

definitionDefinición

APUNTES DEL CUARTO CURSO DE ÁLGEBRA

EDER A. TRUJILLO MONTAÑO
EDGAR D. MIGUEL MONJARAZ.
JAZIEL D. FLORES RODRÍGUEZ
PROFESOR: OCTAVIO FABIÁN LOYZAGA

May 21, 2020

Chapter 1

Primer Parcial

1.1 Paradoja de Russel.

Conceptos Primarios: Conceptos no definidos los cuales se asumen debido a su claridad.

Sea \mathcal{N} el conjunto de todos los conjuntos, entonces $\mathcal{N} \in \mathcal{N}$. Ahora, considere el conjunto \mathcal{A} de todos los conjuntos que no son elementos de sí mismos.

$$\mathcal{N} \notin \mathcal{A}$$

Así $\mathcal{A} \in \mathcal{A} \vee \mathcal{A} \notin \mathcal{A}$ es una tautología, y de hecho se cumple una única de las proposiciones.

Si $\mathcal{A} \in \mathcal{A}$ es verídica, entonces $\mathcal{A} \notin \mathcal{A}$. Se tendría así $\mathcal{A} \in \mathcal{A} \wedge \mathcal{A} \notin \mathcal{A}$. Por lo tanto $\mathcal{A} \in \mathcal{A}$ no es verídica.

Si $\mathcal{A} \notin \mathcal{A}$ es verídica, entonces $\mathcal{A} \in \mathcal{A}$, se tendría así $\mathcal{A} \notin \mathcal{A} \wedge \mathcal{A} \in \mathcal{A}$. Por lo tanto $\mathcal{A} \notin \mathcal{A}$ no es verídica. En ambos casos se ha obtenido una contradicción.

Proposición 0. No existe una biyección entre \mathbb{N} y \mathbb{R} .

Demostración.

Suponga que existe una función $f : \mathbb{N} \longrightarrow \mathbb{R}$, para cada $n \in \mathbb{N}$ sea $A_n.a_{n1}a_{n2}...$ la expresión decimal de la imagen de n bajo f . Así a_{nj} es el decimal j -ésimo de $f(n)$. Considere el número real z cuya expresión decimal es $0.z_1z_2...$ siendo $z_i \in \{1, 2\}$ y además

$$z_i = \begin{cases} 1 & \text{si } a_{ii} \neq 1. \\ 2 & \text{si } a_{ii} = 1 \end{cases}$$

Suponga que para algún $n \in \mathbb{N}$ $z = f(n)$, luego:

$$z_n = \begin{cases} 1 & \text{si } a_{nn} \neq 1. \\ 2 & \text{si } a_{nn} = 1 \end{cases}$$

Si $z_n = 1$, entonces $a_{nn} \neq 1$ y así la identidad $z = f(n)$ implica que a_{nj} . Sea $n \in \mathbb{N}$.

- i) Si $z_n = 1$, entonces $a_{nn} \neq 1$ existen dos posibilidades, para que $z = f(n)$ la primera es $a_{nn} = 0$ y la segunda $a_{nn} = 2$. La primera implica que $a_{nj} = 9 \forall j > n \wedge z_j \notin \{1, 2\} \forall j \in \mathbb{N}$. La segunda posibilidad i.e. $a_{nn} = 2$ implicaría que $a_{nj} = 0 \forall j > n \wedge z_j = 9 \forall j > n$ y esto último no es posible.
- ii) Si $z_n = 2$ entonces $a_{nn} = 1$ la identidad $z = f(n)$ implica $a_{nj} = 9 \forall j > n \wedge z_j = 0 \forall j > n$ lo cual contradice que $z_j = \{1, 2\} \forall j \in \mathbb{N}$.

1.2 Axiomas de Zermelo-Fraenkel

A principios de l siglo XX, fue el matemático alemán **Ernest Zermelo** quien puso la teoría de conjuntos sobre una base aceptable reduciendola a un sistema axiomático más restringido que no permita la obtención de la **Paradoja de Russel**. Las ideas de **Zermelo** fueron después precisadas por **Thoralf Skolen** y **Abrahm Fraenkel**, resultado de ello la primera teoría axiomática de conjuntos, conocida como **teoría de Zermelo-Fraenkel**, aunque sería más adecuado llamarla **teoría de Zermelo-Fraenkel-Skolen**.

Hasta ahora el alumno ha desarrollado una noción de *conjunto*, y se ha hablado y trabajado con conjuntos como \mathbb{N} , \mathbb{R} , \emptyset , *etc...* En éste curso se busca presentar una fundación rigurosa de las matemáticas conocidas en términos de la teoría axiomática de conjuntos. Los axiomas de Zermelo-Fraenkel conforman, junto con el Axioma de Elección, el modelo de facto para la teoría de conjuntos. En las notas, las letras se referirán a conjuntos a menos que se especifique. El orden de presentación de los axiomas es primeramente la noción de igualdad, luego axiomas de construcción de conjuntos, axiomas de existencia de ciertos conjuntos, y posteriormente en las notas, el axioma de elección.:

ZF 1. Axioma de Extensionalidad

Los conjuntos son iguales si tienen los mismos elementos.

$$\forall A, \forall B \quad A = B \iff (\forall x; \quad x \in A \iff x \in B)$$

ZF 2. Axioma del Vacío.

Existe un conjunto sin elementos.

$$\exists B \quad \forall x; \quad x \notin B$$

ZF 3. Axioma de Parejas.

Para cualquiera dos conjuntos, existe un tercer conjunto del cual son elementos.

$$\forall A, \forall B \quad \exists C \quad (\forall x; \quad x \in C \iff x = A \vee x = B)$$

ZF 4. Axioma de la unión.

Para cualquier conjunto, existe un conjunto cuyos elementos son todos los elementos de los miembros del conjunto.

$$\forall A, \forall B \quad (\forall x; \quad x \in B \iff \exists y \in A, x \in y)$$

ZF 5. Axioma del Conjunto Potencia.

Para cada conjunto existe otro cuyos elementos cumplen la propiedad necesaria y suficiente de que en sus elementos están elementos del ya dado.

$$\forall A \quad \exists B \quad [\forall y; \quad y \in B \iff (x \in y \iff x \in A)]$$

ZF 6. Esquema Axiomático de Especificación.

Dado un conjunto y una propiedad independiente de tal conjunto, existe otro cuyos elementos son tales que cumplen tal propiedad. Sea A un conjunto y $\mathcal{P}(x)$ una propiedad independiente de A .

$$\forall A \exists B \quad [\forall x; \quad x \in B \iff x \in A \wedge \mathcal{P}(x)]$$

El axioma anterior presenta una restricción importante, sólo se pueden construir conjuntos a partir de conjuntos cuya existencia es previamente conocida.

Proposición 1. Paradoja de Russell: No existe un conjunto al que pertenezca todo conjunto.

Demostración:

Sea \mathcal{A} un conjunto, para probar la proposición basta demostrar que existe un conjunto que no pertenezca a \mathcal{A} . Considere la propiedad siguiente:

$$\mathcal{P}(x) \quad | \quad x \notin x$$

En virtud de **ZF 6** implica que existe un conjunto \mathcal{B} tal que:

$$\forall x, \quad x \in \mathcal{B} \iff x \in \mathcal{A} \wedge x \notin x$$

Se verificará que $\mathcal{B} \notin \mathcal{A}$. En efecto, procediendo por *Reductio ad absurdum*, suponga que $\mathcal{B} \in \mathcal{A}$, se tiene que:

$$\mathcal{B} \in \mathcal{B} \vee \mathcal{B} \notin \mathcal{B}$$

Si $\mathcal{B} \in \mathcal{B} \implies \mathcal{B} \notin \mathcal{B}$.

Si $\mathcal{B} \notin \mathcal{B} \implies \mathcal{B} \in \mathcal{B}$.

En cualquier caso se tiene una contradicción. Por lo tanto $\mathcal{B} \notin \mathcal{A}$.

Quod erat demonstrandum.

Definiciones Iniciales.

Los axiomas anteriores justifican las siguientes definiciones en el sentido en que se asegura la existencia de los conjuntos que se definen.

I) Para cada par de conjuntos \mathcal{A}, \mathcal{B} se define el conjunto determinado por ellos, como el conjunto cuyos únicos elementos son \mathcal{A}, \mathcal{B} ta conjunto se denotará por $\{\mathcal{A}, \mathcal{B}\}$ y su existencia es asegurada por **ZF 3**.

II) El conjunto definido por **ZF 4**, se denotará por $\bigcup \mathcal{A}$ y se denominará la unión de elementos de \mathcal{A} , o bien se denotará por $\bigcup_{x \in \mathcal{A}} x$.

III) El conjunto definido por **ZF 4** se denomina **conjunto potencia** de \mathcal{A} , siendo \mathcal{A} un conjunto, y se denotará por $\mathcal{P}(\mathcal{A})$.

IV) Sean \mathcal{A}, \mathcal{B} conjuntos, sea $\mathcal{P}(x)$ la propiedad $x \in \mathcal{B}$. Por el **ZF 6** para el conjunto \mathcal{A} .

$$\exists \mathcal{D} \quad (\forall x; \quad x \in \mathcal{D} \iff x \in \mathcal{A} \wedge x \in \mathcal{B})$$

\mathcal{D} se denomina **intersección** de \mathcal{A} y \mathcal{B} y se denota por $\mathcal{A} \cap \mathcal{B}$.

V) Sean \mathcal{A}, \mathcal{B} conjuntos, sea $\mathcal{P}(x)$ la propiedad $x \notin \mathcal{B}$. Por **ZF 6**, para el conjunto \mathcal{A} .

$$\exists \mathcal{D} \quad (\forall x; \quad x \in \mathcal{A} \iff x \in \mathcal{A} \wedge x \notin \mathcal{B})$$

\mathcal{D} se denomina la diferencia de \mathcal{A} con \mathcal{B} , o el complemento de \mathcal{B} en \mathcal{A} , y se denota como $\mathcal{A} \setminus \mathcal{B}$.

VI) Sean \mathcal{A}, \mathcal{B} conjuntos, por el axioma de parejas existe un conjunto cuyos únicos elementos son \mathcal{A} y \mathcal{B} , sea C tal conjunto, i.e. $C = \{\mathcal{A}, \mathcal{B}\}$. Por **ZF 4** existe un conjunto \mathcal{D} tal que:

$$\exists \mathcal{D} \quad (\forall x; \quad x \in \mathcal{D} \iff \exists y \in C, x \in y)$$

Es decir tenemos que $\mathcal{D} = \bigcup_{x \in C} x$, \mathcal{D} se denomina la unión de \mathcal{A} y \mathcal{B} , y se denotará por $\mathcal{A} \cup \mathcal{B}$. El axioma **ZF 6** garantiza la unicidad de los conjuntos así definidos.

VII) Sea \mathcal{A} un conjunto distinto del vacío. Por el axioma **ZF 6** existe un conjunto \mathcal{B} , tal que

$$\exists \mathcal{B} \quad [\forall x; \quad x \in \mathcal{B} \iff (\forall y; \quad y \in \mathcal{A} \implies x \in y)]$$

\mathcal{B} se denomina la intersección de \mathcal{A} , se denotará por $\bigcap \mathcal{A}$ o bien $\bigcap_{x \in \mathcal{A}} x$.

VIII) El conjunto cuya existencia se justifica por **ZF 2**, es decir el conjunto sin elementos se denotará por \emptyset .

Proposición 2. Unicidad del Vacío: Hay un único conjunto que no tiene elementos.

Demostración. (La demostración es elemental)

Proposición 3. Sean $\mathcal{A}, \mathcal{B}, \mathcal{C}$ conjuntos. Entonces se cumplen las siguientes propiedades.

Leyes Distributivas.

$$\mathcal{A} \cap (\mathcal{B} \cup \mathcal{C}) = (\mathcal{A} \cap \mathcal{B}) \cup (\mathcal{A} \cap \mathcal{C}).$$

$$\mathcal{A} \cup (\mathcal{B} \cap \mathcal{C}) = (\mathcal{A} \cup \mathcal{B}) \cap (\mathcal{A} \cup \mathcal{C}).$$

Leyes de DeMorgan.

$$\mathcal{C} \setminus (\mathcal{A} \cup \mathcal{B}) = (\mathcal{C} \setminus \mathcal{A}) \cap (\mathcal{C} \setminus \mathcal{B}).$$

$$\mathcal{C} \setminus (\mathcal{A} \cap \mathcal{B}) = (\mathcal{C} \setminus \mathcal{A}) \cup (\mathcal{C} \setminus \mathcal{B}).$$

Leyes Asociativas.

$$\mathcal{A} \cup (\mathcal{B} \cup \mathcal{C}) = (\mathcal{A} \cup \mathcal{B}) \cup \mathcal{C}.$$

$$\mathcal{A} \cap (\mathcal{B} \cap \mathcal{C}) = (\mathcal{A} \cap \mathcal{B}) \cap \mathcal{C}.$$

Leyes de Idempotencia.

$$\mathcal{A} \cup \mathcal{A} = \mathcal{A}.$$

$$\mathcal{A} \cap \mathcal{A} = \mathcal{A}.$$

Demostración:

Se verificará que $\mathcal{A} \cap (\mathcal{B} \cup \mathcal{C}) = (\mathcal{A} \cap \mathcal{B}) \cup (\mathcal{A} \cap \mathcal{C})$. Para probar la identidad anterior, basta verificar en virtud del axioma de extensionalidad que los conjuntos $\mathcal{A} \cap (\mathcal{B} \cup \mathcal{C})$ y $(\mathcal{A} \cap \mathcal{B}) \cup (\mathcal{A} \cap \mathcal{C})$ tienen los mismos elementos.

Dado $x, x \in \mathcal{A} \cap (\mathcal{B} \cup \mathcal{C})$ es equivalente a cada una de las siguientes afirmaciones siguientes:

$$x \in \mathcal{A} \quad \wedge \quad x \in \mathcal{B} \cup \mathcal{C}$$

$$x \in \mathcal{A} \quad \wedge \quad [x \in \mathcal{B} \vee x \in \mathcal{C}]$$

$$[x \in \mathcal{A} \wedge x \in \mathcal{B}] \quad \vee \quad [x \in \mathcal{A} \wedge x \in \mathcal{C}]$$

$$x \in \mathcal{A} \cap \mathcal{B} \quad \vee \quad x \in \mathcal{A} \cap \mathcal{C}$$

$$x \in (\mathcal{A} \cap \mathcal{B}) \cup (\mathcal{A} \cap \mathcal{C})$$

Se verificará ahora $\mathcal{C} \setminus (\mathcal{A} \cup \mathcal{B}) = (\mathcal{C} \setminus \mathcal{A}) \cap (\mathcal{C} \setminus \mathcal{B})$. Dado $z, z \in \mathcal{C} \setminus (\mathcal{A} \cup \mathcal{B})$ es equivalente a cada una de las siguientes proposiciones:

$$z \in \mathcal{C} \quad \wedge \quad z \notin (\mathcal{A} \cup \mathcal{B}), \quad z \in \mathcal{C} \quad \wedge \quad \neg[z \in \mathcal{A} \cup \mathcal{B}]$$

$$z \in \mathcal{C} \quad \wedge \quad \neg[z \in \mathcal{A} \vee z \in \mathcal{B}], \quad z \in \mathcal{C} \quad \wedge \quad [z \notin \mathcal{A} \wedge z \notin \mathcal{B}]$$

$$z \in \mathcal{C} \quad \wedge \quad [z \notin \mathcal{A} \wedge z \notin \mathcal{B}], \quad [z \in \mathcal{C} \wedge z \notin \mathcal{A}] \quad \wedge \quad [z \in \mathcal{C} \wedge z \notin \mathcal{B}]$$

$$* (z \in \mathcal{C} \setminus \mathcal{A}) \quad \wedge \quad (z \in \mathcal{C} \setminus \mathcal{B}), \quad z \in (\mathcal{C} \setminus \mathcal{A}) \cap (\mathcal{C} \setminus \mathcal{B})$$

\therefore el axioma de extensionalidad permite concluir la identidad $\mathcal{C} \setminus (\mathcal{A} \cup \mathcal{B}) = (\mathcal{C} \setminus \mathcal{A}) \cap (\mathcal{C} \setminus \mathcal{B})$.

Las demás propiedades se demuestran de manera análoga.

Quod erat demonstrandum.

Definición: Sean \mathcal{A}, \mathcal{B} conjuntos se dice que \mathcal{A} es subconjunto de \mathcal{B} si $\forall x(x \in \mathcal{A} \implies x \in \mathcal{B})$.
Ello se denotará por $\mathcal{A} \subset \mathcal{B}$.

Proposición 4. Sean $\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D}$ conjuntos. Entonces se cumplen las siguientes propiedades.

$$I) \mathcal{A} \cap \mathcal{B} \subset \mathcal{A} \quad \wedge \quad \mathcal{A} \subset \mathcal{A} \cup \mathcal{B}$$

$$II) \text{ Si } \mathcal{A} \subset \mathcal{C} \quad \wedge \quad \mathcal{B} \subset \mathcal{D}, \quad \text{entonces } \mathcal{A} \cap \mathcal{B} \subset \mathcal{C} \cap \mathcal{D} \quad \wedge \quad \mathcal{A} \cup \mathcal{B} \subset \mathcal{C} \cup \mathcal{D}.$$

Demostración:

I) Sea $x \in \mathcal{A} \cap \mathcal{B}$, entonces $x \in \mathcal{A} \quad \wedge \quad x \in \mathcal{B}$. $\therefore \quad \forall x(x \in \mathcal{A} \cap \mathcal{B} \longrightarrow x \in \mathcal{A})$ i.e. $\mathcal{A} \cap \mathcal{B} \subset \mathcal{A}$. Sea $y \in \mathcal{A}$, entonces $y \in \mathcal{A} \quad \vee \quad y \in \mathcal{B}$, i.e. $y \in \mathcal{A} \cup \mathcal{B}$. $\therefore \quad \forall y(y \in \mathcal{A} \longrightarrow y \in \mathcal{A} \cup \mathcal{B})$ i.e. $\mathcal{A} \subset \mathcal{A} \cup \mathcal{B}$.

II) Sea $x \in \mathcal{A} \cup \mathcal{B}$, entonces $x \in \mathcal{A} \quad \vee \quad x \in \mathcal{B}$. Por hipótesis se tiene:

$$x \in \mathcal{A} \longrightarrow x \in \mathcal{C}, \quad x \in \mathcal{B} \longrightarrow x \in \mathcal{D}$$

Por el silogismo disyuntivo se concluye que $x \in \mathcal{C} \quad \vee \quad x \in \mathcal{D}$ i.e. $x \in \mathcal{C} \cup \mathcal{D}$. Se ha verificado que $\forall x[x \in (\mathcal{A} \cup \mathcal{B}) \longrightarrow x \in (\mathcal{C} \cup \mathcal{D})] \quad \mathcal{A} \cup \mathcal{B} \subset \mathcal{C} \cup \mathcal{D}$.

Sea $y \in \mathcal{A} \cap \mathcal{B}$, entonces $y \in \mathcal{A} \quad \wedge \quad y \in \mathcal{B} \quad \therefore \quad y \in \mathcal{C} \quad \wedge \quad y \in \mathcal{D}$, i.e. $y \in \mathcal{C} \cap \mathcal{D}$.
Quod erat demonstrandum.

Proposición 5. Sean \mathcal{A}, \mathcal{B} conjuntos. Son equivalentes las siguientes proposiciones:

$$\mathcal{A} \subset \mathcal{B}.$$

$$\mathcal{A} = \mathcal{A} \cap \mathcal{B}.$$

$$\mathcal{B} = \mathcal{A} \cup \mathcal{B}.$$

Demostración:

I) \implies II) Desde que $\mathcal{A} \cap \mathcal{A} = \mathcal{A}$ (Ley de Idempotencia). Por la **Proposición x-II)**, dado que $\mathcal{A} \subset \mathcal{A} \quad \wedge \quad \mathcal{A} \subset \mathcal{B}$. Se tiene que $\mathcal{A} \cap \mathcal{A} \subset \mathcal{A} \cap \mathcal{B}$ i.e. $\mathcal{A} \subset \mathcal{A} \cap \mathcal{B}$ y por la **Proposición x-I)**, $\mathcal{A} \cap \mathcal{B} \subset \mathcal{A}$. $\therefore \quad \forall x(x \in \mathcal{A} \iff x \in \mathcal{A} \cap \mathcal{B})$. El axioma de extensionalidad implica que $\mathcal{A} = \mathcal{A} \cap \mathcal{B}$.

II) \implies III) Por la **Proposición x-I)** $\mathcal{B} \subset \mathcal{A} \cup \mathcal{B}$. Por hipótesis $\mathcal{A} = \mathcal{A} \cap \mathcal{B}$.
 $\therefore \quad \mathcal{A} \cup \mathcal{B} = (\mathcal{A} \cap \mathcal{B}) \cup \mathcal{B} = (\mathcal{A} \cup \mathcal{B}) \cap (\mathcal{B} \cup \mathcal{B}) = (\mathcal{A} \cup \mathcal{B}) \cap \mathcal{B}$ (Ley Distributiva y de Idempotencia).

Además $(\mathcal{A} \cup \mathcal{B}) \cap \mathcal{B} \subset \mathcal{B}$ por la **Proposición X-I)** $\therefore \mathcal{A} \cup \mathcal{B} \subset \mathcal{B}$. Como $\mathcal{B} \subset \mathcal{A} \cup \mathcal{B} \quad \wedge \quad \mathcal{A} \cup \mathcal{B} \subset \mathcal{B} \quad \forall x(x \in \mathcal{B} \iff x \in \mathcal{A} \cup \mathcal{B})$. Por el axioma de extensionalidad, se concluye que $\mathcal{B} = \mathcal{A} \cup \mathcal{B}$.

III) \implies I) Por hipótesis $\mathcal{B} = \mathcal{A} \cup \mathcal{B}$, $\mathcal{A} \subset \mathcal{A} \cup \mathcal{B}$ **Proposición X-I)** $\therefore \mathcal{A} \subset \mathcal{B}$.
Quod erat demonstrandum.

