) tenemos que $(A \cap B) \subset A \cap (B \cup C)$. En forma similar $(A \cap C) \subset A \cap (B \cup C)$. Usando ahora la propiedad 5) tenemos que $(A \cap B) \cup (A \cap C) \subset [A \cap (B \cup C)] \cup [A \cap (B \cup C)]$ y por la propiedad 1) obtenemos que $(A \cap B) \cup (A \cap C) \subset A \cap (B \cup C)$, lo cual prueba la primera relación.

Ahora en la otra dirección: sea $x \in A \cap (B \cup C)$,entonces $x \in A$ y $x \in B \cup C$ y por lo tanto $x \in B$ o $x \in C$. Si $x \in B \Rightarrow x \in A \cap B$ y por lo tanto $x \in (A \cap B) \cup (A \cap C)$. Si $x \in C \Rightarrow x \in A \cap C$ y por lo tanto $x \in (A \cap B) \cup (A \cap C)$. Así pues, en cualquier caso $x \in (A \cap B) \cup (A \cap C)$ y por lo tanto $[A \cap (B \cup C)] \subset [(A \cap B) \cup (A \cap C)]$ con lo cual se demuestra la segunda relación. ■

Ejercicio 4 *Demuestre las propiedades 4 y 5.*

Definición 7 *Sean A, B conjuntos. Al conjunto de los pares ordenados (a, b) tal que $a \in A$ y $b \in B$ se le llama producto cartesiano de A con B y se le denota por $A \times B$, tal que $(a_1, b_1) = (a_2, b_2)$ si y solo si $a_1 = a_2$ y $b_1 = b_2$.*

Definición 8 *Sean A, B conjuntos, definimos una **Relación** R entre A y B como una regla de correspondencia entre los elementos $a \in A$ y $b \in B$, la cual denotamos $a \leftrightarrow b$. Una Relación en A se define de manera análoga tomando simplemente $B = A$.*

Ejemplo 12 *Sea IA el conjunto de los alumnos del grupo IA y IB el conjunto de los alumnos del grupo IB del IFUG. Sean $a \in IA$, $b \in IB$, la asociación (regla de correspondencia):$a \leftrightarrow b$ si y solo si el apellido de a y el de b comienzan con la misma letra, es una relación entre IA y IB.*

Ejemplo 13 *Sean $a_1, a_2 \in IA$, la correspondencia $a_1 \leftrightarrow a_2$ si y solo si a_1 y a_2 provienen de la misma escuela preparatoria, es una relación en IA.*

Definición 9 *Una Relación R en un conjunto A se llama relación de equivalencia en A si se cumplen las tres condiciones siguientes:*

1. Para toda $a \in A$, $a \leftrightarrow a$ (reflexividad).
2. si $a_1 \leftrightarrow a_2$, entonces $a_2 \leftrightarrow a_1$ (simetría).
3. si $a_1 \leftrightarrow a_2$ y $a_2 \leftrightarrow a_3$, entonces $a_1 \leftrightarrow a_3$ (transitividad).

Si R es una relación de equivalencia de un conjunto A, escribiremos $x \sim y$ en lugar de $x \leftrightarrow y$.

Nótese que en general una Relación satisface 1) y 2) pero no la propiedad 3) que es exclusiva de las Relaciones de Equivalencia. Por ejemplo, la relación de noviazgo es una Relación entre dos conjuntos, pero usualment no es transitiva!

Ejercicio 5 *Sean $x, y \in \mathbf{R}$, definimos la relación: $x \leftrightarrow y$ si y solo si $x - y$ es un entero . Probar que ésta es una relación de equivalencia en $\mathbf{R}$.*

1.4. Funciones

Definición 10 *Si A y B son conjuntos, entonces una **función** de A en B, que se escribe como $f : A \to B$, es una Relación que asocia a cada elemento a en A un elemento **único** llamado $f(a)$ en B.*

Definición 11 *El elemento $f(a)$ se llama **imagen** de a (bajo f) y a se llama **preimagen** de b (bajo f). Si $f : A \to B$ entonces A se llama **dominio** de f y el conjunto $\{f(a) \pitchfork a \in A\}$ de todas las imágenes de los elementos de A se llama **rango** de f. Nótese que el rango de f es un subconjunto de B. Si $S \subset A$, denotaremos por $f(S)$ al conjunto $\{f(a) \pitchfork a \in S\}$ de todas las imágenes de los elementos de S. De la misma forma, si $T \subset B$ denotaremos por $f^{-1}(T)$ al conjunto $\{a \pitchfork f(a) \in T\}$ de todas las preimágenes de los elementos de T. Finalmente, dos funciones $f : A \to B$ y $g : A \to B$ son iguales si $f(a) = g(a)$ para toda $a \in A$.*

