Capítulo 1

Números Naturales

1.1. Nociones de Estructura Algebraica

1.1.1. Grupos

Definición 1 *Se dice que $(G, *)$ es un **grupo**, si y sólo si, G es un conjunto no vacío, provisto de una función*

$$\begin{array}{rccc} * & : & G \times G & \longrightarrow & G \\ & & (a, b) & \longmapsto & a * b, \end{array}$$

también llamada operación binaria $*$ y que cumple con

Asociatividad

Para todo a, b, c en G, se cumple

$$a * (b * c) = (a * b) * c.$$

Existencia del elemento neutro

Existe e elemento neutro de G, tal que para todo a en G, se cumple

$$a * e = a = e * a.$$

Existencia del elemento inverso

Para todo a en G, existe b en G, tal que

$$a * b = e = b * a,$$

en tal caso el elemento b se denota por a^{-1}, llamado el inverso de a. Es fácil demostrar que el inverso es único, cuando existe.

Diremos que $(G, *)$ es un grupo, para indicar que G bajo la operación $*$ es un grupo.

Algunos grupos cumplen una propiedad adicional dada por:

Conmutatividad

Para todo $a, b \in G$ se cumple

$$a * b = b * a$$

En tal caso, se dice que G es un grupo abeliano o conmutativo

Definición 2 *Sea H un subconjunto no vacío de un grupo G.*

Se dice que H es un ***subgrupo*** *de G, si y sólo si H es un grupo con la misma operación de G. En tal caso se denota por $H \leq G$.*

Propiedad 1 *Sea H un subconjunto no vacío de un grupo $(G, *)$.*

H es un subgrupo de G, si y sólo si cumple:

1. *Para todo $x, y \in H$, se tiene que $x * y \in H$.*
2. *Para todo $x \in H$, se tiene que $x^{-1} \in H$.*

Ejemplo 1 *Algunos ejemplo de grupos*

1. *$G = \{e\}$ es el grupo trivial, $e * e = e$*
2. *$G = \{e, a\}$, es un grupo con la operación*

$*$	e	a
e	e	a
a	a	e

3. *$G = \{e, a, b\}$, es un grupo con la operación y $b = a^2$*

$*$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

4. *$G = \{e, a, b, c\}$, es un grupo, llamado grupo de Klein con la operación*

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

5. *$G = \{e, a, b, c\}$, es un grupo, con la operación*

$*$	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

Ejemplo 2 *Algunos ejemplos de grupos no conmutativo, se obtiene al considerar los movimientos rígidos de los n-agonos regulares, con la operación de realizar consecutivamente la respectiva simetrías respectivamente de otra manera la composición.*

1. *Los movimiento rígido del triángulo equilátero son seis, las rotaciones en 120,240 y 360 grados, y las reflexiones o simetría respecto a las bisectriz del triángulo*

$$Sim(T) = \{r_0, r_{120}, r_{240}, s_1, s_2, s_3\}$$

Construir la tabla del grupo $Sim(T)$

2. *Los movimiento rígido del cuadrado son ocho, las rotaciones en 90,180,270,360 y las reflexiones o simetría respecto a las diagonales y a la recta que une los puntos medio de los lados paralelos.*

1.1.2. Anillo y Cuerpo

Definición 3 *Se dice que $(A, +, \cdot)$ es un anillo, si y sólo si, A es un conjunto no vacío, provisto de dos operaciones $+$ y $\cdot$, tales que:*

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

2. ***Asociatividad***

   Para todo $x, y, z \in A$ se tiene que

$$(x \cdot y) \cdot z = x \cdot (y \cdot z).$$

3. ***Neutro***

   Existe $1 \in A - \{0\}$, tal que para todo $x \in A$ se cumple

$$x \cdot 1 = 1 \cdot x = x.$$

4. ***Distributiva***

   Para todo $x, y, z \in A$ se tiene que

$$x \cdot (y + z) = x \cdot y + x \cdot z, \qquad (x + y) \cdot z = x \cdot z + y \cdot z.$$

Además se dice que A es una anillo conmutativo si la operación " $\cdot$ " lo es.

Notación: Habitualmente el neutro con la primera operación se denota con el símbolo 0 y el neutro de la segunda operación con el símbolo 1. Además el inverso aditivo por $-a$ y el multiplicativo cuando existe por a^{-1}.

Ejemplo 3 *El conjunto de las matrices*

$$M_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{R} \right\}$$

es un anillo no conmutativo, con las siguientes operaciones
Suma:

$$\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} + \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} = \begin{pmatrix} a_1 + a_2 & b_1 + b_2 \\ c_1 + c_2 & d_1 + d_2 \end{pmatrix}$$

Producto:

$$\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} \cdot \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} = \begin{pmatrix} a_1a_2 + b_1c_2 & a_1b_2 + b_1d_2 \\ c_1a_2 + d_1c_2 & c_1b_2 + d_1d_2 \end{pmatrix}$$

Además note que

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

Observación: no todas la matrices tiene inverso multiplicativo o con el producto.

Sea $A \in M_2(\mathbb{R})$, se dice que A es invertible si y sólo si existe $B \in M_2(\mathbb{R})$ tal que

$$AB = BA = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I$$

Ejercicio 4 *En* $(M_2(\mathbb{R}), +, \cdot)$

1. *Demostrar que* $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ *es invertible si y sólo si* $ad - bc \neq 0$
2. *Si* $B = \begin{pmatrix} 3 & 1 \\ 4 & 5 \end{pmatrix}$. *Determine* B^{-1}
3. *Si* $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, $B = \begin{pmatrix} 3 & 0 \\ 1 & 4 \end{pmatrix}$. *Determine* $X \in M_2(\mathbb{R})$, *tal que*

$$A \cdot X \cdot B = I$$

Definición 4 *Sea* $(A, +, \cdot)$ *un anillo.*

Se define el conjunto de los elementos invertibles

$$\mathcal{U}(A) = \{x \in A \mid \text{ existe el inverso multiplicativo de } x \}$$

Ejercicio 5 *Sea* $(A, +, \cdot)$ *un anillo.*

Demuestre que

1. $(\forall a \in A)(a \cdot 0 = 0)$
2. $(-1)(-1) = 1$
3. $(\forall a, b \in A)(\ (-a)b = -(ab)\ )$

Definición 5 *Se dice que un anillo* $(K, +, \cdot)$ *es un* ***cuerpo*** *si y sólo si* $(K^*, \cdot)$ *es un grupo abeliano, donde* $K^* = K - \{0\}$.

Es decir $(K, +, \cdot)$ *es un cuerpo si y solo si,* $(K, +, \cdot)$ *es un anillo conmutativo, tal que* $\mathcal{U}(A) = K^*$

1.2. Números Naturales $\mathbb{N}$

La más conocida presentación de los números naturales, es la que presentó el matemático italiano Giuseppe Peano (1858-1932) por primera vez en 1889 en un pequeño libro publicado en Turin, titulado "Arithmetices Principia Nova Methodo Exposita"Traducido al inglés: Van Heijenoort. The Principles of Arithmetic, presented by a new method. Este texto incluye sus famosos axiomas, pero más que un texto de aritmética, este documento contiene una introducción a la lógica en la cual se presentan por primera vez los símbolos actuales para representar la pertenencia, la existencia, la unión y la intersección, algunas otras presentaciones son:

On the Logic of Number, de **Charles S. Pierce**, fue publicado en 1881 en las páginas 85 a 95 del volumen 4 de la revista The American Journal of Mathematics.