Ejercicios 1: Sean \mathcal{A}, \mathcal{B} subconjuntos de \mathcal{D} . Demuestre:

I) $\mathcal{A} \cap (\mathcal{D} \setminus \mathcal{A}) = \emptyset$

II) $\mathcal{D} \setminus (\mathcal{D} \setminus \mathcal{A}) = \mathcal{A}$

III) $\mathcal{A} \subset \mathcal{B}$, si y sólo si, $(\mathcal{D} \setminus \mathcal{B}) \subset (\mathcal{D} \setminus \mathcal{A})$

Sean \mathbf{a}, \mathbf{b} conjuntos, elementos de un conjunto \mathcal{A} , se define la pareja ordenada determinada por \mathbf{a}, \mathbf{b} y denotada por (\mathbf{a}, \mathbf{b}) como el conjunto $\{\{\mathbf{a}, \{\mathbf{a}, \mathbf{b}\}\}$.

Observe que $\{\mathbf{a}\}$ es un conjunto por el axioma de especificación, ya que por tal axioma existe un conjunto \mathcal{B} tal que:

$$\forall \mathbf{x} \quad [\mathbf{x} \in \mathcal{B} \iff \mathbf{x} \in \mathcal{A} \wedge \mathcal{P}(\mathbf{x})]$$

Siendo $\mathcal{P}(\mathbf{x})$ la propiedad $\mathbf{x} = \mathbf{a}$. Por otra parte $\{\mathbf{a}, \mathbf{b}\}$ es un conjunto en virtud del axioma de parejas. Este mismo axioma justifica que $\{\{\mathbf{a}, \{\mathbf{a}, \mathbf{b}\}\}$ es un conjunto.

Proposición 6. Sea (N, R) un conjunto parcialmente ordenado tal que toda cadena contenida en N tiene un supremo en N . Sea $f : N \rightarrow N$ una función tal que $\forall x \in N \quad x < f(x)$. Entonces, existe algún $n \in N \quad f(n) = n$.

Definición 1.2.1. Dado $u \in N$ se dice que $A \subset N$ es **admisibile** con relación a u si se cumple:

- $u \in A$.
- $f(A) \subset A$.
- Si B es una cadena contenida en A , entonces en A mismo existe el supremo de B .

Proof. Dado $u \in N$, sea M el conjunto de todos los conjuntos admisibles de u en relación a N .

Definamos: $S = \bigcap_{x \in M} x$. Veamos que:

- $u \in S$ ya que $u \in S$
- Sea $t \in S, t \in x, \therefore f(t) \in x \forall x \in M$, lo cual muestra que $f(S) \subset S$.
- Sea B una cadena contenida en S . $B \subset x \forall x \in N \therefore \sup B \in S$.

Así S es admisible con respecto a u . Observe que si $S' \subset S \wedge S'$ es u -admisibile, entonces $S' = S$.

Hecho 1 u es el primer elemento de S , es decir, $u < x \forall x \in S$. Sea $A = \{x \in S \mid u < x\}$. Se demostrará que $A = S$. Como $A \subset S$, bastará probar que A es u admisible.

- Como R es en particular reflexiva: $u < u$. Además $u \in S$. Así $u \in A$.
- Sea $x \in A$, veamos que $f(x) \in A$ ya que $u < x$, por transitividad $u < f(x)$. Así $x \in S$ y al ser u -admisibile, $f(x) \in A$. Así $f(A) \subset A$.
- Sea B una cadena contenida en A ,

□

1.3 Problemas

Definición 1.3.1. Sean R_1, R_2 relaciones en A , se define la relación **composición** $R_1 \circ R_2$

$$R_1 \circ R_2 = \{ (a, b) \in A \times A \mid (a, c) \in R_1 \wedge (c, b) \in R_2, c \in A \}$$

Definición 1.3.2. Sea R una relación binaria en A , se define la relación **inversa** R^{-1} como sigue:

$$(a, b) \in R^{-1} \Leftrightarrow (b, a) \in R$$

Problema 1.3.1. Sean R, S y T relaciones binarias en A , demuestre que $(R \circ S) \circ T = R \circ (S \circ T)$. Muestre que si R y S son relaciones de equivalencia, $R \circ S$ no es necesariamente una relación de equivalencia.

Solución:

Considere $(a, b) \in (R \circ S) \circ T$ arbitrario. Existe entonces $c \in A$ tal que $(a, c) \in (R \circ S)$, $(c, b) \in T$. Existe entonces $d \in A$ tal que $(a, d) \in R$, $(d, c) \in S$. Así $(d, b) \in (S \circ T)$, y como $(a, d) \in R$, $(a, b) \in R \circ (S \circ T)$. $(R \circ S) \circ T \subset R \circ (S \circ T)$; la segunda contención se demuestra análogamente. \square Considere $A = \{\clubsuit, \spadesuit, \diamondsuit\}$, $R = \{(\clubsuit, \clubsuit), (\spadesuit, \spadesuit), (\diamondsuit, \diamondsuit), (\clubsuit, \spadesuit), (\spadesuit, \clubsuit)\}$ y $S = \{(\clubsuit, \clubsuit), (\spadesuit, \spadesuit), (\diamondsuit, \diamondsuit), (\diamondsuit, \clubsuit), (\clubsuit, \diamondsuit)\}$. Veamos que $(\spadesuit, \diamondsuit) \in R \circ S$ pero $(\diamondsuit, \spadesuit) \notin R \circ S$. Lo cual asegura que $R \circ S$ no es de equivalencia. \blacksquare

Problema 1.3.2. Sea R una relación binaria en A , R es de equivalencia si y solo si $R = R \circ R \wedge R = R^{-1}$.

Solución:

\Rightarrow

Se probará que $R = R \circ R$ y $R = R^{-1}$.

Suponga que R es una relación de equivalencia, y suponga que $x = (a, b) \in R$, veamos que $(b, b) \in R$ al ser R reflexiva, entonces $(a, b) \in R \circ R$ entonces $R \subset R \circ R$, como R es simétrica $(b, a) \in R$, así $(a, b) \in R^{-1} \therefore R \subset R^{-1}$. Ahora suponga que $x = (a, b) \in R \circ R$, entonces $\exists c \in A$ $(a, c) \in R \wedge (c, b) \in R$, pero al ser R transitiva $(a, b) \in R \therefore R \circ R \subset R$. Finalmente suponga que $x = (a, b) \in R^{-1}$, entonces $(b, a) \in R$, pero como R es simétrica, $(a, b) \in R$ así $R^{-1} \subset R$, y $R = R \circ R \wedge R = R^{-1}$.

\Leftarrow

Suponga ahora que $R = R \circ R$ y $R = R^{-1}$. Se probará que R es de equivalencia.

Suponga que $(a, b) \in R$, arbitrario; como $R = R^{-1}$, $(b, a) \in R$ por lo tanto es simétrica. Veamos que al ser $R = R \circ R$ $(a, a) \in R \wedge (b, b) \in R$, y por ser (a, b) arbitrario, R es reflexiva. Finalmente suponga que $(a, b) \in R \wedge (b, c) \in R$, entonces $(a, c) \in R \circ R$, $(a, c) \in R$, así R es transitiva, por lo tanto, de equivalencia. \blacksquare

Problema 1.3.3. Sea R una relación binaria reflexiva y transitiva en A . Demuestre que $S = R \cap R^{-1}$ es de equivalencia.

Solución:

Considere $a \in A$ arbitrario, como R es reflexiva, $(a, a) \in R$, $(a, a) \in R^{-1} \therefore (a, a) \in S$. Suponga que $(a, b) \in S$, entonces $(a, b) \in R$, $(a, b) \in R^{-1}$, así $(b, a) \in R^{-1} \wedge (b, a) \in R \therefore (b, a) \in S$.

Finalmente suponga que $(a, b) \in S$, $(b, c) \in S$ como R es transitiva, $(a, c) \in R$, como S es simétrica $(c, b), (b, a) \in R$ así, $(c, a) \in R$ por lo tanto $(a, c) \in R^{-1}$, $(a, c) \in S$. Así, S es una relación de equivalencia. ■

Problema 1.3.4. Sean R y S relaciones en A y B respectivamente. Se define la relación $R \times S$ como el conjunto $\{((a, b), (c, d)) \in (A \times B) \times (A \times B) \mid (a, c) \in R, (b, d) \in S\}$. Si R y S son de equivalencia, demuestre que $R \times S$ es de equivalencia.

Solución:

Considere (a, b) arbitrario en $A \times B$, como R, S , son de equivalencia $(a, a) \in R$, $(b, b) \in S$; así $((a, b), (a, b)) \in R \times S$, $R \times S$ es reflexiva. Considere ahora a $((a, c), (b, d)) \in R \times S$ arbitrario. Por la definición $(a, b) \in R \wedge (c, d) \in S$; así $(b, a) \in R$, $(d, c) \in S$, de forma que $((b, d), (a, c)) \in R \times S$, $R \times S$ es simétrica. Finalmente considere $((a, c), (b, d)), ((b, d), (f, e)) \in R \times S$. Las relaciones $(a, b), (b, f) \in R$, así $(a, f) \in R$; y $(c, d), (d, e) \in S$ con $(c, e) \in S$. Ésto último nos asegura que $((a, c), (f, e)) \in R \times S$, es decir, $R \times S$ es transitiva; lo que demuestra que es de equivalencia. ■

Problema 1.3.5. Sea A un conjunto, se define la diagonal de A , $\Delta A = \{(a, a) \in A \times A \mid a \in A\}$. Sea R una relación binaria, demuestre que R es un preorden si y solo si $\Delta A \subset R \wedge R = R \circ R$.

Solución:

\Rightarrow

Suponga que R es un preorden, como R es reflexivo $(a, a) \in R \forall a \in A$ así $\Delta A \subset R$. Considere $(a, b) \in R$, como R es reflexivo, $(b, b) \in R$, por lo tanto $(a, b) \in R \circ R$.

Ahora considere $(a, b) \in R \circ R$, entonces existe $c \in A$ tal que $(a, c) \in R \wedge (c, b) \in R$; pero al ser R transitiva $(a, b) \in R$, así $R = R \circ R$.

\Leftarrow

Suponga ahora que $\Delta A \subset R \wedge R = R \circ R$. Trivialmente R es reflexiva ya que $(a, a) \in \Delta A \forall a \in A$. Considere ahora $(a, b), (b, c) \in R$ por la definición $(a, c) \in R \circ R = R \therefore R$ es transitiva. ■

Observación. El siguiente problema no tiene mucho caso según como se planteó en la lista, la idea interesante del problema sucede cuando se retira al 1, y así lo voy a resolver.

Problema 1.3.6. Defínase R en $A = \mathbb{Z}^+ \setminus \{1\}$ como $\{(n, m) \in R \mid m|n\}$. Muestre que R es un orden parcial, que toda cadena tiene cota superior y determine el conjunto de elementos maximales.

Solución:

Sea $n \in A$, trivialmente $n|n$, así $(n, n) \in R$. Considere ahora $(m, n), (n, p) \in R$, entonces $m = na$, $n = pb \Rightarrow m = pab$, $p|m$, así $(m, p) \in R$. Finalmente suponga que $(m, n) \in R \wedge (n, m) \in R$, entonces $m|n \wedge n|m$; lo cual implica $n \geq m \wedge n \leq m$. así $n = m$. Lo cual prueba que R es un orden parcial. Sea B una cadena no vacía de A , veamos que $B \subset \mathbb{N}$, así B tiene un primer elemento u respecto al orden de los naturales. Suponga que existe $v \in B$ tal que $(u, v) \in R$, entonces $v|u$ y $v \leq u$, como u era un primer elemento $v = u$. Así, en particular, u es cota superior de B . Como B fue arbitrario, cualquier cadena está acotada superiormente. Ahora veamos que el conjunto de elementos maximales de A es el conjunto $P = \{p \mid p \text{ es primo}\}$. Sea $p \in P$, entonces si $(p, b) \in A$,

$b|p$; por la definición de primo, $b = p \vee b = 1$. Como $b \in A$, $b = p$, lo cual prueba que p es un elemento maximal de A . Se puede proceder de la definición de primo, recíprocamente, para demostrar que si un elemento es maximal, entonces es primo. ■

Problema 1.3.7. Suponga que R es un buen orden en A , demuestre que si A no es finito R^{-1} no es un buen orden.

Solución:

Suponga que A no es finito, entonces para cualquier conjunto finito B_i no vacío, existe un conjunto finito B_{i+1} que lo contiene propiamente $\forall i \in \mathbb{N}$. A es no vacío, así podemos tomar un x_0 cualquiera y tomar a $B_0 = \{x_0\}$, y a cada $B_{i+1} = B_i \cup \{x_i\}$ $x_i \notin B_i$. Veamos que cada B_i es una cadena en A , y consideremos a $C = \bigcup_{x \in B_i} x$ $i \in \mathbb{N}$. Como C es una cadena, podemos ordenarlos en una sucesión $\{x_k\}$ tal que $(x_k, x_{k+1}) \in R \wedge x_k \neq x_{k+1} \forall k \in \mathbb{N}$. Veamos que $(x_{k+1}, x_k) \in R^{-1} \forall k \in \mathbb{N}$. Así por el problema 1.3.10, R^{-1} no puede ser un buen orden. ■

Problema 1.3.8. Considere a A el conjunto de las sucesiones en \mathbb{R} , definimos el orden lexicográfico como $R = \{(\{x_k\}, \{y_k\}) \mid x_k = y_k \forall k \vee x_n < y_n \text{ si } x_i = y_i \forall i < n\}$. Demuestre que R es un orden total en A .

Solución:

Considere $\{x_k\}$ arbitrario en A . $(\{x_k\}, \{x_k\}) \in R$. Así, R es reflexiva. Considere ahora $(\{x_k\}, \{y_k\}) \in R$, $(\{y_k\}, \{z_k\}) \in R$. Podemos considerar entonces los casos siguientes:

- $x_k = y_k \forall k \wedge y_k = z_k \forall k$
Trivialmente $\{x_k\} = \{z_k\}$.
- $x_k = y_k \forall k \wedge y_i = z_i \forall i < n$ si $x_n < y_n$
Como $\{x_k\} = \{y_k\}$. $x_i < z_i \forall i < n$ si $x_n < z_n$.
- $x_i = y_i \forall i < n$ si $x_n < y_n \wedge y_k = z_k \forall k$.
Como $\{y_k\} = \{z_k\}$, se tiene $x_i = z_i \forall i < n$ si $x_n < z_n$.
- $x_k = y_k \forall k < n$ si $x_n < y_n \wedge y_i = z_i \forall i < n$ si $y_n < z_n$
Como el orden en \mathbb{R} es ya un orden total, por transitividad. $x_k = z_k \forall k < n$ si $x_n < z_n$.

En cualquiera de los casos concluimos que $(\{x_k\}, \{z_k\}) \in R$. Así R es transitiva. Suponga ahora que $(\{x_k\}, \{y_k\}) \in R$ y que $(\{y_k\}, \{x_k\}) \in R$. En el primer caso de la disyunción $\{x_k\} = \{y_k\}$, no hay nada que hacer. En el segundo caso, $x_k = y_k \forall k < n$ si $x_n < y_n$, $y_k = x_k \forall k < n$ si $y_n < x_n$. En tal caso no existe n tal $x_n \neq y_n$, entonces $x_n = y_n \forall n$. Así R es un orden parcial. Demostremos ahora que es una cadena.

Sean $x = \{x_k\}$, $y = \{y_k\}$ sucesiones arbitrarias, en el caso que sean iguales, trivialmente $(x, y) \in R$. Si son distintas, existe un primer k_0 (dado que cualquier subconjunto de los naturales tiene un primer elemento) tal que $x_{k_0} \neq y_{k_0} \wedge x_i = y_i \forall i < k_0$. En dado caso $(x, y) \in R$ ó $(y, x) \in R$. ■

Problema 1.3.9. Sea A un conjunto finito, demuestre que todo orden total es un buen orden.

Solución:

Sea R un orden total en A , y B una cadena arbitraria no vacía. Al ser A finito, B es finito, se demostrará que B tiene primer elemento. Suponga que B tiene n elementos y que no tiene un primero, es decir, para cualquier $a \in B$ $\exists b, c \neq a \in B$, $a < b \wedge c < a$. Considere un $c_0 \in B$ arbitrario, se puede entonces construir una secuencia $\{c_0, c_1, \dots, c_n\}$ de forma inductiva ya que B es no vacío y B no tiene un primer elemento, con la condición de que cada $c_i < c_{i-1}$, $c_i \neq c_{i-1}$ $i = \{0, 1, \dots, n\}$. Como observación ésta secuencia es un subconjunto de B . Veamos que por transitividad cada $c_i < c_j$ si $j > i$. De igual forma, todos son distintos, pero esto contradiría que B tiene n elementos ya que la secuencia tiene $n + 1$. Así B tiene primer elemento. Como fue arbitrario R es un buen orden. ■

Problema 1.3.10. Sea (A, R) un conjunto bien ordenado. Demuestre que no existe una sucesión $\{x_n\}$ tal que $x_{n+1} < x_n \wedge x_{n+1} \neq x_n \quad \forall n \in \mathbb{N}$

Solución:

Procediendo por contradicción, suponga que dicha sucesión $\{x_k\}$ existe. Por la forma en que está definida, el conjunto $B = \{x_k \mid \forall k \in \mathbb{N}\}$ es una cadena en A . Así B tiene un primer elemento. Existe entonces $i_0 \in \mathbb{N}$ tal que $x_k < x_{i_0} \forall k \in \mathbb{N}$, se llega aquí a una contradicción ya que $x_{i_0+1} < x_{i_0} \wedge x_{i_0+1} \neq x_{i_0}$. Así R no sería un buen orden, por lo tanto dicha sucesión no puede existir. ■

Chapter 2

Segundo Parcial

2.1 Los Números Naturales

Definición 2.1.1. Definimos la función sucesor de un conjunto x como $x^+ = x \cup \{x\}$.

Se denota al conjunto \emptyset como 0, y al conjunto \emptyset^+ como 1.

ZF 7. de Infinitud

$$\exists A \quad x \in A \Leftrightarrow \emptyset \in x \wedge x \in x^+$$

Definición 2.1.2. Se dice que un conjunto X es un conjunto sucesor si

- a. $\emptyset \in X$
- b. $\forall x (x \in X \Rightarrow x^+ \in X)$

Así el axioma del infinito postula la existencia de un conjunto sucesor.

Sea A un conjunto sucesor. Note que la existencia de A está garantizada por el axioma del infinito.

Sea $B = \{x \in \mathcal{P}(A) \mid \emptyset \in x \wedge [\forall z (z \in x \Rightarrow z^+ \in x)]\}$.

Por el axioma de especificación el conjunto B es un conjunto. Se definirá el conjunto \mathbb{N} de los números naturales como $\bigcap B$.

Proposición 7. La definición de \mathbb{N} es independiente de la elección de A .

Proof. Observe que

- a. $\emptyset \in x \quad \forall x \in B. \therefore \emptyset \in \mathbb{N}$.
- b. Si $x \in \mathbb{N}$, entonces $x \in z \quad \forall z \in B$.

Como todo elemento de B es un conjunto sucesor, se tiene que $x^+ \in z \quad \forall z \in B \quad \therefore x \in \mathbb{N}$. Así \mathbb{N} es un conjunto sucesor.

Sea H un conjunto sucesor. Veamos que $A \cap H$ es un conjunto sucesor. Además:

$$\begin{aligned} A \cap H &\in \mathcal{P}(A) \\ \therefore A \cap H &\in B \end{aligned}$$

Lo anterior implica que $\mathbb{N} \subset A \cap H \subset H$. Así $\mathbb{N} \subset X \quad \forall X, X$ conjunto sucesor. □

Se tiene:

- a. $0 \in \mathbb{N}$
- b. $\forall x \quad (x \in \mathbb{N} \rightarrow x^+ \in \mathbb{N})$
- c. Si $S \subset \mathbb{N}$ que satisface:
 - (a) $0 \in S$
 - (b) $\forall x \quad (x \in S \rightarrow x^+ \in S)$
- d. $\forall x \quad (x \in \mathbb{N} \rightarrow x^+ \neq 0)$ ya que $x \in x^+$
- e. $\forall x \forall y \quad [(x \in \mathbb{N} \wedge y \in \mathbb{N} \wedge x^+ = y^+) \Rightarrow x = y]$

La última afirmación se verificará a partir de la siguiente definición y los siguientes dos lemas:

Definición 2.1.3. Un conjunto A se dice **transitivo** sí $\forall x \forall y [(x \in A \wedge y \in x) \Rightarrow y \in A]$.

Observación. Son equivalentes las siguientes afirmaciones:

- a. A es un conjunto transitivo.
- b. $\forall x (x \in A \Rightarrow x \subset A)$.
- c. $\bigcup A \subset A$.
- d. $A \subset \mathcal{P}(A)$.

Proof. $i \rightarrow ii$

Si $x \in A \wedge y \in x$, al ser A transitivo, $y \in A \therefore x \subset A$. $ii \rightarrow iii$

$iii \rightarrow iv$

$iv \rightarrow i$

□

Definición 2.1.4. Por número natural se entiende cualquier $x, x \in \mathbb{N}$.

Lema 2.1.1. Todo elemento de \mathbb{N} es un conjunto transitivo.

Proof. Sea

$$S = \{n \in \mathbb{N} \mid \forall x (x \in n \Rightarrow x \subset n)\}$$

Observe que:

- a. $0 \in S$ ya que $0 \in \mathbb{N}$ y $\forall x (x \in \emptyset \Rightarrow x \subset \emptyset)$
- b. Suponga que $n \in S$, entonces $n \in \mathbb{N}$. Además $n^+ \in \mathbb{N}$. Sea $x \in n^+$ entonces $x \in n \vee x = n$.
- Si $x \in n$ entonces, dado que $n \in S$, $x \subset n$. Además, $n \subset n^+$, por lo cual $x \subset n^+$.
 - Si $x = n$, entonces $x \subset n^+$

Así $S = \mathbb{N}$ que era lo que se quería demostrar.

