Índice general

0.1. Introducción

El objetivo central del curso de Algebra IV que se imparte en la Escuela Superior de Física y Matemáticas del IPN es el presentar una construcción axiomática de los sistemas númericos que más se usan en matemáticas, a saber: el sistema de los números enteros, el campo de los números racionales y el campo de los números reales. Dicha construcción suele iniciarse con un sistema de Peano, cuya existencia puede darse por cierta o hacer uso de un axioma de la teoría de conjuntos para construirlo. Una vez dado un sistema de Peano, la construcción de los reales, a partir de los axiomas de Peano sigue un método paso a paso, el cual toma una cantidad considerable de tiempo y esfuerzo. Construído el campo de los números racionales, hay dos procedimientos más o menos estándar para construir el campo de los números reales; esto se refiere a los métodos que usan sucesiones de Cauchy de racionales y cortaduras de Dedekind respectivamente. En el fondo estos métodos difieren poco, si bien, uno pudiera decirse método de análisis y el otro método algebraico, los dos comparten ideas de análisis.

En la década de los 70's, Conway [2] propuso un método para construir el sistema de los números reales evitando el proceso paso por paso cuando se inicia con los axiomas de Peano. Indudablemente, el método propuesto por Conway tiene ventajas y desventajas, una de las ventajas de este método es el evitar la ruta larga de los métodos antes citados, y conectar conceptos numéricos con algunos conceptos de la teoría de juegos.

Una de las mayores desventajas del método de Conway para ser presentado en un curso de licenciatura, es que se requiere una formación más sólida por parte del alumno, pues hace uso de ciertos conocimientos de la teoría de juegos, teoría axiomática de conjuntos y algunos conceptos de teoría de grupos. El siguiente es uno de los comentarios del propio Conway en cuanto a presentar su método en un curso de licenciatura

> ... The remaining disadvantages are that the dyadic rationals receive a curiously special treatment, and that the inductive definitions are of an unusual character. From a purely logical point of view these are unimportant quibbles but they would predispose me against teaching this to undergraduates as "the theory of real numbers"

Pudiera decirse, exagerando un poco, que el método de Conway es plantear de forma más general el concepto de cortadura de Dedekind[1] en los racionales. Para una discusión detallada del método de Conway se sugiere consultar [2] y [3].

El método que se discute en el presente trabajo para construir el sistema de los números reales es el que utiliza sucesiones de Cauchy. Algunas razones por las que se optó por este procedimiento, es la familiaridad que el alumno de cuarto semestre de licenciatura tiene con sucesiones y límites. Otro argumento en favor de este método se debe a que es el que se utiliza en la completación de un espacio métrico, uno de cuyos casos especiales es el muy importante — en teoría de números — proceso de completar el campo de los números racionales cuando se consideran todas las posibles valuaciones en éste; obteniéndose en un caso los números reales y en los restantes los números p-ádicos, para cada primo p.

[1] Ver definición después del teorema 51

Finalmente, la idea de escribir unas notas para el curso de Algebra IV, tiene entre otras motivaciones, el presentar una referencia al alumno que le ayude en su preparación para dicho curso. El material que se presenta es el que describe el programa vigente del curso de Algebra IV que se imparte en la ESFM del IPN.

Agradezco a René Villanueva Barrera su valiosa colaboración en la transcripción de estas notas. Los errores tipográficos y de otra índole son de mi completa responsabilidad.

Fernando Barrera Mora

septiembre de 1996

0.2. Teoría de Conjuntos

Antes de iniciar la discusión, una nota aclaratoria sobre cierta notación que usaremos hace falta. El símbolo ■ denotará el fin de una demostración. Otro símbolo que usaremos es $\Longrightarrow\Longleftarrow$, el cual denotará que se ha encontrado una contradicción en un argumento por reducción al absurdo.

La palabra "conjunto" será un término no definido y usaremos la idea intuitiva de conjunto como una "colección" de objetos con una propiedad específica. La notación para conjuntos y las relaciones entre conjuntos y elementos es la usual, por ejemplo: $A \subseteq B$ significa que A es un subconjunto de B, es decir todo elemento de A es un elemento de B, $a \in A$ expresa que a es un elemento de A.

Tomamos como punto de inicio los siguientes hechos evidentes.

1. $A \subseteq A$
2. $A \subseteq B$ y $B \subseteq C \Longrightarrow A \subseteq C$.
3. $A = B \iff A \subseteq B$ y $B \subseteq A$.

Aceptamos como válido lo siguiente: si A es un conjunto y P es una propiedad de algunos elementos de A, entonces $\{a \in A : x \text{ satisface } P\}$ es un conjunto, de hecho un subconjunto de A. Para un conjunto A, se define el subconjunto *vacío* de A, denotado por $\emptyset_A = \{a \in A : a \neq a\}$, el cual no tiene elementos.

Observación 1. *Hay solamente un conjunto vacío, es decir $\emptyset \subseteq A$ para todo conjunto A.*

Demostración. Sean A y B dos conjuntos, si por ejemplo $\emptyset_A \nsubseteq \emptyset_B$ entonces existe un elemento en $\emptyset_B$ el cual no pertenece a $\emptyset_A$, imposible, de aquí se concluye que $\emptyset_A \subseteq \emptyset_B$ y un argumento análogo prueba $\emptyset_B \subseteq \emptyset_A$. ■

Definición. *Si $A, B \subseteq \Gamma$, se define:*

1. $A \cup B := \{x \in \Gamma : \ x \in A \text{ y/o } x \in B\}$ *(A unión B).*
2. $A \cap B := \{x \in \Gamma : \ x \in A \text{ y } x \in B\}$ *(A intersección B).*

Las siguientes propiedades se tienen directamente de las definiciones.

1. $A \cup B = A \iff B \subseteq A$.
2. $A \cap B = A \iff A \subseteq B$.
3. $A \cap B \subseteq A, B \subseteq A \cup B$.

Teorema 1. *Sean A, B, C subconjuntos de un mismo conjunto Γ. Entonces se tiene:*

i) $A \cup A = A \cap A = A$.

ii) $A \cup (B \cup C) = (A \cup B) \cup C$, *asociatividad de la unión.*

iii) $A \cap (B \cap C) = (A \cap B) \cap C$, *asociatividad de la intersección.*

iv) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$, *distributividad de la intersección respecto a la unión.*

Demostración. Las tres primeras conclusiones son claras.
iv) Sea $x \in \Gamma$, $x \in A \cap (B \cup C) \iff x \in A$ y $x \in B \cup C \iff x \in A$ y $(x \in B$ y/o $x \in C)$ $\iff x \in A \cap B$ y/o $x \in A \cap C \iff x \in (A \cap B) \cup (A \cap C)$. ■

Otras operaciones de utilidad en teoría de conjuntos son la diferencia y complemento que se definen en seguida.

Si A, B son subconjuntos de E se define la diferencia de A y B denotada $A \setminus B := \{x \in A : x \notin B\}$. Si $A \subseteq B$ se define el complemento de A respecto a B denotado $A_B^c := B \setminus A$. Si es claro que A es subconjuto de B, el complemento de A respecto a B se denotará simplemente por A^c. Si $A, B \subseteq E$, entonces se tiene $A \setminus B = A \cap B_E^c$.

Las siguientes propiedades se verifican directamente.

Para cada $A, B \subseteq E$ se tiene

i) $A \cap A_E^c = \emptyset$, $E = A \cup A_E^c$.

ii) $(A_E^c)_E^c = A$.

iii) $\emptyset_E^c = E$, $E_E^c = \emptyset$.

iv) $A \subseteq B \iff B_E^c \subseteq A_E^c$.

Teorema 2 (Leyes de De Morgan). *Suponga que $A, B \subseteq E$. Si los complementos son tomados respecto a E entonces se tiene.*

i) $(A \cap B)^c = A^c \cup B^c$.

ii) $(A \cup B)^c = A^c \cap B^c$.

Demostración. i) $x \in (A \cap B)^c \iff x \notin (A \cap B), \iff x \notin A$ y/o $x \notin B, \iff x \in A^c$ y/o $x \in B^c, \iff x \in A^c \cup B^c$.
ii) Se prueba de manera análoga al caso anterior. ■

0.2.1. Producto Cartesiano de Conjuntos

La interpretación intuitiva del producto cartesiano de dos conjuntos es considerar "parejas" de elementos uno de cada conjunto, es decir, si A y B son dos conjuntos entonces los elementos de $A \times B$ (A cruz B) son de la forma (a, b) con $a \in A$ y $b \in B$. Esta forma de interpretar a los elementos del producto cartesiano de A y B es de gran utilidad, sin embargo la formulación precisa requiere hacer uso solamente de los términos ya considerados.

Por una pareja ordenada (a, b) entenderemos al conjunto $\{\{a\}, \{a, b\}\}$, es decir la pareja ordenada (a, b) es el conjunto cuyos elementos son los conjuntos $\{a\}$ y $\{a, b\}$ con $a \in A$ y $b \in B$. En la pareja (a, b), a se llama la primera coordenada y b la segunda coordenada de la pareja. Después de formular la definición de pareja ordenada resta verificar que existe un conjunto cuyos elementos sean las parejas ordenadas con primera entrada en A y segunda entrada en B.

Notemos que para que exista un conjunto cuyos elementos sean parejas ordenadas se requiere garantizar la existencia de un conjunto cuyos elementos sean subconjuntos de la forma $\{a\}$ y $\{a, b\}$ es decir cuyos elementos sean subconjutos, para esto requerimos:

Axioma del Conjunto Potencia. *Para cada conjunto A existe un conjunto denotado por $\mathcal{P}(A)$ cuyos elementos son los subconjuntos de A.*

Con el Axioma del Conjunto Potencia y la definición de pareja ordenada se tiene que $(a, b) \in \mathcal{P}(\mathcal{P}(A \cup B))$, entonces el producto cartesiano de A y B denotado $A \times B$ es subconjunto de $\mathcal{P}(\mathcal{P}(A \cup B))$ y sus elementos satisfacen:
$A \times B := \{(a, b) : \ a \in A, \, b \in B\}$.

Observación 2. $A \times B = \emptyset \iff A = \emptyset$ *y/o* $B = \emptyset$.

Demostración. Si $A \times B \neq \emptyset$ entonces existe $(a, b) \in A \times B$ con $a \in A$ y $b \in B$, de lo cual se tiene que A y B son no vacíos. Recíprocamente, si A y B son no vacíos entonces $A \times B$ es no vacío. ■

Si $C \times D \neq \emptyset$ entonces $C \times D \subseteq A \times B \iff C \subseteq A$ y $D \subseteq B$.

Demostración. Ejercicio.

El siguiente resultado muestra la relación que hay entre las operaciones de unión, intersección y producto cartesiano de conjuntos.

Teorema 3. *Sean A, B, C tres conjuntos. Entonces*

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

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

iii) $A \times (B \setminus C) = (A \times B) \setminus (A \times C)$.