An Elementary Theory of the Category of Sets.**Lawvere, F. William.** Proc. Nat. Acad. Sci. 52 (1964): 1506-1511.

Ahora veremos la construcción de los números naturales a través de los llamados axiomas de **Peano**. Estos son:

Axioma 1 *Existe un conjunto denotado por* $\mathbb{N}$*, cuyos elementos se llaman* ***números naturales*** *y existe número natural llamado "cero" e indicado por el símbolo* 0*.*

$$0 \in \mathbb{N}.$$

Axioma 2 *Existe una relación simbolizada por "suc", tal que se escriba* $suc(x)$ *debe leerse sucesor de* x*.*

$$(\forall x \in \mathbb{N})(\exists! y \in \mathbb{N})(y = suc(x)).$$

Axioma 3

$$(\forall x \in \mathbb{N})(suc(x) \neq 0).$$

Axioma 4

$$(\forall x, y \in \mathbb{N})(suc(x) = suc(y) \Rightarrow x = y).$$

Axioma 5 *Si $I \subseteq \mathbb{N}$ y se verifican:*

1. $0 \in I$.
2. $(\forall x \in I)(suc(x) \in I)$.

Entonces $I = \mathbb{N}$.

Teorema 2 *Ningún número natural es sucesor de si mismo, es decir,*

$$(\forall x \in \mathbb{N})(suc(x) \neq x).$$

Demostración: Definamos el conjunto $M = \{x \in \mathbb{N} \mid suc(x) \neq x\}$, y demostraremos que $M = \mathbb{N}$.

Para lo anterior usaremos el Axioma (5), lo que significa que demos verificar cada una las hipótesis:

En primer lugar es claro que $M \subseteq \mathbb{N}$.

La segunda condición se obtiene del Axiomas (1), ya que $0 \in \mathbb{N}$ y cumple con $suc(0) \neq 0$, luego $0 \in M$.

Por último, consideremos $x \in M$, luego se tiene que

$$x \in \mathbb{N} \text{ y } suc(x) \neq x.$$

Por el Axioma (4), se obtiene tenemos que $suc(suc(x)) \neq suc(x)$, luego $suc(x) \in M$.

Por lo tanto M cumples las todas las hipótesis del Axioma (5), de lo cual se obtiene $M = \mathbb{N}$. □

Teorema 3 *Todo número natural no nulo es sucesor de uno y sólo un número natural, es decir,*

$$(\forall x \in \mathbb{N} - \{0\})(\exists! y \in \mathbb{N})(x = suc(y)).$$

Demostración: Definamos el conjunto

$$M = \{x \in \mathbb{N} - \{0\} \quad | \quad (\exists! y \in \mathbb{N})(x = suc(y))\} \cup \{0\}$$

y demostremos que $M = \mathbb{N}$ usando el Axioma (5).

Notemos primero que: $M \subseteq \mathbb{N}$ y $0 \in M$ por definición del conjunto M.

Para la segunda parte, sea $x \in M$, luego se tiene que

$$x \in \mathbb{N} \text{ y existe } y \in \mathbb{N} \text{ tal que } suc(y) = x.$$

por el Axioma (2) se tiene que $suc(x) \in \mathbb{N}$ y por el Axioma (3) se tiene que $suc(x) \neq 0$, como se tiene que $x = suc(y)$, luego $suc(x) = suc(suc(y))$.

Para la unicidad, el Axioma 4, no puede haber dos antecesores, luego $suc(y) = x$, es el único elemento en los naturales tal que

$$suc(x) = suc(suc(y)).$$

es decir, dado $x \in M$, existe un único $z \in \mathbb{N}$ tal que $suc(x) = suc(z)$

Por lo tanto, $M = \mathbb{N}$, concluyendo así la demostración. □

1.2.1. Suma en $\mathbb{N}$

En el conjunto de los números Naturales se puede definir una operación binaria, dada por el teorema .

Propiedad 4 *Sea $x \in \mathbb{N}$ fijo, se define la siguiente relación por recurrencia*

$$x + 0 \;:=\; x$$

Si $x + y$ esta definido, entonces

$$x + suc(y) \;:=\; suc(x + y).$$

entonces la anterior relación define la función

$$\begin{array}{rccc} + \;:\; & \mathbb{N} & \longrightarrow & \mathbb{N} \\ & y & \longmapsto & x + y, \end{array}$$

Demostración: Sea $x \in \mathbb{N}$ fijo, definimos el conjunto

$$J = \{y \in \mathbb{N} \;\mid x + y \;\text{ esta bien definido }\}$$

Claramente $0 \in \mathbb{N}$, no tiene un antecesor y además se tiene $x + 0 = x$. Luego $0 \in J$.

Supongamos que $y \in J$, luego $x + y \in \mathbb{N}$ y esta bien definido, por lo tanto, tenemos que $suc(x + y) \in \mathbb{N}$ es único, es decir $x + suc(y)$ esta bien definido, por ende $suc(y) \in J$, luego por Axioma (5), tenemos que $J = \mathbb{N}$.

De este modo, $+$ es una función con x esta fijo. □

Observación: Notemos que el lema anterior nos permite definir, para cualquier par de números naturales la suma de ellos

Teorema 5 *En el conjunto de los números naturales, existe una operación suma $(+)$ que cumple:*

1. $(\forall x \in \mathbb{N})(\, x + 0 = x\,)$.
2. $(\forall x \in \mathbb{N})(\forall y \in \mathbb{N})(\, x + suc(y) = suc(x + y)\,)$.

Notación: Denotemos $suc(0) = 1$ y reemplazando $y = 0$ en Teorema 5.2, obtenemos

$$suc(x) \;=\; x + 1. \tag{1.1}$$

Ahora bien, a partir de (1.1) tomando $x = 1$, obtenemos $suc(1) = 1+1$, lo que anotaremos como $suc(1) = 2$ siguiendo del mismo modo

$$\begin{array}{rcl} suc(0) & = & 1 \\ suc(1) & = & 2 \\ suc(2) & = & 3 \\ & \vdots & \\ suc(n) & = & n + 1. \end{array}$$

La siguiente propiedad completa la demostración del neutro

Propiedad 6

$$(\forall y \in \mathbb{N})(0 + y = y). \tag{1.2}$$

Demostración: Se define el conjunto

$$J = \{y \in \mathbb{N} \mid 0 + y = y\}$$

y demostremos que $J = \mathbb{N}$.

Para la primera parte, tenemos que $0 \in \mathbb{N}$ y por la propiedad 4 tenemos que $0 + 0 = 0$, de este modo concluimos que $0 \in J$.

Supongamos $y \in J$, es decir, $y \in \mathbb{N}$ y $0 + y = y$, ahora bien como $y \in \mathbb{N}$ por Axioma (2), se tiene que $suc(y) \in \mathbb{N}$, por la Propiedad 4, se tiene que

$$0 + suc(y) = suc(0 + y) = suc(y),$$

es decir $suc(y) \in J$.