□

Lema 2.1.2. Ningún número natural es subconjunto de alguno de sus elementos.

$$\forall n [(n \in \mathbb{N} \wedge x \in n) \Rightarrow n \setminus x \neq \emptyset]$$

Proof. Sea $S = \{n \in \mathbb{N} \mid \forall x (x \in n \Rightarrow n \setminus x \neq \emptyset)\}$

- a. $0 \in S$ ya que $\emptyset \in \mathbb{N} \wedge \forall x (x \in \emptyset \Rightarrow \emptyset \setminus x \neq \emptyset)$
- b. Suponga que $n \in S$, entonces, en particular $n \in \mathbb{N} \therefore n^+ \in \mathbb{N}$. Se verificará que $n^+ \in S$.
Sea $x \in n^+$, entonces $x \in n \vee x = n$.
- Suponga que $x \in n$. Entonces dado que $n \in S$, $n \setminus x \neq \emptyset$. En consecuencia $n^+ \setminus x \neq \emptyset$ ya que si $n^+ \setminus x = \emptyset$ todo elemento de n^+ pertenecería a x , en particular, como $n \subset n^+$ todo elemento de n pertenecería a x lo cual contradice que $n \setminus x \neq \emptyset$.
 - Suponga ahora que $x = n$. Así, procediendo por reducción al absurdo, considere $n^+ \subset n$. Como $n \in S \wedge n \setminus n = \emptyset$ se tiene $n \notin n$. Como $n \in n^+$, se tiene $\neg(n^+ \subset n)$, así como $n^+ \subset n$, se tiene una contradicción $\therefore n^+ \setminus x \neq \emptyset$.

Así $S = \mathbb{N}$

□

Los lemas anteriores permiten justificar la propiedad *e*.

Proof. Sean x, y números naturales tales que $x^+ = y^+$. Así por ser elementos de \mathbb{N} se tienen dos posibilidades $x = y$ ó $x \in y \wedge y \in x$ lo cual implica del lema ?? que $x = y$. □

Las propiedades 1, 2, 3, 4, y 5 fueron postuladas en 1889 por Peano como un conjunto de axiomas, y la existencia de un conjunto con dichas propiedades. Consigo se construyeron los conjuntos $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ y sus propiedades analíticas y aritméticas. Peano reconoce que sus axiomas fueron postulados un año antes por Richard Dedekind.

Considere la función: $S : \mathbb{N} \rightarrow \mathbb{N}$. $S(n) = n^+$.

- S es inyectiva, ya que si $S(n) = S(m)$, de la propiedad 5 se sigue que $n = m$.

- S no es suprayectiva, ya que la propiedad 4 indica $0 \notin S(\mathbb{N})$. De hecho $S(\mathbb{N}) = \mathbb{N} \setminus \{0\}$. Veamos que, como $0 \notin S(\mathbb{N})$ se tiene que $S(\mathbb{N}) \subset \mathbb{N}$.

Además siendo $M = S(\mathbb{N}) \cup \{0\}$ se tiene que:

- $0 \in M$
- si $n \in M$ entonces $n^+ \in M$.

La propiedad 3 implica $\mathbb{N} = M \therefore$ si $x \in \mathbb{N} \setminus \{0\}$, entonces $x \in M \setminus \{0\}$ por lo cual $x \in S(\mathbb{N})$.
 $\therefore S(\mathbb{N}) = \mathbb{N} \setminus \{0\}$

Definición 2.1.5. Sea X un conjunto; $g : X \rightarrow X$ una función, y $x_0 \in X$. Decimos que la terna (X, g, x_0) es un sistema de Peano si:

- g es inyectiva
- $g(X) = X \setminus \{x_0\}$
- $[A \subset X \wedge x_0 \in A \wedge (g(x) \in A \ \forall x \in A)] \Rightarrow A = X$

Observación. $(\mathbb{N}, S, 0)$ es un sistema de Peano.

Definición 2.1.6. Dado un conjunto A , una operación binaria en A es una función $f : A \times A \rightarrow A$.

- Si $B \subset A$, se dice que B es cerrado bajo f si $f(B \times B) \subset B$.
- f es conmutativa si $f(x, y) = f(y, x) \ \forall x, y \in A$
- f es asociativa si $f(x, f(y, z)) = f(f(x, y), z) \ \forall x, y, z \in A$

Proposición 8. (de recurrencia) Sea A un conjunto no vacío, $G : A \rightarrow A$ una función y $a \in A$. Entonces existe una única función $F : \mathbb{N} \rightarrow A$ tal que $\forall n \in \mathbb{N} \ F(n^+) = G(F(n))$ y $F(0) = a$.

Proof. Sea $C = \{T \in \mathcal{P}(\mathbb{N} \times A) \mid (0, a) \in T \wedge [(n, b) \in T \rightarrow (n^+, G(b)) \in T]\}$ Veamos que C es no vacío ya que $\mathbb{N} \times A \in C$.

Sea $F = \bigcap C$. Veamos que $F \in C$ ya que $(0, a) \in T \ \forall T \in C$ y si $(n, b) \in F$, se tiene que $(n, b) \in T \ \forall T \in C \therefore (n^+, G(b)) \in T \ \forall T \in C \therefore (n^+, G(b)) \in F$

Se verificará que F es función.

Sea $M = \{n \in \mathbb{N} \mid \exists! b \in S \ (n, b) \in F\}$

Hecho 1: $0 \in M$

Veamos que $0 \in \mathbb{N}$, y $(0, a) \in F$.

Suponga que existe $b \in A$ tal que $(0, b) \in F \wedge b \neq a$. Sea $F_b = F \setminus \{(0, b)\}$. Se tiene que $F_b \neq F$, ya que $(0, b) \in F \setminus F_b$; además $F_b \subset F$.

Como $F \subset \mathbb{N} \times A$ se tiene $F_b \subset \mathbb{N} \times A$; además $(0, a) \in F_b$.

Sea $(n, b) \in F_b$, entonces $(n, b) \in F \therefore$ como $F \in C \Rightarrow (n^+, G(n)) \in F$ Además como $n^+ \neq 0$, se tiene $(n^+, G(b)) \in F_b \therefore (n^+, G(b)) \in F \setminus \{(0, b)\}$ i.e $(n^+, G(b)) \in F_b$

Se ha probado que $F_b \in C \therefore F \subset F_b$. Así, $F = F_b$ lo cual es una contradicción, por lo tanto $a = b$, por ende $0 \in M$.

Hecho 2: $n^+ \in M \quad \forall n \in M$

Sea $n \in M$, entonces $\exists! b \in A$ tal que $(n, b) \in F$. Como $F \in C$, se tiene entonces que $(n^+, G(b)) \in F$. Suponga que existe $c \in A$ tal que $(n^+, c) \in F \wedge c \neq G(b)$.

Sea $F_c = F \setminus \{(n^+, c)\}$. Se tiene que $F \neq F_c$, ya que $(n^+, c) \in F \setminus F_c$. Además $F_c \subset F$.

Observe que $F_c \in \mathcal{P}(\mathbb{N} \times A)$, además $(0, a) \in F$ y como $0 \neq n^+$, se tiene: $(0, a) \neq (n^+, c) \therefore (0, a) \in F_c$.

Sea $(m, d) \in F_c$, entonces $(m, d) \in F$ y como $F \in C$, se tiene que $(m^+, G(d)) \in F \wedge (m^+, G(d)) \neq (n^+, c)$; ya que de lo contrario, $n^+ = m^+ \wedge G(d) = c \neq G(b) \therefore n = m \wedge G(d) \neq G(b)$. Así $n = m \wedge d \neq b$.

Se tiene por lo anterior que seleccionando $n = m$, $d \neq b$. Así $(n, b), (n, d) \in F$ lo cual contradiría que $n \in M$. Por lo cual $c = G(b)$ entonces $n^+ \in M$.

Los hechos 1 y 2 implican que $M = \mathbb{N}$, es decir que $\forall n \in \mathbb{N} \quad \exists! b : F(n) = b$. Así F es función.

Suponga ahora que $\bar{F} : \mathbb{N} \rightarrow S$ es una función tal que $\bar{F}(0) = a \wedge \bar{F}(n^+) = G(F(n))$. Sea $H = \{n \in \mathbb{N} \mid F(n) = \bar{F}(n)\}$. Veamos que $0 \in H$ ya que $F(0) = \bar{F}(0) = a$. Considere ahora a $n \in H$ (ya que es no vacío), entonces $F(n^+) = G(F(n)) = G(\bar{F}(n)) = \bar{F}(n^+)$; así $n^+ \in H$. Por lo cual $H = \mathbb{N}$ entonces $F = \bar{F}$. \square

Proposición 9. Sean A un conjunto, $G : \mathbb{N} \times A \rightarrow A$ una función, y $0 \in A$. Entonces existe una única función $F : \mathbb{N} \rightarrow A$ tal que:

a. $F(0) = a$

b. $F(n^+) = G(n, F(n)) \quad \forall n \in \mathbb{N}$

Para la demostración se procede de forma similar a la prueba anterior.

Proof. Considere $C = \{T \in \mathcal{P}(\mathbb{N} \times A) \mid (0, a) \in T \wedge (n, b) \in T \Rightarrow (n^+, G(n, b)) \in T\}$. Trivialmente C es no vacío ya que para cualquier $(n, b) \in \mathbb{N} \times A$, $G(n, b) \in A$ así, $\mathbb{N} \times A \in C$. Considere ahora a $F = \bigcup C$; de la misma forma que la prueba anterior $F \in C$. Sea $M = \{n \in \mathbb{N} \mid \exists! b \quad (n, b) \in F\}$. Se verificará que $0 \in M$, y que si $n \in M$ entonces $n^+ \in M$.

Hecho 1. $0 \in M$.

Suponga que existe $b \in A$ tal que $b \neq a \wedge (0, b) \in F$. Sea $F_b = F \setminus (0, b)$ veamos que $(0, b) \in F \setminus F_b$ de forma que $F_b \subset F$.

Considere ahora $n \in \mathbb{N}$ de forma que como $n^+ \neq 0$, si $(n, c) \in F_b$, entonces $(n^+, G(n, c)) \in F_b$; así $F_b \in C$. La condición anterior implica que $F \subset F_b$ así $F = F_b$ lo cual contradice que $(0, b) \in F \setminus F_b$, por lo tanto $a = b$, así $0 \in M$.

Hecho 2. $n \in M \Rightarrow n^+ \in M$.

Sea $n \in \mathbb{N} \wedge (n, b) \in F$. Suponga que $\exists c$ tal que $c \neq G(n, b) \wedge (n^+, c) \in F$. Considere ahora $F_c = F \setminus \{(n^+, c)\}$. Veamos que $(n^+, c) \in F \setminus F_c$ así $F_c \subset F$. Como $0 \neq n^+$ y $(0, a) \in F$, $(0, a) \in F_c$.

Así también $(n, b) \in F_c$ ya que $n \neq n^+ \therefore (n, b) \neq (n^+, c)$. Y, $(n^+, G(n, b)) \in F_c$ puesto que $(n^+, G(n, b)) \neq (n^+, c)$ así $F_c \in C$ por lo cual $F \subset F_c$. Lo cual contradice que $(n^+, c) \in F \setminus F_c$. Así, de los hechos anteriores se tiene que $0 \in M$ y si $n \in M$, entonces $n^+ \in M$. De lo cual se concluye que $M = \mathbb{N}$ así F es función.

Finalmente, la unicidad se concluye de un razonamiento idéntico al de la proposición anterior. \square

Proposición 10. Existe una única función $f : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ tal que:

- a. $f(0, n) = n \quad \forall n \in \mathbb{N}.$
- b. $f(n^+, m) = f(m, n)^+ \quad \forall n, m \in \mathbb{N}$

Proof. Considere la función:

$$G : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$$

$$(x, y) \rightarrow y^+$$

La proposición 8 garantiza la existencia de una función $f_n : \mathbb{N} \rightarrow \mathbb{N}$ única tal que:

- a. $f(0) = n$
- b. $f(m^+) = G(m, f(m)) \quad \forall m \in \mathbb{N}$

Sea $f : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ la función definida como $f(m, n) = f_n(m)$. Se tiene así:

- a. $f(0, n) = f_n(0) = n$
- b. $f(n^+, m) = f_m(n^+) = G(n, f(n)) = f_m(n)^+ = f(m, n)^+$

Se verificará que f es única.

Suponga que existe $h : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ tal que:

- a. $h(0, n) = n$
- b. $h(n^+, m) = h(m, n)^+$

Sea $h_n : \mathbb{N} \rightarrow \mathbb{N}$ tal que $h_n(m) = h(m, n)$; y dado $n \in \mathbb{N}$, definamos a $M = \{x \in \mathbb{N} \mid h_n(x) = f_n(x)\}$. Veamos que $h_n(0) = n = f_n(0) \therefore 0 \in M$.

Suponga que $x \in M$; así $h_n(x) = f_n(x)$. Se sigue entonces que:

$$h_n(x^+) = h(x^+, n) = G(x, h_n(x)) = G(x, f_n(x)) = f_n(x^+)$$

Así $M = \mathbb{N}$. Al ser la elección de n arbitraria se tiene que $f(n, m) = h(n, m) \quad \forall n, m \in \mathbb{N}$. □

A la operación binaria dada por la proposición anterior se le denominará adición en \mathbb{N} y $f(n, m)$ se denotará por $n + m$.

Proposición 11. Sean m, n, p números naturales, entonces:

- a. $(n + m) + p = n + (m + p)$
- b. $m + n = n + m$
- c. Si $m + p = n + p$ entonces $m = n$

d. Si $m + p = 0$ entonces $m = 0 \wedge n = 0$

Proof.

a. Definamos a $M = \{x \in \mathbb{N} \mid x + (y + z) = (x + y) + z \quad \forall y, z \in \mathbb{N}\}$.

Veamos que $0 \in M$ ya que

$$\begin{aligned} 0 + (y + z) &= (y + z) \\ &= y + z \\ &= (0 + y) + z \end{aligned}$$

Así $0 \in M$.

Supongamos ahora que $x \in M$, es decir, que

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

Entonces se tiene que:

$$\begin{aligned} x^+ + (y + z) &= (x + (y + z))^+ \\ &= ((x + y) + z)^+ \\ &= ((x + y)^+ + z) \\ &= (x^+ + y) + z \end{aligned}$$

Así $M = \mathbb{N}$.

b. Definamos a $M = \{x \in \mathbb{N} \mid x + y = y + x \quad \forall y \in \mathbb{N}\}$.

- Se verificará que $0 \in M$.

- Caso 1: $y = 0$.

En dado caso se tiene:

$$\begin{aligned} y + 0 &= 0 + 0 \\ &= 0 + y \end{aligned}$$

- Caso 2: $y \neq 0$.

En dado caso $\exists y_-$ tal que $y_-^+ = y$

$$\begin{aligned} 0 + y &= y \\ y + 0 &= (0 + y_-)^+ \\ &= y_-^+ \\ &= y \end{aligned}$$

Así, verificamos que $0 \in M$.

- Ahora verificaremos que si $x \in M \Rightarrow x^+ \in M$.

Sea $M' = \{x \in \mathbb{N} \mid x^+ + y = x + y^+\}$.

- Se probará que $0 \in M'$.

Veamos que $\forall y \in \mathbb{N}$:

$$\begin{aligned} 0^+ + y &= 1 + y \\ &= (y + 0)^+ \quad \text{Como } 0 \in M \\ &= (0 + y)^+ \\ &= y^+ + 0 \quad \text{Además} \\ y^+ + 0 &= 0 + y^+ = 0 \end{aligned}$$

Así $0 \in M'$.

Observación. Ésto último prueba que $1 + y = y^+$.

- Se probará que si $x \in M'$ entonces $x^+ \in M'$
 $\forall y \in \mathbb{N}$

$$\begin{aligned} x^+ + y &= (y + x)^+ \\ &= (y + x) + 1 \\ &= y + (x + 1) \\ &= y + (x + 0^+) \\ &= y + (x^+ + 0) \\ &= y + (0 + x^+) \\ &= y + x^+ \end{aligned}$$

Así $x^+ \in M'$. Por lo tanto $M' = \mathbb{N}$.

Suponga que $x \in M$, entonces $x + y = y + x \quad \forall y \in \mathbb{N}$. Así:

$$\begin{aligned} x^+ + y &= (y + x)^+ \\ &= (y + x) + 1 \\ &= y + (x + 1) \\ &= y + (0 + x^+) \\ &= y + x^+ \end{aligned}$$

Así $M = \mathbb{N}$

c. Sea $M = \{p \in \mathbb{N} \mid (m + p = n + p \Rightarrow m = n) \quad \forall n, m \in \mathbb{N}\}$.

- $0 \in M$.

Veamos que $\forall m, n \in \mathbb{N}$: Suponga que $m + 0 = n + 0$

$$\begin{aligned} m + 0 &= n + 0 \\ 0 + m &= 0 + n \\ m &= n \end{aligned}$$

Así $0 \in M$

- $\forall m, n \in \mathbb{N}$ suponga que $(p + m = p + n) \Rightarrow m = n \quad p \in \mathbb{N}$. Vemos que si:

$$\begin{aligned} p^+ + m &= p^+ + n \\ (m + p)^+ &= (n + p)^+ \\ (p + m)^+ &= (p + n)^+ \Rightarrow \\ p + m &= p + n \Rightarrow \\ m &= n \end{aligned}$$

Así $M = \mathbb{N}$.

d. Sea $M = \{x \in \mathbb{N} \mid x + y = 0 \Rightarrow x = 0 \wedge y = 0 \quad \forall x, y \in \mathbb{N}\}$. Considere a $x, y \in \mathbb{N}$ tales que $x + y = 0$. Entonces:

$$\begin{aligned} x + y &= 0 \\ &= 0 + y \end{aligned}$$

De la propiedad 3, tenemos que $x = 0$. Como x, y fueron arbitrarios: $x \in M$ entonces $\mathbb{N} \subset M$. Así $M = \mathbb{N}$.

□

Proposición 12. Existe una única función $g : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ tal que:

$$a. g(0, n) = 0 \quad \forall n \in \mathbb{N}$$

$$b. g(n^+, m) = g(n, m) + m \quad \forall n, m \in \mathbb{N}$$

Proof. La proposición 8 implica que existe una única función $F_n : \mathbb{N} \rightarrow \mathbb{N}$ así se tiene que la □

Definición 2.1.7. Sea $x \in \mathbb{N}$. Se define el conjunto de descendientes de x denotado por Dx como el conjunto $\{S^n(x) \mid n \in \mathbb{N}\}$.

Observación. $x \in Dx$.

Definición 2.1.8. Sea $A \subset \mathbb{N}$. Se define el conjunto de sucesores de elementos de A , denotado por A^Δ , como el conjunto $\{S(x) \mid x \in A\}$.

Proposición 13. Sean $x, y \in \mathbb{N}$, entonces:

$$i) Dx = \{x\} \cup Dx^+$$

$$ii) Dx^+ \subset [Dx]^\Delta$$

$$iii) x \notin Dx^+$$

$$iv) Dx = Dy \text{ entonces } x = y$$

Proof. i) Sea $u \in Dx$, entonces $\exists n \in \mathbb{N}$ tal que $u = S^n(x)$. Entonces $u = x \vee u \neq x$.

Si $u = x$, entonces $u \in x \cup Dx^+$.

Si $u \neq x$, entonces $n \neq 0$. Así, como $S(\mathbb{N}) = \mathbb{N} \setminus \{0\}$ se tiene $\in S(\mathbb{N})$, por lo tanto $\exists m \in \mathbb{N}$ tal que $n = S(m)$, i.e., $n = m^+ \therefore u = S^{m^+}(x) = S \circ S^m(x) = S^m \circ S(x) = S^m(x^+)$ lo cual muestra que $u \in Dx^+ \therefore u \in \{x\} \cup Dx^+$. Así se demuestra i).

ii) Sea $m \in Dx^+$. Se debe verificar que $m \in [Dx]^\Delta$. Como $m \in Dx^+$, existe $n \in \mathbb{N}$ tal que: $m = S^n(x^+) = S^n \circ S(x) = S \circ S^n(x)$, lo cual muestra que $m \in [Dx]^\Delta$.

$$iii) \text{ Sea } M = \{x \in \mathbb{N} \mid x \notin Dx^+\}$$

Si $0 \in D0^+$, entonces $\exists r \in \mathbb{N}$ tal que:

$0 = S^r(0^+) = S^r \circ S(0) = S \circ S^r(0)$, lo cual implica que $0 \in S(\mathbb{N})$ en contradicción con el hecho $S(\mathbb{N}) = \mathbb{N} \setminus \{0\}$ por lo tanto $0 \notin D0^+$, i. e., $0 \in M$.

Sea $x \in M$. Se verificará que $x^+ \in M$.

Suponga que $x^+ \notin M$, entonces $x^{++} \in D0^{++}$. De ii) $Dx^{++} \subset [Dx^+]^\Delta \therefore x^+ \in [Dx^+]^\Delta$. Así $\exists q \in Dx^+$ tal que $x^+ = S(q)$, es decir, $x^+ = q^+ \therefore x = q$, y así $x \in Dx^+$, lo cual contradice que $x \in M \therefore x^+ \in M$. Así $M = \mathbb{N}$.

iv) Por hipótesis $Dx = Dy$. Suponga que $x \neq y$. Observe que, como $x \in Dx$ y $Dx = Dy$, se tiene que $x \in Dy$. Además $Dy = \{y\} \cup Dy^+$. Así como $x \neq y$, se tiene $x \in Dy^+ \therefore Dx \subset Dy$ (ya que si $u \in Dx$, $\exists n \in \mathbb{N}$ tal que $u = S^n(x)$. Además, como $x \in Dy^+ \exists m \in \mathbb{N}$ tal que $x \in S^m(y^+) \therefore u = S^n \circ S^m(y^+)$ lo cual muestra que $u \in Dy^+$). Así $Dy \subset Dy^+ \therefore y \in Dy^+$ lo cual contradice a iii). Así $x = y$. □

Proposición 14. Sea $R = \{(m, n) \in \mathbb{N} \times \mathbb{N} \mid n \in Dm\}$. R es un orden parcial en \mathbb{N} .

Proof. 1) Dado $n \in \mathbb{N}$ $n \in Dn \therefore (n, n) \in R$. Es decir, R es reflexiva.