Ejemplo 14 *Supóngase que* $A = [-10, 10] \equiv \{x \in \mathbf{R} \Cap -10 \leq x \leq 10\}$ *y* $B = \mathbf{R}$*, el conjunto de los números reales. Sea* $f : A \to B$ *la función que asigna a cada elemento* x *en* A *el elemento* $x^2 + 1$ *en* B*; esto es* f *está definida mediante* $f(x) = x^2 + 1$ *entonces* A *es el dominio de* f *y* $[1, 101]$ *es rango de* f*. Como* $f(2) = 5$ *la imagen de* 2 *es* 5 *y* 2 *es la preimagen de* 5*. Nótese que* -2 *es otra preimagen de* 5*. Más aún, si* $S = [1, 2]$ *y* $T = [82, 101]$ *entonces* $f(S) = [2, 5]$ *y* $f^{-1}(T) = [-10, -9] \cup [9, 10]$.

Ejercicio 6 *Establezca una función entre* IA *y* IB.

Tal como lo muestra el ejemplo anterior la preimagen de un elemento del rango no necesariamente es única (y por lo tanto la correspondencia f^{-1} no siempre es una función). Existen esencialmente tres tipos de funciones:

i) Sea $f : A \to B$. Si $\forall\ a_1, a_2 \in A$ con $a_1 \neq a_2$ se tiene que $f(a_1) \neq f(a_2)$ decimos que la funcion es *inyectiva (o uno a uno)*. En forma equivalente f es inyectiva si $f(a_1) = f(a_2)$ implica que $a_1 = a_2$.

ii) Sea $f : A \to B$. Si $\forall\ b \in B$ existe $a \in A$ tal que $f(a) = b$ decimos que la función es *sobreyectiva* (o simplemente "*sobre*").

iii) A una funcion que es a la vez inyectiva y sobreyectiva (uno a uno y sobre) se le denomina *biyectiva.*

Supóngase que $f : A \to B$ es una función y $S \subseteq A$, entonces puede formarse una función $f_S : S \to B$, que se denomina restricción de f a S, definiendo $f_S(x) = f(x)$ para cada $x \in S$.

El ejemplo siguiente ilustra estos conceptos.

Ejemplo 15 *Sea* $f : [-1, 1] \to [0, 1]$ *definida mediante* $f(x) = x^2$*. Esta función es sobreyectiva pero no uno-a-uno ya que* $f(-1) = f(1) = 1$*. Nótese que si* $S = [0, 1]$ *entonces* f_S *es sobreyectiva y uno-a-uno. Por último, si* $T = [\frac{1}{2}, 1]$*, entonces* f_T *es uno-a-uno pero no sobreyectiva.*

Definición 12 *Sean* A*,* B *y* C *conjuntos y* $f : A \to B$ *y* $g : B \to C$ *funciones. Aplicando* f *seguida de* g *obtenemos una función* $g \circ f : A \to C$ *llamada la función compuesta (o composición) de* g *y* f*. Entonces* $(g \circ f)(x) \equiv g(f(x))$ *para todo* $x \in A$.

Ejemplo 16 *Sean* $A = B = C = \mathbf{R}$ *(el conjunto de los números reales),* $f(x) = \sin(x)$ *y* $g(x) = x^2 + 3$*. Entonces* $(g \circ f)(x) = g(f(x)) = g(\sin(x)) = \sin^2(x) + 3$*, mientras que* $(f \circ g)(x) = f(g(x)) = f(x^2 + 3) = \sin(x^2 + 3)$.

Esto muestra que , en general, $(g \circ f)(x) \neq (f \circ g)(x)$. *Sin embargo, la composición de funciones es asociativa; esto es, si* $h : C \to D$, *entonces* $h \circ (g \circ f) = (h \circ g) \circ f$. *En efecto*

$$(h \circ (g \circ f))(x) = h((g \circ f)(x)) = h(g(f(x)))$$
$$((h \circ g) \circ f)(x) = (h \circ g)(f(x)) = h(g(f(x)))$$

Definición 13 *Se dice que una función* $f : A \to B$ *es* ***invertible*** *si existe una función* $g : B \to A$ *tal que* $(f \circ g)(y) = y$ *para todo* $y \in B$ *y* $(g \circ f)(x) = x$ *para todo* $x \in A$. *Si tal función g existe, entonces es única y se llama* inversa *de f. Escribiremos la inversa de f (cuando exista) como* f^{-1}.