Luego en virtud del Axioma (5) tenemos que $J = \mathbb{N}$. □

Teorema 7 (Conmutatividad) *La suma en* $\mathbb{N}$ *es conmutativa, esto es*

$$(\forall x, y \in \mathbb{N})(x + y = y + x).$$

Demostración: Sea

$$M = \{x \in \mathbb{N} \mid (\forall y \in \mathbb{N})(x + y = y + x)\}$$

y demostremos que $M = \mathbb{N}$.

Por definición de suma y la Propiedad (6), tenemos se cumple

$$(\forall y \in \mathbb{N})(0 + y = y = y + 0),$$

así $0 \in M$.

Ahora veremos la segunda parte del axioma 5, es decir,

$$(\forall x \in M)(suc(x) \in M)$$

Supongamos $x \in M$, es decir, $x \in \mathbb{N}$ y para todo $y \in \mathbb{N}$ se tiene $x + y = y + x$.

Como $x \in \mathbb{N}$ por Axioma (2)tenemos que $suc(x) \in \mathbb{N}$, para ello debemos demostrar que $suc(x) \in M$, es decir

$$(\forall y \in \mathbb{N})(suc(x) + y = y + suc(x)).$$

Para demostrar lo anterior definimos el conjunto

$$I = \{y \in \mathbb{N} \mid suc(x) + y = y + suc(x)\}$$

y demostremos que $I = \mathbb{N}$, para ello recurrimos al axioma 5.

Sabemos que $suc(x) + 0 = 0 + suc(x)$, luego se tiene que $0 \in I$, primera hipótesis del axioma.

Supongamos $y \in I$, es decir, $y \in \mathbb{N}$ y

$$suc(x) + y = y + suc(x).$$

Como $y \in \mathbb{N}$, se tiene que $suc(y) \in \mathbb{N}$, ahora bien

$$\begin{aligned} suc(x) + suc(y) &= suc(suc(x) + y) \\ &= suc(y + suc(x)) \\ &= suc(suc(y + x)) \\ &= suc(suc(x + y)) \\ &= suc(x + suc(y)) \\ &= suc(suc(y) + x) \\ &= suc(y) + suc(x). \end{aligned}$$

Por lo tanto $suc(y) \in I$, Así tenemos en virtud del Axioma (5) que $I = \mathbb{N}$, con lo cual, se concluye que M también cumple las hipótesis del axioma 5, por lo tanto $M = \mathbb{N}$. □

Corolario 8 *Sean* $x, y \in \mathbb{N}$

$$suc(x) + y = suc(x + y) = suc(y) + x.$$

Teorema 9 (Asociatividad) *La suma* $(+)$ *en* $\mathbb{N}$ *es asociativa, en símbolos*

$$(\forall x, y, z \in \mathbb{N})((x + y) + z = x + (y + z)).$$

Demostración: Sea

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

y demostremos que $M = \mathbb{N}$.

Por propiedad 6 tenemos que

$$(\forall y, z \in \mathbb{N})((0 + y) + z = 0 + (y + z)) \Leftrightarrow (\forall y, z \in \mathbb{N})(y + z = y + z)$$

es decir, $0 \in M$.

Para la segunda parte, suponemos que $x \in M$, esto es

$$(\forall y, z \in \mathbb{N})((x + y) + z = x + (y + z)),$$

y queremos demostrar que $suc(x) \in M$, es decir

$$(\forall y, z \in \mathbb{N})((suc(x) + y) + z = suc(x) + (y + z)),$$

Para lo cual usaremos hipótesis y corolario anterior,

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

lo cual es verdadero, por lo tanto $M=\mathbb{N}$, es decir,

$$(\forall x,y,z\in\mathbb{N})((x+y)+z=x+(y+z)).$$

□

Teorema 10 (Cancelación) *En* $\mathbb{N}$ *existe la ley de cancelación, es decir*

$$(\forall x,y,z\in\mathbb{N})((x+y=x+z)\Leftrightarrow(y=z)).$$

Demostración: Considere el conjunto

$$M=\{x\in\mathbb{N}\mid(\forall y,z\in\mathbb{N})((x+y=x+z)\Leftrightarrow(y=z))\ \}$$

y demostremos que $M=\mathbb{N}$.

Para la primera parte, debemos verificar

$$(\forall y,z\in\mathbb{N})(0+y=0+z))\Leftrightarrow y=z)$$

es decir, propiedad 6, del neutro

$$(\forall y,z\in\mathbb{N})(y=z\Leftrightarrow y=z)$$

esto es, $0\in M$.

Para la segunda parte, suponemos que $x\in M$, esto es

$$(\forall y,z\in\mathbb{N})((x+y=x+z)\Leftrightarrow(y=z)),$$

y queremos demostrar que $suc(x)\in M$, es decir

$$(\forall y,z\in\mathbb{N})((suc(x)+y=suc(x)+z)\Leftrightarrow(y=z)).$$

Para lo cual usaremos hipótesis y corolario anterior,

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

lo cual es verdadero, por lo tanto $M=\mathbb{N}$, es decir,

$$(\forall x,y,z\in\mathbb{N})((x+y=x+z)\Leftrightarrow(y=z)).$$

□

1.2.2. Producto en $\mathbb{N}$

Propiedad 11 *Sea $x \in \mathbb{N}$ fijo, se define la siguiente relación por recurrencia*

$$x \cdot 0 \;:=\; 0$$

Si $x \cdot y$ esta definido, entonces

$$x \cdot suc(y) \;:=\; x \cdot y + x.$$

entendiendo que primeros multiplicamos y luego sumamos, entonces la anterior relación define la función

$$\begin{array}{rccc} \cdot \;:\; & \mathbb{N} & \longrightarrow & \mathbb{N} \\ & y & \longmapsto & x \cdot y, \end{array}$$

Demostración: Sea $x \in \mathbb{N}$ fijo, definimos el conjunto

$$J = \{\; y \in \mathbb{N} \;\mid x \cdot y \;\text{ esta bien definido }\}$$

Claramente $0 \in \mathbb{N}$, ya que $x \cdot 0 = 0$ y además 0 no tiene un antecesor.

Ahora supongamos que $y \in J$, luego $x \cdot y \in \mathbb{N}$ esta bien definido, por lo tanto, tenemos que $x \cdot y + x \in \mathbb{N}$ es único, es decir $x \cdot suc(y)$ esta bien definido, por ende $suc(y) \in J$, luego por axioma 5, tenemos que $J = \mathbb{N}$, con lo cual, $\cdot$ es una operación binaria con x fijo. □

Observación: La anterior propiedad nos define de el producto de dos números naturales

Teorema 12 *En el conjunto de los números naturales, existe una operación producto " $\cdot$ " que cumple:*

1. $(\forall x \in \mathbb{N})(\, x \cdot 0 = 0\,)$.
2. $(\forall x \in \mathbb{N})(\forall y \in \mathbb{N})(\, x \cdot suc(y) = x \cdot y + x\,)$.