Demostración. i) Si $(a,x) \in A \times (B \cup C)$ entonces $a \in A$ y $x \in B \cup C$, de lo anterior $(a,x) \in (A \times B) \cup (A \times C)$. Recíprocamente, si $(a,x) \in (A \times B) \cup (A \times C)$, entonces $(a,x) \in A \times (B \cup C)$.

ii) y iii) se prueban de manera análoga. ■

0.2.2. Funciones

El concepto de función es uno de los más útiles en matemáticas, de hecho este concepto ha sido usado desde los primeros cursos de matemáticas. La idea intuitiva de función, por cierto de mucha utilidad, es el considerarla como una "regla" de correspondencia entre los elementos de un conjunto A, (llamado el dominio de la función) y los elementos de un conjunto B, (llamado el contradominio de la función) con la condición que para un elemento $a \in A$ exista un único elemento $b \in B$ asociado a a. Esta idea intuitiva de función es la que da origen a la definición formal.

Definición. *Sean X y Y dos conjuntos, una función f de X a Y es un subconjunto del producto cartesiano $X \times Y$ tal que $(a,b),(a,c) \in f$ implica $b = c$. Si f es una función de X a Y usaremos la notación $f : X \to Y$ y si $(x,y) \in f$, y se llamará el valor de f en x y esto lo denotaremos por $f(x) = y$.*

Observación 3. *Note que la definición de función es lo que en cálculo se llama la gráfica de la función f.*

Observación 4. *Si X ó Y es vacío, entonces $X \times Y = \emptyset$*

i) Si $X = \emptyset$, entonces $\emptyset$ es una función, y es única.

ii) Si $Y = \emptyset$, entonces $\emptyset$ no es función de X en Y, pues de ser función el conjunto vacío, se tiene que para $x \in X$ existe un único $y \in Y$ tal que $(x,y) \in \emptyset$, imposible.

Dada una función f de X a Y, f induce dos funciones, una tiene por dominio a $\mathcal{P}(X)$ y contradominio a $\mathcal{P}(Y)$ denotada también por f y definida como sigue, si $A \subseteq X$, $f(A) := \{y \in Y : \ y = f(x) \text{ para algún } x \in A\}$, al conjunto $f(A)$ se le llama la imagen directa de A bajo f. La otra función se denota por f^{-1}, tiene por dominio a $\mathcal{P}(Y)$ y contradominio a $\mathcal{P}(X)$ y se define de la siguiente manera, si $B \subseteq Y$, $f^{-1}(B) := \{x \in X : \ f(x) \in B\}$, al conjunto $f^{-1}(B)$ se le llama la imagen inversa de B bajo f.

Nota. La función f^{-1} no debe confundirse con la función inversa de f (definición que se dará más adelante), pues tienen diferentes dominios, desafortunadamente se usa la misma notación para ambas.

Ejemplo. Sean $X = \mathbb{R}^2$, $Y = \mathbb{R}^3$ considerados como espacios vectoriales, $f(x,y) = (x - y, x, y)$, es claro que f es una transformación lineal no singular, pues el único elemento que va al cero bajo f es el cero. Si W es un subespacio de $\mathbb{R}^2$ de dimensión uno, entonces $f(W)$

también es un subespacio de dimensión uno, en particular, si $W = \{(x, y) \in \mathbb{R}^2 : \ y = x\}$ se tiene que $f(W) = \{(0, x, x) \in \mathbb{R}^3 : \ x \in \mathbb{R}\}$. Como un ejercicio determine $f(\mathbb{R}^2)$ y $f^{-1}(\{(0, 1, -2)\})$.

En algunas ocasiones es de utilidad considerar más de dos conjuntos a la vez, en este caso se tiene la necesidad de considerar lo que llamaremos una "familia" de conjuntos. Una familia de conjuntos puede considerarse siempre como una colección de subconjuntos de un conjunto. Para precisar lo anterior, supongamos que Ω y Γ son dos conjuntos y $f : \Omega \to \mathcal{P}(\Gamma)$ una función, es decir a cada elemento $\alpha \in \Omega$ le corresponde, bajo f, un único subconjunto $A_\alpha \subseteq \Gamma$. A la colección $\{A_\alpha\}_{\alpha\in\Omega}$ le llamaremos una familia de conjuntos con índices en Ω.

Observación 5. *Si $\{A_\alpha\}_{\alpha\in\Omega}$ es una familia de conjuntos entonces:*

i) $\cap\mathcal{P}(A_\alpha) = \mathcal{P}(\cap A_\alpha)$. *La intersección se toma sobre los elementos de* Ω.

ii) $\cup\mathcal{P}(A_\alpha) \subseteq \mathcal{P}(\cup A_\alpha)$. *La unión se toma sobre los elementos de* Ω. *El siguiente ejemplo muestra que la igualdad no siempre se tiene.*

Demostración. Ejercicio.

Ejemplo. Sean $A = \{1\}$ y $B = \{2\}$, entonces $\mathcal{P}(A) = \{\emptyset, A\}$, $\mathcal{P}(B) = \{\emptyset, B\}$ y $\mathcal{P}(A) \cup \mathcal{P}(B) = \{\emptyset, A, B\}$, por otro lado $\mathcal{P}(A \cup B) = \{\emptyset, A, B, \{1, 2\}\}$, es decir no se tiene igualdad en ii) de la observación anterior.

El siguiente resultado muestra como es el comportamiento de la función f^{-1} cuando actúa en subconjuntos de su contradominio.

Teorema 4. *Sea $f : X \to Y$ una función, entonces se tiene:*

i) $f^{-1}(\cup B_\alpha) = \cup f^{-1}(B_\alpha)$.

ii) $f^{-1}(\cap B_\alpha) = \cap f^{-1}(B_\alpha)$.

iii) $f^{-1}(B_1 \setminus B_2) = f^{-1}(B_1) \setminus f^{-1}(B_2)$.

Las operaciones de unión e intersección son tomadas sobre un conjunto de índices Ω.

Demostración. i) Sea $x \in f^{-1}(\cup B_\alpha)$ entonces $f(x) \in \cup B_\alpha$, por lo tanto existe $\alpha \in \Omega$ tal que $f(x) \in B_\alpha$, de esto se tiene que $x \in f^{-1}(B_\alpha) \subseteq \cup f^{-1}(B_\alpha)$. La otra inclusión se prueba invirtiendo las implicaciones anteriores.
Las pruebas de ii) y iii) se dejan de ejercicio. ■

En contraste con f^{-1}, la función $f : \mathcal{P}(X) \to \mathcal{P}(Y)$ no tiene el mismo comportamiento con las operaciones entre subconjuntos, sin embargo se tiene lo siguiente.

Observación 6.

i) $f(\cup A_\alpha) = \cup f(A_\alpha)$.

ii) $f(\cap A_\alpha) \subseteq \cap f(A_\alpha)$.

iii) *Si* $A \subseteq X$ *entonces* $A \subseteq f^{-1}(f(A))$.

iv) *Si* $A \subseteq X$ *y* $B \subseteq Y$ *entonces* $f(f^{-1}(B) \cap A) = B \cap f(A)$. *En particular* $f(f^{-1}(B)) = B \cap f(X)$.

Demostración. Ejercicio.

Ejercicio. Enuncie la definición formal de la composición de dos funciones.

Si $f : X \to Y$ es una función, $A \subseteq X$, entonces f induce una función $f_{|A} : A \to Y$ llamada la restricción de f en A. Formalmente se tiene $f_{|A} = f \cap (A \times Y)$. Si $g : A \to Y$ es una función y existe una función $G : X \to Y$ tal que $G_{|A} = g$, G se llama una extensión de g. El problema de extender una función definida en un subconjunto, a un conjunto X más grande es de gran importancia en varias áreas de matemáticas. Si no se piden condiciones sobre la función, el problema de extensión siempre se resuelve positivamente, si los conjuntos bajo consideración tienen cierta estructura, digamos algebraica, entonces se requieren condiciones adicionales sobre la función a extender.

El siguiente resultado muestra cuando se puede extender una función a un conjunto, sabiendo que está definida en ciertos subconjuntos.

Teorema 5. *Sea* X *un conjunto,* $\{A_\alpha : \alpha \in \Omega\}$ *una familia de subconjuntos de* X *tal que* $X = \cup A_\alpha$ *(en este caso a la familia se le llama una cubierta de* X*). Supongamos que para todo* α *existe* $f_\alpha : A_\alpha \to Y$ *con la condición* $f_{\alpha|A_\alpha \cap A_\beta} = f_{\beta|A_\alpha \cap A_\beta}$ *para todo* $(\alpha, \beta) \in \Omega \times \Omega$. *Entonces existe una y solo una función* $f : X \to Y$ *tal que* $f_{|A_\alpha} = f_\alpha$ *para todo* $\alpha \in \Omega$.

Demostración. Puesto que la familia $\{A_\alpha\}$ es una cubierta, entonces dado $x \in X$ existe un α tal que $x \in A_\alpha$. Definamos $f(x) := f_\alpha(x)$; f está bien definida, pues si $x \in A_\beta$ para algún $\beta \neq \alpha$ entonces la condición sobre las f_α garantiza $f_\alpha(x) = f_\beta(x) = f(x)$. También se tiene que cada f_α es la restricción de f a A_α para cada α. La unicidad se obtiene directamente de la definición de f. ■

Observación 7. *Si las funciones del teorema anterior tienen condiciones adicionales, por ejemplo de continuidad o diferenciabilidad, entonces la extensión no necesariamente tiene las mismas propiedades.*

Definición. *Sea* $f : X \to Y$ *una función.*

i) f *se dice suprayectiva si* $f(X) = Y$.

ii) f *se dice inyectiva si* $f^{-1}(\{y\})$ *tiene a lo más un elemento para cada* $y \in Y$.

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

Si f es inyectiva entonces existe una única función llamada la inversa de f y denotada por $f^{-1} : f(X) \to X$ dada por, $f^{-1}(y) = x$ si $y = f(x)$.

Si $f : X \to Y$ y $g : Y \to X$ son dos funciones que satisfacen $g \circ f = I_X$, con I_X la función identidad en X entonces f es inyectiva y g es suprayectiva, pues si $f(x) = f(x_1)$ entonces aplicando g se tiene $x = g(f(x)) = g(f(x_1)) = x_1$, dado $x \in X$, $x = g(f(x))$.

0.2.3. Relaciones Binarias y Relaciones de Equivalencia

El concepto de relación binaria en un conjunto, generaliza al de función, recordemos que en el caso de funciones de los reales en los reales, para saber si una "gráfica" corresponde a la gráfica de una función, se usa la "regla" de trazar rectas verticales, si cada recta vertical intersecta a la gráfica en a lo más un punto, entonces se tiene la gráfica de una función. Con este "criterio" se prueba que la gráfica de la ecuación $x^2 + y^2 = 1$ no es una función, sin embargo considerando a la misma ecuación con la restricción $y \geq 0$ entonces su gráfica si es una función. Hay muchos otros subconjuntos del plano cartesiano que no son gráfica de función alguna, a estos subconjuntos los llamaremos relaciones, más precisamente:

Definición. *Por una relación binaria en un conjunto X entenderemos cualquier subconjunto de $X \times X$.*

La anterior definición se puede generalizar en varias formas: tomando un número n de variables, en este caso se tiene una relación n-aria, ó tomando diferentes conjuntos, por ejemplo una relación binaria entre los elementos del conjunto X y el conjunto Y ó más precisamente una relación binaria R con dominio X y contradominio Y es un subconjunto de $X \times Y$. En lo sucesivo las relaciones que usaremos serán binarias en casi todos los casos, por esta razón no discutiremos relaciones más generales.