Ejemplo 17 *Las funciones* $f : \mathbf{R} \to \mathbf{R}$ *y* $g : \mathbf{R} \to \mathbf{R}$ *definidas por*

$$f(x) = 2x^3 - 1 \quad y \quad g(y) = \sqrt[3]{\frac{y+1}{2}}$$

son mutuamente inversas:

$$\begin{aligned} f(g(y)) &= 2\left(\sqrt[3]{\frac{y+1}{2}}\right)^3 - 1 \\ &= 2\left(\frac{y+1}{2}\right) - 1 = y \end{aligned}$$

y

$$\begin{aligned} g(f(x)) &= \sqrt[3]{\frac{2x^3 - 1 + 1}{2}} \\ &= \sqrt[3]{x^3} = x \end{aligned}$$

Teorema 3 $f : A \to B$ *es invertible si y sólo si es biyectiva..*

Demostración. $\Rightarrow$)

Supongamos que $f : A \to B$ es invertible, es decir, existe $g : B \to A$ tal que

$$g(f(a)) = a \text{ y } f(g(b)) = b$$

para toda $b \in B$ y $a \in A$. Supongamos también que $f(a_1) = f(a_2)$. Entonces tenemos que

$$g(f(a_1)) = g(f(a_2))$$

lo cual implica que que $a_1 = a_2$, ya que $g(f(a_1)) = a_1$ y $g(f(a_2)) = a_2$. Esto prueba que si f es invertible entonces es uno-a-uno.

Puesto que $g : B \to A$ está definida para todo $a \in B$, a cada a le corresponde un único $a \in A$ y viceversa, a cada $a \in A$, le correspone un único $b \in B$, es decir, el rango de f es B. En otras palabras f es sobreyectiva.

$\Leftarrow$)

Sea $f : A \to B$ sobreyectiva y uno-a-uno, esto es

$$f(A) = B \quad \text{y} \quad f(a_1) \neq f(a_2) \text{ si } a_1 \neq a_2.$$

Nótese que a toda $b \in B$ le corresponde un único elemento de A y podemos definir una función $g : B \to A$ tal que

$$g(b) = a \text{ si } f(a) = b.$$

Para todo $a \in A$ y para todo $b \in B$, puesto que $g(b) = a$ si $f(a) = b$ entonces

$$g(f(a)) = a \text{ y } f(g(b)) = b,$$

y por lo tanto f es invertible. ■

Ejemplo 18 *La función $f : \mathbf{R} \to \mathbf{R}$ definida mediante $f(x) = 3x + 1$ es uno-a-uno y sobre; por lo tanto es invertible. La inversa de f es la función $f^{-1} : \mathbf{R} \to \mathbf{R}$ definida mediante $f^{-1}(x) = (x - 1)/3$.*

Las siguientes proposiciones acerca de las funciones invertibles pueden demostrarse fácilmente:

1. Si $f : A \to B$ es invertible, entonces f^{-1} es invertible y $(f^{-1})^{-1} = f$.
2. Si $f : A \to B$ y $g : B \to C$ son invertibles entonces $g \circ f$ también es invertible y $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

Para 1, por definición, intercambiando los papeles de g y f resulta que f es la inversa de g, pero $g = f^{-1}$, luego $(f^{-1})^{-1} = f$.

Para 2 basta con mostrar que $g \circ f$ es uno-a-uno y sobre. Como $f(A) = B$ y $g(B) = C$, entonces $(g \circ f)(A) = C$. Ademas $g \circ f = g(f(x))$, $g(y_1) \neq g(y_2)$ implica $y_1 \neq y_2$ si $y_1 = f(x_1)$ y $y_2 = f(x_2)$ esto demuestra que $x_1 \neq x_2$ por lo tanto, $g \circ f$ es sobre y uno-a-uno Para demostra que $f^{-1} \circ g^{-1}$ es la inversa de $g \circ f$ demostramos que $[g \circ f] \circ [f^{-1} \circ g^{-1}](y) = y$ esto se lee

$$g\left\{f\left[f^{-1}\left(g^{-1}(y)\right)\right]\right\} = g\left[g^{-1}(y)\right] = y.$$

de igual manera para $[f^{-1} \circ g^{-1}] \circ [g \circ f](x) = x$.