2) Sean (n, m) y $(m, r) \in R$, entonces $m \in Dn \wedge r \in Dm \therefore Dm \subset Dn \wedge Dr \subset Dm \therefore Dr \subset Dn$ entonces $r \in Dn \therefore (n, r) \in R$. 3) Suponga que (n, m) y $(m, n) \in R$. Entonces $m \in Dn \wedge n \in Dm \therefore Dm \subset Dn \wedge Dn \subset Dm \therefore Dm = Dn$, y de la proposición anterior se tiene que $m = n$. Así R es antisimétrica. \square

Lema 2.1.3. Sea $x \in \mathbb{N}$, entonces:

$$Dx = \bigcap \{A \in \mathcal{P}(\mathbb{N}) \mid x \in A \wedge n \in A \Rightarrow n^+ \in A\}$$

Proof. Sea $B = \bigcap \{A \in \mathcal{P}(\mathbb{N}) \mid x \in A \wedge \forall n \in \mathbb{N} n \in A \Rightarrow n^+ \in A\}$. Sea $M = \{n \in \mathbb{N} \mid S^n(x) \in B\}$. Sea $Z = \{A \in \mathcal{P}(\mathbb{N}) \mid x \in A \wedge \forall n \in \mathbb{N} n \in A \Rightarrow n^+ \in A\}$. Entonces $B = \bigcap Z$. Observe que $x \in A \forall A \in Z \therefore x \in \bigcap Z$, es decir $x \in B$, i.e., $S^0(x) \in B \therefore 0 \in M$.

Sea $n \in M$, entonces, $S^n(x) \in B \therefore S^{n+}(x) = S^n \circ S(x) = S \circ S^n(x) \in B$. Como $B \in Z \wedge S^n(x) \in B$, se tiene que $S \circ S^n(x) \in B \therefore S^{n+}(x) \in B \therefore n^+ \in M$. Así $M = \mathbb{N}$. En consecuencia $Dx \subset B$.

se tiene que $x \in Dx$. Además $u \in Dx$ implica $u^+ \in Dx$. Por lo tanto $B \subset Dx$. Así $B = Dx$. \square

Proposición 15. Sea $M \subset \mathbb{N}$, $M \neq \emptyset$. Si $x^+ \in M \forall x \in M$, entonces existe un único $n \in \mathbb{N}$ tal que $M = Dn$.

Proof. **Hecho 1:** Sea $K = \{n \in \mathbb{N} \mid n \notin M \Rightarrow M \subset Dn^+\}$.

Por el lema anterior $D0 = \bigcap \{A \in \mathcal{P}(\mathbb{N}) \mid 0 \in A \wedge (\forall n \in \mathbb{N} n \in A \Rightarrow n^+ \in A)\}$. Se tiene entonces $0 \in D0 \wedge (n \in D0 \Rightarrow n^+ \in D0) \therefore D0 = \mathbb{N}$. Por otra parte $D0 = \{0\} \cup D0^+$. En consecuencia $\mathbb{N} \setminus \{0\} \subset D0^+$.

Así mismo como $0 \notin D0^+$. y $D0^+ \subset \mathbb{N}$. Se tiene $D0^+ \subset \mathbb{N} \setminus \{0\} \therefore D0^+ = \mathbb{N} \setminus \{0\}$ y así si $0 \notin M$, se tiene $M \subset D0^+ \therefore 0 \in K$.

Sea $n \in K$, se verificará que $n^+ \in K$.

Suponga $n^+ \notin M$, entonces $n \notin M$ ya que $x^+ \in M \forall x \in M$. Así como $n \in k$, se tiene $M \subset Dn^+$, y como $Dn^+ = \{n^+\} \cup Dn^{++}$. Además $n^+ \notin M$, luego $M \subset Dn^{++}$, lo cual implica que $n^+ \in K \therefore K = \mathbb{N}$.

Hecho 2: $\forall n \in \mathbb{N} [(n \notin M \wedge n^+ \in M) \Rightarrow M = Dn^+]$.

Sea $n \in \mathbb{N}$ tal que $n \notin M \wedge n^+ \in M$. Como $n \notin M$, por el hecho 1 se tiene que $M \subset Dn^+$. Por el lema anterior $Dn^+ \subset A \subset \mathbb{N}$ tal que $n^+ \in A \wedge \forall x \in \mathbb{N} (x \in A \Rightarrow x^+ \in A)$. Como $n^+ \in M \wedge x^+ \in M \forall x \in M$, se concluye que $Dn^+ \subset M \therefore Dn^+ = M$.

$$0 \in M \vee 0 \notin M$$

- Si $0 \in M$, entonces se tiene que $M = \mathbb{N}$ y así $M = D0$.

- Suponga que $0 \notin M$.

Se verificará que existe $n \in \mathbb{N}$ tal que $n \notin M \wedge n^+ \in M$, de esta manera, por el hecho 2 se tendrá que $M = Dn^+$.

Procediendo por reducción al absurdo suponga que no existe tal $n \in \mathbb{N}$. Entonces: $\forall n \in \mathbb{N} \quad n \in M \vee n^+ \notin M \dots (\lambda)$.

Considere el conjunto $T = \{n \in \mathbb{N} \mid n \notin M\}$.

-Se tiene $0 \in T$ ya que se está considerando el caso en que $0 \notin M$.

-Sea $n \in T$, entonces $n \notin M \therefore$ de (λ) se tiene $n^+ \notin M \therefore n^+ \in T$. Teniendo así $T = \mathbb{N}$, por lo cual $M = \emptyset$, lo cual contradice que $M \neq \emptyset$. Por lo tanto sí existe $n \in \mathbb{N}$ tal que $n \notin M \wedge n^+ \in M$ y por ello, del hecho 2: $M = Dn^+$. De la proposición 13 se tiene que si $M = D^n \wedge M = D^m$, entonces $n = m$, así n es único. \square

Proposición 16. $R = \{(m, n) \in \mathbb{N} \times \mathbb{N} \mid n \in Dm\}$ es un buen orden en \mathbb{N} .

Proof. Se ha probado previamente que R es un orden parcial. Sea $A \subset \mathbb{N}$, $A \neq \emptyset$. Se debe probar que A tiene un primer elemento. Considere el conjunto $B = \{R \in \mathcal{P}(\mathbb{N}) \mid A \subset R \wedge S(R) \subset R\}$; veamos que $B \neq \emptyset$, ya que $\mathbb{N} \in B$.

Sea $M = \bigcap B$, observe que $M \subset B$. Como $A \subset M \wedge A \neq \emptyset$, se tiene $M \neq \emptyset$. Además, como $M \in B \forall x (x \in M \Rightarrow x^+ \in M)$. La proposición 15 implica que existe un único $n \in \mathbb{N}$ tal que $M = Dn$. Se verificará que dicho $n \in A$. Procediendo por contradicción suponga que $n \notin A$. Se tiene por la proposition 13 que $Dn = \{n\} \cup Dn^+$. Como $A \subset M$, entonces $A \subset \{n\} \cup Dn^+$, y así como $n \notin A$, se tiene: $A \subset Dn^+ \dots (i)$.

Además, $\forall x (x \in Dn^+ \Rightarrow x^+ \in Dn^+)$, es decir, $S(Dn^+) \subset Dn^+ \dots (ii)$.

$i)$, y $ii)$ implican que $Dn^+ \in B \therefore M \subset Dn^+$, i.e., $Dn \subset Dn^+$. Así, como $n \in Dn$, se tiene $n \in Dn^+$, lo cual contradice la parte $iii)$ de la proposición 13 $\therefore n \in A$.

Se mostrará que n es el primer elemento de A .

Sea $x \in A \mid x = n \vee x \neq n$.

a) Si $x = n$, se tiene $(n, x) \in R$, ya que R es en particular reflexiva. b) Suponga que $x \neq n$.

Como $A \subset M \wedge M = Dn$, se tiene $A \subset \{n\} \cup Dn^+$. Y así, como $x \neq n$, se tiene $x \in Dn^+ \therefore (n^+, x) \in R$. Por otra parte $(n, n^+) \in R$ ya que $n^+ \in Dn$. Y, como R es transitiva, se concluye que $(n, x) \in R$, finalmente mostrando que n es el primer elemento de A . \square

Notación: $(n, m) \in R$ se denotará $n \leq m$. Si, además $n \neq m$, se escribirá $n < m$.

Proposición 17. Sean $n, m \in \mathbb{N}$. Entonces se cumple una única de las siguientes tres afirmaciones:

$$i) n = m \quad ii) n < m \quad iii) m < n$$

Proof. Como R es un buen orden en \mathbb{N} , se tiene que R es un orden total en \mathbb{N} . Así $(n, m) \in R \vee (m, n) \in R$. Así, como R es antisimétrica, si $n \neq m$, solo se puede cumplir una única de las siguientes condiciones: $(n, m) \in R$ o $(m, n) \in R$, así se tiene únicamente una de $n < m$, $m < n$. Si $n = m$, no se cumple ni $n < m$ ni $m < n$. \square

Proposición 18. Sean $n, m \in \mathbb{N}$, si $n^+ > m$, entonces $n \geq m$.

Proof. Por hipótesis $n^+ > m$. Procediendo por contradicción, suponga que no se cumple $n \geq m$, entonces $(m, n) \notin R \therefore m \neq n \wedge \neg(m < n)$. La proposición 17 implica que $n < m \leq m \wedge n \neq m$. En particular $(n, m) \in R$. Así $m \in Dn \therefore \exists r \in \mathbb{N}$ tal que $m = S^r(n)$.

Como $m \neq n$, se tiene $r \neq 0 \therefore r \in \mathbb{N} \setminus \{0\}$, i.e., $r \in S(\mathbb{N})$, por lo cual $\exists q \in \mathbb{N}$ tal que $r = q^+$.

Así $m = S^{q^+} = S^q \circ S(n) = S^q(n^+)$ lo cual implica que $m \in Dn^+ \therefore (n^+, m) \in R \dots (\lambda)$. Por

hipótesis se tiene $n^+ > m \dots (\alpha) \therefore n^+ \neq m$. De (λ) se tiene $n^+ < m \dots (\beta)$. De (α) y (β) se tiene $m < n^+ \wedge n^+ < m$, lo cual contradice la proposición 17. \square

Proposición 19. i) $\forall n, m \in \mathbb{N} \leq m$ sí y sólo sí $\exists p \in \mathbb{N}$ tal que $n + p = m$.

ii) $\forall n, m, p \in \mathbb{N} n < m$ sí y sólo sí $n + p < m + p$.

iii) $\forall n, m, p \in \mathbb{N}$, si $p \neq 0$, entonces $n < m$ sí y sólo sí $np < mp$.

Proof. i) Dados $n, m \in \mathbb{N}$, considere el conjunto $K = \{t \in \mathbb{N} \mid S^t(n) = n + t\}$.

$\cdot S^0(n) = n = n + 0 \therefore 0 \in K$.

\cdot Sea $t \in K$, entonces $S^{t^+} = S \circ S^t(n) = S(S^t(n)) = S(n + t) = S(t + n) = (t + n)^+ = t^+ + n = n + t^+$.

Se tiene así que $t^+ \in K \therefore K = \mathbb{N}$.

\Rightarrow) Por hipótesis $n \leq m$, i.e., $m \in Dn \therefore \exists p \in \mathbb{N}$ tal que $m = S^p(n)$. Como $K = \mathbb{N}$, $p \in K \therefore S^p(n) = n + p$ i.e., $m = n + p$.

\Leftarrow) Ahora por hipótesis, $\exists p \in \mathbb{N}$ tal que $n + p = m$. Como $p \in \mathbb{N} \wedge K = \mathbb{N}$, se tiene que $p \in K \therefore n + p = S^p(n)$, i.e. $m \in Dn \therefore n \leq m$.

ii) Sean $n, m, p \in \mathbb{N}$.

\Rightarrow) Suponga que $n < m$, entonces $(n, m) \in R \wedge n \neq m$. En particular $m \in Dn \therefore \exists r \in \mathbb{N}$ tal que $m = S^r(n)$, i.e., $m = n + r$. Observe que $r \neq 0$, ya que $n \neq m$.

Como $m = n + r$, se tiene:

$m + p = (n + r) + p = (n + p) + r \Rightarrow S^r(n + p) \therefore m + p \in D_{n+p}$. En consecuencia $n + p \leq m + p$. Además,

como: $m + p = (n + p) + r$ y $r \neq 0$ se tiene de A_3 que $m + p \neq n + p \therefore n + p < m + p$.

\Leftarrow) Por hipótesis $n + p < m + p$.

Suponga que no se cumple $n < m$. Entonces $n = m \vee m < n$. En el primer caso $n + p = m + p$, lo cual no ocurre. En el segundo caso, de la suficiencia probada previamente, se tendría: $m + p < n + p$, lo cual no ocurre. $\therefore n < m$.

iii) Sean $n, m, p \in \mathbb{N}, p \neq 0$.

\Rightarrow) Suponga que $n < m$. Entonces, de i) $\exists q \in \mathbb{N}$ tal que $m = n + q$. Además $q \neq 0$ ya que $n \neq m \therefore mp = (n + q)p = np + qp$.

M_4 implica que $qp \neq 0$ ya que $q \neq 0 \wedge p \neq 0 \therefore mp > np$.

\Leftarrow) Asuma ahora $np < mp$, se debe probar $n < m$.

Suponga que no se cumple $n < m$. Entonces $n = m \vee m < n$. En el primer caso se tendría $np = mp$, lo cual no ocurre. En el segundo caso se tendría, por la suficiencia previamente probada, $mp < np$ lo cual no ocurre $\therefore n < m$. \square

2.1.1 Ejercicios

Problema 2.1.1. a) Sea $m \in \mathbb{N}$ Demuestre que existe una única función $F_m : \mathbb{N} \rightarrow \mathbb{N}$ tal que $F_m(0) = 1$, $F_m(n^+) = g_m(F_m(n))$, siendo g_m la función: $g_m : \mathbb{N} \rightarrow \mathbb{N} \quad n \rightarrow nm$

b) Considere la función $f : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N} \quad (m, n) \rightarrow F_m(n)$.

Verifique que:

a. $f(m, 0) = 1, \forall m \in \mathbb{N}$

$$b. f(m, n^+) = F_m(n)m$$

Denotando $f(m, n)$ por m^n , verifique lo siguiente:

Dados $m, n, u \in \mathbb{N}$

$$a. u^m \cdot u^n = u^{m+n}$$

$$b. (u^m)^n = u^{mn}$$

$$c. (un)^m = u^m n^m$$

$$d. 1^n = 1$$

2.2 Equivalencias del Axioma de Elección

Proposición 12. Sea (N, R) un conjunto parcialmente ordenado, tal que toda cadena contenida en N , tiene un supremo en N . Sea $f : N \rightarrow N$ una función que satisface:

$$\forall x \in N \quad (x, f(x)) \in R$$

Entonces existe $n \in N$ tal que $f(n) = n$.

Proof. Dado $u \in N$ se dice que $A \subset N$ es admisible con relación a u si cumple:

$$i) u \in A$$

$$ii) f(A) \subset A$$

iii) Si B es una cadena contenida en A , entonces en A mismo existe el supremo de B

Sea M el conjunto cuyos elementos son todos los subconjuntos admisibles con respecto a u de N y sea: $S = \bigcap_{x \in M} x$.

Proof. a)

$$v \in S \quad \text{ya que} \quad u \in x \quad \forall x \in M$$

$$b) \text{ Sea } t \in S$$

$$t \in x \quad \forall x \in M$$

$$f(t) \in x \quad \forall x \in M$$

Lo cual muestra que $f(S) \subset S$

c) Sea B una cadena contenida en S

$$B \subset x \quad \forall x \in M$$

$$\therefore \text{Sup}(B) \in S$$

a), b) c) muestra que S es admisible con relación a u

□

Observe que: si $S' \subset S \wedge S'$ es u-admisibile entonces $S' = S$

Hecho 1: u es el primer elemento de S , i.e.:

$$(u, x) \in R \quad \forall x \in S$$

Proof. Sea $A = \{x \in S \mid (u, x) \in R\}$

Para probar el hecho anterior se debe probar que $A = S$. Como $A \subset S$, por la observacion anterior basta con verificar que A es u-admisibile.

i) Como R es en particular reflexiva $(u, u) \in R$. Además $u \in S$ ya que S es u-admisibile.

ii) Sea $x \in A$, se verificara que $f(x) \in A$ Como $x \in A$, $(u, x) \in R$. Además $(x, f(x)) \in R$ Por hipotesis de la proposición.

\therefore siendo R transitiva se tiene $(u, f(x)) \in R$

Como $x \in A \wedge A \subset S$, $x \in S$ y por ser S u-admisibile $f(x) \in S \therefore f(x) \in A$. En consecuencia $f(A) \subset A$

iii) Sea B una cadena contenida en A . Por hipotesis, $\sup B$ existe en N .

Como $A \subset S$ se tiene a $B \subset S$.

Así siendo S u-admisibile se tiene $\sup B \in S$

$$(t, \sup B) \in R \quad \forall t \in B$$

Además como $B \subset A$ se tiene que $(u, t) \in R \quad \forall t \in B$.

$$\therefore (u, \sup B) \in R \quad \therefore \sup B \in A$$

.

i), ii), iii) muestran que A es u-admisibile

□

Dado $x \in P$, denotara la propiedad

$$[y \in S \setminus x \wedge (y, x) \in R]$$

Hecho 2: Si $\bar{x} \in S \wedge P(\bar{x})$ entonces $\forall z \in S \quad (z, \bar{x}) \in R \vee (f(\bar{x}), z) \in R$

Proof. Sea

$$B = \{z \in S \mid (z, \bar{x}) \in R \vee (f(\bar{x}), z) \in R\}$$

Se debe probar que $B = S$.

Como $B \subset S$, basta con probar que B es u-admisibile

i) Como $u \in S$ puesto que S es u -admisble

Como u es el primer elemento de S y $\bar{x} \in S$ se tiene $(u, \bar{x}) \in R$

$$\therefore u \in B$$

ii) Sea $x \in B$ se verificará que $f(x) \in B$

Como $x \in B \wedge B \subset S$, se tiene $x \in S \therefore$ por ser S u -admisble se tiene $f(x) \in S$

$$x = \bar{x} \vee x \neq \bar{x}$$

a) Si $x = \bar{x}$, entonces $f(x) = f(\bar{x})$

$$\therefore (f(x), f(\bar{x})) \in R$$

y así $f(x) \in B$

b) Considere $x \neq \bar{x}$

Como $x \in B$ se tiene $(x, \bar{x}) \in R \vee (f(\bar{x}), x) \in R$.

I) Si $(x, \bar{x}) \in R$, como $x \neq \bar{x}$ y además se tiene $P(\bar{x})$, entonces $(f(x), \bar{x}) \in R$ lo cual muestra que $f(x) \in B$

II) Suponga que $(x, f(x)) \in R$ se tiene que $(f(x), f(\bar{x})) \in R$
 $\therefore f(x) \in B$

Se ha probado que $f(B) \subset B$

iii) Sea $F \subset B$ una cadena, F es entonces una cadena en S ,

entonces $\therefore F \in S$

Como $F \subset B$

$\forall z \in F$ se tiene $(z, \bar{x}) \in R \vee (f(\bar{x}), z) \in R$

$$\therefore (\forall z \in F (z, \bar{x}) \in R \vee (\exists z \in F \wedge (f(\bar{x}), z) \in R))$$

a) Suponga que $\forall z \in F (z, \bar{x}) \in R$ entonces \bar{x} es una cota superior de F

$\therefore (sup F, \bar{x}) \in R$ lo cual implica $sup F \in B$

b) Suponga ahora que $\exists z \in F$ tal que $(f(\bar{x}), z) \in R$

Como

$$z \in F \quad (z, sup F) \in R \quad \therefore (sup F, f(\bar{x})) \in R$$

Por lo cual $sup F \in B$

i), ii), iii) muestran que B es u -admisble $\therefore B = S$. □

Hecho 3:

$$\forall x \in S \text{ se tiene } P(x)$$

Proof. Como $C \subset S$ basta probar que C es u-admisibile

i) Como S es u-admisibile, $u \in S$ se verificara $P(u)$.

Suponga $\neg P(u)$

Entonces $\exists y \in S \setminus \{u\}$ tal que $(y, u) \in R$

Como $y \in S$ y u es el primer elemento de S , se tiene $(u, y) \in R$. Dado que $(y, u) \in R$ se tiene $u = y$ (por ser R un orden parcial) lo cual contradice

$$y \in S \setminus \{u\}$$

Lo cual implica $u \in C$

ii) Se verificara ahora que $f(C) \subset C$ Sea $x \in C$, se debe probar que $f(x) \in C$

Como $x \in C \wedge C \subset S$ se tiene $x \in S$ y asi, por ser S u-admisibile

Se tiene $f(x) \in S$.