Note que el concepto de relación binaria extiende al de función, pues una relación binaria R es una función si y sólo si para $(x, y), (x, z) \in R$ se tiene $y = z$.

De las relaciones binarias en un conjunto nos interesan aquellas que tienen propiedades similares a la relación "igualdad" de elementos, es decir en un conjunto X siempre se tiene la relación $R = \{(x, y) : x = y\}$ esta relación también se le llama la "diagonal" de X. La relación diagonal denotada R satisface:

i) $(x, x) \in R$ para todo $x \in X$.

ii) Si $(x, y) \in R$ entonces $(y, x) \in R$, pues si $x = y$ entonces $y = x$.

iii) Si $(x, y) \in R$ y $(y, z) \in R$ entonces $(x, z) \in R$, esto es simplemente la transitividad de la igualdad.

Las relaciones binarias que satisfacen las tres propiedades anteriores, de alguna forma, extienden el concepto de igualdad y juegan un papel central en todas las áreas de las matemáticas,

pues como veremos pronto, una relación que satisface las propiedades descritas tiene la característica de partir al conjunto en cuestión, en subconjuntos ajenos y los elementos de cada subconjunto tienen propiedades en común, es decir una relación del tipo en la discusión clasifica a los elementos que tienen una propiedad común, y uno de los problemas centrales en matemáticas es la clasificación de los objetos bajo estudio.

Definición. *Sea A un conjunto, R una relación binaria en A. Se dice que R es una relación de equivalencia si satisface las siguientes condiciones*

i) Para todo $a \in A$, $(a, a) \in R$, propiedad reflexiva.

ii) Si $(a, b) \in R$ entonces $(b, a) \in R$, propiedad de simetría.

iii) Si $(a, b) \in R$ y $(b, c) \in R$ entonces $(a, c) \in R$, propiedad transitiva.

Notación: si R es una relación en A y $(a, b) \in R$ diremos que a se relaciona con b respecto a R y lo denotaremos por aRb.

Anteriormente mencionamos que el concepto de relación de equivalencia en un conjunto extiende al concepto de igualdad entre los elementos. El siguiente ejercicio muestra que de las relaciones de equivalencia en un conjunto, la igualdad es la más pequeña.

Ejercicio. Demuestre que la intersección de una familia de relaciones de equivalencia es una relación de equivalencia y por lo tanto la igualdad es la relación más pequeña en un conjunto.

En conexión con el concepto de relación de equivalencia está el concepto de partición de un conjunto el cual se precisa en la siguiente definición.

Definición. *Sea X un conjunto y $\{A_\alpha\}$ una familia de subconjuntos de X. Se dice que $\{A_\alpha\}$ es una partición de X si $X = \cup A_\alpha$ y $A_\alpha \cap A_\beta = \emptyset$ si $\alpha \neq \beta$.*

La relación entre partición y relación de equivalencia se precisa en el Teorema 6. En seguida presentamos varios ejemplos de relaciones de equivalencia, algunos de los cuales han sido considerados con anterioridad en cursos previos.

Ejemplos.

1. Sean $A = \{2n : n \in \mathbb{Z}\}$ y $B = \{2k + 1 : k \in \mathbb{Z}\}$ entonces $\{A, B\}$ forma una partición de los enteros. Más generalmente, si m es cualquier entero positivo, sea $A_i = \{km + i : k \in \mathbb{Z}\}$, $i = 1, \ldots, m$ entonces $\{A_1, \ldots, A_m\}$ es una partición de $\mathbb{Z}$. Este ejemplo será considerado cuando estudiemos congruencias en los enteros y juega un papel muy importante en teoría de números.

2. Sea $\mathcal{M}(\mathbb{R})_{m\times n}$ el conjunto de las matrices $m \times n$ con entradas en los reales. Se define la relación R en $\mathcal{M}(\mathbb{R})_{m\times n}$ como sigue $(A, B) \in R$ si existen matrices no singulares P y Q de orden $m \times m$ y $n \times n$ respectivamente tales que $A = PBQ$. En álgebra lineal se dice que las matrices A y B son *equivalentes* cuando satisfacen la ecuación anterior.

3. Sea $\mathcal{M}(\mathbb{R})_{n\times n}$ el conjunto de matrices $n \times n$, se define en $\mathcal{M}(\mathbb{R})_{n\times n}$ la relación R como sigue $R = \{(A, B) : A = P^{-1}BP$ para alguna matriz P no singular $\}$. Si $(A, B) \in R$ se dice que A y B son *similares*, la condición de similaridad es equivalente a que A y B representen al mismo operador lineal sobre un espacio vectorial de dimensión n.

4. En $\mathcal{M}(\mathbb{R})_{n\times n}$ se define R como sigue, $R = \{(A, B) : A = P^tBP$ para alguna matriz P no singular $\}$, si $(A, B) \in R$ se dice que A y B son *congruentes*. Dos matrices son congruentes si y sólo si representan a la misma forma quadrática.

5. Sea n un entero positivo y $R_n = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} : n$ divide a $b - a\}$. Si $(a, b) \in R_n$ se dice que a es congruente con b módulo n y se denota por $a \equiv b \pmod{n}$.

6. Sea $f : X \to Y$ una función, se define $R_f = \{(a, b) \in X \times X : f(a) = f(b)\}$.

Si R es una relación de equivalencia en A y $a \in A$, se define la clase de equivalencia de a denotada $Ra = [a]_R := \{b \in A : bRa\}$. El siguiente resultado caracteriza a las relaciones de equivalencia de un conjunto A en términos de particiones.

Teorema 6. *Sea A un conjunto y R una relación de equivalencia en A. Entonces las clases de equivalencia determinadas por R constituyen una partición de A. Recíprocamente, si $\{A_\alpha\}$ es una partición de A, entonces existe una relación de equivalencia en A cuyas clases de equivalencia son precisamente los subconjuntos A_α.*

Demostración. Puesto que R es reflexiva entonces $A = \bigcup_{a\in A} Ra$. Como R es simétrica entonces aRb implica bRa, de esto se tiene que $Ra = Rb \iff aRb$. Supongamos que $Ra \cap Rb \neq \emptyset$, entonces existe $x \in Ra \cap Rb$, es decir xRa y xRb, por simetría y transitividad de R se obtiene aRb, por lo observado anteriormente se tiene $Ra = Rb$. De lo anterior se tiene que tomando clases diferentes $\{Ra\}_{a\in A}$ es una partición de A.

Recíprocamente, si $\{A_\alpha\}$ es una partición de A se define la relación en A como sigue: aRb si existe α tal que $a, b \in A_\alpha$. Debemos probar que R satiface las condiciones de una relación de equivalencia.

i) Para todo $a \in A$, aRa, pues $a \in A_\alpha$ para algún α.

ii) Claramente se tiene aRb implica bRa.

iii) Si aRb y bRc entonces $a, b \in A_\alpha$ y $b, c \in A_\beta$ para algunos α, β, de esto se tiene que $b \in A_\alpha \cap A_\beta$. La definición de partición implica $\alpha = \beta$ por lo que aRc. ■

Note que si en A hay una relación de equivalencia R, entonces $Ra \in \mathcal{P}(A)$ para todo $a \in A$, por lo tanto, invocando el axioma del conjunto potencia tiene sentido hablar del conjunto de clases de equivalencia, a este conjunto lo denotaremos por A/R. Si R es una relación de equivalencia en A, existe una función $\pi_R : A \to A/R$ definida por $\pi_R(a) := Ra$. La función π_R es claramente suprayectiva y se le llama la proyección natural.

Sean A y B dos conjuntos en los cuales hay relaciones de equivalencia R y S respectivamente, una función $f : A \to B$ se dice que preserva relaciones si cuando aRa' se tiene $f(a)Sf(a')$. El siguiente resultado es importante cuando se consideran funciones que preservan relaciones.

Por un diagrama conmutativo entre conjuntos y funciones definidas en ellos, entenderemos un diagrama como el siguiente,

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ h\downarrow & & \downarrow j \\ C & \xrightarrow{g} & D \end{array}$$

en donde $j \circ f = g \circ h$.

Teorema 7. *Sea $f : A \to B$ una función que preserva relaciones. Si R y S son relaciones de equivalencia en A y B respectivamente, entonces existe una y sólo una función $f_* : A/R \to B/S$ tal que el siguiente diagrama es conmutativo.*

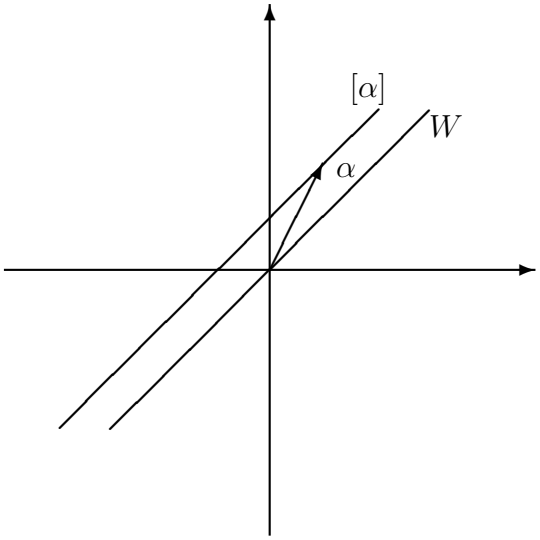
$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ \pi_R\downarrow & & \downarrow \pi_S \\ \frac{A}{R} & \xrightarrow{f_*} & \frac{B}{S} \end{array}$$

Recíprocamente, si para cualesquiera dos funciones f y f_* el diagrama anterior es conmutativo entonces f preserva relaciones.

Demostración. Note que $aRb \iff Ra = Rb$, esto y la condición sobre f garantiza que $Rb = Ra$ implica $Sf(a) = Rf(b)$. Definamos f_* por $f_*(Ra) := Sf(a)$. Por el argumento anterior, $f_*(Ra)$ es independiente del representante de la clase Ra. La conmutatividad del diagrama se obtiene directamente de la definición de f_*. Si g_* es otra función que hace el diagrama conmutativo, es decir $g_* \circ \pi_R = \pi_S \circ f$ entonces para todo $a \in A$, $(g_* \circ \pi_R)(a) = (\pi_S \circ f)(a)$, de lo cual se obtiene $g_*(Ra) = Sf(a) = f_*(Ra)$, es decir $g_* = f_*$.
Recíprocamente, supongamos que f y f_* hacen el diagrama conmutativo.
Si aRa', entonces de la definición de π_R se tiene $\pi_R(a) = \pi_R(a')$ por lo tanto $f_*(Ra) = f_*(Ra')$, de esto y la conmutatividad del diagrama se obtiene $Sf(a) = Sf(a')$ lo cual equivale a $f(a)Sf(a')$, probando lo afirmado. ■

El siguiente ejemplo es de importancia en álgebra lineal.