Observación: Con las notaciones anteriores tenemos que

$$x \cdot 1 = x \cdot suc(0) = x \cdot 0 + x = x$$

y también

$$x \cdot 2 = x \cdot suc(1) = x \cdot 1 + x = x + x$$

La siguiente propiedad completa la demostración del neutro

Propiedad 13

$$(\forall y \in \mathbb{N})(1 \cdot y = y). \tag{1.3}$$

Demostración: Se define el conjunto

$$J = \{y \in \mathbb{N} \mid 1 \cdot y = y\}$$

y demostremos que $J = \mathbb{N}$.

Para la primera parte, tenemos que $0 \in \mathbb{N}$ y por la propiedad 4 tenemos que $1 \cdot 0 = 0$, de este modo concluimos que $0 \in J$.

Supongamos $y \in J$, es decir, $y \in \mathbb{N}$ y $1 \cdot y = y$, ahora bien como $y \in \mathbb{N}$, se tiene que $suc(y) \in \mathbb{N}$, por la Propiedad 4, se tiene que

$$1 \cdot suc(y) = 1 \cdot y + 1 = y + 1 = suc(y),$$

es decir $suc(y) \in J$.

Luego en virtud del Axioma (5) tenemos que $J = \mathbb{N}$. □

Propiedad 14

$$(\forall x \in \mathbb{N})(0 \cdot x = 0).$$

Demostración: Dado el conjunto

$$J = \{x \in \mathbb{N} \mid 0 \cdot x = 0\},$$

por demostrar que $J = \mathbb{N}$.

Por definición de " $\cdot$ ", se tiene $0 \cdot 0 = 0$ por lo tanto $0 \in J$.

Supongamos $x \in J$, es decir, $x \in \mathbb{N}$ y $0 \cdot x = 0$, ahora bien como $x \in \mathbb{N}$ por Axioma (2) $suc(x) \in \mathbb{N}$, además como

$$0 \cdot suc(x) = 0 \cdot x + 0 = 0 + 0 = 0$$

Luego se tiene que $suc(x) \in J$. Por lo tanto y en virtud del Axioma (5) tenemos que $J = \mathbb{N}$. □

Teorema 15 *El producto " $\cdot$ " en $\mathbb{N}$ es conmutativo, es decir*

$$(\forall x, y \in \mathbb{N})(x \cdot y = y \cdot x).$$

Demostración: Sea

$$M = \{x \in \mathbb{N} \mid (\forall y \in \mathbb{N})(x \cdot y = y \cdot x)\}$$

y demostremos que $M = \mathbb{N}$.

Sabemos que $0 \in \mathbb{N}$ y también que $0 \cdot y = y \cdot 0$ es verdadero, luego se tiene que $0 \in M$.

Supongamos $x \in M$, es decir $x \in \mathbb{N}$ y $x \cdot y = y \cdot x$ para todo $y \in \mathbb{N}$. Como $x \in \mathbb{N}$ se tiene que $suc(x) \in \mathbb{N}$, ahora debemos demostrar que $suc(x) \in M$ para esto consideremos el conjunto

$$I = \{y \in \mathbb{N} \mid suc(x) \cdot y = y \cdot suc(x)\}$$

y demostremos que $I = \mathbb{N}$.

Ya que $0 \in \mathbb{N}$ por Axioma (1) y que $suc(x) \cdot 0 = 0 \cdot suc(x)$ tenemos que $0 \in I$. Supongamos $y \in I$, es decir $y \in \mathbb{N}$ y $suc(x) \cdot y = y \cdot suc(x)$.

Como $y \in \mathbb{N}$ por Axioma (2) se tiene que $suc(y) \in \mathbb{N}$, ahora bien

$$\begin{aligned} suc(x) \cdot suc(y) &= suc(x) \cdot y + suc(x) \\ &= y \cdot suc(x) + suc(x) \\ &= (y \cdot x + y) + suc(x) \\ &= (x \cdot y + y) + suc(x) \\ &= suc((x \cdot y + y) + x) \\ &= suc((x \cdot y + x) + y) \\ &= x \cdot y + x + suc(y) \\ &= x \cdot suc(y) + suc(y) \\ &= suc(y) \cdot x + suc(y) \\ &= suc(y) \cdot suc(x). \end{aligned}$$

Así tenemos en virtud del Axioma (5) que $I = \mathbb{N}$, con lo cual $M = \mathbb{N}$. □

Teorema 16 *En $\mathbb{N}$ se cumple la propiedad distributiva, esto es*

$$(\forall x, y, z \in \mathbb{N})((x + y) \cdot z = x \cdot z + y \cdot z).$$

Demostración: Sea

$$M = \{z \in \mathbb{N} \mid (\forall x, y \in \mathbb{N})((x + y) \cdot z = x \cdot z + y \cdot z)\}$$

y demostremos que $M = \mathbb{N}$.

Veamos que $0 \in M$

$$(x + y) \cdot 0 = x \cdot 0 + y \cdot 0$$

es verdadero, luego se tiene que $0 \in M$.

Supongamos $z \in M$, es decir, $(\forall x, y \in \mathbb{N})((x + y) \cdot z = x \cdot z + y \cdot z)$.

Por demostrar que $suc(x) \in M$, debemos justificar que,

$$(\forall x, y \in \mathbb{N})((x + y) \cdot suc(z) = x \cdot suc(z) + y \cdot suc(z)),$$

para ello

$$\begin{aligned} (x + y) \cdot suc(z) &= (x + y) \cdot z + (x + y) && \text{definición del producto} \\ &= (x \cdot z + y \cdot z) + (x + y) && \text{Hipótesis} \\ &= (x \cdot z + x) + (y \cdot z + y) && \text{Asociatividad y Conmutatividad} \\ &= x \cdot suc(z) + y \cdot suc(z) \end{aligned}$$

Así tenemos que $suc(z) \in M$, y en virtud del Axioma (5) se tiene $M = \mathbb{N}$. □

Corolario 17 *En $\mathbb{N}$ es válida también la siguiente ley distributiva*

$$(\forall x, y, z \in \mathbb{N})(x \cdot (y + z) = x \cdot y + x \cdot z)$$

Demostración: Sean $x, y, z \in \mathbb{N}$ cualesquiera, entonces

$$\begin{aligned} x \cdot (y+z) &= (y+z) \cdot x && \text{Teorema (15)} \\ &= y \cdot x + z \cdot x && \text{Teorema (16)} \\ &= x \cdot y + x \cdot z && \text{Teorema (15)} \end{aligned}$$

□

Teorema 18 *En* $\mathbb{N}$ *se cumple la propiedad asociativa, esto es*

$$(\forall x, y, z \in \mathbb{N})((x \cdot y) \cdot z = x \cdot (y \cdot z)).$$

Demostración: Sea

$$M = \{x \in \mathbb{N} \mid (\forall y, z \in \mathbb{N})((x \cdot y) \cdot z = x \cdot (y \cdot z))\}$$

y demostremos que $M = \mathbb{N}$.

Por propiedad 14 tenemos que

$$(\forall y, z \in \mathbb{N})((0 \cdot y) \cdot z = 0 \cdot (y \cdot z)) \Leftrightarrow (\forall y, z \in \mathbb{N})(0 \cdot z = 0)$$

así $0 \in M$.