Para concluir que $f(x) \in C$ basta probar que $P(f(x))$

Asuma que $y \in S \setminus \{f(x)\}$ tal que $(y, f(x)) \in R$

Se verificara que $(y, f(x)) \in R$

Como $x \in C$ se tiene $x \in S \wedge P(x)$

dado que $y \in S$, y el **Hecho 2**, se tiene $(y, x) \in R \vee (y, f(x)) \in R$

Observe que $\neg((f(x), y) \in R)$ ya que si $(f(x), y) \in R$, como $(y, f(x)) \in R$ se tendría $y = f(x)$ lo cual contradice que $y \in S \setminus \{f(x)\}$

$$\therefore (y, x) \in R$$

$$y = x \vee y \neq x$$

a) Si $y = x$, $f(y) = f(x)$ Por lo cual $(f(y), f(x)) \in R$

b) Considere ahora $y \neq x$, entonces

$$y \in S \setminus \{x\} \quad (y)$$

por lo cual, dado $P(x)$ se concluye que $(f(y), x) \in R$. Así mismo se tiene que $(f(y), x) \in R$ por transitividad se tiene $(f(y), f(x)) \in R$

iii) Sea $F \subset C$ y una cadena. Se proba que $\sup F \in C$

Como $C \subset S$ y $F \subset S$ por lo cual siendo S u-admisible se tiene

$$\sup F \in S$$

Así para probar que $\sup F \in F$ basta verificar que se cumple $P(\sup F)$

Sea $w = \sup F$

Sea $y \in S \setminus \{w\}$ tal que $(y, w) \in R$. Se debe probar $(f(y), w) \in R$ Observe $\exists y_1 \in F$ tal que (y, y_1)

(Ya que en caso contrario dado cualquier elemento $y_1 \in F$ se tiene $\neg(y, y_1)$ Además como $F \subset C$; $y_1 \in C$ y así $P(y_1)$ y por el Hecho 2, como $y_1 \in S \wedge P(y_1)$ y además $y \in S$, necesariamente

$$(y, y_1) \in R \vee (y, f(y_1)) \in R$$

Así como se tiene $\neg((y, y_1) \in R)$ se tendría $(f(y_1), y) \in R$. Además

$$(y_1, f(y_1)) \in R \quad \therefore (y_1, y) \in R$$

Lo cual implicaría que y es cota superior de $F \therefore (w, y) \in R$

y como se tiene además que $(y, w) \in R$ se concluiría $y = w$ lo cual contradice que $y \in S \setminus \{w\}$

$$y_1 = y \vee y_1 \neg y$$

a) Si $y_1 = y$, entonces $y \in F$ por lo tanto se tiene $P(y_1)$

Así como $y \in S \wedge P(y)$ del **Hecho 2**

dado que $w \in S$ se tiene

$$(w, y) \in R \vee (f(y), w) \in R$$

No ocurre $(w, y) \in R$ ya que así como $(y, w) \in R$

Se tendría que $w = y$ lo cual contradice $y \in S \setminus \{w\}$

$$\therefore (f(y), w) \in R$$

b) Suponga ahora que $y_1 \neq y$ Como $y_1 \in F$ se tiene $P(y_1)$, así como

$$(y, y_1) \in R \quad \wedge \quad y \neq y_1 \quad y \in S \setminus \{y_1\}$$

por lo cual se concluye que $(f(y), y_1) \in R$ y como $(y_1, w) \in R$ se concluye $(f(y), w) \in R$

i), ii), iii) muestran que C es u-admisibles y por ello $C = S$

□

Sea $x \in S$, entonces por el **Hecho 3** se tiene $P(x)$

Por el **Hecho 2**, para cualquier $y \in S$ se tiene $(y, x) \in R \quad \vee \quad (f(x), y) \in R$

Además S es u-admisibles así, siendo S una cadena contenida en S , se tiene $\sup S \in S$

Sea $x_0 = \sup S$

Como $f(S) \subset S \quad \therefore f(x_0) \in S$

$$(f(x_0), x_0) \in R \quad \wedge \quad (x_0, f(x_0)) \in R$$

$$\therefore x_0 = f(x_0)$$

□

El teorema anterior fue probado por Baurbaki en 1939 y se conoce como el teorema del punto fijo de Baurbaki

Definición 2.2.1. Axioma de elección Sea A un conjunto cuyos elementos son ajenos no vacíos existe un conjunto B tal que $\forall x \in A \setminus \{\emptyset\} \quad B \cap x$ es un conjunto con un único elemento.

Proposición 13. Son equivalentes las siguientes proposiciones

I) Axioma de elección

II) Para cada conjunto X , existe una función

$$f : P(X) \setminus \{\emptyset\} \longrightarrow X$$

Tal que $f(A) \in A$ para cada $A \in P(X) \setminus \{\emptyset\}$

Proof. I) \rightarrow II) Sea X un conjunto.

Considere al conjunto $N = \{\{A\} \times A \mid A \in P(X) \setminus \{\emptyset\}\}$

El axioma de especificación permite probar que N es un conjunto.

Se verificara que N satisface las hipótesis del axioma de elección.

Sea $x \in N$ entonces $\exists A \in P(X) \setminus \{\emptyset\}$ tal que

$$x = \{A\} \times A \quad \{A\} \neq \emptyset$$

Así mismo $A \neq \emptyset \quad \therefore x \neq \emptyset$.

Considere otro elemento $y \in N \quad \exists A' \in P(X) \setminus \{\emptyset\}$ tal que $y = \{A'\} \times A'$ Sea $t \in x \cap y$ Como $t \in y \quad \therefore t = (A', a')$ con $a' \in A'$

Así mismo como $t \in x \quad \therefore t = (A, a)$ con $a \in A$

$$\therefore (A, a) = (A', a')$$

Se tiene en particular que $A = A'$

$$x = y$$

Dado que N satisface las hipótesis del axioma de elección, existe un conjunto B tal que

$$\forall A \in P(X) \setminus \{\emptyset\}, \quad B \cap (\{A\} \times A)$$

tiene un único elemento.

Sea $f = B \cap (\cup N)$.

$u \in f$, entonces $u \in B \quad \wedge \quad u \in (\cup N)$.

Como $u \in (\cup N) \quad \exists m \in N$ tal que $u \in m$. Por ser m un elemento de N existe $A \in P(X) \setminus \{\emptyset\}$ tal que $m = \{A\} \times A \quad \therefore$ como $u \in m$ existe $a \in A$ tal que $u = (A, a)$.

$$\therefore u \in [P(X) \setminus \{\emptyset\}] \times X$$

Suponga que $(A, b) \in f$ se verificara que $a = b$

Como $(A, b) \in (\cup N) \quad \exists s \in N$ tal que $(A, b) \in s$

Como $s \in N$ existe $A' \in P(X) \setminus \{\emptyset\}$ tal que $s = \{A'\} \times A'$

$$A = A' \quad \wedge \quad b \in A$$

\therefore como $f \subset B$

$$(A, b) \in B \cap (\{A\} \times A)$$

$$(A, a) \in B \cap (\{A\} \times A)$$

Dado que $b \cup (\{A\} \times A)$ tiene un único elemnto, se concluye que $a = b$

Lo anterior muestra que f es función.

Sea $k \in P(X) \setminus \{\emptyset\}$ se verificara que existe $w \in X$ tal que

$$(k, x) \in f$$

$$k \subset V \quad \wedge \quad k \neq \emptyset$$

$$\therefore \quad \{k\} \times k \in N$$

$B \cup (\{k\} \times k)$ Tiene un solo elemento Sea r tal elemnto $r = (k, w)$ con $w \in K$

Así $w \in X$, $(k, w) \in B$ y $(k, w) \in \text{cup} N$

$$(k, w) \in f$$

Se probara que el dominio de f es $P(X) \setminus \{\emptyset\}$

Para concluir que $f(A) \in A$

$\forall A \in P(X) \setminus \{\emptyset\}$ si $A \in P(X) \setminus \{\emptyset\}$ $(A, f(A)) \in f$

$$\therefore (A, f(A)) \in \cup N \quad \therefore \exists \{T\} \times T \in N$$

tal que

$$(A, f(A)) \in \{T\} \times T \quad \therefore A = T \quad \wedge \quad f(A) \in T \quad \therefore f(A) \in A$$

ii) \Rightarrow i)

. Sea A un conjunto cuyos elemntos son ajenos no vacios. Se debe probar que existe un conjunto B tal que $B \cap x$ tiene un único elemnto $\forall x \in A$.

Sea $X = \cup A$ Por hipotesis existe.

$$f : P(\cup A) \setminus \{\emptyset\} \longrightarrow \cup A$$

Tal que $f(y) \in y \quad \forall y \in P(\cup A) \setminus \{\emptyset\}$ Observe que si $y \in A$ entonces $y \in P(\cup A)$

(Ya que si $t \in y$, entonces $t \in \cup A$ y así $y \subset \cup A$)

Además si $y \in A$, $y \neq \emptyset$

$$\therefore y \in P(\cup A) \setminus \{\emptyset\}$$

i.e. y pertenece al dominio de f por lo cual esta definido $f(y)$

Por el axioma de especificación existe

$$B \quad \forall x(x \in B \Leftrightarrow x \in \cup A \quad \wedge \quad P(x))$$

Siendo $P(x)$ la propiedad $\exists y \quad x = f(y)$

Se verificará que $B \cap z$ tiene un único elemento $\forall z \in A$

Sea $z \in A$, entonces $z \in P(\cup A) \setminus \{\emptyset\}$

\therefore esta definida $f(z)$

Se tiene $f(z) \in B \quad \wedge \quad f(z) \in Z \quad f(z) \in B \cap Z$

Así $\{f(z)\} \subset B \cap Z$

Sea $v \in B \cap Z$. Como $v \in B \quad \exists z' \in P(\cup A) \setminus \{\emptyset\}$

tal que $v = f(z')$. Como $f(z') \in Z'$, se tiene $v \in z'$

Además $v \in Z \quad Z' \cap Z \neq \emptyset \quad \therefore z' = z$ y así.

$$v = f(z)$$

Lo anterio demuestra que $B \cap Z \subset \{f(z)\}$

$$\therefore B \cap Z = \{f(z)\}$$

□

Proposición 14. *Son equivalentes las siguientes proposiciones.*

i) *Axioma de elección*

ii) *(Principio maximal de Hausdorff)*

Todo conjunto parcialmente ordenado tiene una cadena maximal, i.e. una cadena que no está contenida propiamente en otra cadena

iii) *(Lema de Zorn) Todo conjunto parcialmente ordenado no vacío, en el cual cada cadena tiene una cota superior, tiene un elemento maximal*

iv) *(Principio del buen orden) Todo conjunto puede ser un buen orden*

Proof. i) \Rightarrow ii)

Sea (A, R) un conjunto parcialmente ordenado, por el axioma de especificación

Sea $C = \{x \in P(A) \mid \forall a, b \in x \ a < b \ \vee \ b < a\}$

$$\emptyset \in C \quad \therefore C \neq \emptyset$$

Procediendo por reducción al absurdo, suponga que A no tiene una cadena maximal.

Entonces $\forall x \in C$

$C_x = \{y \in C \mid x \subset y \wedge x \neq y\}$ Es un conjunto no vacío de C

Como hipótesis de cumple el Axioma de elección, la proposición 13 implica, tomando $X = C$, que existe $f : P(C) \setminus \{\emptyset\} \Rightarrow C$, tal que

$$f(u) \in u \quad \forall u \in P(C) \setminus \{\emptyset\} \quad \text{Se tiene así}$$

$$f(C_x) \in C_x \quad \forall x \in C$$

Sea $R_c = \{(x, y) \in C \times C \mid x \subset y\}$

i) (C, R_c) es un conjunto ordenado

ii) Considere la función

$$g : C \longleftrightarrow C$$

$$x \mapsto f(C_x)$$

Observe que

$$(x, g(x)) \in R_c$$

$$x \subset g(x) = f(C_x) \in C_x$$

Si se verifica que

iii) Toda cadena en C tiene un supremo en C

Entonces (C, R_c) satisface las hipótesis de la proposición 12, por lo cual existe $x_0 \in C$ tal que $g(x_0) = x_0$

$$\therefore f(C_{x_0}) = x_0 \quad \text{Sin embargo } f(C_{x_0}) \in C_{x_0} \therefore f(C_{x_0}) \neq x_0$$

Se tendría así una contradicción.

Por lo tanto para concluir que $i) \Rightarrow ii)$ basta probar que toda cadena en C tiene un supremo en C .

Sea N una cadena en C .

Se verificará que $\cup N$ es supremo de N en C .

Sea $t \in \cup N$, entonces existe $z \in N$ tal que $t \in z$. Como $z \in N \quad \forall N \subset C$

$\therefore t \in A$. Así $\cup N \subset A$

Sean $a, b \in \cup N$ entonces existen $u, v \in N$ tales que $a \in u \quad \wedge \quad b \in v$

Como N es una cadena en C se tiene $u \subset v \vee v \subset u$.

$\therefore a, b \in V \vee a, b \in U$. En cualquier caso como u y v son cadenas en A se tiene $a < b \vee b < a$ lo anterior muestra que $\cup N \in C$

a) Sea $w \in N$

entonces $r \in w, \quad r \in \cup N \therefore w \subset \cup N$

Así $(w, \cup N) \in R_c \quad \forall w \in N$

$\cup N$ es cota superior de N

b) Suponga que $M \in C$ satisface $(w, M) \in R_c \quad \forall w \in N$

Entonces $w \subset M \quad \forall w \in N$.

Sea $s \in \cup N$, entonces existe $m \in N$ tal que $s \in m$.

Como $m \in N \quad (m, M) \in R_c$

$\therefore m \subset M \Rightarrow s \in M \therefore \cup N$ y así $(\cup N, M) \in R_c$

a), b) muestran que $\cup N$ es supremo de N en C

iii) \Rightarrow iv) Sea X un conjunto.

Se debe probar que en X se puede definir un buen orden.

Sea

$$S = \{(A, R) \in P(X) \times P(X \times X) \mid R \text{ es un buen orden en } A\}$$

$$\rho = \{((A_1, R_1), (A_2, R_2)) \in S \times S \mid A_1 \subset A_2 \quad R_1 \subset R_2 \quad \wedge \quad [(x \in A_1 \wedge y \in A_2 \setminus A_1) \rightarrow (x, y) \in R_2]\}$$

Hecho (S, ρ) es un conjunto parcialmente ordenado no vacío en el que toda cadena tiene una cota superior.

Proof. $i)$ Sea $(A, R) \in S$

□

□

Chapter 3

Tercer Parcial

3.1 Enteros

Considere la siguiente relación en $\mathbb{N} \times \mathbb{N}$:

$$R = \{((n, m), (r, s)) \in (\mathbb{N} \times \mathbb{N}) \times (\mathbb{N} \times \mathbb{N}) \mid n + s = r + m\}$$

Lema 3.1.1. *R es una relación de equivalencia.*

Proof. Sean $n, m \in \mathbb{N}$. Note que $n + m = n + m \therefore ((n, m), (n, m)) \in R$, así R es reflexiva.

Sea $((n, m), (r, s)) \in R$, entonces $n + s = m + r$ o bien, $m + r = n + s$, así R es simétrica.

Sean $((n, m), (r, s)), ((r, s), (u, v)) \in R$, entonces se tiene que $n + s = m + r \wedge r + v = s + u$. Así

$$n + s + r + v = r + m + u + s$$

Así tenemos que $n + v = m + u$, por lo tanto $((n, m), (u, v)) \in R$. Concluyendo que R es una relación de equivalencia. \square

Definición 3.1.1. *Dada la relación de equivalencia anterior, se define el conjunto de **números enteros** denotado por \mathbb{Z} como el conjunto cociente $\mathbb{N} \times \mathbb{N}_R$.*

Los elementos de $\mathbb{N} \times \mathbb{N}$ se denominarán diferencias.

Definición 3.1.2. *Una diferencia se dice positiva si $n > m$.*

Lema 3.1.2. *Sea (n, m) una diferencia positiva. Si $(r, s) \in [(n, m)]$, entonces (r, s) también es una diferencia positiva.*

Proof. Se tiene que $n > m$, por lo tanto, existe un $p \in \mathbb{N} \setminus \{0\}$ tal que $n = m + p$. Si $(r, s) \in [(n, m)]$, entonces: $n + s = r + m$. Así $m + p + s = r + m$, por lo tanto $p + s = r$. Como $p \neq 0$, se concluye que $r > s$, luego (r, s) es positiva. \square

Lema 3.1.3. *Sea (n, m) una diferencia positiva. Entonces existe un único $p \in \mathbb{N}$ tal que $(p, 0) \in [(n, m)]$.*

Proof. Como (n, m) una diferencia positiva. Entonces existe $p \in \mathbb{N}$ tal que $n = m + p$. Como $n = n + 0$, se tiene así: $n + 0 = m + p \therefore ((n, m), (0, p)) \in R$.

Sea $q \in \mathbb{N}$ tal que $(q, 0) \in [(n, m)]$, entonces $((q, 0), (p, 0)) \in R \Rightarrow q + 0 = p + 0$, así $q = p$. \square

Definición 3.1.3. En $\mathbb{N} \times \mathbb{N}$ se define la operación binaria f , denominada **adición**, en la forma siguiente:

$$\begin{aligned} f : (\mathbb{N} \times \mathbb{N}) \times (\mathbb{N} \times \mathbb{N}) &\rightarrow \mathbb{N} \times \mathbb{N} \\ ((n, m), (r, s)) &\rightarrow (n + r, m + s) \end{aligned}$$

Se define así mismo la operación binaria g en $\mathbb{N} \times \mathbb{N}$ denominada **producto** de la forma siguiente:

$$\begin{aligned} g : (\mathbb{N} \times \mathbb{N}) \times (\mathbb{N} \times \mathbb{N}) &\rightarrow \mathbb{N} \times \mathbb{N} \\ ((n, m), (r, s)) &\rightarrow (nr + ms, mr + ns) \end{aligned}$$

$f((n, m), (r, s))$ se denotará $(n, m) + (r, s)$, y $g((n, m), (r, s))$ se denotará $(n, m)(r, s)$.

Lema 3.1.4. Sean $x, y, u, v \in \mathbb{N} \times \mathbb{N}$ tales que $(x, u) \in R \wedge (y, v) \in R$, entonces $(x + y, u + v) \in R$.

Proof. Sean $x = (x_1, x_2); y = (y_1, y_2); u = (u_1, u_2); v = (v_1, v_2)$.

Por hipótesis: $x_1 + u_2 = x_2 + u_1 \wedge y_1 + v_2 = y_2 + v_1 \dots (\lambda)$.

Se debe probar que $((x_1 + y_1, x_2 + y_2), (u_1 + v_1, u_2 + v_2)) \in R$. Pero como consecuencia de $\lambda)$ $x_1 + y_1 + u_2 + v_2 = x_2 + y_2 + u_1 + v_1$. \square

Lema 3.1.5. a. La adición en $\mathbb{N} \times \mathbb{N}$ es asociativa y conmutativa.

b. La suma de dos diferencias positivas es una diferencia positiva.

c. Sean $x, y, u \in \mathbb{N} \times \mathbb{N}$, si $(x + y, x + u) \in R$, entonces $(y, u) \in R$.

Proof. a. Sean $(n, m), (r, s), (a, b)$ elementos de $\mathbb{N} \times \mathbb{N}$.

$$(n, m) + (r, s) = (n + r, m + s) = (r + n, s + m) = (r, s) + (n, m).$$

Así mismo:

$$\begin{aligned} [(n, m) + (r, s)] + (a, b) &= (n + r, m + s) + (a, b) = ((n + r) + a, (m + s) + b) \\ &= (n + (r + a), (m + (s + b))) = (n, m) + (r + a, s + b) \\ &= (n, m) + [(r, s) + (a, b)] \end{aligned}$$

b. Sean $(n, m), (r, s)$ diferencias positivas. Entonces $n > m \wedge r > s$ Así, existen $q, p \in \mathbb{N}$ tales que: $n = m + p$, y $r = s + q$.

Así, $n + r = m + s + p + q$, como $q \neq 0 \wedge p \neq 0$. se tiene que $q + p \neq 0$, así $n + r > m + s$. Se tiene entonces que $(n, m) + (r, s)$ es una diferencia positiva.

c. Suponga que $(x + y, x + u) \in R$. Sean $x = (x_1, x_2); y = (y_1, y_2); u = (u_1, u_2)$. Entonces $x_1 + y_1 + x_2 + u_2 = x_2 + y_2 + x_1 + u_1$. Así $y_1 + u_2 = u_1 + y_2$, i.e., $(y, u) \in R$.

□

Lema 3.1.6. Sean x, y, u, v diferencias. Si $(x, u) \in R \wedge (y, v) \in R$ entonces $(xy, uv) \in R$.

Proof. HAY QUE HACERLA.

□

Lema 3.1.7. a. El producto de diferencias es asociativo y conmutativo.

b. Si $x, y, u \in \mathbb{N} \times \mathbb{N}$, entonces $(x + y)u = xu + yu$.

c. El producto de dos diferencias positivas es una diferencia positiva.

d. Si $x, y, u \in \mathbb{N} \times \mathbb{N}$ satisfacen $(xu, yu) \in R$ y además, siendo $u = (u_1, u_2)$, con $u_1 \neq u_2$, entonces $(x, y) \in R$.

Proof. HAY QUE HACERLA.

□

Definición 3.1.4. Un entero $[(n, m)]$ se dice positivo si existen $(p, q) \in [(n, m)]$ tal que (p, q) es positivo; i.e. tal que $p > q$.

Observación. Si $[(n, m)]$ es un entero positivo, y $(r, s) \in [(n, m)]$, entonces (r, s) es una diferencia positiva.

Definición 3.1.5. El conjunto de los enteros positivos se denotará por \mathbb{Z}^+ . En notación de construcción de conjuntos:

$$\mathbb{Z}^+ = \{x \in \mathbb{Z} \mid \exists (n, m) \in x, n > m\}$$

Considere la función $f : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$

$$([x], [y]) \rightarrow ([x + y])$$

Se debe verificar que f está bien definida. Suponga que $[x] = [u]$, y $[y] = [v]$. Entonces $(x, u) \in R \wedge (y, v) \in R$. El lema 3.1.4 implica que $(x + y, u + v) \in R$, es decir, $[x + y] = [u + v]$.

Definición 3.1.6. A la operación binaria f en \mathbb{Z} se le denomina adición y $f([x], [y])$ se denotará por $[x] + [y]$.

Proposición 20. a. La adición en \mathbb{Z} es asociativa y conmutativa.

b. Dados $a, b, c \in \mathbb{Z}$, si $a + c = b + c$ entonces $a = b$.

c. Si $a, b \in \mathbb{Z}^+$, entonces $a + b \in \mathbb{Z}^+$.

Proof. Sean $a, b, c \in \mathbb{Z}$. Existen $x, y, z \in \mathbb{N} \times \mathbb{N}$ tales que $a = [x]$, $b = [y]$, $c = [z]$.

- a. Se tiene del lema 3.1.5 $a + b = [x + y] = [y + x] = b + a$.

Así mismo.

$$\begin{aligned}
 (a + b) + c &= [x + y] + [z] \\
 &= [(x + y) + z] \\
 &= [x + (y + z)] \\
 &= [x] + [y + z] \\
 &= a + (b + c)
 \end{aligned}$$

Así $+$ es asociativa y conmutativa.

- b. Se tiene por hipótesis $[x] + [z] = [y] + [z]$, i.e., $[x + z] = [y + z] \therefore (x + z, y + z) \in R$. El lema 3.1.3 implica que $(x, y) \in R \therefore [x] = [y]$.

- c. Sean $a, b \in \mathbb{Z}^+$ El lema 3.1.5 implica que $x + y$ es una diferencia positiva, así $[x + y] \in \mathbb{Z}^+$.

□

Proposición 21. Sean $a, b, c \in \mathbb{Z}$, entonces existe un único $c \in \mathbb{Z}$ tal que $a + c = b$.