Ejemplo. Sea V un espacio vectorial, W un subespacio, se define en V la relación inducida por W como sigue: dados $\alpha, \beta \in V$, $\alpha R_W \beta$ si $\alpha - \beta \in W$. Se prueba sin dificultad que R_W es una relación de equivalencia. Si $\alpha \in V$ denotemos por $[\alpha]$ a la clase de equivalencia de α y por V/W al conjunto de clases de equivalencia. La interpretación geométrica de las clases de equivalencia es como sigue. Dado $\alpha \in V$, $[\alpha] = \{\beta \in V : \beta - \alpha \in W\} = \{\alpha + \gamma : \gamma \in W\} = \{\alpha\} + W$, de aquí se tiene que si $V = \mathbb{R}^n$, entonces las clases de equivalencia son hiperplanos paralelos a W, en particular, si $V = \mathbb{R}^2$ y W tiene dimensión uno entonces las clases de equivalencia son rectas paralelas a W como se muestra en la siguiente figura.



Dados $[\alpha], [\beta] \in V/W$ y r un escalar se definen las operaciones

i) $[\alpha] + [\beta] := [\alpha + \beta]$

ii) $r[\alpha] := [r\alpha]$

Probaremos que la suma de clases está bien definida y se deja como ejercicio el mostrar que el producto por escalar también está bien definido. Si $[\alpha_1] = [\alpha]$ y $[\beta] = [\beta_1]$ entonces $\alpha - \alpha_1, \beta - \beta_1 \in W$, como W es subespacio se tiene $(\alpha + \beta) - (\alpha_1 - \beta_1) \in W$, es decir $[\alpha+\beta] = [\alpha_1+\beta_1]$. Con las operaciones definidas anteriormente, es rutina mostrar que V/W es un espacio vectorial con elemento cero $[0] = W$. En seguida determinamos su dimensión suponiendo que V tiene dimensión finita.

Supongamos que V tiene dimensión finita y sea $T : V \to V/W$ definida por $T(\alpha) = [\alpha]$. De la definición de las operaciones en V/W se obtiene directamente que T es una transformación lineal suprayectiva, cuyo núcleo N_T es W, por lo tanto dim V = dim V/W + dim N_T, de lo anterior se tiene dim V/W = dim V − dim W. Si $\{\alpha_1, \ldots, \alpha_r\}$ es una base de W y se extiende a una base de V $\{\alpha_1, \ldots \alpha_r, \alpha_{r+1}, \ldots, \alpha_n\}$, entonces $\{[\alpha_{r+1}], \ldots, [\alpha_n]\}$ es una base de V/W. También se tiene $V \cong W \oplus V/W$, abusando de la notación se escribe $V = W \oplus V/W$ (lo anterior es correcto vía isomorfismo).

Definición. *En la construción anterior al espacio V/W se le llama el espacio cociente de V módulo W.*

0.2.4. Relaciones de Orden

Uno de los conceptos más importantes en cálculo es el de límite y éste a su vez, está ligado con la idea de "medir" distancias. En cálculo de una variable real, la distancia entre reales se

mide con el valor absoluto y el valor absoluto se define en términos del orden en los reales. En otras palabras, el hecho de tener un orden en los reales que es compatible con las operaciones de suma y producto juega un papel central en cálculo. Lo que haremos en seguida es definir el concepto de orden en un conjunto y mostrar que éste juega un papel muy importante aunque lo que se estudia no tenga relación directa con cálculo.

Definición. *Una relación binaria R en un conjunto A se llama un orden parcial si*

i) Para todo $a \in A$, aRa, propiedad reflexiva.

ii) Si aRb y bRc entonces aRc, propiedad transitiva.

iii) Si aRb y bRa entonces $a = b$, propiedad de antisimetría.

Si en A hay definido un orden parcial R, a la pareja (A, R) se le llama un conjunto parcialmente ordenado.

Puesto que la relación de orden en los reales es denotada por $\leq$, cuando hablemos de una relación de orden parcial usaremos el símbolo $\preceq$, es decir si R es una relación de orden parcial en A y aRb escribiremos $a \preceq b$ y el conjunto parcialmente ordenado se denotará por $(A, \preceq)$.

Ejemplos.

1. En el conjunto de los enteros positivos se define $m \preceq n$ si m divide a n. Esta relación es un orden parcial.

2. En el conjunto de los números reales, el orden usual es un orden parcial.

3. Si X es un conjunto, en $\mathcal{P}(X)$ se define un orden parcial mediante la inclusión, es decir si $A, B \subseteq X$ se declara $A \preceq B$ si $A \subseteq B$.

En los tres ejemplos anteriores, los conjuntos resultan ser parcialmente ordenados. Note que un conjunto puede tener varios órdenes, por ejemplo los enteros positivos tienen al menos dos: el usual y el que se da en el ejemplo 1.

Definición. *Sea $(A, \preceq)$ un conjunto parcialmente ordenado.*

i) $m \in A$ se llama un elemento maximal si $m \preceq a$ implica $a \preceq m$ para todo $a \in A$.

ii) Si $B \subseteq A$, $a_0 \in A$ se llama una cota superior para B si $b \preceq a_0$ para todo $b \in B$.

iii) Un subconjunto $C \subseteq A$ se llama una cadena si cualesquiera dos elementos de C se relacionan.

iv) Si A es una cadena, A se dice totalmente ordenado.

Definición. *Un conjunto parcialmente ordenado $(A, \preceq)$ se dice bien ordenado si cada subconjunto no vacío B tiene un primer elemento, i.e. si para todo $B \neq \emptyset$ existe $b_0 \in B$ tal que $b_0 \preceq b$ para todo $b \in B$.*

Observación 8. *Si A es bien ordenado, entonces A es totalmente ordenado. Esto se obtiene tomando dos elementos a y b y formando el subconjunto $\{a, b\}$ el cual tiene un primer elemento.*

0.2.5. La Axiomática de la Teoría de Conjuntos

Para hacer la teoría de conjuntos precisa, hace falta introducir lo que se llama un sitema axiomático, esto nos apartaría del objetivo central que tenemos en mente: la construcción del sistema de los números reales partiendo de un sistema axiomático para el conjunto de los enteros positivos. Es cierto que si ha de establecerse la construcción de los enteros positivos con todo rigor se requiere formular la teoría de conjuntos de manera axiomática, pues uno de los axiomas (axioma del infinito) garantiza la existencia de un sistema de Peano (definición más abajo). Lo que haremos es enunciar solamente los axiomas que se vayan requiriendo y lo haremos en el momento necesario. Iniciamos con

Axioma de elección. *Dada una familia no vacía $\{A_\alpha : \alpha \in \Omega\}$ de conjuntos no vacíos y disjuntos a pares, existe un conjunto S que contiene exactamente un elemento de cada A_α.*

Anteriormente se definió el producto cartesiano de dos conjuntos A y B y sus elementos se interpretaron como parejas ordenadas de la forma (a, b) con $a \in A$ y $b \in B$. Indicando los conjuntos $A = A_1$ y $B = A_2$, una pareja ordenada puede ser interpretada como una función $f : \{1, 2\} \to A_1 \cup A_2$ tal que $f(i) \in A_i$. Esta idea permite formular la definición general de producto cartesiano de una familia de conjuntos, más precisamente:

Definición. *Sea* $\{A_\alpha : \alpha \in \Omega\}$ *una familia de conjuntos, se define el producto cartesiano de la familia denotado por* $\Pi A_\alpha := \{c : \Omega \to \cup A_\alpha \mid c(\alpha) \in A_\alpha \, \forall \, \alpha\}$.

Observación 9. *Si tomamos por hecho que existe el conjunto unión de una familia y el conjunto potencia de un conjunto dado, entonces se tiene, de la definición de función, que el producto cartesiano de la familia* $\{A_\alpha : \alpha \in \Omega\}$ *es, en efecto, un subconjunto de* $\mathcal{P}(\Omega \times (\cup A_\alpha))$.

El siguiente teorema el cual se presenta sin prueba, garantiza la equivalencia de varios hechos importantes.

Teorema 8. *Los siguientes hechos son equivalentes.*

i) El axioma de elección.

ii) El Lema de Zorn: Sea X un conjunto parcialmente ordenado. Suponga que toda cadena en X tiene una cota superior en X, entonces X tiene elementos maximales.

iii) Teorema de Zermelo: Todo conjunto puede ser bien ordenado.

iv) Sea $\{A_\alpha : \alpha \in \Omega\}$ una familia no vacía de conjuntos. Si cada A_α es no vacío, entonces $\Pi A_\alpha \neq \emptyset$.

Para establecer algunos resultados que son de gran importancia para garantizar la existencia de ciertos objetos matemáticos, como es la base de un espacio vectorial (de dimensión infinita), se requiere usar un argumento basado en el lema de Zorn.

A continuación mostramos como se usa el lema de Zorn para probar que todo espacio vectorial admite una base.

Sea V un espacio vectorial (sobre cualquier campo F), un subconjuto S de V se dice linealmente independiente, denotado esto por, S es l.i. si todo subconjunto finito $\{\alpha_1, \ldots, \alpha_n\}$ de S es l.i. es decir, si $a_1\alpha_1 + \cdots + a_n\alpha_n = 0$ implica $a_i = 0$ para todo $i = 1, \ldots, n$. Se dice que S genera a V si $V, = \mathcal{L}(S) = \{a_1\alpha_1 + \cdots + a_n\alpha_n : \alpha_i \in S,\ n \in \mathbb{N}$ y $a_i \in F\}$. Un subconjunto $\mathcal{B}$ de V es una base de V si $\mathcal{B}$ es l.i. y genera a V.