Supongamos ahora $x \in M$, esto es

$$(\forall y, z \in \mathbb{N})((x \cdot y) \cdot z = x \cdot (y \cdot z)),$$

queremos demostrar que $suc(x) \in M$, esto es,

$$(\forall y, z \in \mathbb{N})((suc(x) \cdot y) \cdot z = suc(x) \cdot (y \cdot z)),$$

lo cual se obtiene de

$$\begin{aligned} (suc(x) \cdot y) \cdot z &= (y \cdot x + y) \cdot z \\ &= (y \cdot x) \cdot z + y \cdot z \\ &= (x \cdot y) \cdot z + y \cdot z \\ &= x \cdot (y \cdot z) + 1 \cdot (y \cdot z) \\ &= (x+1) \cdot (y \cdot z) \\ &= suc(x) \cdot (y \cdot z) \end{aligned}$$

por lo tanto $M = \mathbb{N}$, es decir,

$$(\forall x, y, z \in \mathbb{N})((x \cdot y) \cdot z = x \cdot (y \cdot z)).$$

□

Observación: $(\mathbb{N}, +, \cdot)$, no es un anillo, ya que no cumple la propiedad de inverso aditivo.

1.2.3. Orden en $\mathbb{N}$

En esta sección definiremos un orden total en $\mathbb{N}$, para ello veremos la siguiente propiedad de los números naturales.
Notación: $\mathbb{N}^* = \mathbb{N} - \{0\}$.

Teorema 19 *Dados $x, y \in \mathbb{N}$ se presenta uno y sólo uno de los siguientes casos:*

1. *$x = y$.*
2. *Existe $u \in \mathbb{N}, u \neq 0$ tal que $x + u = y$.*
3. *Existe $v \in \mathbb{N}, v \neq 0$ tal que $y + v = x$.*

Demostración: Notemos que las tres proposiciones no pueden ser verdadera al mismo tiempo, ya que por el teorema 10 de cancelación $u = v = 0$ lo cual es una contradicción, luego definimos el conjunto

$$M = \{x \in \mathbb{N} \mid (\forall y \in \mathbb{N})[(x = y) \veebar (\exists u \in \mathbb{N}^*,\, x + u = y) \veebar (\exists v \in \mathbb{N}^*,\, y + v = x)]\}$$

y demostremos que $M = \mathbb{N}$.

Para demostrar que $0 \in M$, debemos justificar la siguiente proposición

$$(\forall y \in \mathbb{N})[(0 = y) \veebar (\exists u \in \mathbb{N}^*,\, u = y) \veebar (\exists v \in \mathbb{N}^*,\, y + v = 0)]$$

Veamos que la tercera condición es falsa, para ello $y + v = 0$ con $v \neq 0$, es decir, existe $z \in \mathbb{N}$, tal que $v = suc(z)$, luego

$$0 = y + v = y + suc(z) = suc(y + z),$$

lo cual contradice el Axioma (3).

Por lo tanto, $0 \in M$ es equivale a

$$(\forall y \in \mathbb{N})[(y = 0) \veebar (y \neq 0) \veebar F]$$

lo cual es verdadero.

Ahora demostraremos $(\forall x \in M)(suc(x) \in M)$, esto es:

Suponemos que

$$(\forall y \in \mathbb{N})[(x = y) \veebar (\exists u \in \mathbb{N}^*, x + u = y) \veebar (\exists \in \mathbb{N}^*, y + v = x)]$$

Queremos demostrar que

$$(\forall y \in \mathbb{N})[(suc(x) = y) \veebar (\exists u \in \mathbb{N}^*, suc(x) + u = y) \veebar (\exists v \in \mathbb{N}^*, y + v = suc(x))],$$

Sea $x \in M$, tal que cumpla una de las siguientes proposiciones

I. $y = x$.

II. $x + u = y$ para algún $u \neq 0$.

III. $x = y + v$ para algún $v \neq 0$.

Prime Caso: Si $x = y$ entonces se aplicando el sucesor obtenemos

$$suc(x) = y + 1$$

a. $y = suc(x)$.

b. $suc(x) + u = y$ para algún $u \neq 0$.

c. $suc(x) = y + v$ para algún $v \neq 0$.

Claramente Cumple (c), y al reemplazar en las otras dos obtenemos

$$y = y + 1 \qquad y + 1 + u = y$$

ambas son imposibles.

Segundo Caso: Si existe $u \in \mathbb{N}^*$ tal que $x+u = y$, luego existe $w \in \mathbb{N}$ tal que $suc(w) = u$ entonces se tiene

$$\begin{aligned} suc(x) + u &= suc(y), \\ suc(x) + suc(w) &= suc(y) \\ suc(suc(x) + w) &= suc(y) \\ suc(x) + w &= y \end{aligned}$$

Claramente se cumple una de las siguientes proposiciones

$$suc(x) = y) \veebar (\exists u \in \mathbb{N}^*, suc(x) + u = y)$$

Además reemplazando en la otra, la proposición

$$suc(x) = suc(x) + w + v$$

es falsa.

Tercer Caso: Si existe $v \in \mathbb{N}^*$ tal que $x = y + v$, aplicando el sucesor se tiene $suc(x) = y + suc(v)$, luego se cumple (c)

$$suc(x) = y + w \text{ para algún } w \neq 0.$$

Las otras proposición son falsas (a), (b), ya que al reemplazar obtenemos

$$y = y + suc(v) \quad y + suc(v) + u = y \text{ para algún } u \neq 0.$$

Cancelando

$$0 = suc(v) \quad suc(v) + u = 0 \text{ para algún } u \neq 0.$$

De este modo se tiene que $suc(x) \in M$, de lo cual obtenemos $M = \mathbb{N}$. □

Definición 6 *Sean $x, y \in \mathbb{N}$. Se dice que*

1. *x es **menor o igual** a y (o y es **mayor o igual** que x) si y sólo si existe $u \in \mathbb{N}$ de modo que $x + u = y$, este hecho lo anotaremos indistintamente por*

$$x \leq y \quad \vee \quad y \geq x.$$

Es decir,

$$x \leq y \Leftrightarrow (\exists u \in \mathbb{N})(x + u = y).$$

2. *x es **menor que** y (o y es **mayor que** x) si y sólo si existe $u \in \mathbb{N}^*$ de modo que $x + u = y$, este hecho lo anotaremos indistintamente por*

$$x < y \quad \vee \quad y > x.$$

Es decir,

$$x < y \Leftrightarrow (\exists u \in \mathbb{N}^*)(x + u = y).$$

Propiedad 20 *Sean $x, y \in \mathbb{N}$, entonces se tiene*

$$[x < y \Leftrightarrow (x \leq y) \wedge (x \neq y)]$$

o bien

$$[y > x \Leftrightarrow (y \geq x) \wedge (y \neq x)].$$

Notación: En adelante usaremos las siguientes notaciones:

1. $x \ngeq y$, quiere decir que x no es mayor o igual a y.
2. $x \nleq y$, quiere decir que x no es menor o igual a y.
3. $x \not< y$, quiere decir que x no es mayor que y.
4. $x \not> y$, quiere decir que x no es menor que y.