Proof. Existen x, y diferencias, con $x = (x_1, x_2), y = (y_1, y_2)$ tales que $a = [x] \wedge b = [y]$, así $a = b \vee a \neq b$.

i) Si $a = b$. Sea $c = [(0, 0)]$, entonces: $a + c = [(x_1, x_2)] + [(0, 0)] = [(x_1, x_2)] = a = b$.

ii) Si $a \neq b$, tenemos que $((x_1, x_2), (y_1, y_2)) \notin R$. Así

$$x_1 + y_2 < x_2 + y_1 \quad \vee \quad x_1 + y_2 > x_2 + y_1$$

Sin pérdida de la generalidad asumamos que: $x_1 + y_2 < x_2 + y_1$. Así, existe $z \in \mathbb{N}$ tal que $x_1 + y_2 + z = x_2 + y_1$, Así $a + [(0, z)] = a + c = b$, con $c = [(0, z)]$. Suponga que existe d tal que $a + d = b$, entonces $a + d = a + c$, pero por proposición anterior $c = d$, así d es único. □

Observación. Veamos que $[(0, 0)] + a = a$, así denotaremos a $[(0, 0)]$ como 0_z y se denomina neutro aditivo de \mathbb{Z} .

Considere la función:

$$\begin{aligned}
 g : \mathbb{Z} \times \mathbb{Z} &\rightarrow \mathbb{Z} \\
 ([x], [y]) &\rightarrow [xy]
 \end{aligned}$$

Se verificará que g está bien definida:

Si $[x] = [u] \wedge [y] = [v]$ entonces $(x, u), (y, v) \in R$. El lema 3.1.6 implica que $(xy, uv) \in R$ así, $[xy] = [uv]$.

Definición 3.1.7. g es una operación binaria en \mathbb{Z} que se denomina **producto** en \mathbb{Z} y $g(a, b)$ se denota ab .

Proposición 22. a. El producto es asociativo y conmutativo.

b. El producto de dos enteros positivos es un entero positivo.

c. Sean $a, b, c \in \mathbb{Z}$ tales que $ab = ac$ con $a \neq 0_q$ entonces $b = c$.

Proof. La demostración se sigue inmediatamente del lema 3.1.7 □

Definición 3.1.8. Al c descrito en la proposición 21, tal que $a + c = 0_q$ se denomina **inverso aditivo** de a y se denota $-a$.

Dados $a, b \in \mathbb{Z}$, $a + (-b)$ se denotará $a - b$.

Proposición 23. Sean $a, b, c \in \mathbb{Z}$, entonces $a(b + c) = ab + ac$.

Proof. La demostración se sigue inmediatamente del lema 3.1.7 □

Sean $\mathbb{Z}^0 = \{(n, 0) \in \mathbb{Z} \mid n \in \mathbb{N}\}$, y $\mathbb{Z}_0 = \{(0, n) \in \mathbb{Z} \mid n \in \mathbb{N} \setminus \{0\}\}$.

Proposición 24. $\mathbb{Z}^0 \cap \mathbb{Z}_0 = \emptyset \wedge \mathbb{Z}^0 \cup \mathbb{Z}_0 = \mathbb{Z}$.

Proof. Suponga que $\mathbb{Z}^0 \cap \mathbb{Z}_0 \neq \emptyset$, es decir $[(p, q)] \in \mathbb{Z}^0 \cap \mathbb{Z}_0$. Así se tiene que $\exists n, m \in \mathbb{N}$, $m \neq 0$ tales que $((n, 0), (0, m)) \in R$. Así $n + m = 0$. La proposición ?? implica que $n = 0 \wedge m = 0$. Se tiene así que $m \neq 0 \wedge m = 0$, lo cual no puede suceder, por lo tanto $\mathbb{Z}^0 \cap \mathbb{Z}_0 = \emptyset$.

Sea ahora $[(r, s)] \in \mathbb{Z}$. Se tiene $r \geq s \vee r < s$.

Si $r \geq s$, entonces $\exists p \in \mathbb{N}$ tal que $r = s + p$, así $((r, s), (p, 0)) \in R$. Lo cual implica que $[(r, s)] \in \mathbb{Z}^0$.

Si $r < s$, entonces $\exists q \in \mathbb{N} \setminus \{0\}$ tal que $s = r + q$, así $((r, s), (0, q)) \in R$. Así $[(r, s)] \in \mathbb{Z}_0$. Por lo cual se concluye que $\mathbb{Z}^0 \cup \mathbb{Z}_0 = \mathbb{Z}$. □

Considere

$$f : \mathbb{Z}^0 \rightarrow \mathbb{Z}^0$$

$$[(n, 0)] \rightarrow [(n^+, 0)]$$

Si $[(n, 0)] = [(m, 0)]$ entonces $((n, 0), (m, 0)) \in R$, así $n = m \Rightarrow n^+ = m^+$ entonces $[(n^+, 0)] = [(m^+, 0)]$, así f es independiente de la elección del representante de clase.

Proposición 25. $(\mathbb{Z}^0, f, 0_z)$ es un sistema de Peano.

Proof. a. $0_z \in \mathbb{Z}^0$.

b. Sean m, n tales que $f([(n, 0)]) = f([(m, 0)])$, así $[n^+, 0] = [m^+, 0]$, $n^+ = m^+ \therefore n = m$. Así f es inyectiva.

c. Se verificará que $f(\mathbb{Z}^+) = \mathbb{Z}^0 \setminus \{0_z\}$.

Sea $a \in f(\mathbb{Z}^+)$, entonces existe $[(n, 0)] \in \mathbb{Z}^0$ tal que $a = f([(n, 0)])$ así $a = [(n^+, 0)]$. Como $n^+ \neq 0$ se tiene que $a \neq 0_z$. Considere ahora $b \in \mathbb{Z}^0 \setminus \{0_z\}$, entonces $\exists m \in \mathbb{N} \setminus \{0\}$ tal que $b = [(m, 0)]$, como $m \neq 0$, entonces $\exists r \in \mathbb{N}$ tal que $r^+ = m$. Así, $f([(r, 0)]) = [(m^+, 0)]$ así $b \in f(\mathbb{Z}^0)$. Por lo cual $f(\mathbb{Z}^0) = \mathbb{Z} \setminus \{0\}$.

d. Sea $M \subset \mathbb{Z}^0$ tal que $[(0,0)] \in M \wedge f(M) = M \setminus \{0\}$. Se debe probar que $M = \mathbb{Z}^0$.

Sea $K = \{n \in \mathbb{N} \mid [(0,n)] \in M\}$.

Veamos que $0 \in K$.

Suponga que $n \in K$, entonces $[(n,0)] \in M$. Como $f(M) \subset M$, se tiene $[(n^+,0)] \in M$, así $n^+ \in K$, por lo cual $K = \mathbb{N}$, así $\mathbb{Z}^0 \subset M \Rightarrow \mathbb{Z}^0 = M$.

□

Sea A un conjunto:

$$A^1 = A; \quad A^2 = A \times A; \dots$$

En general A^n denota a A^{n-1} donde $n \in \mathbb{N} \setminus \{0,1\}$.

Definición 3.1.9. Dado $n \in \mathbb{N} \setminus \{0\}$. Una **operación** en A es una función $f : A^n \rightarrow A$.

Definición 3.1.10. Una **relación** en A es un subconjunto de $A^n \times A$.

Definición 3.1.11. Si $f : A^n \rightarrow A$ es una operación en A , se dirá que n es la característica de f . Así mismo, si $R \subset A^n \times A$ es una relación en A , se dirá que n es la característica de R .

Definición 3.1.12. Se dice que A tiene una **estructura algebraica**, si en A , están definidas f_1, \dots, f_m operaciones, R_1, \dots, R_s relaciones, y si se definen además a_1, \dots, a_r elementos, siendo así la estructura algebraica la $1 + m + s + r$ -ada $(A; f_1, \dots, f_m; R_1, \dots, R_s; a_1, \dots, a_r)$. Dos estructuras algebraicas A, A' se dicen del mismo tipo si tienen la misma cantidad de operaciones, relaciones, y elementos.

Definición 3.1.13. Considere dos estructuras algebraicas del mismo tipo A, A' . Una función $f : A \rightarrow A'$ se dice un **morfismo** si:

a. f preserva operaciones, es decir:

$$f(f_i(x_i, \dots, x_{w_i})) = f_i(f(x_1), \dots, f(x_{w_i})) \quad \forall i \in \{1, \dots, m\} \wedge w_i = \text{car } f_i$$

b. f preserva relaciones.

c. $f(a_i) = a'_i \quad \forall i \in \{1, \dots, r\}$

Si f es inyectiva, f se denomina **monomorfismo**.

Si f es suprayectiva, f se denomina **epimorfismo**.

Si f es biyectiva, f se denomina **isomorfismo**.

Proposición 26 (Teorema de recurrencia). Considere un sistema de Peano (X, f, x_0) . Sean A un conjunto, y $G : A \rightarrow A$ una función, y $a \in A$, entonces existe una única función $F : X \rightarrow A$ que satisfice:

$$F(f(x)) = G(F(x)) \quad \forall x \in X$$

$$F(x_0) = a$$

Proof. HAY QUE HACERLA.

□

Proposición 27. *Cualesquiera dos sistemas de Peano son isomorfos.*

Proof. Sean $(X, f, x_0), (X', f, x'_0)$ dos sistemas de Peano.

Considerando el sistema de Peano (X, f, x_0) , la proposición 26 implica que existe $F : X \rightarrow X'$ tal que:

$$\begin{aligned} F \circ f &= f' \circ F \\ F(x_0) &= x'_0 \end{aligned}$$

Nuevamente, por la proposición 26, se verifica que existe $F' : X' \rightarrow X$, tal que:

$$\begin{aligned} F' \circ f' &= f \circ F' \\ F'(x'_0) &= x_0 \end{aligned}$$

Veamos que:

$$\begin{aligned} (F' \circ F) \circ f &= F' \circ (F \circ f) \\ &= (F' \circ f') \circ F \\ &= (f \circ F') \circ F \\ &= f \circ (F' \circ F) \end{aligned}$$

Se tiene así que $F' \circ F : X \rightarrow X$ satisface $(F' \circ F) \circ f = f \circ (F' \circ F)$. Además $F' \circ F(x_0) = x_0$. Observe que la identidad $I : X \rightarrow X$ satisface:

$$I \circ f = f \circ I \wedge I(x_0) = x_0$$

La proposición 26, considerando el sistema de Peano (X, f, x_0) afirma que existe una única función $H : X \rightarrow X$ tal que:

$$H(x_0) = x_0 \quad H \circ f = f \circ H$$

Por lo tanto $F' \circ F = I$. Se verifica análogamente que $F \circ F'$ es la identidad en X' . Así F es biyectiva. Además F preserva operaciones y $F(x_0) = x'_0$. Por lo cual es un isomorfismo. \square

Problema 3.1.1. $g : \mathbb{N} \rightarrow \mathbb{Z}^0, n \rightarrow [(n, 0)]$ es un isomorfismo entre $(\mathbb{Z}^0, f, 0_z)$ y $(\mathbb{N}, S, 0)$. g es así mismo un isomorfismo entre las estructuras algebraicas $(\mathbb{Z}^0, +, \cdot, 0_z, 1_z)$ y $(\mathbb{N}, +, \cdot, 0, 1)$.

Problema 3.1.2. Sea $x \in \mathbb{Z}$, demuestre que se cumple una única de las siguientes afirmaciones:

$$x \in \mathbb{Z}^+ \quad x = 0_z \quad -x \in \mathbb{Z}^+$$

Proposición 28. Sea $x \in \mathbb{Z} \setminus \{0_z\}$, entonces $xx \in \mathbb{Z}^+$.

Proof. Por el ejercicio 3.1.2 anterior, se tiene $x \neq 0_z \vee x \in \mathbb{Z}^+ \vee -x \in \mathbb{Z}^+$. i) Si $x \in \mathbb{Z}^+$, entonces la proposición 30 implica que $xx \in \mathbb{Z}^+$.

ii) Suponga ahora que $-x \in \mathbb{Z}^+$. Así $(-x)(-x) \in \mathbb{Z}^+$. Se tiene $\mathbb{Z}^0 \cup \mathbb{Z}_0 = \mathbb{Z}$ así $x \in \mathbb{Z}^0 \vee x \in \mathbb{Z}_0$.

- a) Si $x \in \mathbb{Z}^0 \exists n \in \mathbb{N}$ tal que $x = [(n, 0)] \therefore xx = [(n, 0)(n, 0)] = [(nn, 0)]$. Por otra parte $-x = [(0, n)]$, así $(-x)(-x) = [(0, n)(0, n)] = [(nn, 0)] = xx$.
- b) Si $x \in \mathbb{Z}_0 \exists n \in \mathbb{N}$ tal que $x = [(0, m)] \therefore xx = [(0, m)(0, m)] = [(mm, 0)]$ Así mismo $(-x)(-x) = [(m, 0)(m, 0)] = [(mm, 0)] = xx \therefore xx \in \mathbb{Z}^+$.

□

Resumen Si $x, y, z \in \mathbb{Z}$:

- $x + y = y + x$
- $(x + y) + z = x + (y + z)$
- $0_z + x = x$
- $\exists (-x) \in \mathbb{Z}$ tal que $(x) + (-x) = 0_z$
- $xy = yx$
- $(xy)z = x(yz)$
- $1_z x = x$
- $x(y + z) = xy + xz$

Las 8 propiedades anteriores permiten afirmar que $(\mathbb{Z}, +, \cdot, 0_z, 1_z)$ es un anillo conmutativo con identidad.

Además:

- Si $xy \in \mathbb{Z}^+$, entonces $x + y \in \mathbb{Z}^+ \wedge xy \in \mathbb{Z}^+$.
- $1_z \neq 0_z$ ya que $((1, 0), (0, 0)) \notin R$ i.e. $[(1, 0)] \neq [(0, 0)]$.
- Si $z \neq 0_z$ y $yx = yz$ se tiene $x = y$.

3.2 Racionales

Definición 3.2.1. Sean $a, b \in \mathbb{Z}$, $b \neq 0_z$, la pareja (a, b) se denominará **cociente**. Al conjunto $\mathbb{Z} \times \mathbb{Z} \setminus \{0_z\}$.

Sea $T = \{((a, b), (c, d)) \in (\mathbb{Z} \times \mathbb{Z} \setminus \{0_z\}) \times (\mathbb{Z} \times \mathbb{Z} \setminus \{0_z\}) \mid ad = bc\}$

Se verificará que T es una relación de equivalencia.

- $((a, b), (a, b)) \in T$, ya que $ab = ab$, así T es reflexiva.
- Suponga que $((a, b), (c, d)) \in T$ entonces: $ad = bc \wedge bc = ac$, así $((a, b), (c, d)) \in T$. Así T es simétrica.
- Suponga que $((a, b), (c, d)) \in T$ y que $((c, d), (e, f)) \in T$ entonces: $ad = bc$ y $cf = de \dots (\sigma)$. Así $(ad)(cf) = (bc)(de)$. Además $b \neq 0_z \wedge d \neq 0_z$, lo cual implica que $bd \neq 0_z$. Si $c \neq 0_z$, se tiene $dc \neq 0_z$, y así de λ , se tendría que $af = be$. Por otra parte, si $c = 0_z$, se tendría

de σ) que $ad = 0_z$, por lo cual como $d \neq 0_z$, $a = 0_z$.

Así mismo de σ) $de \neq 0_z$, como $d \neq 0$, $e = 0$. Por ello $af = be$. De ésta forma se concluye que $((a, b), (e, f)) \in T$, así T es transitiva. Así T es una relación de equivalencia.

Definición 3.2.2. $\mathbb{Z} \times \mathbb{Z} \setminus \{0_z\} / T$ se denomina conjunto de **números racionales** y se denotará por \mathbb{Q} .

Considere las funciones:

$$\begin{aligned} f : (\mathbb{Z} \times (\mathbb{Z} \setminus \{0_z\})) \times (\mathbb{Z} \times (\mathbb{Z} \setminus \{0_z\})) &\rightarrow \mathbb{Z} \times (\mathbb{Z} \setminus \{0_z\}) \\ ((a, b), (c, d)) &\mapsto (ad + bc, bd) \\ g : (\mathbb{Z} \times (\mathbb{Z} \setminus \{0_z\})) \times (\mathbb{Z} \times (\mathbb{Z} \setminus \{0_z\})) &\rightarrow \mathbb{Z} \times (\mathbb{Z} \setminus \{0_z\}) \\ ((a, b), (c, d)) &\mapsto (ac, bd) \end{aligned}$$

Observe que en la definición de f y g se tiene que $b \neq 0_z$ y $d \neq 0_z$, entonces $bd \neq 0_z$.

f y g son operaciones binarias en el conjunto de cocientes, que se denominan respectivamente adición y producto. Denotados de la forma usual.

Lema 3.2.1. Sean x, y, u, v cocientes, $(x, u), (y, v) \in T$. Entonces: $(x + y, u + v) \in T \quad \wedge \quad (xy, uv) \in T$.

Proof. Sean $x_1, x_2 \in \mathbb{Z}$, $x_2 \neq 0_z$, los componentes de x i.e. $x = (x_1, x_2)$. Análogamente se tiene $y = (y_1, y_2)$, $u = (u_1, u_2)$, y $v = (v_1, v_2)$.

Por hipótesis se tiene que $x_1 u_2 = x_2 u_1$ y que $y_1 v_2 = y_2 v_1 \dots (\lambda)$

Se tiene $x + y = (x_1 y_2 + y_2 x_1, x_2 y_2)$; $u + v = (u_1 v_2 + v_2 u_1, u_2 v_2)$. Así mismo $xy = (x_1 y_1, x_2 y_2)$ y $uv = (u_1 v_1, u_2 v_2)$.

Se debe probar que

$$(x_1 y_2 + x_2 y_1) u_2 v_2 = x_2 y_2 (u_1 v_2 + u_2 v_1) \quad (3.1)$$

y también

$$x_1 y_1 u_2 v_2 = x_2 y_2 u_1 v_1 \quad (3.2)$$

De λ) se tiene que

$$(x_1 y_2 + x_2 y_1) u_2 v_2 = x_1 y_2 u_2 v_2 + x_2 y_1 u_2 v_2 = x_2 u_1 y_2 v_2 + y_2 v_1 x_2 u_2 = (u_1 v_2 + v_1 u_2) x_2 y_2$$

Con lo cual se justifica (3.1).

Así mismo se tiene de λ):

$$x_1 y_1 u_2 v_2 = x_2 u_1 y_2 v_1$$

lo cual justifica a (3.2) □

El lema anterior muestra que las siguientes relaciones son operaciones binarias en \mathbb{Q} .

Definición 3.2.3.

$$\begin{aligned} F &= \{([x], [y], [x + y]) \in (\mathbb{Q} \times \mathbb{Q}) \times \mathbb{Q}\} \\ G &= \{([x], [y], [xy]) \in (\mathbb{Q} \times \mathbb{Q}) \times \mathbb{Q}\} \end{aligned}$$

Se denominan respectivamente *adición* y *producto* en \mathbb{Q} .

Así mismo, $0_q = [(0_z, 1_z)]$, $1_q = [(1_z, 1_z)]$ se denominan *neutro aditivo* y *neutro multiplicativo* respectivamente.

Proposición. Sea $\mathbb{Q}' = \{[(x_1, x_2)] \in \mathbb{Q} \mid x_2 = 1_z\}$. $(\mathbb{Z}, +, \cdot, 1_z, 0_z)$ y $(\mathbb{Q}', +, \cdot, 1_q, 0_q)$ son isomorfas.

Proof. Considere la función:

$$\begin{aligned} h : \mathbb{Z} &\rightarrow \mathbb{Q}' \\ x &\mapsto [(x, 1_z)] \end{aligned}$$

Sean $x, y \in \mathbb{Z}$ tales que $h(x) = h(y)$, entonces $[(x, 1_z)] = [(y, 1_z)]$.

Así, $x1_z = 1_z y$, $x = y$, entonces h es inyectiva.

Sea $u \in \mathbb{Q}'$, entonces existe $x \in \mathbb{Z}$ tal que $u = [(x, 1_z)] \wedge u = h(x)$, lo cual muestra que h es suprayectiva.

Se tiene además que si $u, v \in \mathbb{Z}$, entonces:

$$h(u + v) = [(u + v, 1_z)] = [(u, 1_z)] + [(v, 1_z)] = h(u) + h(v)$$

Así mismo:

$$h(uv) = [(uv, 1_z)] = [(u, 1_z)][(v, 1_z)] = h(u)h(v)$$

Finalmente observe que:

$$h(1_z) = [(1_z, 1_z)] = 1_q$$

$$h(0_z) = [(0_z, 1_z)] = 0_q$$

h es en consecuencia un isomorfismo. □

Proposición 29. Sean $x, y, x \in \mathbb{Q}$ entonces:

$$\begin{array}{lll} x + y = y + x & (x + y) + z = x + (y + z) & x + 0_q = x \\ \exists u \in \mathbb{Q} \mid x + u = 0_q & xy = yx & (xy)z = x(yz) \\ x1_q = x & \text{si } x \neq 0_q \quad \exists v \in \mathbb{Q} \mid xv = 1_q & (x + y)z = xz + yz \end{array}$$

Observación. a. Sea $a \in \mathbb{Z}$, entonces $0_z = a0_z$.

b. $(-1_z)a = -a \forall a \in \mathbb{Z}$.

Definición 3.2.4. Un cociente (a, b) se dice **positivo** si $ab \in \mathbb{Z}^+$.

Lema 3.2.2. Sean x, y cocientes, x positivo y $[x] = [y]$, entonces y es positivo.

Proof. Sea $x = (a, b)$, $y = (c, d)$.

Por hipótesis $ab \in \mathbb{Z}^+$. Se probará que $cd \in \mathbb{Z}^+$.

Como $[x] = [y]$, se tiene

$$ad = bc \therefore (ab)(cd) = (ad)(bc) = (ad)(ad)$$

La proposición (28) implica que $(ad)(ad) \in \mathbb{Z}^+$

Se tiene así que $(ab)(cd) \in \mathbb{Z}^+$.

Para concluir la prueba, basta demostrar que si $u, v \in \mathbb{Z}$, tales que $u \in \mathbb{Z}^+$, entonces $v \in \mathbb{Z}^+$.

Suponga entonces que $u, v \in \mathbb{Z}$, $u, uv \in \mathbb{Z}^+$.

Observe que $v \neq 0_z$, ya que en caso contrario $uv = 0_z$.