Hecho. *Todo espacio vectorial $V \neq \{0\}$ admite una base.*

Demostración. Sea $\mathcal{F} = \{S \subseteq V : S$ es l.i.$\}$. Como V es no cero entonces $\mathcal{F} \neq \emptyset$. Se define en $\mathcal{F}$ un orden parcial mediante la inclusión de conjuntos. Sea $\mathcal{C} \subseteq \mathcal{F}$ una cadena, debemos mostrar que $\mathcal{C}$ tiene una cota superior en $\mathcal{F}$. Sea $S_0 = \bigcup_{S\in\mathcal{C}} S$. Afirmamos que $S_0 \in \mathcal{F}$, en efecto, si T es un subconjunto finito de S_0 digamos $T = \{\alpha_1, \ldots, \alpha_n\}$, entonces existen $S_1, \ldots, S_n \in \mathcal{C}$ tales que $\alpha_i \in S_i$. Como $\mathcal{C}$ es una cadena, entonces $S_1 \subseteq S_2$ y/o $S_2 \subseteq S_1$. Podemos suponer que $S_1 \subseteq S_2$. Continuando de esta forma y cambiando la numeración de los S_i's, si hace falta, se puede suponer que $S_i \subseteq S_n$, entonces $T \subseteq S_n$ probando que T es l.i. es decir $S_0 \in \mathcal{F}$. Claramente se tiene que S_0 es una cota superior para $\mathcal{C}$. Sea $\mathcal{B}$ un elemento maximal de $\mathcal{F}$, por elección, $\mathcal{B}$ es l.i. Si $\alpha \in V$ es tal que $\alpha \notin \mathcal{L}(\mathcal{B})$ entonces $B = \mathcal{B} \cup \{\alpha\}$ es l.i. por lo tanto $B \in \mathcal{F}$ y $\mathcal{B}$ es un subconjunto propio de B, contradiciendo la maximalidad de $\mathcal{B}$, es decir $\mathcal{B}$ es una base de V. ■

0.2.6. Operaciones en Conjuntos y Sistemas Algebraicos

Desde el punto de vista algebraico, los ingredientes esenciales en un conjunto son las operaciones y sus propiedades, así como las relaciones binarias y su conexión con las operaciones. Como veremos a lo largo de estas notas, las operaciones y sus propiedades en un conjunto son lo que hacen que diferentes áreas de las matemáticas se ocupen de estudiarlo. Por ejemplo,

el sistema de los números reales y algunos de sus subconjuntos son objeto de estudio del análisis matemático y las operaciones que interesan son aquellas que son continuas, diferenciables, etc. Desde el punto de vista del álgebra, el énfasis se hará en las operaciones que describan ciertas estructuras algebraicas. En seguida precisamos el concepto de operación en un conjunto y también el de sistema algebraico.

Definición. *Sea A un conjunto no vacío, una operación binaria en A es una función $F : A \times A \to A$. Si $F : A \to A$, se dice que F es una operación unaria.*

Note que se pueden tener operaciones n-arias en un conjunto para toda $n \geq 1$.

Si F es una operación binaria en A se dice que F es:

i) Asociativa, si $F(F(a,b),c) = F(a,F(b,c))$ para todo $a,b,c \in A$.

ii) Conmutativa, si $F(a,b) = F(b,a)$ para todo $a,b \in A$.

Si $B \subseteq A$ y F es una operación binaria en A, se dice que B es cerrado bajo F si $F(B \times B) \subseteq B$. Si F es unaria la condición anterior se traduce a $F(B) \subseteq B$.

Definición. *Por un sistema algebraico ó estructura algebraica entenderemos una $(k+l+m+1)$-ada $(S, F_1, \ldots, F_l, R_1, \ldots, R_k, a_1, \ldots, a_m)$ donde S es un conjunto no vacío, F_i es una operación en S para todo i, R_j es una relación en S para todo j, a_t es un elemento "distinguido" de S para todo t.*

Note que en la definición anterior no se está suponiendo que todas las operaciones y relaciones sean binarias.

Dos sistemas algebraicos $(S, F_1, \ldots, F_l, R_1, \ldots, R_k, a_1, \ldots, a_m)$ y $(S', F'_1, \ldots, F'_{l'}, R'_1, \ldots R_{k'}, a'_1, \ldots, a'_{m'})$ son del mismo tipo si

i) $k = k'$, $l = l'$ y $m = m'$.

ii) F_i y F'_i tienen el mismo número de argumentos para todo i, es decir, si F_i es n_i-aria, también lo es F'_i.

iii) La condición anterior la cumplen R_i y R'_i para todo i.

Ejemplos.

1. Las estructuras aditivas de dos espacios vectoriales $(V, +, 0_V)$ y $(W, +, 0_W)$ son del mismo tipo.

2. $(\mathbb{R}, +, \bullet, <, 0, 1)$ y $(\mathbb{C}, +, \bullet, 0, 1)$ no son del mismo tipo.

Definición. *Dos sistemas algebraicos $(S, F_1, \ldots, F_l, R_1, \ldots, R_k, a_1, \ldots, a_m)$ y $(S', F'_1, \ldots, F'_{l'}, R'_1, \ldots R_{k'}$, son isomorfos si, son del mismo tipo y existe una función biyectiva $f : S \to S'$ tal que*

i) $f(a_i) = a'_i$ *para todo* i.

ii) f *preserva operaciones, es decir* $f \circ F_i = F'_i \circ f$ *para todo* i.

iii) f *preserva relaciones, es decir* $(a, b) \in R_i$ *entonces* $(f(a), f(b)) \in R'_i$ *para todo* i. *En caso de relaciones* n*-arias la adaptación es natural.*

Si dos sistemas algebraicos son isomorfos lo denotaremos por $S \cong S'$, en caso de no haber confusión.
Ejemplos.

1. Si V y W son espacios vectoriales isomorfos entonces son isomorfos considerando sus estructuras aditivas.

2. Denotemos por $\mathbb{R}^+$ a los reales positivos, entonces $(\mathbb{R}, +, <, 0) \cong (\mathbb{R}^+, \bullet, <, 1)$. En efecto, sea $f : \mathbb{R} \to \mathbb{R}^+$ la función exponencial, es decir $f(x) = e^x$, f satisface las condiciones de la definición anterior.

Observación 10. *Si* S *y* S' *no tienen operaciones y existe una función* $f : S \to S'$ *biyectiva diremos que* S *y* S' *son isomorfos ó númericamente equivalentes. En este caso también se dice que* S *y* S' *tienen la misma cardinalidad y se usa la notación* $S \cong S'$.

Definición. *Un conjunto* S *se dice finito si para todo subconjunto propio* T, $S \ncong T$.

Ejercicio. Demuestre que para todo conjunto X, $X \ncong \mathcal{P}(X)$. Sugerencia: es suficiente mostrar que no existe una función suprayectiva de X a $\mathcal{P}(X)$, para esto suponga que tal función existe y denótela por f. Considere el conjunto $A = \{x \in X : x \notin f(x)\}$, puesto que f es suprayectiva, existe un $x \in X$ tal que $f(x) = A$, ¿es esto posible?

0.2.7. Ejercicios

1.- Resuelva todos los ejercicios asignados en las notas.

2.- Sea A un conjunto con n elementos. Demuestre que el conjunto potencia de A tiene 2^n elementos.

3.- Sean $A, B \subseteq E$ conjuntos. Demuestre que $A \cap B = \emptyset \iff A \subseteq B^c \iff B \subseteq A^c$.

4.- Sean A, B conjuntos no vacios tales que $(A \times B) \cup (B \times A) = C \times C$. Demuestre que $A = B = C$.

5.- Sea $\{A_n\}$ una familia de conjuntos, $S_k = \cup_0^k A_i$, $k = 0, 1, \ldots$. Demuestre que $\cup_0^\infty A_n = A_0 \cup (A_1 - S_0) \cup \cdots \cup (A_n - S_{n-1}) \cup \cdots$ Los conjuntos que aparecen a la derecha son disjuntos a pares.

7.- Sean R, S relaciones en el conjunto A. Se define la composición de R y S denotada por $R \circ S$ como $aR \circ Sb$ si y sólo si existe un $c \in A$ tal que aRc y cSb. Demuestre que la composición de relaciones es asociativa. Si R y S son relaciones de equivalencia, ¿es la composición una relación de equivalencia?

8.- Para una relación R en A se define R^{-1} por $aR^{-1}b$ si y sólo si bRa. Sea R una relación reflexiva, demuestre que R es una relación de equivalencia $\iff R \circ R = R$ y $R = R^{-1}$.

9.- Sean A, B conjuntos y R, S relaciones en A, B respectivamente. Se define la relación producto $R \times S$ en $A \times B$ por $(a, b)R \times S(c, d)$ si y sólo si aRc y bSd. Si R y S son relaciones de equivalencia entonces $R \times S$ también lo es. ¿Es cierto el recíproco?

10.- Sea V un espacio vectorial sobre $\mathbb{R}$ de dimensión finita, W un subespacio de V. Se define en V la relación R_W dada por $\alpha R_W \beta$ si $\alpha - \beta \in W$. Demuestre

a) R_W es una relación de eqivalencia.

b) Si V/W denota al conjunto de las clases de eqivalencia se definen en V/W operaciones suma, y producto por escalar como sigue. $[\alpha] + [\beta] = [\alpha + \beta]$ y $r[\alpha] = [r\alpha]$, $[\alpha], [\beta] \in V/W$ y $r \in \mathbb{R}$. Demuestre que con estas operaciones V/W es un espacio vectorial. Describa la dimensión de V/W en términos de las dimensiones de V y W.

11.- En $\mathbb{R}^3 \setminus \{0\}$ se define la siguiente relación R: $\alpha R \beta$ si existe un $\lambda \in \mathbb{R} \setminus \{0\}$ tal que $\alpha = \lambda\beta$. Demuestre que R es una relación de equivalencia, el conjunto de las clases de eqivalencia se le llama el plano proyectivo real. La construcción anterior se puede hacer en $\mathbb{R}^n$ para todo $n \geq 2$. Si $n = 2$ el conjunto de las clases de equivalencia se llama la recta proyectiva real. Encuentre el significado geométrico en las construcciones anteriores.

12.- En el conjunto de los enteros positivos se define la relación $m \preceq n$ si n divide a m. Demuestre que la relación definida es una relación de orden parcial, que toda cadena tiene cota superior y determine los elementos maximales.

13.- Sea A el conjunto de las sucesiones reales. Se ordena A con el orden lexicográfico, es decir $(a_1, a_2, \ldots) \preceq (b_1, b_2, \ldots)$ si $a_i = b_i$ para todo i, ó $a_n < b_n$ para el primer n tal que $a_n \neq b_n$. Demuestre que este es un orden total en A.

14.- Sea A un conjunto bien ordenado por R. Demuestre que R^{-1} es un buen orden solamente cuando A es finito.

15.- Demuestre que si A es finito entonces cada orden total es un buen orden.

16.- Demuestre que cualquier espacio vectorial admite una base. Sugerencia: Use el lema de Zorn.

17.- Demuestre que el campo de los números complejos no admite un orden compatible con las operaciones de suma y producto. ¿Contradice ésto al teorema de Zermelo?

18.- Sea $V = \mathbb{R}$ con la suma usual de reales, los escalares restrínjalos a los números racionales. En este caso se dice que los reales forman un espacio vectorial sobre los racionales. ¿Es $\mathbb{R}$ un espacio vectorial de dimensión finita sobre los racionales?

19.- Sea A un conjunto parcialmente ordenado, A se dice una *red* si para todo par de elementos $a, b \in A$, el conjunto $\{a, b\}$ tiene mínima cota superior y máxima cota inferior en A. Demuestre que $\mathcal{P}(X)$ es una red con el orden inducido por la inclusión de conjuntos. Proporcione varios ejemplos de redes.

20.- Sea V un espacio vectorial, Y el conjunto de todos los subespacios de V, si Y se ordena con la inclusión de conjuntos, ¿es Y una red?