1.5. Conjuntos finitos, infinitos, enumerables.

La noción de biyección nos permite de çomparar"los conjuntos. Sea E y F dos conjuntos.

Definición 14 *Decimos que E es equipotente a F si existe una biyección B de E sobre F.*

Es obvio que E es equipotente a E, que E es equipotente a F si y solamente si F es equipotente a E visto que B es una biyección de E si y solamente si B^{-1} es una biyección de F sobre E y que si E es equipotente a F y si F es equipotente a G, entonces E es equipotente a G visto que la composición de dos biyecciones es una biyección. Asi la relación .^{es} equipotente a.^{es} entonces una relación de equivalencia.

Ejemplo 19 *Para cada $n \in \mathbb{N}$, definimos $J_n = \{1, 2, ..., n\}$ y para unificar las notaciones , definimos $J_0 = \emptyset$. Es facil de verificar que J_n es equipotente a J_m si y solamente si $n = m$.*

Definición 15 *El conjunto E es finito si existe $n \in \mathbb{N}$ tal que E sea equipotente a J_n. En el caso contrario, E es llamado conjunto infinito.*

Entonces, los elementos de un conjunto finito non vacio podrian a ser numerados por los enteros $1, 2, ..., n$ hasta un valor entero de n. El ejemplo anterior nos demostra que el entero n asi asociado al conjunto finito E es unico, y lo llamamos numero de elementos o cardinal de E y se nota $\#E$.

Proposición 4 *Si E es finito y si existe una biyección C de E sobre F, entonces, F es finito y $\#E = \#F$.*

Demostración. : Si $\#E = n$, existe una biyección B de E sobre J_n y entonces, $B \circ C^{-1}$ es una biyección de F sobre J_n. ■

Corollario 1 *Si E es infinito y si existe una biyección B de E sobre F, entonces F es infinito.*

Demostración. : Si F es finito, E lo es tambien por la proposición anterior y entonces hay contradicción con las hipotesis. ■

La definición de conjunto finito tiene como consecuencia que *un conjunto finito no puede ser equipotente a ninguna de sus partes propias* (esta propiedad de hecho puede ser usada como definición de un conjunto finito). La existencia de la biyección del conjunto de los numeros naturales sobre el conjunto $2\mathbb{N}$ de los enteros naturales pares, parte propia de $\mathbb{N}$, nos demostra que $\mathbb{N}$ es infinito.

$$B : \mathbb{N} \to 2\mathbb{N}, n \longmapsto 2n$$

Podemos ahora introducir una clase muy importante de conjuntos infinitos. Intuitivamente, son los conjuntos infinitos de los cuales los elementos pueden ser numerados por todos los enteros naturales.

Definición 16 *El conjunto E es enumerable si es equipotente a $\mathbb{N}$.*

Como $\mathbb{N}$ es infinito, un conjunto enumerable es obviamente infinito.

Ejemplo 20 *Asi los conjuntos $2\mathbb{N}$ y $\mathbb{N}^*$ son enumerables (tomar respectivamente las aplicaciones B definifas sobre $\mathbb{N}$ por $B(n) = 2n$ y $B(n) = n + 1$ para cada $n \in \mathbb{N}$.*

Ejemplo 21 *Tambien el conjunto $\mathbb{N} \times \mathbb{N}$ es enumerable, porque la aplicación*

$$B : \mathbb{N} \times \mathbb{N} \to \mathbb{N} : (m, n) \longmapsto \frac{(m+n)(m+n+1)}{2} + n$$

es biyectiva.