Observe de la misma forma que $-v \notin \mathbb{Z}^+$, ya que si ésto no ocurriese:

$$\begin{aligned} u(-v) &\in \mathbb{Z}^+ \quad \text{pero} \\ u(-v) &= u[(-1_z)v] = (-1_z)(uv) = -(uv) \end{aligned}$$

Por lo cual $-(uv) \in \mathbb{Z}^+$, lo cual contradice el que $uv \in \mathbb{Z}^+$ por lo tanto $v \in \mathbb{Z}^+$. \square

Definición 3.2.5. Sea $x \in \mathbb{Q}$. Se dice que x es positivo si existe u cociente positivo y $u \in x$. se denotará \mathbb{Q}^+ al conjunto de los racionales positivos.

Observación. $1_q \neq 0_q$ ya que lo contrario implicaría que $1_z = 0_z$.

Proposición 30. i) Sean $x, y \in \mathbb{Q}^+$, entonces $x + y \in \mathbb{Q}^+$, y $xy \in \mathbb{Q}^+$.

ii) Dado $x \in \mathbb{Q}$ se cumple una única de las siguientes tres afirmaciones:

$$x = 0_q \qquad x \in \mathbb{Q}^+ \qquad -x \in \mathbb{Q}^+$$

Proof. i) Sean $[(a, b)] = x$, $[(c, d)] = y$. Por hipótesis $ab \in \mathbb{Z}^+ \wedge cd \in \mathbb{Z}^+$.

$$x + y = [(ad + bc, bd)] \qquad \wedge \qquad xy = [(ac, bd)]$$

Observe que:

$$(ad + bc)bd = abdd + bbcd$$

Como $b \neq 0_z \wedge d \neq 0_z$, se tiene $bb \in \mathbb{Z}^+ \wedge dd \in \mathbb{Z}^+$.

Así mismo, como $ab \in \mathbb{Z}^+ \wedge cd \in \mathbb{Z}^+$

$$(ad + bc)bd \in \mathbb{Z}^+ \qquad \wedge \qquad acbd \in \mathbb{Z}^+$$

Así $x + y \in \mathbb{Q}^+$ y $xy \in \mathbb{Q}^+$.

ii) Sea $[(a, b)] = x$.

Si $x \neq 0_1$, entonces $a \neq 0_z$. Como $a \neq 0_z \wedge b \neq 0_z$, se tienen las siguientes posibilidades:

$$\begin{aligned} \text{i)} \quad & a \in \mathbb{Z}^+ \wedge b \in \mathbb{Z}^+ \\ \text{ii)} \quad & -a \in \mathbb{Z}^+ \wedge -b \in \mathbb{Z}^+ \\ \text{iii)} \quad & (a \in \mathbb{Z}^+ \wedge -b \in \mathbb{Z}^+) \vee (-a \in \mathbb{Z}^+ \wedge b \in \mathbb{Z}^+) \end{aligned}$$

En el caso *i*) se tendría $ab \in \mathbb{Z}^+, x \in \mathbb{Q}^+$.

En el caso *ii*) se tendría $(-a)(-b) \in \mathbb{Z}^+$; observe que

$$(-a)(-b) = (-1)a(-b) = (-1)(-1)ab = (-1)(-ab) = ab$$

$x \in \mathbb{Q}^+$.

Finalmente considere el caso *iii*). Si $a \in \mathbb{Z}^+ \wedge -b \in \mathbb{Z}^+$, se tiene: $(-a)b = a(-b) \in \mathbb{Z}^+$.

Además $-x = -[(a, b)] = [(-a, b)]$, ya que:

$$[(a, b)] + [(-a, b)] = [(a, b) + (-a, b)] = [(0_z, bb)] = 0_q$$

Así $-x \in \mathbb{Q}^+$. De la misma forma se verifica que si $-a \in \mathbb{Z}^+ \wedge b \in \mathbb{Z}^+$, se tiene que $-x \in \mathbb{Q}^+$. Se ha probado así que si $x \neq 0_q$, se tiene: $x \in \mathbb{Q}^+ \vee -x \in \mathbb{Q}^+$.

Supóngase que $x \in \mathbb{Q}^+ \wedge -x \in \mathbb{Q}^+$, entonces $ab \in \mathbb{Z}^+ \wedge -ab \in \mathbb{Z}^+$ lo cual contradice la tricotomía en \mathbb{Z}^+ . Tampoco ocurre que $x \in \mathbb{Q}^+ \wedge x = 0_q$, ya que se tendría que $0_z \in \mathbb{Z}^+$. \square

Observación. Dados $x, y \in \mathbb{Q}$ $x + (-y)$ se denotará $x - y$. Sea $\mathfrak{M} = \{(x, y) \in \mathbb{Q} \times \mathbb{Q} \mid x - y \in \mathbb{Q}^+\}$. $(x, y) \in \mathfrak{M}$ se denotará $x > y$.

Proposición 31. *i) $\forall x \in \mathbb{Q}^+$ sii $x > 0_q$.*

ii) Dados $x, y \in \mathbb{Q}$, se cumple una única de las siguientes afirmaciones:

$$x = y$$

$$x > y$$

$$x < y$$

iii) Si $x, y, z \in \mathbb{Q}$, $x > y$, si y sólo si $x + z > y + z$. Si, además $z \in \mathbb{Q}^+$, entonces $x > y$ si y sólo si $xz > yz$.

Proof. *i)* Son equivalentes $x \in \mathbb{Q}^+, x - 0_q \in \mathbb{Q}^+, x > 0_q$.

ii) Por la proposición (30) se cumple una única de las siguientes afirmaciones:

$$x - y = 0_q$$

$$x - y \in \mathbb{Q}^+$$

$$-(x - y) \in \mathbb{Q}^+$$

es decir, se cumple alguna única de las siguientes afirmaciones:

$$x = y$$

$$x > y$$

$$x < y$$

iii) Son equivalentes:

$$\begin{array}{llll} x > y & \Leftrightarrow & x - y \in \mathbb{Q}^+ & \Leftrightarrow & x - y + 0_q \in \mathbb{Q}^+ \\ x - y + (z - z) \in \mathbb{Q}^+ & \Leftrightarrow & (x + z) - (y + z) \in \mathbb{Q}^+ & \Leftrightarrow & x + z > y + z \end{array}$$

Así mismo son equivalentes:

$$\begin{array}{llll} x > y & \Leftrightarrow & x - y \in \mathbb{Q}^+ & \Leftrightarrow & (x - y)z \in \mathbb{Q}^+ \\ xz - yz \in \mathbb{Q}^+ & \Leftrightarrow & xz > yz & & \end{array}$$

□

Notación. Sea $z \in \mathbb{Q} \setminus \{0_q\}$. La proposición (29) implica que existe $u \in \mathbb{Q}$ tal que $zu = 1_q$. u se denomina **inverso multiplicativo** de z , y se denotará por el símbolo z^{-1} .

Observación. Si $z \in \mathbb{Q}^+$ entonces $z^{-1} \in \mathbb{Q}^+$, ya que $zz^{-1} = 1_q \in \mathbb{Q}^+$.

Se ha probado previamente que \mathbb{Q}' y \mathbb{Z} (como anillos) son estructuras algebraicas isomorfas. Dado $n \in \mathbb{Z}$, denotaremos a $h(n)$ como n_q . Los elementos de \mathbb{Q}' se denominarán **racionales enteros**.

Observación. Todo racional puede ser escrito en términos de racionales enteros.

Ya que h es un isomorfismo, sea $x \in \mathbb{Q}$, $x = [(a, b)]$,

$$[(a, 1_z)][(1_z, b)] = [(a, 1_z)][(b, 1_z)]^{-1} = ab^{-1}$$

Notación. $a_q b_q^{-1}$ se escribirá en la forma $\frac{a_q}{b_q}$.

Dados $x, y \in \mathbb{Q}$, si $x > y \vee x = y$, ello se escribirá de la forma $x \geq y$.

Problema 3.2.1. i) Sean $x, y \in \mathbb{Q}^+$. Verifique que existen a_q, b_q, c_q, d_q racionales enteros positivos tales que:

$$x = \frac{a_q}{b_q} \qquad y = \frac{c_q}{d_q}$$

ii) Sean $x, y \in \mathbb{Q}$. Con $x = \frac{a_q}{b_q}$, $y = \frac{c_q}{d_q}$. Verifique que:

$$x + y = \frac{a_q d_q + c_q b_q}{b_q d_q} \qquad xy = \frac{a_q c_q}{b_q d_q}$$

iii) Sean a_q, b_q racionales enteros positivos, demuestre que $a_q b_q$ es un racional entero positivo, y $a_q b_q \geq 1_q$.

Observación. 1_q y 0_q son el mismo objeto ya sea en la definición del elemento neutro, o como racionales enteros.

Proposición 32 (Propiedad arquimedean). Sean $r, s \in \mathbb{Q}^+$, entonces existe un racional entero n_q tal que $s < n_q r$.

Proof. Existen a_q, b_q, c_q, d_q racionales enteros, tales que:

$$r = \frac{a_q}{b_q} \qquad s = \frac{c_q}{d_q}$$

De acuerdo con el ejercicio previo, se puede asumir que $a_q, b_q, c_q, d_q \in \mathbb{Q}^+$.

Observe que son equivalentes las afirmaciones:

$$s < n_q r \qquad n_q r - s \in \mathbb{Q}^+ \qquad \frac{n_1 a_q}{b_q} - \frac{c_q}{d_q} \in \mathbb{Q}^+$$

Por el ejercicio anterior, se tiene también que $b_q d_q \in \mathbb{Q}^+$. En general, se tiene que:

$$\frac{u_q}{v_q} \in \mathbb{Q}^+ \wedge v_q \in \mathbb{Q}^+ \Rightarrow u_q \in \mathbb{Q}^+$$

Así $s < n_q r$ es equivalente a $n_q a_q d_q - c_q b_q \in \mathbb{Q}^+$.

Basta entonces demostrar que existe n_q racional entero tal que $n_q a_q d_q > c_q b_q$.

Sea $n_q = 2_q c_q b_q$, entonces n_q es un racional entero positivo. Observe que $1_q > 0_1$. De la proposición (31) se tiene que $1_q + 1_q = 2_q > 0_q + 1_q = 1_q$. Además, como $c_q b_q \in \mathbb{Q}^+$, se tiene que:

$$n_q = 2_q c_q b_q > 1_q c_q b_q = c_q b_q$$

Además $a_q d_q \geq 1_q$, por lo cual $n_q a_q d_q \geq n_q$. Por transitividad

$$n_q a_q d_q > c_q b_q$$

Así $s < n_q r$.

3.3 Los Números Reales

Definición 3.3.1. Sea $x \in \mathbb{Q}$. Se define el valor absoluto de x , denotado por $|x|$, como:

$$|x| = \begin{cases} x & \text{si } x \in \mathbb{Q}^+ \cup \{0_q\} \\ -x & \text{si } x \notin \mathbb{Q}^+ \cup \{0_q\} \end{cases}$$

Problema 3.3.1. Demuestre que si $x, y \in \mathbb{Q}$

$$i) |x| \geq 0_q \quad ii) |xy| = |x||y| \quad iii) |x + y| \leq |x| + |y| \quad iv) |x| - |y| \leq |x - y|$$

Definición 3.3.2. Sea A un conjunto. Una **sucesión** en A es una función de \mathbb{N} en A . Para cada $n \in \mathbb{N}$, $f(n)$ se denotará por x_n , y f por $\{x_n\}$.

Definición 3.3.3. Sea $\{x_n\}$ una sucesión en \mathbb{Q} . Se dice que la sucesión es de **Cauchy** si

$$\forall \epsilon \in \mathbb{Q}^+ \quad \exists N \in \mathbb{N} \text{ tal que } |x_n - x_m| < \epsilon \quad \forall n \geq N, \forall m \geq N.$$

Definición 3.3.4. Dadas dos sucesiones $\{x_n\}, \{y_n\}$ en \mathbb{Q} , se define su **suma**, denotada por $\{x_n\} + \{y_n\}$ como la sucesión $\{x_n + y_n\}$ y se define su **producto**, denotado por $\{x_n\}\{y_n\}$ como la sucesión $\{x_n y_n\}$.

C denotará al conjunto de sucesiones de Cauchy en \mathbb{Q} .

Proposición 33. Sea $\{x_0, \dots, x_N\}$ un subconjunto de \mathbb{Q} . Existe $K \in \{0, \dots, N\}$ tal que $x_K \geq x_i \forall i \in \{0, \dots, N\}$. x_K se denotará como $\max\{x_0, \dots, x_N\}$.

Proof. Se procederá por inducción sobre N .

Si $N = 0$, entonces $K = 0$.

Suponga que la proposición se cumple para algún N .

Considere el conjunto $\{x_0, \dots, x_N, x_{N+1}\}$.

Se tiene que $x_K \leq x_{N+1} \vee x_K \geq x_{N+1}$. En el primer caso $K' = N + 1$, en el segundo caso $K' = K$.

En cualquiera de ellos, $K' \in \{0, \dots, N + 1\}$, y $x'_{K'} \geq x_i \forall i \in \{0, \dots, N + 1\}$. \square

Proposición 34. Sea $\{x_n\}$ una sucesión de Cauchy en \mathbb{Q} . Entonces existe $M \in \mathbb{Q}^+$, tal que $|x_n| \leq M \forall n \in \mathbb{N}$.

Proof. Como $\{x_n\}$ es de Cauchy, y $1_q \in \mathbb{Q}^+$, existe $N \in \mathbb{N}$ tal que $|x_n - x_m| < 1_q \forall n \geq N, \forall m \geq N$. En particular se tiene que si $n \geq N$

$$|x_n| - |x_N| \leq |x_n - x_N| < 1_q \quad \therefore \quad |x_n| \leq |x_N| + 1_q \quad \forall n \geq N.$$

Sea $K = \max\{|x_0|, \dots, |x_N|\}$, considere $M = K + 1_q$. Entonces

$$|x_n| + 1_q \leq M \wedge K \leq M \quad \therefore \quad |x_n| \leq M \quad \forall n \in \mathbb{N}$$

\square

Proposición 35. Sean $\{x_n\}, \{y_n\}$ sucesiones de Cauchy en \mathbb{Q} . Entonces $\{x_n\} + \{y_n\}$, y $\{x_n\}\{y_n\}$ son sucesiones de Cauchy.

Proof. Sea $\epsilon \in \mathbb{Q}^+$. Como $\{x_n\}$ es sucesión de Cauchy, $\exists N \in \mathbb{N}$ tal que si $n, m \geq N$, entonces:

$$|x_n - x_m| < \epsilon \cdot 2_q^{-1}$$

Así mismo existe $N' \in \mathbb{N}$ tal que si $n, m \geq N'$, entonces:

$$|y_n - y_m| < \epsilon \cdot 2_q^{-1}$$

Sea $K = \max\{N, N'\}$, entonces $n, m \geq K$, así:

$$|(x_n + y_n) - (x_m + y_m)| = |x_n - x_m + y_n - y_m| \leq |x_n - x_m| + |y_n - y_m| < \epsilon \cdot (2_q^{-1} + 2_q^{-1}) = \epsilon$$

Lo anterior muestra que $\{x_n\} + \{y_n\}$ es de Cauchy.

Para la segunda parte, como $\{x_n\}$ y $\{y_n\}$ son de Cauchy, existen M y M' tales que:

$$|x_n| \leq M \quad \forall n \in \mathbb{N} \quad \wedge \quad |y_n| \leq M' \quad \forall n \in \mathbb{N}$$

Dado $\epsilon \in \mathbb{Q}^+$, sean $\epsilon' = \epsilon 2_q^{-q} (M')^{-1}$, y $\epsilon' = \epsilon'' = 2_q^{-q} M^{-1}$, entonces $\exists K', K'' \in \mathbb{N}$, tales que:

$$|x_n - x_m| < \epsilon' \text{ si } n, m \geq K' \quad \wedge \quad |y_n - y_m| < \epsilon'' \text{ si } n, m \geq K''$$

Sea $L = \max\{K', K''\}$, entonces si $n, m \geq L$, se tiene:

$$\begin{aligned}
 |x_n y_n - x_m y_m| &= |x_n y_n - x_n y_m + x_n y_m - x_m y_m| \\
 &\leq |x_n(y_n - y_m)| + |x_n y_m - x_m y_m| \\
 &\leq |x_n||y_n - y_m| + |x_n - x_m||y_m| \\
 &< M\epsilon'' + \epsilon' M' \\
 &= \epsilon(2_q^{-1} + 2_q^{-1}) = \epsilon
 \end{aligned}$$

Lo anterior demuestra que $\{x_n\}, \{y_n\}$ es de Cauchy. □

Definición 3.3.5. La proposición (35) muestra que en C están definidas 2 operaciones binarias:

$$\begin{array}{ll}
 f : C \times C \rightarrow C & g : C \times C \rightarrow C \\
 (\{x_n\}, \{y_n\}) \mapsto \{x_n\} + \{y_n\} & (\{x_n\}, \{y_n\}) \mapsto \{x_n\}\{y_n\}
 \end{array}$$

A f , y g se le denominan respectivamente adición y producto en C .

Proposición 36. Sean $\{x_n\}, \{y_n\}, \{z_n\} \in C$. Entonces:

- a. $\{x_n\} + \{y_n\} = \{y_n\} + \{x_n\}$
- b. $\{x_n\} + (\{y_n\} + \{z_n\}) = (\{x_n\} + \{y_n\}) + \{z_n\}$
- c. $\exists \{u_n\} \in C$ tal que $\{u_n\} + \{v_n\} = \{v_n\} \forall \{v_n\} \in C$.
- d. $\exists \{h_n\} \in C$ tal que $\{x_n\} + \{h_n\} = \{u_n\}$
- e. $\{x_n\}\{y_n\} = \{y_n\}\{x_n\}$
- f. $\{x_n\}(\{y_n\}\{z_n\}) = (\{x_n\}\{y_n\})\{z_n\}$
- g. $\exists \{w_n\} \in C$ tal que $\{w_n\}\{v_n\} = \{v_n\} \forall \{v_n\} \in C$.
- h. $\{x_n\}(\{y_n\} + \{z_n\}) = \{x_n\}\{y_n\} + \{x_n\}\{z_n\}$.

Sea $R = \{(\{x_n\}, \{y_n\}) \in C \times C \mid \forall \epsilon \in \mathbb{Q}^+ \exists N \in \mathbb{N} |x_n - y_n| < \epsilon \forall n \geq N\}$.

Observe que R es transitiva; ya que si $(\{x_n\}, \{y_n\}), (\{y_n\}, \{z_n\}) \in R$. Se tiene que para $\epsilon \in \mathbb{Q}^+$ existen $M, N \in \mathbb{N}$ tales que:

$$|x_n - y_n| < \epsilon 2_q^{-1} \forall n \geq M \quad \wedge \quad |y_n - z_n| < \epsilon 2_q^{-1} \forall n \geq N$$

Sea $K = \max\{N, M\}$. Si $n > K$, entonces:

$$|x_n - z_n| = |x_n - y_n + y_n - z_n| \leq |x_n - y_n| + |y_n - z_n| < \epsilon 2_q^{-1} + \epsilon 2_q^{-1} = \epsilon$$

Así $(\{x_n\}, \{z_n\}) \in R$.

Se tiene así mismo que $(\{x_n\}, \{x_n\}) \in R \quad \forall \{x_n\} \in C$. Y si $(\{x_n\}, \{y_n\}) \in R$, entonces $(\{y_n\}, \{x_n\}) \in R$.

Así R es una relación de equivalencia en C .

Definición 3.3.6. Se define al conjunto cociente C/R como el conjunto de **números reales**, y se denotará por el símbolo \mathbb{R} .

Proposición 37. Sean $\{x_n\}, \{y_n\}, \{r_n\}, \{z_n\} \in C$. Si $(\{x_n\}, \{r_n\}), (\{y_n\}, \{z_n\}) \in R$, entonces:

$$i) (\{x_n\} + \{y_n\}, \{r_n\} + \{z_n\}) \in R \qquad ii) (\{x_n\}\{y_n\}, \{r_n\}\{z_n\}) \in R$$

Proof. ii) Sea $\epsilon \in \mathbb{Q}^+$. Sea $\epsilon' = \epsilon 2_q^{-1}$.

Como $(\{x_n\}, \{r_n\}) \in R \quad \exists N \in \mathbb{N}$ tal que $|x_n - r_n| < \epsilon' \quad \forall n \geq N$.

Así mismo $\exists N' \in \mathbb{N}$ tal que $|y_n - z_n| < \epsilon' \quad \forall n \geq N'$.

Sea $K = \max\{N, N'\}$. Entonces $\forall n \geq K$, se tiene:

$$\begin{aligned} |(x_n + y_n) - (r_n + z_n)| &= |(x_n - r_n) + (y_n - z_n)| \\ &\leq |x_n - r_n| + |y_n - z_n| \\ &< \epsilon' + \epsilon' = \epsilon \end{aligned}$$

lo anterior muestra que $(\{x_n\} + \{y_n\}, \{r_n\} + \{z_n\}) \in R$.

ii) Como $\{y_n\}, \{r_n\}$ pertenecen a C . $\exists M, M' \in \mathbb{Q}^+$ tales que:

$$|y_n| < M \quad \forall n \in \mathbb{N} \quad \wedge \quad |r_n| < M' \quad \forall n \in \mathbb{N}$$

Dado $\epsilon \in \mathbb{Q}^+$, sean $\epsilon' = \epsilon 2_q^{-1} M^{-1}$, y $\epsilon'' = \epsilon 2_q^{-1} M'^{-1}$.

Como $(\{x_n\}, \{r_n\}) \in R$, para $\epsilon' \exists N \in \mathbb{N}$, tal que $|x_n - r_n| < \epsilon' \quad \forall n \geq N$.

Así mismo $\exists N' \in \mathbb{N}$, tal que $|y_n - z_n| < \epsilon'' \quad \forall n \geq N'$.