Propiedad 21 *Notemos que*

$$x \ngeq y \Leftrightarrow x < y.$$

Teorema 22 *La relación $\leq$ es una relación de orden en $\mathbb{N}$, es decir la relación es refleja, antisimétrica y transitiva.*

Demostración:
Refleja: Por la definición de suma se tiene que $x + 0 = x$, definición de $\leq$ se tiene que

$$x \leq x \quad \forall x \in \mathbb{N}.$$

Antisimétrica: Supongamos que $x \leq y \ \wedge \ y \leq x$. Luego existen $u, v \in \mathbb{N}$ tales que

$$x + u = y \quad \wedge \quad y + v = x$$

Si u, v uno de ellos es nulo, esta listo.

Supongamos que u, v son no nulo, luego

$$y = x + u = (y + v) + u = y + (v + u)$$

tenemos entonces que

$$y + 0 = y + (v + u)$$

cancelando tenemos que

$$u + v = 0.$$

Ahora bien, como $u \neq 0$ entonces $u = suc(z)$ para algún $z \in \mathbb{N}$ pero

$$0 = v + u = v + suc(z) = suc(v + z)$$

lo cual es una contradicción con el Axioma (2).Luego $u = 0 \vee v = 0$ entonces se cumple

$$x = y.$$

Transitiva: Supongamos $x \leq y \wedge y \leq z$. Luego existen $u, v \in \mathbb{N}$ tales que

$$x + u = y \quad \wedge \quad y + v = z$$

de esto es claro que

$$x + u + v = z$$

es decir

$$x + (u + v) = z$$

por lo tanto

$$x \leq z.$$

□

Observación: La transitividad se mantiene al cambiar $\leq$ por $<$, es decir, dados $x, y, z \in \mathbb{N}$

$$[(x < y) \wedge (y < z)] \Rightarrow (x < z).$$

Teorema 23 (Totalidad) *Dados x e $y \in \mathbb{N}$ se cumple una y sólo una de las siguientes proposición*

1. $x = y$.
2. $x < y$.
3. $y < x$.

Demostración: Inmediata a partir del Teorema (19) y la definición del símbolo $<$.

□

Teorema 24 *La suma en $\mathbb{N}$ es monótona, es decir*

$$(\forall x, y, z \in \mathbb{N})(x \leq y \Rightarrow (x + z \leq y + z)).$$

Demostración: Supongamos $x \leq y$, luego existe $u \in \mathbb{N}$ tal que $x + u = y$ de donde

$$\begin{array}{rrcl} & (x+u)+z & = & y+z, \quad \forall z \in \mathbb{N} \\ \Leftrightarrow & x+(u+z) & = & y+z \\ \Leftrightarrow & x+(z+u) & = & y+z \\ \Leftrightarrow & (x+z)+u & = & y+z \end{array}$$

de esto es claro que

$$x + z \leq y + z.$$

□

Corolario 25 *Sea $x \in \mathbb{N}$, entonces*

$$x \leq suc(x).$$

Teorema 26 *Para todo $x \in \mathbb{N}$ se tiene que $x \geq 0$.*

Demostración: Por Propiedad (6) tenemos que $0 + x = x$, $\forall x \in \mathbb{N}$, es decir existe $u = x$ tal que $0 + u = x$, y por definición de mayor o igual se tiene que $x \geq 0$ □

Corolario 27 *Si $x \in \mathbb{N}^*$ entonces $x \geq 1$.*

Demostración: Supongamos $x \neq 0$.

Entonces $x = suc(y)$ para algún $y \in \mathbb{N}$, luego como $suc(y) = y + 1$ se tiene que

$$x = y + 1 = 1 + y,$$

de donde

$$x \geq 1.$$

Corolario 28 *Sean $x, y \in \mathbb{N}$, tal que $x < y$ entonces,*

$$suc(x) \leq y$$

Demostración: Supongamos $y > x$. Luego existe $u \in \mathbb{N}, u \neq 0$ tal que $x + u = y$, ahora bien como $u \neq 0$ entonces $u = suc(v)$ para algún $v \in \mathbb{N}$, luego

$$y = x + suc(v) = suc(x + v) = suc(v + x) = v + suc(x),$$

de donde obtenemos que

$$y \geq suc(x) \quad \forall x, y \in \mathbb{N}.$$

□

Teorema 29 *Sean $x, y \in \mathbb{N}$.*

$$Si\ x > 0\ e\ y > 0\ entonces\ xy > 0.$$

Demostración: Como $y > 0$ es decir $y \neq 0$ tenemos que existe $u \in \mathbb{N}$ tal que $y = suc(u)$, ahora

$$xy = xsuc(u)$$

luego existe xu tal que

$$xy = xu + x$$

es decir

$$xy \geq x$$

además $x > 0$, así tenemos que

$$xy \geq x > 0.$$

A partir de esto, tenemos los siguientes casos:

1. $xy > x$, es decir $xy > x > 0$, luego por transitividad obtenemos que

$$xy > 0.$$

2. $xy = x$, es decir $xy = x > 0$ de donde

$$xy > 0.$$

□

Teorema 30 *El producto en* $\mathbb{N}$ *es monótono.*
Sean $x, y, z \in \mathbb{N}$

$$(x < y) \wedge (z > 0) \Rightarrow (xz < yz).$$

Demostración: Supongamos $(x < y) \wedge (z > 0)$. Luego como

$$x < y \Leftrightarrow (\exists u \in \mathbb{N}, u \neq 0)(x + u = y)$$

tenemos que

$$(x + u)z = yz$$

de esto

$$xz + uz \;\; = \;\; yz. \tag{1.4}$$

Ahora bien como $u \in \mathbb{N} \wedge u \neq 0$ se tiene que $u > 0$, y $z > 0$ (por hipótesis), tenemos que $uz > 0$ teorema anterior, por lo tanto, de la relación (1.4) se obtiene que $xz \leq yz$ pero como $uz > 0$, tenemos que $uz \neq 0$ entonces podemos concluir que

$$xz < yz.$$

□

Teorema 31 *Si* $x \neq 0$ *e* $y \neq 0$ *entonces* $xy \neq 0$ *para todo* $x, y \in \mathbb{N}$.

Demostración: Supongamos $x \neq 0$ e $y \neq 0$. además como todo número natural es mayor o igual a cero tenemos en particular que $x \geq 0$, luego se obtiene que $x > 0$. Del mismo modo podemos se concluye que $y > 0$.