Ejemplo 22 *El producto cartesiano de dos conjuntos enumerable es enumerables.*

Asi, podemos ver que los conjuntos enumerables son los mas pequeños conjuntos infinitos que se puede considerar

Proposición 5 *Cualquier parte infinita de un conjunto enumerable es enumerable.*

Demostración. Sea E un conjunto enumerable y A una parte infinita de E. Existe una biyección $B : E \to \mathbb{N}$. Como A es infinito, el conjunto $B(A)$ es una parte infinita de $\mathbb{N}$. Sea n_0 lo mas pequeño elemento de $B(A)$, n_1 lo mas pequeño elemento de $B(A) \setminus \{n_0\}$, y de cerca en cerca, n_k lo mas pequeño elemento de $B(A) \setminus \{n_0, ..., n_{k-1}\}$. Como $B(A)$ es infinito, podemos definir asi una biyección C:$\mathbb{N} \to B(A), k \longmapsto n_k$ lo que nos da la biyección $C \circ B$ de A sobre $\mathbb{N}$ y eso nos demostra que A es enumerable. ■

Corollario 2 *Cualquier conjunto conteniendo una parte infinita no enumerable es infinita no enumerable.*

Definición 17 *Un conjunto E es a lo mas enumerable si es finito o enumerable.*

Podemos verificar facilmente que E es a lo mas enumerable si existe una sobreycción de $\mathbb{N}$ sobre E.

Es obvio que cualquier parte de un conjunto a lo mas enumerable es a lo mas enumerable. El siguiente resultado nos enseña que una unión enumerable de conjuntos a lo mas enumerables es todavia un conjunto a lo mas enumerable.

Proposición 6 *Sea $(E_n)_{n\in\mathbb{N}}$ una sucesión de conjuntos E_n tal que cada E_n sea a lo mas enumerable. Entonces, el conjunto $E = \cup_{n\in\mathbb{N}} E_n$ es a lo mas enumerable.*

Demostración. *Por hipotesis, para cada $n \in \mathbb{N}$, existe una sobreyección $B_n : \mathbb{N} \to E_n$. Resulta que la aplicación:*

$$B : \mathbb{N} \times \mathbb{N} \to E, (n, m) \to B_n(m)$$

es tambien sobreyectiva. Y como vimos antes que existe una biyección C:$\mathbb{N} \to \mathbb{N} \times \mathbb{N}$, obtenemos una sobreyección $B \circ C$ de $\mathbb{N}$ sobre E. ■

1.6. Estructuras algebraicas

1.6.1. Grupos

Definición 18 *Un grupo es un conjunto G con una ley de composición:*

$$\begin{aligned} * \ &: \ G \times G \to G \\ &: \ (x, y) \mapsto x * y \end{aligned}$$

sometida a las siguientes condiciones:

1. asociatividad: para cualquier $x, y, z \in G$:

$$(x * y) * z = x * (y * z)$$

2. existencia de un elemento neutral: existe $c \in G$ tal que para cualquier $x \in G$, tenemos

$$x * c = x = c * x$$

3. Inversibilidad: para cualquier $x \in G$, existe un elemento $x' \in G$ tal que

$$x * x' = c = x' * x$$

Si ademas, $x * y = y * x$ para cualquier $x, y \in G$, el grupo es llamado comutativo.

1.6.2. Anillos

Definición 19 *Un anillo es un conjunto E sobre lo cual definimos dos leyes de composición interna: una llamada ley de adición $(+)$ y la otra llamada ley de multiplicación $(\times)$ tal que $(E, +)$ tiene una estructura de grupo comutativo y que la ley $\times$ es asociativa y distributiva en relación a la ley de adición.*

Ejemplo 23 *el conjunto $\mathbb{Z}$ de los enteros positivos y negativos con la ley de adición y de multiplicación usuales tiene una estructura de anillo.*

1.6.3. Campos

El conjunto de los números reales es un ejemplo de una estructura algebraica llamada "**campo**". Básicamente, un campo es un conjunto en el cual se pueden definir cuatro operaciones (llamadas adición, multiplicación, substracción y división) tales que, con excepción de la división entre cero, la suma, el producto, la diferencia y el cociente de cualquier par de elementos del conjunto, es un elemento del conjunto. Más detalladamente, un campo se define de la siguiente manera.

Definición 20 *Un campo* $\mathbf{F}$ *es un conjunto en el cual se definen dos operaciones $+$ y $\cdot$ (llamadas respectivamente, adición y multiplicación) de modo que para cualquier par de elementos a y b en* $\mathbf{F}$*, existen elementos únicos $a + b$ y $a \cdot b$ en* $\mathbf{F}$ *tales que se cumplen las siguientes condiciones para todos los elementos a, b y c en F.*

(F 1) $a + b = b + a$ *y* $a \cdot b = b \cdot a$
(conmutatividad de la adición y multiplicación)

(F 2) $(a + b) + c = a + (b + c)$ *y* $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
(asociatividad de la adición y multiplicación)