0.3. Sistemas de Peano, Los Enteros Positivos

En 1889 el matemático Italiano G. Peano [9], presentó una formulación axiomática del sistema de los enteros positivos, la cual en parte había sido influenciada por el trabajo de Dedekind [3]. Peano, en su trabajo presenta una formulación axiomática de los enteros positivos ligeramente diferente de lo que llamaremos un sistema de Peano. Con un sistema de Peano se inicia la construcción de los sistemas de los enteros, racionales y reales. Kronecker, uno de los matemáticos del siglo XIX que más contribuciones hizo en las matemáticas resume lo anterior en su famosa frase: *Dios creo a los números naturales, lo demás es producto del hombre*. Dedekind, otro de los grandes del siglo pasado, refuta de alguna forma el enunciado de Kronecker, afirmando que aún los números naturales son producto del hombre, y esto se logra mediante una axiomatización de la teoría de conjuntos, pues uno de los axiomas en teoría de conjuntos es equivalente a la existencia de un sistema de Peano.

Definición. (Axiomas de Peano) *Por un sistema de Peano entenderemos un sistema algebraico $(P, Sc, 1)$ con $1 \in P$ y $Sc : P \to P$ satisfaciendo:*

P1 $Sc(x) \neq 1$ *para todo* $x \in P$.

P2 Sc *es inyectiva.*

P3 Si $A \subseteq P$, $1 \in A$ *y* $Sc(A) \subseteq A$ *entonces* $A = P$.

Observación 11. *El axioma P3 es lo que usualmente se conoce como el principio de inducción. Este axioma es el que usaremos repetidamente cuando estemos probando que un subconjunto de P debe ser todo P. A los axiomas anteriores se les conoce como axiomas de Peano .*

Axioma P. *Existe un sistema de Peano.*

El axioma anterior no hace falta si se ha iniciado con una formulación axiomática de la teoría de conjuntos.

Teorema 9. *Sea $(P, Sc, 1)$ un sistema de Peano, entonces $P = \{1\} \cup Sc(P)$.*

Demostración. Sea $A = \{1\} \cup Sc(P)$. Por $P3$ es suficiente mostrar que $Sc(A) \subseteq A$. Sea $x \in A$. Si $x = 1 \in P$ entonces $Sc(1) \in Sc(P)$. Si $x \neq 1$ entonces $x = Sc(y)$ para algún $y \in P$, por lo tanto $Sc(x) = Sc(Sc(y)) \in Sc(P) \subseteq A$, i.e. $A = P$. ■

0.3.1. Operaciones en un Sistema de Peano

Teorema 10 (Teorema de Recursión, Dedekind 1888). *Suponga que X es un conjunto, $f : X \to X$ una función, y $a \in X$. Si $(P, Sc, 1)$ es un sistema de Peano, entonces existe una única función $F : P \to X$ tal que*

i) $F(1) = a$.

ii) $\forall\, x \in P$, $F(Sc(x)) = f(F(x))$.

Demostración. `Unicidad`. Suponga que existen F_1 & F_2 satisfaciendo i) y ii). Sea $A = \{x \in P : F_1(x) = F_2(x)\}$. Por i) $1 \in A$. Si $x \in A$ entonces $F_1(x) = F_2(x)$. Se debe probar que $F_1(Sc(x)) = F_2(Sc(x))$. Por ii) se tiene $F_1(Sc(x)) = f(F_1(x)) = f(F_2(x)) = F_2(Sc(x))$. Por lo tanto $A = P$.
`Existencia`. Considérese la familia de subconjuntos $\mathcal{F}$ cuyos elementos $H \subseteq P \times X$ satisfacen:

a) $(1, a) \in H$.

b) Si $(x, y) \in H$, entonces $(Sc(x), f(y)) \in H$.

Ya que $P \times X$ satisface a) & b), se tiene que $\mathcal{F}$ es no vacía.
Sea $F = \bigcap_{H \in \mathcal{F}} H$.
`Afirmación` F es una función. Sea $A = \{x \in P \mid \exists!\, y \in X \text{ con } (x, y) \in F\}$. Se probará que $A = P$.
Si $1 \notin A$, entonces $\exists\ c \neq a$ tal que $(1, a), (1, c) \in F$, definiendo $F_1 = F \backslash \{(1, c)\}$ se tiene que F satisface a) & b), por lo tanto $F_1 \in \mathcal{F}$, entonces $F \subseteq F_1$, $\Rightarrow\Leftarrow$. De esta forma $1 \in A$.
Sea $x \in A$, se debe probar que $Sc(x) \in A$. Si $x \in A$ entonces existe un único $y \in X$ tal que $(x, y) \in F$. Por b), $(Sc(x), f(y)) \in F$. Si $(Sc(x), c) \in F$ con $c \neq f(y)$ entonces $F_1 = F \backslash \{(Sc(x), c)\}$ satisface también a) & b), por lo que $F \subseteq F_1$, es una contradicción. De aquí $A = P$, i.e. F es una función que satisface a) & b) y esto significa que $F(1) = a$ y si $F(x) = y$ entonces $F(Sc(x)) = f(F(x))$ como se pedía. ■

El siguiente teorema es una pequeña generalización del teorema de recursión y será de utilidad, especialmente cuando se definan la suma y el producto de varios elementos en un sistema de Peano, en particular es útil para definir el factorial de un entero positivo.

Teorema 10′ (Teorema Generalizado de Recursión). *Sea $(P, Sc, 1)$ un sistema de Peano, X un conjunto y $a \in X$. Suponga que $f : P \times X \to X$ es una función. Entonces existe una única función $F : P \to X$ tal que*

i) $F(1) = a$.

ii) $\forall\, x \in P,\ F(Sc(x)) = f(x, F(x))$.

Demostración. `Unicidad`. Si F_1 y F_2 son funciones que satisfacen i) y ii), sea $A = \{z \in P \mid F_1(z) = F_2(z)\}$, entonces por i) $1 \in A$. Si $F_1(z) = F_2(z)$ entonces $F_1(Sc(z)) = f(z, F_1(z)) = f(z, F_2(z)) = F_2(Sc(z))$, de esta manera $A = P$.
`Existencia`. Considérese la familia $\mathcal{F}$ de subconjuntos $H \subseteq P \times X$ tales que

a) $(1, a) \in H$.

b) Si $(x, y) \in H$, entonces $(Sc(x), f(x, y)) \in H$.

Ahora la demostración continúa como en el teorema anterior. ■

El siguiente teorema garantiza que sólo existe un sistema de Peano.

Teorema 11 (Unicidad de un sistema de Peano). *Si* $(P, Sc, 1)$ *y* $(P', S'c, 1')$ *son dos sistemas de Peano, entonces existe un único isomorfismo* $\varphi : P \longrightarrow P'$ *con* $\varphi(1) = 1'$ *&* $S'c \circ \varphi = \varphi \circ Sc$.

Demostración. Aplicando el teorema de recursión a $(P, Sc, 1)$ y $X = P'$, $f = S'c$ y $a' = 1'$, se tiene que existe una única función $\varphi : P \longrightarrow P'$ con $\varphi(1) = 1'$ y

$$\varphi \circ Sc = S'c \circ \varphi \tag{1}$$

Intercambiando los papeles entre P & P', y aplicando nuevamente el teorema de recursión se encuentra que existe $\Psi : P' \longrightarrow P$ (única) tal que $\Psi(1') = 1$ y

$$\Psi \circ S'c = Sc \circ \Psi \tag{2}$$

De (1) & (2) se tiene $\Psi \circ \varphi \circ Sc = \Psi \circ S'c \circ \varphi = Sc \circ \Psi \circ \varphi$, también se tiene que la función identidad $I : P \to P$ satisface $I \circ Sc = Sc \circ I$ & $I(1) = 1$. Ahora tomando $X = P$, $a = 1$ y $g = Sc$ se tiene que $\Psi \circ \varphi$ e I ambas satisfacen las condiciones del teorema de recursión , por lo que $\Psi \circ \varphi = I$. Un argumento análogo muestra que $\varphi \circ \Psi = I$. ■

Definición. *El sistema de Peano único* $(P, Sc, 1)$ *es llamado el conjunto de enteros positivos.*

Teorema 12. *Sea* $(P, Sc, 1)$ *un sistema de Peano,* $G : P \times P \to P$, $H : P \to P$ *funciones. Entonces* $\exists!\ F : P \times P \to P$ *tal que*

i) $F(x, 1) = H(x)\ \forall\, x \in P$.

ii) $F(x, Sc(y)) = G(x, F(x, y))\ \forall\, x, y, \in P$.

Demostración. Para una $x \in P$ fija, sea $C_x = H(x)$, $G_x(z) = G(x, z)$. Por el teorema de recursión $\exists!$ $F_x : P \longrightarrow P$ tal que $F_x(1) = C_x$ y $F_x(Sc(y)) = G_x(F_x(y))$. Para $x, y \in P$, defina $F(x, y) := F_x(y)$ entonces

i) $F(x, 1) = F_x(1) = C_x = H(x)$.

ii) $F(x, Sc(y)) = F_x(Sc(y)) = G_x(F_x(y)) = G(x, F(x, y))$

La unicidad se tiene a partir de la unicidad de F_x. ■

0.3.2. Adición de Elementos en un Sistema de Peano

Sea $G : P \times P \to P$ dada por $G(x, y) = Sc(y)$, $H(x) = Sc(x)$. Del teorema anterior $\exists!$ una función $F : P \times P \to P$ satisfaciendo

a) $F(x, 1) = Sc(x)$, y

b) $F(x, Sc(y)) = G(x, F(x, y)) = Sc(F(x, y))$.

Definición. *Con la notación anterior, denótese por $x + y$ al valor de $F(x, y)$. Esta operación es llamada la suma o adición de x & y.*

Observación 12. *Con la notación anterior y las propiedades a) y b) se tiene que la adición satisface:*

a)' $Sc(x) = x + 1$.

b)' $x + Sc(y) = Sc(x + y)$.

Se hará algún trabajo para probar todas las propiedades aritméticas de un sistema de Peano basado en la definición de **adición**. El siguiente teorema establece las propiedades básicas de esta operación.

Teorema 13. *Sea $(P, Sc, 1)$ un sistema de Peano, entonces + satisface.*

i) $x + (y + z) = (x + y) + z$, $\forall\, x, y, z \in P$ *(Propiedad asociativa).*

ii) $x + y = y + x$, $\forall\, x, y \in P$ *(propiedad conmutativa).*

iii) Si $x + z = y + z$, *entonces* $x = y$ *(propiedad de cancelación).*

iv) Para cualquier $x, y \in P$, exactamente una de las siguientes condiciones se cumple (propiedad de tricotomía para +).

a) $x = y$.

b) $\exists!\, u \in P$ *tal que* $x = y + u$.

c) $\exists!\, v \in P$ *tal que* $y = x + v$.