Así tenemos que $x > 0 \wedge y > 0$ con lo cual $xy > 0$, por la definición de mayor que se tiene que

$$xy \neq 0$$

□

Teorema 32 *Sean $x, y, z \in \mathbb{N}$ tales que $z \neq 0$ entonces se cumple.*

$$[(x \neq y) \Rightarrow (zx \neq zy)]$$

Demostración: Sean $x, y, z \in \mathbb{N}$ tales que $z \neq 0$ $x \neq y$

Por el teorema 23 consideremos entonces los siguientes casos:

1. Supongamos $x > y$, luego existe $u \in \mathbb{N}, u \neq 0$ de modo que $y + u = x$ de esto

$$zx = z(y + u) = zy + zu. \tag{1.5}$$

   Ahora bien como $z \neq 0$ y $u \neq 0$ tenemos que $zu \neq 0$, este hecho y la igualdad en (1.5) implican que $zx > zy$ con lo cual

$$zx \neq zy.$$

2. Análogo al caso anterior suponiendo $x < y$.

□

Teorema 33 (Principio del Buen Orden)

Todo subconjunto no vacío de $\mathbb{N}$ tiene un menor elemento, en símbolos

$$(\forall A \subseteq \mathbb{N}, A \neq \emptyset)(\exists a \in A)(\forall x \in A)(a \leq x).$$

Demostración: Sea $\emptyset \neq A \subseteq \mathbb{N}$ y consideremos el conjunto

$$B = \{x \in \mathbb{N} \mid (\forall y \in A)(\, x \leq y \,)\}.$$

En primer lugar notemos que el conjunto B verifica las siguientes propiedades:

1. $0 \in B$ pues como $x \geq 0$ para todo $x \in \mathbb{N}$ en particular

$$(\forall y \in A)(\, y \geq 0 \,)$$

2. Como $A \neq \emptyset$, luego existe $x \in A$ y además $x < suc(x)$, luego $suc(x) \notin B$, luego $B \neq \mathbb{N}$, por lo tanto B no puede cumplir la condición

$$(\forall x \in B)(\, suc(x) \in B \,)$$

   Por ello, existe $u \in B$, tal que $u + 1 \notin B$,

   Ahora bien para probar el teorema basta probar que $u \in A$.

   Supongamos lo contrario, esto es $u \in B \wedge u \notin A$. Luego $(\forall y \in A)(\, u < y \,)$, por corolario 28 tenemos que $(\forall y \in A)(\, u + 1 \leq y \,)$ lo cual implica que $u + 1 \in B$ y esto es una contradicción.

   Por lo tanto $u \in A$, es decir, $(\exists u \in A)(\forall y \in A)(\, u \leq y \,)$. □

Teorema 34 (Principio de Inducción)
Sea $n \in \mathbb{N}$ y $p(n)$ una proposición en la variable n. Si se cumple

1. *$p(0)$ es verdadera.*

2. *$(\forall n \in \mathbb{N})(p(n) \Rightarrow p(suc(n))$ es verdadera.*

Entonces la proposición $p(n)$ es válida para todo $n \in \mathbb{N}$.

Demostración: Sea

$$M = \{n \in \mathbb{N} \mid p(n) \text{ es verdadera}\}$$

y demostremos que $M = \mathbb{N}$.

Por hipótesis tenemos que $p(0)$ es verdadera, luego $0 \in M$.

Supongamos $n \in M$, es decir, $p(n)$ es verdadera, pero por hipótesis si $p(n)$ es verdadera entonces $p(suc(n))$ es verdadera, luego se tiene que $suc(n) \in M$, ahora bien en virtud del Axioma (5)tenemos que $M = \mathbb{N}$ lo cual concluye la demostración.

□

Observación: Sabemos que $suc(n) = n + 1$, luego el teorema precedente se puede escribir como sigue:

Corolario 35 (Teorema de Inducción)
Sea $p(n)$ una función proposicional en la variable $n \in \mathbb{N}$. Si

1. *$p(0)$ y*

2. *$(\forall n \in \mathbb{N})(p(n) \Rightarrow p(n+1))$*

Entonces la proposición $p(n)$ es válida para todo $n \in \mathbb{N}$.

Corolario 36 (Segundo Teorema de Inducción)
Sea $p(n)$ una función proposicional en la variable $n \in \mathbb{N}$. Si

1. *$(\exists k_0 \in \mathbb{N})(p(k_0))$ y*

2. *$(\forall n \in \mathbb{N})((n \geq k_0 \wedge p(n)) \Rightarrow p(n+1))$*

Entonces la proposición $n \geq k_0 \Rightarrow p(n)$ es válida para todo $n \in \mathbb{N}$.

Corolario 37 (Tercer Teorema de Inducción)
Sea $p(n)$ una función proposicional en la variable $n \in \mathbb{N}$. Si

1. *$p(0)$ y*

2. *$(\forall n \in \mathbb{N})((p(0) \wedge p(1) \wedge \cdots \wedge p(n)) \Rightarrow p(n+1))$*

Entonces la proposición $p(n)$ es válida para todo $n \in \mathbb{N}$.

1.3. Ejercicios Desarrollados

Ejemplo 6 *Sea A un subconjunto de números reales que cumple las siguientes propiedades:*

$Ax.$I. $4 \in A \ \wedge \ 7 \notin A$.

$Ax.$II. $(\forall x \in A)(3x + 1 \in A)$.

$Ax.$III. $(\forall x, y \in A)(x + y \in A)$.

Demuestre las siguientes propiedades

a. $3 \in A \Rightarrow 14 \in A$.

b. $9 \in A \Rightarrow (21 \in A \vee 31 \notin A)$.

c. $(\forall x, y \in A)(-3x - 2y \notin A)$.

Demostración:

a. Si $3 \in A$, implica que $3 \cdot 3 + 1 = 10 \in A$.
Pero $4 \in A \wedge 10 \in A$, por lo tanto $10 + 4 = 14 \in A$.
De esta manera se tiene que, si $3 \in A$ entonces $14 \in A$.

b. Supongamos que $9 \in A, 4 \in A$, por propiedad Ax.III se tiene que $9 + 4 = 13 \in A$.
Análogamente $13 \in A, 4 \in A$, por propiedad Ax.III se tiene que $13 + 4 = 17 \in A$.
Finalmente $17 \in A, 4 \in A$, por propiedad Ax.III se tiene que $17 + 4 = 21 \in A$.
Como $21 \in A$, luego la proposición $21 \in A \vee 31 \notin A$ es verdadera.
De esta manera se obtiene que, $9 \in A \Rightarrow (21 \in A \vee 31 \notin A)$.

c. Por absurdo, supongamos $(\forall x, y \in A)(-3x - 2y \notin A)$ es falso, es decir,

$$(\exists x, y \in A)(-3x - 2y \in A) \text{ es verdadero.}$$

Sean $x, y \in A$ tal que $-3x - 2y \in A$, luego

$$\begin{aligned} x \in A &\Rightarrow 3x + 1 \in A \quad \text{Prop Ax.II} \\ -3x - 2y \in A \wedge 3x + 1 \in A &\Rightarrow -2y + 1 \in A \quad \text{Prop Ax.III} \end{aligned}$$

$$\begin{aligned} -2y + 1 \in A \wedge y \in A &\Rightarrow -y + 1 \in A \\ -y + 1 \in A \wedge y \in A &\Rightarrow 1 \in A \\ 1 \in A \wedge 4 \in A &\Rightarrow 5 \in A \\ 1 \in A \wedge 5 \in A &\Rightarrow 6 \in A \\ 1 \in A \wedge 4 \in A &\Rightarrow 7 \in A \end{aligned}$$

Lo cual es una contradicción, por lo tanto

$$(\forall x, y \in A)(-3x - 2y \notin A), \quad \text{es Verdadero}$$

□

Ejemplo 7 *Demostrar por inducción*

$$(\forall n \in \mathbb{N} - \{0\})(\forall a \in \mathbb{Z})[a(2a+1) \mid ((a+1)^{2n} - a^{2n} - 2a - 1)]$$