(F 3) Existen elementos distintos 0 *y* 1 *en* $\mathbf{F}$ *tales que*

$$0 + a = a \quad y \quad 1 \cdot a = a$$

(existencia de elementos identidad para la adición y multiplicación)

(F 4) Para cada elemento a *en* $\mathbf{F}$ *y cada elemento* $b \neq 0$ *en* F *existen elementos* c *y* d *en* $\mathbf{F}$ *tales que*

$$a + c = 0 \quad y \quad b \cdot d = 1$$

(existencia de elementos inversos para la adición y multiplicación)

(F 5) $a \cdot (b + d) = a \cdot b + a \cdot c$
(distribuitidad de la multiplicación sobre la adición).

Los elementos $a+b$ y $a \cdot b$ se llaman, respectivamente suma y producto de a y b. Los elementos 0 (léase "cero") y 1 (léase "uno") mencionados en *(F 3)* se llaman elementos identidad para la adición y multiplicación, respectivamente, los elementos c y d dictados en *(F 4)* se denominan, respectivamente, inverso aditivo para a e inverso multiplicativo para b.

Otra definición equivalente a la definición anterior es la siguiente

Definición 21 *Un cuerpo (comutativo) o campo es un conjunto* K *con dos leyes de composición, una notada aditivamente y la otra multiplicativamente que satisfacen las siguientes condiciones:*

1. K es un grupo comutativo por la adición.

2. $K \setminus \{0\}$ es un grupo comutativo por la multiplicación.

3. para $x, y, z \in K$,

$$(x + y)z = xz + yz$$

Ejemplo 24 *El conjunto de los números reales con las definiciones ordinarias de adición y multiplicación es un campo que se denotará por* $\mathbf{R}$.

Ejemplo 25 *El conjunto de los números racionales con las definiciones ordinarias de adición y multiplicación es un campo.*

Ejemplo 26 *Otros ejemplos pueden ser construidos de la siguiente manera: si* K *es un cuerpo, el conjunto de las fraciones racionales en una indeterminada* X *a coeficientes en* K *es el conjunto de cocientes de polinomios:*

$$K(X) = \left\{ \frac{P(X)}{Q(X)} | P(X), Q(X) \in K[X], Q(X) \neq 0 \right\}$$

Este conjunto es un cuerpo para las operaciones usuales.

Ejemplo 27 *El conjunto de todos los números reales con* $a + b\sqrt{2}$ *donde* a *y* b *son números racionales, con la adicion y la multiplicación en* $\mathbf{R}$*, es un campo.*

Ejemplo 28 *El campo* Z_2 *consta de dos números* 0 *y* 1 *con las operaciones de adición y multiplicación de finidas por las ecuaciones*

$$0 + 0 = 0, \quad 0 + 1 = 1 + 0 = 1, \quad 1 + 1 = 0$$
$$0 \cdot 0 = 0, \quad 0 \cdot 1 = 1 \cdot 0 = 0, \quad 1 \cdot 1 = 1.$$

Ejemplo 29 *Ni el conjunto de los enteros positivos ni el conjunto de los enteros con las definiciones ordinarias de la adición y multiplicación es un campo, puesto que en ambos (F 4) no se satisface.*

Ejemplo 30 *El conjunto de los número complejos, denotado por* $\mathbb{C}$*, se define a través de pares ordenados de números reales* $z = (x, y)$ $x, y \in \mathbf{R}$*, es decir*

$$\mathbf{C} = \{z = (x, y) \Uparrow x, \ y \in \mathbf{R}\} \tag{1.3}$$

con las siguientes operaciones de suma y multiplicación, si $z_1 = (x_1, y_1)$ *y* $z_2 = (x_2, y_2)$ *son elementos de* $\mathbb{C}$*, entonces*

$$z_1 + z_2 = (x_1 + x_2, y_1 + y_2) \in \mathbf{C} \tag{1.4}$$
$$z_1 \cdot z_2 = (x_1 x_2 - y_1 y_2, x_1 y_2 + x_2 y_1) \in \mathbf{C}. \tag{1.5}$$

El conjunto de los números complejos bajo estas operaciones de suma y multiplicación forman un campo. En seguida se demostrará esta afirmación probando cada uno de los axiomas de campo. Sean $z_1 = (x_1, y_1)$*,* $z_2 = (x_2, y_2)$ *y* $z_3 = (x_3, y_3) \in \mathbf{C}$*. Entonces.*

(F 1) ***Conmutación de la suma y multiplicación***

$$z_1 + z_2 = (x_1 + x_2, y_1 + y_2) = (x_2 + x_1, y_2 + y_1) = z_2 + z_1 \tag{1.6}$$

y

$$z_1 \cdot z_2 = (x_1x_2 - y_1y_2, x_1y_2 + x_2y_1) = z_2 \cdot z_1 \tag{1.7}$$

por las leyes de conmutación de la suma y multiplicación de los numeros reales.