Demostración. i) Dados $x, y \in P$, sea $A = \{z \in P \mid x + (y + z) = (x + y) + z\}$ se tiene $x + (y + 1) \overset{a)'}{=} x + Sc(y) \overset{b)'}{=} Sc(x + y) \overset{a)'}{=} (x + y) + 1$, por lo tanto $1 \in A$.
Si $z \in A$, se necesita mostrar que $Sc(z) \in A$.
$x + (y + Sc(z)) \overset{b)'}{=} x + Sc(y + z) \overset{b)'}{=} Sc(x + (y + z)) \overset{z \in A}{=} Sc((x + y) + z) \overset{b)'}{=} (x + y) + Sc(z)$, i.e. $Sc(z) \in A$, por lo tanto $A = P$.
ii) Primero se mostrará que $x+1 = 1+x$, $\forall\, x$. Sea $A = \{x \in P : x+1 = 1+x\}$. Obviamente $1 \in A$; si $x \in A$, entonces se debe probar que $Sc(x) \in A$.
$Sc(x) + 1 = ((x + 1) + 1) = (1 + x) + 1 \overset{i)}{=} 1 + (x + 1) = 1 + Sc(x)$, entonces $Sc(x) \in A$, i.e. $P = A$.
Sea $x \in P$ un elemento fijo, $A = \{y \in P : x + y = y + x\}$. Por el argumento anterior $1 \in A$. Suponga $y \in A$.
$x + Sc(y) = Sc(x + y) = Sc(y + x) = y + Sc(x) = y + (x + 1) = y + (1 + x) = (y + 1) + x = Sc(y) + x$.
iii) Sean $x, y \in P$, $A = \{z \in P : x + z = y + z \Rightarrow x = y\}$. $1 \in A$ ya que $x + 1 = y + 1 \Rightarrow Sc(x) = Sc(y)$. Debido a que Sc es inyectiva entonces $x = y$. Suponga $z \in A$, y que $x + Sc(z) = y + Sc(z)$, entonces
$x + (z + 1) = y + (z + 1) \Rightarrow (x + z) + 1 = (y + z) + 1 \Rightarrow x + z = y + z \Rightarrow x = y$, por lo tanto $A = P$.
iv) Primero se demostrará que para cualesquiera $x, y, \in P$, $y \neq x + y$. Dado $x \in P$, sea $A = \{y : y \neq x + y\}$. $1 \in A$, ya que $1 \neq x + 1 = Sc(x)$ (recuerde que $1 \notin Sc(P)$). Si $y \in A$ & $Sc(y) \notin A$, entonces $Sc(y) = x + Sc(y)$, i.e. $y + 1 = x + (y + 1) = (x + y) + 1$, por la propiedad de cancelación $y = x + y$, i.e. $y \notin A$ $\Rightarrow\Leftarrow$, por lo tanto $A = P$. Por lo anterior, a) & b) , a) & c) no se cumplen simultáneamente, si b) & c) se cumplen entonces $x = y + u = (x + v) + u = x + (v + u)$ $\Rightarrow\Leftarrow$.
La propiedad de la cancelación garantiza la unicidad de u & v. Ahora se demostrará que a), b) ó c) se cumplen. Sea $x \in P$, $A = \{y \in P :$ a) ó b) ó c) se satisfacen$\}$. $1 \in A$ ya que $1 = x$ ó $1 \neq x$. Si $x \neq 1$, entonces $x = Sc(v)$, es decir a) ó c) se cumplen para $1, x$.
Suponga $y \in A$, se necesita mostrar que $Sc(y) \in A$. Si $x = y$, entonces $x+1 = Sc(x) = Sc(y)$, por lo tanto c) se cumple para $x, Sc(y)$.
Como ejercicio verifique las otras posibilidades. ■

0.3.3. Multiplicación en el Conjunto de Enteros Positivos

Sea $(P, Sc, 1)$ el conjunto de enteros positivos, $H(x) = x$ para $x \in P$, $G(x, y) = x + y$, $\forall\, x, y \in P$. Denotemos por $x \bullet y$ el valor de la única función F garantizada por el Teorema 12, entonces $\bullet$ satisface

a) $F(x, 1) = x \bullet 1 = H(x) = x,\ \forall\, x \in P.$

b) $F(x, Sc(y)) = G(x, F(x, y))$, i.e. $x \bullet Sc(y) = x + x \bullet y.$

El siguiente teorema proporciona las propiedades básicas de la operación $\bullet$ (multiplicación de enteros positivos) y su relación con la adición.

Teorema 14. *Sea $(P, Sc, 1)$ un sistema de Peano, entonces:*

i) Para cualesquiera $x, y, z \in P$, $x \bullet (y+z) = x \bullet y + x \bullet z$; propiedad distributiva izquierda de $\bullet$ respecto a $+$

ii) Para cualesquiera $x, y, z \in P$, $(x+y) \bullet z = x \bullet z + y \bullet z$; propiedad distributiva derecha de $\bullet$ respecto a $+$.

iii) Para cualesquiera $x, y \in P$, $x \bullet y = y \bullet x$; propiedad conmutativa para $\bullet$

iv) Para cualesquiera $x, y, z \in P$, $x \bullet (y \bullet z) = (x \bullet y) \bullet z$; propiedad asociativa de $\bullet$

v) Para cualesquiera $x, y, z \in P$, si $x \bullet z = y \bullet z$ entonces x=y; propiedad de cancelación de $\bullet$

Demostración. i) Sean $x, y \in P$, $A = \{z \in P : x \bullet (y + z) = x \bullet y + x \bullet z\}$.
$1 \in A$; en efecto, $x \bullet (y + 1) = x \bullet Sc(y) = x + x \bullet y = x \bullet 1 + x \bullet y = x \bullet y + x \bullet 1$. Suponga $z \in A$, entonces $x \bullet (y + z) = x \bullet y + x \bullet z$, por lo que $x \bullet (y + Sc(z)) = x \bullet (Sc(y + z)) \overset{b)}{=} x \bullet (y + z) + x = x \bullet y + x \bullet z + x = x \bullet y + (x \bullet z + x) = x \bullet y + x \bullet Sc(z)$, así $Sc(z) \in A$.

ii) Sean $x, y \in P$, $A = \{z \in P : (x+y)\bullet z = x\bullet z + y\bullet z\}$. Se tiene $(x+y)\bullet 1 \overset{a)}{=} x+y \overset{a)}{=} x\bullet 1 + y\bullet 1$, por lo tanto $1 \in A$. Suponga $z \in A$, i.e. $(x + y) \bullet z = x \bullet z + y \bullet z$, entonces $(x + y) \bullet Sc(z) \overset{b)}{=} (x+y) + (x+y) \bullet z = (x+y) + [x \bullet z + y \bullet z] = (x + x \bullet z) + (y + y \bullet z) = x \bullet Sc(z) + y \bullet Sc(z)$. Así $S_c(z) \in A$

iii) Primero se demostrará que $1 \bullet x = x$, $\forall\, x$. Sea $A = \{x \in P : 1 \bullet x = x\}$. Está claro que $1\bullet 1 \overset{a)}{=} 1$. Suponga $1\bullet x = x$, entonces $1\bullet Sc(x) = 1+1\bullet x = 1+x\bullet 1 \overset{a)}{=} 1+x = Sc(x) = Sc(x)\bullet 1$. Sea $x \in P$ y $A = \{y \in P :\ x\bullet y = y\bullet x\}$. Por lo probado antes, $1 \in A$. Supongamos que $y \in A$ y probemos que $S_c(y) \in A$. Se tiene $x\bullet S_c(y) = x\bullet(y+1) = x\bullet y + x\bullet 1 = y\bullet x + 1\bullet x = (y+1)\bullet x$, probando lo deseado.

iv) Dados $x, y \in P$, sea $A := \{z \in P : (x \bullet y) \bullet z = x \bullet (y \bullet z)\}$, $1 \in A$; en efecto, $(x \bullet y) \bullet 1 \overset{a)}{=} x \bullet y = x \bullet (y) \overset{a)}{=} x \bullet (y \bullet 1)$. Suponga $z \in A$, i.e. $(x \bullet y) \bullet z = x \bullet (y \bullet z)$, entonces $(x \bullet y) \bullet Sc(z) \overset{b)}{=} (x \bullet y) + (x \bullet y) \bullet z = x \bullet y + x \bullet (y \bullet z) \overset{i)}{=} x \bullet (y + y \bullet z) \overset{b)}{=} x \bullet (y \bullet Sc(z))$. Luego $S_c(z) \in A$.

v) Suponga $x \neq y$. Por el Teorema 13 iv), se tiene $x = y + u$ ó $y = x + v$. Si $x = y + u$, entonces $x\bullet z = (y+u)\bullet z \overset{ii)}{=} y\bullet z + u\bullet z$. Nuevamente por el Teorema 13 iv) $y\bullet z + u\bullet z \neq y\bullet z$. Se aplica un argumento similar para $y = x + v$. ■

0.3.4. Exponenciación de Enteros Positivos

Sea $(P, Sc, 1)$ el conjunto de enteros positivos, $H(x) = x$ y $G(x, y) = x \bullet y$, denotando por x^y el valor de la única función $F(x, y)$ garantizado por el Teorema 12, entonces la función exponenciación satisface:

a) $F(x,1) = H(x) = x^1 = x$.

b) $F(x, Sc(y)) = G(x, F(x,y))$, i.e. $x^{Sc(y)} = x \bullet x^y$.

Las propiedades básicas de la exponenciación están contenidas en el siguiente teorema.

Teorema 15. *Sean $x, y, z \in P$, con $(P, Sc, 1)$ un sistema de Peano, entonces*

i) $1^y = 1$.

ii) $x^y \bullet x^z = x^{y+z}$.

iii) $(x^y)^z = x^{y \bullet z}$.

iv) $(x \bullet y)^z = x^z \bullet y^z$.

Demostración. i) Sea $A = \{y \in P : 1^y = 1\}$. Por la propiedad a) de la función exponenciación, $1^1 = 1$, es decir $1 \in A$. Suponga $y \in A$, entonces $1^{Sc(y)} \overset{\text{b)}}{=} 1 \bullet 1^y = 1 \bullet 1 = 1$, por lo tanto $A = P$.
ii) Suponga $x, y \in P$. Si $A = \{z \in P : x^y \bullet x^z = x^{y+z}\}$, se debe mostrar que $A = P$. $1 \in A$, en efecto, $x^y \bullet x^1 = x^y \bullet x = x \bullet x^y \overset{\text{b)}}{=} x^{Sc(y)} = x^{y+1}$. Suponga $z \in A$, i.e. $x^y \bullet x^z = x^{y+z}$, entonces $x^y \bullet x^{Sc(z)} = x^y \bullet x^{z+1} = x^y \bullet (x^z \bullet x) = (x^y \bullet x^z) \bullet x = x^{y+z} \bullet x = x^{(y+z)+1} = x^{y+(z+1)} = x^{y+Sc(z)}$.
iii) Suponga $x, y \in P$. Sea $A = \{z \in P : (x^y)^z = x^{y \bullet z}\}$.
$1 \in A$, en efecto $(x^y)^1 \overset{\text{a)}}{=} x^y = x^{(y \bullet 1)}$. Suponga $z \in A$, i.e. $(x^y)^z = x^{y \bullet z}$, entonces $(x^y)^{Sc(z)} = (x^y)^{(z+1)} \overset{\text{b)}}{=} (x^y) \bullet (x^y)^z = x^y \bullet (x^{yz}) \overset{\text{ii)}}{=} x^{y+yz} = x^{(1+z)y} = x^{Sc(z)y}$.
iv) Ejercicio. ■

0.3.5. Orden Parcial en un Sistema de Peano

Una de las propiedades básicas de los enteros positivos es, relacionar las operaciones de adición y multiplicación con el orden. La definición siguiente jugará un papel importante en la teoría general para definir el sistema de los números reales.