Demostración: Sea

$$p(n) : (\forall a \in \mathbb{Z})[a(2a+1) \mid ((a+1)^{2n} - a^{2n} - 2a - 1)]$$

Veamos

$$\begin{aligned} p(1) &: (\forall a \in \mathbb{Z})[a(2a+1) \mid ((a+1)^2 - a^2 - 2a - 1)] \\ &: (\forall a \in \mathbb{Z})[a(2a+1) \mid 0] \equiv V \end{aligned}$$

Supongamos $p(n)$ y demostremos $p(n+1)$

$$\begin{aligned} p(n) &: (\forall a \in \mathbb{Z})[a(2a+1) \mid ((a+1)^{2n} - a^{2n} - 2a - 1)] \\ p(n+1) &: (\forall a \in \mathbb{Z})[a(2a+1) \mid ((a+1)^{2n+2} - a^{2n+2} - 2a - 1)] \end{aligned}$$

Dado $a \in \mathbb{Z}$, existe $k \in \mathbb{Z}$ tal que $((a+1)^{2n} - a^{2n} - 2a - 1) = a(2a+1)k$ o bien $(a+1)^{2n} = a^{2n} + 2a + 1 + a(2a+1)k$

$$\begin{aligned} & (a+1)^{2n+2} - a^{2n+2} - 2a - 1 \\ = \; & (a+1)^{2n}(a+1)^2 - a^{2n+2} - 2a - 1 \\ = \; & [a^{2n} + 2a + 1 + a(2a+1)k](a+1)^2 - a^{2n+2} - 2a - 1 \\ = \; & a^{2n}(a+1)^2 + (2a+1)(a+1)^2 + a(2a+1)k(a+1)^2 - a^{2n+2} - 2a - 1 \\ = \; & a^{2n}(a+1)^2 - a^{2n+2} + (2a+1)(a+1)^2 - (2a+1) + a(2a+1)k(a+1)^2 \\ = \; & a^{2n}((a+1)^2 - a^2) + (2a+1)((a+1)^2 - 1) + a(2a+1)k(a+1)^2 \\ = \; & a^{2n}(2a+1) + (2a+1)(a^2 + 2a) + a(2a+1)k(a+1)^2 \\ = \; & a(2a+1)a^{2n-1} + a(2a+1)(a+2) + a(2a+1)k(a+1)^2 \\ = \; & a(2a+1)[a^{2n-1} + (a+2) + k(a+1)^2] = a(2a+1)k' \end{aligned}$$

Luego

$$(\forall n \in \mathbb{N}^*))(p(n) \Rightarrow p(n+1))$$

es verdadera. Por teorema de inducción se concluye.

Ejemplo 8 *Demostrar*

$$(\forall n, m \in \mathbb{N})(n + m = 0 \Rightarrow (n = 0 \wedge m = 0)).$$

Demostración: Notemos que la proposición es equivalente a

$$(\forall n, m \in \mathbb{N})((n \neq 0 \vee m \neq 0) \Rightarrow n + m \neq 0).$$

Luego supongamos que $n \neq 0 \vee m \neq 0$
Primer Caso: Si $n \neq 0$ existe $n' \in \mathbb{N}$ tal que $suc(n') = n$

$$n + m = suc(n') + m = suc(n' + m) \in \mathbb{N}^*$$

Por lo tanto $n + m \neq 0$

Segundo Caso: Si $m \neq 0$ existe $m' \in \mathbb{N}$ tal que $suc(m') = m$

$$n + m = n + suc(m') = suc(n + m') \in \mathbb{N}^*$$

Por lo tanto $n + m \neq 0$.

De Primer y Segundo Caso, se tiene que

$$(\forall n, m \in \mathbb{N})((n \neq 0 \vee m \neq 0) \Rightarrow n + m \neq 0).$$

Ejercicio 9 *Sea A un subconjunto de números reales que cumple las siguientes propiedades (axiomas):*

$Ax.$I. $5 \in A \ \wedge \ 7 \notin A.$

$Ax.$II. $(\forall x \in A)(3x + 2 \in A).$

$Ax.$III. $(\forall x, y \in A)(x + y \in A).$

Demuestre los siguientes propiedades

a. $3 \in A \Rightarrow 16 \in A.$

b. $4 \in A \Rightarrow 23 \in A.$

c. $11 \in A \Rightarrow (28 \in A \vee 31 \notin A).$

d. $24 \notin A \Rightarrow (4 \notin A \vee 12 \in A).$

e. $2 \notin A.$

f. $(\forall x, y \in A)(3x + 2y + 17 \in A).$

g. $(\forall x, y \in A)(7x + 3y + 16 \in A).$

h. $(\forall x, y \in A)(-3 - 3x - y \notin A).$

i. $(\forall y, z \in \mathbb{R})((3y + z + 7) \notin A \Rightarrow (y \notin A \vee \frac{z}{2} \notin A)).$

j. $(\forall y, z \in \mathbb{R})((3y \notin A \wedge (z + 10) \notin A) \Rightarrow (y \notin A \vee z \notin A)).$

Ejercicio 10 *Dado el conjunto*

$$A = \{0\} \cup \left\{ n + \frac{1}{m} \mid n \in \mathbb{N}, m \in \mathbb{N}^* \right\}.$$

Determine que Axiomas de Peano satisface el conjunto A.

Ejercicio 11 *Demostrar directamente*

a. $(\forall n \in \mathbb{N})(suc(n) = n + suc(0)).$

b. $(\forall n \in \mathbb{N})(suc(n) + m = suc(m + n))$.

c. $(\forall n \in \mathbb{N})(suc(suc(n)) \neq 1)$.

d. $(\forall n, m \in \mathbb{N})(m + suc(n) \neq m)$.

e. $(\forall n, m \in \mathbb{N})(n + m = 0 \Rightarrow (n = 0 \wedge m = 0))$.

f. $(\forall n, m \in \mathbb{N})(n \cdot m = 0 \Rightarrow (n = 0 \vee m = 0))$.

g. $(\forall r \in \mathbb{N}^*)(\forall n, m \in \mathbb{N})(r \cdot n = r \cdot m \Rightarrow (n = m))$.

Ejercicio 12 *Demostrar usando las propiedades*

a. $(\forall n, m \in \mathbb{N})(suc(m \cdot suc(n)) = m \cdot n + suc(m))$.

b. $(\forall n, m \in \mathbb{N})(suc(m) + suc(n) = suc(n + m) + 1 = suc(suc(n + m)))$.

Ejercicio 13 *Sea* $\{a_n\}$ *una sucesión definida por recurrencia, tal que*

$$f(0) = 0;\ f(1) = 1;\ a_n = a_{n-1} + a_{n-2},\ \text{con } n \leq> 1.$$

Demostrar que

1. $(\forall n \in \mathbb{N})(f(n) < \left(\frac{7}{4}\right)^n)$.
2. $(\forall 4 < n \in \mathbb{N})(\left(\frac{4}{3}\right)^n < f(n))$.
3. $(\forall n \in \mathbb{N})(\forall m \in \mathbb{N}^*)(f(n + m) = f(m - 1)f(n) + f(m)f(n + 1))$.
4. $$(\forall n \in \mathbb{N})\left(f(n) = \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right]\right).$$