(F 2) ***Asociatividad de la suma y multiplicación de los números complejos.*** *Para la suma*

$$\begin{aligned}(z_1 + z_2) + z_3 &= (x_1 + x_2, y_1 + y_2) + (x_3, y_3) \qquad (1.8)\\ &= (x_1 + x_2 + x_3, y_1 + y_2 + y_3)\\ &= (x_1, y_1) + (x_2 + x_3, y_2 + y_3)\\ (z_1 + z_2) + z_3 &= z_1 + (z_2 + z_3) \qquad (1.9)\end{aligned}$$

y para la multiplicación

$$\begin{aligned}(z_1 \cdot z_2) \cdot z_3 &= (x_1x_2 - y_1y_2, x_1y_2 + x_2y_1) \cdot (x_3, y_3) \qquad (1.10)\\ &= \begin{pmatrix} (x_1x_2 - y_1y_2)\, x_3 - (x_1y_2 + x_2y_1)\, y_3, \\ (x_1x_2 - y_1y_2)\, y_3 + (x_1y_2 + x_2y_1)\, x_3 \end{pmatrix}\\ &= \begin{pmatrix} x_1\,(x_2x_3 - y_2y_3) - y_1\,(y_2x_3 + x_2y_3)\,, \\ y_1\,(x_2x_3 - y_2y_3) + x_1\,(x_2y_3 + y_2x_3) \end{pmatrix}\\ &= (x_1, y_1) \cdot (x_2x_3 - y_2y_3, y_2x_3 + x_2y_3)\\ (z_1 \cdot z_2) \cdot z_3 &= z_1 \cdot (z_2 \cdot z_3)\,, \qquad (1.11)\end{aligned}$$

por las propiedades de asociatividad de la adición y multiplicación de los números reales

(F 3) ***Existencia de las identidades aditiva y multiplicativa***
Sea $z = (x, y)$, existe un elemento de los número complejos denotado por 0, tal que $z + 0 = z$. Sea $0 = (a, b)$, demostraremos que $a = b = 0$.

$$z + 0 = (x, y) + (a, b) = (x + a, y + b) = (x, y) \tag{1.12}$$

de donde $x + a = x$ y $y + b = y$, entonces $a = b = 0$.

Los elementos de un campo cuya existencia queda garantizada por $(F3)$ y $(F4)$ son únicos; esto es del teorema siguiente.

Teorema 7 ***leyes de cancelación.*** *Sean a, b y c elementos cualesquiera de un campo F.*

(a) Si $a + b = c + b$, entonces $a = c$.

(b) Si $a \cdot b = c \cdot b$ y $b \neq 0$, entonces $a = c$.

Demostración. Las demostraciones de (a) y (b) son semejantes por lo que demostratará (b).

Si $b \neq 0$, entonces *(F 4)* garantiza la existencia de un elemento d en $\mathbf{F}$, talque $b \cdot d = 1$. Multipliquese ambos lados de la igualdad $a \cdot b = c \cdot b$ por d para obtener $(a \cdot b) \cdot d = (c \cdot b) \cdot d$. Considérese el lado izquierdo de la igualdad: en virtud de *(F 2)* y *(F 3)* tenemos

$$(a \cdot b) \cdot d = a \cdot (b \cdot d) = a \cdot 1 = a$$

De igual manera el lado derecho de igualdad se reduce a c. Entonces

$$a = (a \cdot b) \cdot d = (c \cdot b) \cdot d = c$$

■

Corollario 3 *Los elementos 0 y 1 mencionados en (F 3) y los elementos c y d mencionados en (F 4) son únicos*

Demostración. Supongase que $0' \in F$ satisface $0' + a = a$ para cada $a \in F$. Como $0 + a = a$ para $a \in F$, tenemos que $0' + a = 0 + a$ para cada $a \in F$. Por lo tanto, por el Teorema 7 $0' = 0$.