Sea $K = \max\{N, N'\}$, se tiene entonces, si $n \geq K$:

$$\begin{aligned} |x_n y_n - r_n z_n| &= |x_n y_n - y_n r_n + y_n r_n - r_n z_n| \\ &\leq |x_n y_n - y_n r_n| + |y_n r_n - r_n z_n| \\ &\leq |y_n| |x_n - r_n| + |r_n| |y_n - z_n| \\ &< M \epsilon' + M' \epsilon'' = \epsilon \end{aligned}$$

Lo anterior muestra que $(\{x_n\}\{y_n\}, \{r_n\}\{z_n\}) \in R$. □

Definición 3.3.7. La proposición justifica la definición de las siguientes 2 operaciones binarias en \mathbb{R} :

$$\begin{aligned} F : \mathbb{R} \times \mathbb{R} &\rightarrow \mathbb{R} & G : \mathbb{R} \times \mathbb{R} &\rightarrow \mathbb{R} \\ ([\{x_n\}], [\{y_n\}]) &\rightarrow [\{x_n\} + \{y_n\}] & ([\{x_n\}], [\{y_n\}]) &\rightarrow [\{x_n\}\{y_n\}] \end{aligned}$$

F, G se denominan respectivamente adición y producto en \mathbb{R} .

Denotamos así:

$$0_r = [\{x_n\}] \text{ siendo } x_n = 0_q \quad \forall n \in \mathbb{N}$$

$$1_r = [\{y_n\}] \text{ siendo } y_n = 1_q \quad \forall n \in \mathbb{N}$$

Se tiene entonces de la proposición (36) lo siguiente:

Proposición 38. Sean $a, b, c \in \mathbb{R}$, se tiene entonces:

a. $a + b = b + a$

b. $a + (b + c) = (a + b) + c$

c. $a + 0_r = a$

d. $\exists -a \quad a + (-a) = 0_r$

e. $ab = ba$

f. $a(bc) = (ab)c$

g. $a1_r = a$

h. Si $a \neq 0_r$, $\exists a^{-1} \quad aa^{-1} = 1_r$

i. $a(b + c) = ab + ac$

La prueba de 8. será consecuencia de las proposiciones subsecuentes.

Definición 3.3.8. Una sucesión $\{x_n\} \in C$ se dice positiva, si $\exists \epsilon \in \mathbb{Q}^+ \wedge \exists N \in \mathbb{N}$ tales que $x_n > \epsilon \quad \forall n \geq N$.

Proposición 39. Sea $\{x_n\} \in C$ positiva. Si $(x_n), \{u_n\} \in R$, entonces $\{u_n\}$ también es positiva.

Proof. Como $\{x_n\}$ es positiva, existen $\epsilon \in \mathbb{Q}^+, N \in \mathbb{N}$ tales que $x_n > \epsilon \quad \forall n \geq N$.

Sea $\epsilon' = \epsilon 2_q^{-1}$. entonces $\epsilon' \in \mathbb{Q}^+$.

Como $(\{x_n\}, \{u_n\}) \in R$. Para ϵ' , existe $M \in \mathbb{N}$ tal que $|x_n - u_n| < \epsilon' \quad \forall n \geq M$. Sea $K = \max N, M$, entonces se tiene $\forall n \geq K$:

$$\begin{aligned} \epsilon - u_n &< x_n - u_n \\ &\leq |x_n - u_n| \\ &< \epsilon' \\ \therefore \forall n &\geq K \\ \epsilon' &< u_n \end{aligned}$$

lo cual muestra que $\{u_n\}$ es positiva. □

Definición 3.3.9. Sea $x \in \mathbb{R}$. x se dice positivo si $\exists \{x_n\} \in C$ positiva tal que $\{x_n\} \in x$. \mathbb{R}^+ denotará al conjunto de reales positivos.

Proposición 40. Sean $\{x_n\}, \{y_n\}$ sucesiones de Cauchy positivas, entonces:

- $\{x_n\} + \{y_n\}$ es una sucesión de Cauchy positiva.
- $\{x_n\}\{y_n\}$ es una sucesión de Cauchy positiva.

Proof. Por hipótesis existen $\epsilon_1 \in \mathbb{Q}^+, N_1 \in \mathbb{N}$, tales que $x_n > \epsilon_1 \forall n \geq N_1$.

Así mismo, existen $\epsilon_2 \in \mathbb{Q}^+, N_2 \in \mathbb{N}$ tales que: $y_n > \epsilon_2 \forall n \geq N_2$.

Sea $N = \max\{N_1, N_2\}$, entonces si $n \geq N$:

$$x_n + y_n > \epsilon_1 + \epsilon_2 \in \mathbb{Q}^+$$

Así mismo

$$x_n y_n > \epsilon_1 y_n > \epsilon_1 \epsilon_2 \in \mathbb{Q}^+$$

Así la suma y el producto son sucesiones positivas. □

Proposición 41. Sea $\{x_n\} \in C$, entonces se cumple una única de las siguientes afirmaciones:

$$(\{x_n\}, \{u_n\}) \in R \text{ siendo } u_n = 0_q \forall n \in \mathbb{N} \quad \{x_n\} \text{ es positiva} \quad -\{x_n\} \text{ es positiva}$$

Proof. Suponga que $(\{x_n\}, \{u_n\}) \notin R$, entonces $\exists \epsilon \in \mathbb{Q}^+$ tal que $\forall N \in \mathbb{N} \exists n > N$ para el cual $|x_n| \geq \epsilon$. Por otra parte, como $\{x_n\} \in C$, para $\epsilon' = \epsilon 2_q^{-1} \exists M \in \mathbb{N}$ tal que $|x_n - x_m| < \epsilon' \forall n, m \geq M$. Sea $L = \max\{N, M\}$.

Como $L \in \mathbb{N}$, $\exists K > L$, tal que $|x_K| \geq \epsilon$.

En particular se tiene que $x_K \neq 0_q \therefore x_K > 0_q \vee -x_K > 0_q$.

Suponga que $x_K > 0_q$

Sea $n > L$, entonces $n, K > M$, por lo cual:

$$x_K - x_n \leq |x_L - x_n| < \epsilon' \quad \therefore \quad x_K - \epsilon' < x_n$$

Además, como $x_K > 0_q$, se tiene $x_K = |x_K| \geq \epsilon$

$$\epsilon' = 2_q \epsilon' - \epsilon' = \epsilon - \epsilon' \leq x_K - \epsilon' < x_n$$

Verificándose que $\{x_n\}$ es positiva. Se procede de forma análoga en el segundo caso verificándose que $-\{x_n\}$ es positiva.

Suponga ahora que $(\{x_n\}, \{u_n\}) \in R$ Así $\forall \epsilon'' \in \mathbb{Q}^+, \exists N'$ tal que $\forall n \geq N' |x_n| < \epsilon''$, en cualquier caso contradiría que $\{x_n\}$ ó $-\{x_n\}$ fueran positivas. Los otros dos casos se tratan de manera similar a la primer parte. □

Proposición 42. Sea $\{x'_n\} \in C$ tal que $(\{x_n\}, \{u_n\}) \in R$, siendo $u_n = 0_q \forall n \in \mathbb{N}$ entonces existe $\{y_n\} \in C$, tal que $(\{x_n\}\{y_n\}, \{v_n\}) \in R$, siendo $v_n = 1_q \forall n \in \mathbb{N}$.

Proof. Por la proposición 41, se tiene que $\{x_n\}$ es positiva ó $-\{x_n\}$ lo es. Así existen $\epsilon \in \mathbb{Q}^+, N \in \mathbb{N}$ tales que $x_n > \epsilon \forall n > N$ ó $-x_n > \epsilon \forall n > N$. Entonces $|x_n| > \epsilon \forall n > N$.

Para cada $n \in \mathbb{N}$ sea

$$x'_n = \begin{cases} \epsilon & \text{si } n \leq N \\ x_n & \text{si } n > N \end{cases}$$

Entonces $x'_n \neq 0_q \forall n \in \mathbb{N}$. Observe que $\{x'_n\} \in C$, además $(\{x_n\}, \{x'_n\}) \in R$.

Para cada $n \in \mathbb{N}$ sea $y_n = (x_n)'^{-1}$

Como $(\{y_n\}, \{y_n\}) \in R$ se tiene que:

$$(\{x_n\}\{y_n\}, \{x'_n\}\{y_n\}) \in R$$

Observe que $\{x'_n\}\{y_n\} = \{v_n\}$ lo cual implica que $(\{x'_n\}\{y_n\}, \{v_n\}) \in R$.

Para concluir se verifica que $\{y_n\} \in C$.

$$\begin{aligned} |y_n - y_m| &= |(x'_n)^{-1} - (x'_m)^{-1}| = |(x'_m - x'_n)(x'^{-1}_n)(x'^{-1}_m)| \\ &= |x'_n - x'_m| |x'^{-1}_n| |x'^{-1}_m| \end{aligned}$$

Observe que $|x'_n| > \epsilon \forall n \in \mathbb{N}$ Así:

$$|(x'_n)^{-1}| = |x'_n|^{-1} \leq \epsilon^{-1} \quad \forall n \in \mathbb{N}$$

En consecuencia:

$$|y_n - y_m| \leq |x'_n - x'_m| \epsilon^{-1} \epsilon^{-1} \quad \forall n, m \in \mathbb{N}$$

Sea $\delta \in \mathbb{Q}^+$ como $\{x'_n\}$ es de Cauchy, $\exists L \in \mathbb{N}$ tal que $|x'_n - x'_m| < \delta \epsilon \epsilon \quad \forall n, m > L$.

Así si $n, m > L$ se tiene

$$|y_n - y_m| < \delta$$

Así $\{y_n\} \in C$ lo cual concluye la prueba. □

La proposición anterior justifica la propiedad 9) de la proposición 38, ya que dado $[\{x_n\}] \in R$ existe $\{y_n\} \in C$ tal que $(\{x_n\}\{y_n\}, \{u_n\}) \in R$.

Proposición 43. a. $1_r \neq 0_r$

b. Si $x, y \in \mathbb{R}$ entonces $x + y \in R \wedge xy \in \mathbb{R}^+$

c. Sea $x \in \mathbb{R}$ se cumple una única de las siguientes afirmaciones:

$$x \in \mathbb{R}^+$$

$$x = 0_r$$

$$-x \in \mathbb{R}^+$$

Proof. a. Si $1_r = 0_r$, se tendría que $\{u_n\}, \{v_n\}$ serían sucesiones de Cauchy relacionadas, siendo $u_n = 1_q \forall n \in \mathbb{N} \wedge u_n = 0_1 \forall n \in \mathbb{N}$, lo cual no ocurre

b. Es consecuencia de la proposición 40

c. Es consecuencia de la proposición 41

□

Sea $R = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid y - x \in \mathbb{R}^+\}$.

R es una relación binaria en \mathbb{R} , transitiva ya que si $(x, y) \in R \wedge (y, z) \in R$ entonces $y - x \in \mathbb{R}^+ \wedge z - y \in \mathbb{R}^+$, así $(y - x) + (z - y) \in \mathbb{R}^+ \therefore z - x \in \mathbb{R}^+ \therefore (x, z) \in R$.

Notación. $(x, y) \in R$ se denotará por $y > x$.

Si $y > x$ ó $y = x$, ello se denotará por $y \geq x$.

Proposición 44. a. $x \in \mathbb{R}$ es positivo si y solamente si $x > 0_r$.

b. Sea $x \in \mathbb{R} \setminus \{0_r\}$, entonces $xx \in \mathbb{R}^+$

c. Dados $x, y \in \mathbb{R}$ se cumple una única de las siguientes afirmaciones:

$$y > x$$

$$x = y$$

$$x > y$$

d. Sean $x, y \in \mathbb{R}$, $x < y$ si y sólo si $\forall z \in \mathbb{R} \ x + z < y + z$.

e. Sean $x, y \in \mathbb{R}$, $x \in \mathbb{R}^+$. $x < y$ si y sólo si $xz < yz$.

Proof. b. Como $x \neq 0_r$, la proposición 43 implica que $x \in \mathbb{R}^+ \wedge -x \in \mathbb{R}^+$.

- En el primer caso, trivialmente $xx \in \mathbb{R}^+$
- En el segundo caso la proposición 38 implica que si $a, b \in \mathbb{R}$

$$(-a)(b) + ab = [(-a) + a]b = 0_r b$$

Por otra parte $\forall u \in \mathbb{R}$

$$0_r u + u = (0_r + 1_r)u = 1_r u = u \therefore$$

$$(0_r u + u) - u = u - 1 \therefore 0_r u = 0_r \therefore$$

$$(-a)(b) + ab = 0_r$$

Lo cual muestra que $(-a)b = -(ab)$. Se tiene en consecuencia:

$$\begin{aligned} (-a)(-b) &= -[a(-b)] &= -[(-b)(a)] \\ &= -[-(ba)] &= -[-(ab)] = ab \end{aligned}$$

Así $(-x)(-x) = xx$ así $xx \in \mathbb{R}^+$.

c. La proposición 43 muestra que se cumple una única de las afirmaciones:

$$y - x \in \mathbb{R}^+$$

$$y - x = 0$$

$$-(y - x) \in \mathbb{R}^+$$

d. Son equivalentes:

$$y > x \quad y - x \in \mathbb{R}^+ \quad (y + x = -(x + z) \in \mathbb{R}^+$$

e. Si $x < y \wedge z \in \mathbb{R}^+$, se tiene: $y - x \in \mathbb{R}^+ \wedge z \in \mathbb{R}^+$. Así $(y - x)z \in \mathbb{R}^+$, es decir, $yz - xz \in \mathbb{R}^+ \therefore yz > xz$.

Recíprocamente si $yz > xz \wedge z \in \mathbb{R}^+$, se tiene $z \neq 0_r$ por lo tanto está definido $z^{-1} \in \mathbb{R}$ tal que $zz^{-1} = 1_r$. Como $z^{-1} \neq 0_r$ ya que $0_ru = 0_r \forall u \in \mathbb{R}$ así $z^{-1} \in \mathbb{R}^+ \wedge -z^{-1} \in \mathbb{R}^+$. Si $-z^{-1} \in \mathbb{R}^+$ se tendría que $(z)(-z^{-1}) \in \mathbb{R}^+$, $1_r \in \mathbb{R}^+$ lo cual no ocurre. Por lo cual $z^{-1} \in \mathbb{R}^+$. Así como $yz - xz \in \mathbb{R}^+$ se tiene $(yz - xz)z^{-1} \in \mathbb{R}^+$, es decir $y - x \in \mathbb{R}^+$.

□

Definición 3.3.10. Dado $x \in \mathbb{R}$ se define el valor absoluto de x denotado $|x|$ como:

$$|x| = \begin{cases} x & \text{si } x \geq 0_r \\ -x & \text{si } x < 0_r \end{cases}$$

Proposición 45. Sean $xy \in \mathbb{R}$ entonces:

- a. $|x| \geq 0_q$.
- b. $|x| = 0$ si y sólo si $x = 0$.
- c. $|xy| = |x||y|$.
- d. $|x + y| \leq |x| + |y|$.
- e. $|x| - |y| \leq |x - y|$.

Dado $x \in \mathbb{R}$, considere la función

$$\begin{aligned} G_x : \mathbb{R} &\rightarrow \mathbb{R} \\ y &\mapsto xy \end{aligned}$$

Definición 3.3.11. Por el teorema de recurrencia $\exists! F_x : \mathbb{N} \rightarrow \mathbb{R}$ tal que:

$$F_x(0) = 1_r \quad F_x(n^+) = G_x(F(n))$$

Considere la función

$$\begin{aligned} F : \mathbb{N} \times \mathbb{R} &\rightarrow \mathbb{R} \\ (n, x) &\mapsto F_x(n) \end{aligned}$$

$F(n, x)$ se denotará x^n .

Proposición 46. Sean $a, b \in \mathbb{R}$, $a < b$. Existe $c \in \mathbb{Q}$ tal que $a < c < b$.

Proof. Somo $a < b$, se tiene $a + a < a + b$, i.e., $(1_q + 1_q)a < a + b$, o bien $2_q a < a + b$.

Como $2_q > 0_q$, se tiene $2_q^{-1}(a + b)$.

$$2_q^{-1}(2_q a) < 2_q^{-1}(a + b)$$

Así $a < 2_q^{-1}(a + b)$. Así mismo se tiene $a + b < b + b$, es decir $a + b < 2_q b$, $2_q^{-1}(a + b) < b$. Eligiendo a $c = 2_q^{-1}(a + b)$ se concluye la prueba. \square

Definición 3.3.12. Dado $a \in \mathbb{Q}$, considere la sucesión $\{x_n\}$ tal que $x_n = a \forall n \in \mathbb{N}$. Sea $a_r = [\{x_n\}]$ y $\mathbb{R}' = \{x \in \mathbb{R} \mid \exists a \in \mathbb{Q} x = a_r\}$.

Considere la función:

$$\begin{aligned} h_3 : \mathbb{Q} &\rightarrow \mathbb{R}' \\ a &\mapsto a_r \end{aligned}$$

Se tiene entonces $h_3(0_q) = 0_r$, $h_3(1_q) = 1_r$.

Dados $a, b \in \mathbb{Q}$ se tiene:

$$h_3(a + b) = h_3(a) + h_3(b)$$

$$h_3(ab) = h_3(a)h_3(b)$$

h_3 es además una biyección, así, un isomorfismo. Se ha probado que existen isomorfismos h_1 entre $\{\mathbb{N}, +, \cdot, 0, 1\}$ y $\{\mathbb{Z}^+, +, \cdot, 0_z, 1_z\}$. h_2 entre $\{\mathbb{Z}, +, \cdot, 0_z, 1_z\}$ y $\{\mathbb{Q}^+, +, \cdot, 0_q, 1_q\}$. Así existe un isomorfismo $h_3 \circ h_2 \circ h_1$ entre $\{\mathbb{N}, +, \cdot, 0, 1\}$ y $\{\mathbb{N}', +, \cdot, 0_r, 1_r\}$.

Se denomina a un elemento de \mathbb{N}' , real natural.

Se denomina a un elemento de \mathbb{Q}' , real racional.

Se denomina a un elemento de $h_3 \circ h_2(\mathbb{Z})$, real entero.

Proposición 47. Sean $x, y \in \mathbb{R}$, $x < y$. Existe $z \in \mathbb{R}'$ tal que $x < z < y$.

Proposición 48 (Propiedad Arquimediana). Sean $x, y \in \mathbb{R}^+$, existe n real natural tal que $nx > y$.

Proof. Sean $\{x_n\}, \{y_n\}$ sucesiones en \mathbb{C} positivas tales que $x = [\{x_n\}]$, y $y = [\{y_n\}]$. Como $\{y_n\}$ es de Cauchy, ambas son acotadas, así existe un $\delta \in \mathbb{Q}^+$ tal que $|y_n| \leq \delta \forall n \in \mathbb{N}$. Como $y_n \leq |y_n| \forall n \in \mathbb{N}$, se tiene $y_n \leq \delta \forall n \in \mathbb{N}$.

Sea $d = [\{u_n\}]$, siendo $u_n = \delta \forall n \in \mathbb{N}$.

Como $x \in \mathbb{R}^+$, se tiene $x > 0_r$; la proposición 47 implica que existe $s \in \mathbb{R}'$ tal que $x > s > 0_r$.

Así mismo, como $y \leq d$ existe $t \in \mathbb{R}'$ tal que $y \leq t \leq d$.

La existencia de tal $t \in \mathbb{R}'$ es consecuencia de la proposición 47, si $y < d$; en el caso $y = d$, se elige a $t = d$.

Como $\mathbb{R}' = h_3(\mathbb{Q})$, se tiene que existen $\hat{t}, \hat{s} \in \mathbb{Q}$ tales que: $t = h_3(\hat{t})$ y $s = h_3(\hat{s})$.

Como $t \geq y > 0$, se tiene que tanto s como t , pertenecen a \mathbb{R}^+ . Se verificará que \hat{t} y \hat{s} pertenecen a \mathbb{Q}^+ .

$$t = [\{w_n\}] \quad s = [\{v_n\}] \quad \text{siendo } w_n = \hat{t} \quad \wedge \quad v_n = \hat{s} \quad \forall n \in \mathbb{N}$$

Como $t, s \in \mathbb{R}^+$, $\{w_n\}, \{v_n\}$ son sucesiones de Cauchy positivas y por ello \hat{t}, \hat{s} son racionales positivos.

Por la proposición 32, existe n_q racional entero tal que

$$n\hat{s} > \hat{t} > 0_q$$

Sea $n = h_3(n_q)$. Observe que $n \in \mathbb{R}^+$. Se verificará finalmente que $ns > t$.

Se tiene que $n_q\hat{s} - \hat{t} > 0_q$ con $\{n_q\hat{s} - \hat{t}\}$ una sucesión de Cauchy positiva. Así $ns - t \in \mathbb{R}^+$. $ns > t$.

Por la tricotomía de $>$, $nx > y$ que era lo que se buscaba demostrar.

□

Definición 3.3.13. Sea $a \in \mathbb{R}$. Se dice que A es acotado superiormente si $\exists x \in \mathbb{R}$ tal que $a \leq x \forall a \in A$. En tal caso x se denomina cota superior de A . Se dice que x cota superior de A es supremo de A si $z \leq y \forall y$ cota superior de A .

Proposición 49. Sea $A \subset \mathbb{R}$, $A \neq \emptyset$, conjunto acotado superiormente, entonces existe un supremo en A .

Proof. Como A es acotado superiormente, se puede asumir sin pérdida de generalidad que existe $t \in \mathbb{R}^+$ tal que $x \leq t \forall x \in A$. Como $A \neq \emptyset$, existe $a \in A$.

Se verificará que existe $m \in \mathbb{R}$ real entero tal que m no es cota superior de A .

- Si $a = 0_r$, trivialmente $-1_r < a$.
- Si $-a \in \mathbb{R}^+$, entonces de la proposición 48, existe n real entero tal que $n1_r > -a$. Elijiendo a $m = -n$, se tiene $m < a$.
- Si $a \in \mathbb{R}^+$ trivialmente $-1_r < a$.

Así, existen reales naturales M, m tales que M es cota superior de A , y m no es cota superior de A .

Veamos que $\exists q$ real entero tal que q es cota superior de A , pero $q - 1_r$ no lo es.

Procedamos por reducción al absurdo y supongamos que no existe tal q , es decir, que para cada M cota superior real entero, $M - 1_r$ también es cota superior de A . Considere m real entero tal que m no es cota superior de A . Veamos que como M es un real entero, $m + 1_r$ también lo es, y como cada $M - n1_r$ es cota superior $n \in \mathbb{N}'$, así m es cota superior de A , lo cual no sucede. Así $\exists q$ real entero, cota superior de A con $q - 1$ no cota superior de A .

□