La demostración para la identidad para la multiplicación es similar.

Demostraremos a continuación que el inverso multiplicativo es único. Si $b \neq 0$, entonces existe d, tal que $b \cdot d = 1$, supongase que existe $d' \in F$, tal que $b \cdot d' = 1$. Por lo tanto $b \cdot d = b \cdot d'$. Por el teorema 7 tenemos que $d = d'$.

■

Así, cada elemento b en $\mathbf{F}$ tiene un inverso aditivo único y si $b \neq 0$, también un inverso multiplicativo único. (Se demostrará en el colorario del teorema 8 que 0 no tiene un inverso multiplicativo). El inverso aditivo y multiplicativo de b se escriben $-b$ y b^{-1} respectivamente. Nótese que $-(-b) = b$ y $(b^{-1})^{-1} =$

b. Sea $c = -b$, el inverso aditivo de b.Como $b + c = 0$ tenemos que b es el inverso aditivo de c, es decir, $-c = b$, pero $c = -b$, por lo tanto,$-(-b) = b$. Lo mismo se puede aplicar para $(b^{-1})^{-1} = b$.

La substración y la división se pueden definir en términos de la adición y multiplicación utilizando las inversos aditivo y multiplicativo. Especificamente, la substracción de b se define como la adición de $-b$, y la división entre $b \neq 0$ se define como la multiplicación por b^{-1}; esto es,

$$a - b = a + (-b) \quad \text{y} \quad a/b = a \cdot b^{-1}.$$

La división entre cero es indefinida, pero, con esta excepción, la suma, el producto, la diferencia y el cociente están definidos para cualquier par de elementos de un campo.

Muchas de las propiedades ordinarias de la multiplicación de los números reales son ciertas en cualquier campo, como lo demuestra el teorema siguiente.

Teorema 8 *Sean a y b elementos de cualesquiera de un campo. Entonces es cierto cada uno de los incisos siguientes.*

(a) $a \cdot 0 = 0$

(b) $(-a) \cdot b = a \cdot (-b) = -(a \cdot b)$

(c) $(-a) \cdot (-b) = a \cdot b$

Demostración.

(a) Como $0 + 0 = 0$ (F 5) muestra que

$$a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0$$

Luego, $0 + a \cdot 0 = a \cdot 0 + a \cdot 0$, y eliminado $a \cdot 0$ por el teorema C1, se tiene $0 = a \cdot 0$.

(b) Por definición $-(a \cdot b)$, es el único elemento de F tal que $a \cdot b + [-(a \cdot b)] = 0$. Entonces con objeto de demostrar que $(-a) \cdot b = -(a \cdot b)$ es suficiente con mostrar que $a \cdot b + (-a) \cdot b = 0$. Pero $-a$ es el único elemento de $\mathbf{F}$ tal que $a + (-a) = 0$, y entonces

$$a \cdot b + (-a) \cdot b = [a + (-a)] \cdot b = 0 \cdot b = 0$$

por *(F 5)* y el enciso (a). Así $(-a) \cdot b = -a \cdot b$. La demostración de que $a \cdot (-b) = -a \cdot b$ es similar.

(c) Aplicando dos veces el enciso (b), tenemos que

$$(-a) \cdot (-b) = -[a \cdot (-b)] = -[-(a \cdot b)] = a \cdot b.$$

■

Corollario 4 *La identidad aditiva de un campo no tiene inverso multiplicativo.*

Demostración. Del enciso (a) tenemos que $a \cdot 0 = 0$, para cualquier a de $\mathbf{F}$, luego no existe ningun c en $\mathbf{F}$ tal que $c \cdot 0 = 1$, por lo tanto 0 no tiene inverso multiplicativo. ■

En un campo cualquiera $\mathbf{F}$, puede suceder que una suma $1 + 1 + \ldots + 1$ (p sumandos) sea igual a cero para algún entero positivo p. Por ejemplo, el en campo Z_2 (definido en el ejemplo 4), $1 + 1 = 0$. En este caso el entero más pequeño posible p para el cual una suma de p $1's$ es igual a cero, se llama característica de $\mathbf{F}$; si no existe tal entero positivo, se dice que $\mathbf{F}$ tiene característica cero. Así pues, Z_2 tiene característica dos y $\mathbf{R}$ tiene característica cero.

Finalmente, el producto de dos elementos a y b de un campo también se expresa como ab en lugar de $a \cdot b$.

Capítulo 2