Definición. *Si $(P, Sc, 1)$ es un sistema de Peano, $x, y, \in P$, se dice que x es menor o igual a y (en símbolos) $x \leq y$ si y sólo si $x = y$ ó existe $u \in P$ tal que $y = x + u$.*

Observación 13. *Si W denota la relación de orden dada, entonces $(x, y) \in W \iff x \leq y$. Si $x \leq y$ y $x \neq y$ se escribe $x < y$.*

En el siguiente teorema se presentan las propiedades fundamentales del orden en los enteros positivos.

Teorema 16. *Sea P un sistema de Peano, $x, y, z \in P$, entonces*

i) Exactamente uno de los tres casos se cumple: $x < y$, $x = y$, $y < x$ (propiedad de la tricotomía para $<$).

ii) Si $x < y$ & $y < z$, entonces $x < z$ (propiedad transitiva para $<$).

iii) $x \leq x \; \forall \; x \in P$ (propiedad reflexiva para $\leq$).

iv) Si $x \leq y$ & $y \leq x$ entonces $x = y$ (propiedad antisimétrica para $\leq$).

Demostración. i) Si $x \neq y$, entonces el resultado se obtiene de la propiedad de la tricotomía para $+$.

ii) Si $x < y$ & $y < z$, entonces existen $u, v \in P$ tales que $y = x + u$ & $z = y + v$, por lo que $z = (x + u) + v = x + (u + v)$, i.e. $x < z$.

iii) Obvio.

iv) Se obtiene de i). ■

Observación 14. *Las propiedades ii)-iv) en el teorema anterior establecen que P es un conjunto parcialmente ordenado, por lo tanto del Teorema 16 se tiene que $(P, \leq)$ es totalmente ordenado.*

Nota. Recordemos, un conjunto parcialmente ordenado A es bien ordenado, si cada subconjunto no vacío $B \subseteq A$ tiene un primer elemento, i.e. para cada $B \neq \emptyset$, existe $b_0 \in B$ tal que $b_0 \leq b \; \forall \; b \in B$.

Observación 15. *Si B tiene un primer elemento, éste es único, pues si $b_0, b_1 \in B$ satisfacen $b_0 \leq b_1$ & $b_1 \leq b_0$ entonces $b_0 = b_1$.*

Teorema 17. *Sea $(P, Sc, \leq, 1)$ un sistema de Peano. Para $x, y \in P$ se tiene*

i) $x \not< 1$.

ii) $x < Sc(y) \iff x \leq y$.

iii) $1 \leq x$.

iv) $Sc(y) \leq x \iff y < x$.

v) $y < Sc(y)$ y no hay $x \in P$ tal que $y < x < Sc(y)$.

Demostración. i) Si $x < 1$, entonces $1 = x + u$ con $u \in P = \{1\} \cup Sc(P)$. Si $u = 1$ entonces $1 = x + 1 = Sc(x) \Rightarrow\Leftarrow$. Si $u \neq 1$, entonces $u = Sc(y)$ para algún y, por lo que $1 = x + Sc(y) = (x + y) + 1 = Sc(x + y) \Rightarrow\Leftarrow$. Así $x \not< 1$.

ii) Si $x < Sc(y)$ entonces $Sc(y) = y + 1 = x + u$ para algún $u \in P$. Si $u = 1$, entonces $x = y$. Si $u \neq 1$ entonces $u = Sc(z) = z + 1$, por lo que $y + 1 = x + (z + 1) \Rightarrow y = x + z$ por lo tanto $x < y$. Recíprocamente si $x \leq y$, entonces si $x = y \Rightarrow x < y + 1 = Sc(y)$. Si $x < y$ entonces $x < y < Sc(y)$.

iii) $1 \leq x$ se obtiene de i) y la propiedad de tricotomía.

iv) Si $Sc(y) \leq x$, entonces $y < Sc(y) \leq x \Rightarrow y < x$. Recíprocamente, si $y < x$, entonces $x = y + u \Rightarrow Sc(y) \leq x$.

v) $y < Sc(y)$, es claro ya que $Sc(y) = y+1$. Si $y < x < Sc(y)$ para algún x entonces, $x = y+u$ & $Sc(y) = x + v$ con $u, v \in P$. De lo anterior $Sc(y) = y + 1 = (y + u) + v = y + (u + v)$. Por la propiedad de la cancelación para $+$, se tiene $1 = u + v$, por lo tanto $u < 1$ contradiciendo i). ■

Teorema 18. *Si (P, Sc, 1) es un sistema de Peano entonces $(P, <)$ es un sistema bien ordenado.*

Demostración. Sea $A \subseteq P$, $A \neq \emptyset$. Suponga que A no tiene un primer elemento y sea $B = \{x \in P : x < y \; \forall \; y \in A\}$, se mostrará que B=P.
$1 \in B$, en efecto, por el Teorema 17 iii) $1 \leq y \; \forall \, y \in A$. Si $1 \in A$, 1 sería un primer elemento, contrario a la suposición, por lo que $1 < y \; \forall \, y \in A$, es decir $1 \in B$.
Sea $x \in B$ y suponga $y \in A$, entonces $x < y$. Aplicando el Teorema 17 iv) se tiene $Sc(x) \leq y$. Si $Sc(x) \in A$, entonces $Sc(x)$ es un primer elemento en A, contradiciendo la hipótesis sobre A, así $Sc(x) \notin A$, por lo tanto $Sc(x) < y \; \forall \, y \in A$, demostrando que $Sc(x) \in B$. Por lo tanto B=P como se afirmó.

Afirmación. $B \subseteq A^c = P \backslash A$. Suponga $x \in B \backslash A^c$, entonces $x \in B \cap A$ de esto $x < x \Rightarrow\Leftarrow$. Por lo anterior se debe tener A=$\emptyset$, una contradicción. ■

Definición. *Sea $(S, \preceq)$ un conjunto parcialmente ordenado. Dados $x, y \in S$ se dice que x es un antecesor directo de y, y que y es un sucesor directo de x si $x < y$ y no existe $z \in S$ tal que $x < z$ & $z < y$.*

Teorema 19. *Suponga que $(S, <)$ es un conjunto bien ordenado.*

i) Si $x \in S$ y para algún $z \in S$, $x < z$ entonces x tiene un único sucesor directo en S.

ii) $\forall \, x \in S$, x tiene cuando más un antecesor directo.

Demostración. i) Sea A=$\{\omega \in S : x < \omega\}$. Por hipótesis $A \neq \emptyset$. Debido a que S es un sistema bien ordenado, entonces A tiene un primer elemento a que es único. Claramente a es un sucesor directo de $x \in S$.

ii) Si x tiene dos antecesores directos, digamos a & b entonces el conjunto $\{a, b\}$ tiene un primer elemento, i.e. $a < b$ ó $b < a$, de cualquier forma se tiene una contradición, por lo que x tiene cuando más un antecesor directo. ■

El teorema siguiente caracteriza los sistemas de Peano en términos de las propiedades de orden.

Teorema 20. *Suponga $P \neq \emptyset$ y $(P, <)$ es un sistema bien ordenado con un primer elemento 1. Además, suponga que $(P, <)$ satisface:*

i) Cada elemento x de P tiene un sucesor directo, $Sc(x)$.

ii) Cada elemento x de $P \setminus \{1\}$ tiene un antecesor directo. Entonces $(P, Sc, 1)$ es un sistema de Peano.

Demostración. Se necesita demostrar que $(P, Sc, 1)$ satisface $P1$, $P2$, $P3$

$P1$) Está claro que $1 \neq Sc(x)\ \forall\, x \in P$, ya que 1 es el primer elemento en S.

$P2$) Se necesita mostrar que Sc es inyectiva. Suponga $z = Sc(x) = Sc(y)$, por lo tanto x & y son antecesores directos de z, por el Teorema 19 ii) x=y.

$P3$) Suponga $A \subseteq P$ y que satisface: $1 \in A$ y $x \in A \Rightarrow Sc(x) \in A$, se necesita demostrar que A=P. Sea B=$P \setminus A$. Si $B \neq \emptyset$, entonces B tiene un primer elemento, digamos b.

Por ii), b tiene un antecesor directo, (ya que $b \neq 1$) i.e. $b = Sc(x)$, $\Rightarrow x < b$. Debido a que b es el primer elemento en B, $x \notin B$, entonces $x \in A$, consecuentemente $Sc(x) \in A$, i.e. $b \in A$ contradiciendo lo supuesto. ■

0.3.6. Operaciones y Orden en un Sistema de Peano

Una de las propiedades fundamentales del campo de los números reales es la compatibilidad del orden con las operaciones de suma y producto. Esta propiedad es la característica fundamental que permite hacer de los reales un campo ordenado, lo que a la vez hace de estos el campo fundamental para hacer *análisis real*.
El siguiente teorema contiene las propiedades básicas que relacionan las operaciones y el orden en un sistema de Peano, y esto a su vez nos permitirá ir edificando las mismas propiedades, primeramente en los enteros, racionales, y finalmente en los reales.

Teorema 21. *Sea $(P, Sc, <, 1)$ un sistema de Peano ordenado. Si $x, y, z \in P$, entonces*

i) $x < y \iff x + z < y + z$,

ii) $x < y \iff x \bullet z < y \bullet z$,

iii) $x < y \iff x^z < y^z$,

iv) Si $1 < z$ *entonces* $1 < z^x$,

v) Si $1 < z$ *entonces* $x < y \iff z^x < z^y$,

Demostración. i) $x < y \iff \exists\, u \in P$ tal que $y = x + u$, por lo que $y + z = x + z + u$, de esta forma $x < y \iff x + z < y + z$
ii) $x < y \iff \exists\, u \in P$ tal que $y = x + u$, de aquí $y \bullet z = x \bullet z + u \bullet z$ por lo tanto $x \bullet z < y \bullet z$. Recíprocamente, si $x \bullet z < y \bullet z$, entonces $y \bullet z = x \bullet z + u$

Si $x \not< y$, entonces por tricotomía $x = y$ ó $y < x$; $x = y$ no es posible. Si $y < x$, entonces $x = y + v$, por lo tanto $y \bullet z = (y + v) \bullet z + u = y \bullet z + (v \bullet z + u)$ imposible, de esta manera $x < y$.
iii), iv), v) Ejercicio. ■

Corolario. *Para cualesquiera $x, y, z, \omega \in P$ se tiene:*

i) Si $x < y$ y $z \leq \omega$, entonces $x + z < y + \omega$.

ii) Si $x < y$ y $z \leq \omega$, entonces $x \bullet z < y \bullet \omega$.

iii) Si $x < y$ y $z \leq \omega$, entonces $x^z < y^\omega$.

iv) Si $1 < x \leq y$ y $z < \omega$, entonces $x^z < y^\omega$.

v) Si $x^z = y^z$ entonces $x = y$.

vi) Si $1 < z$ y $z^x = z^y$, entonces $x = y$.

Demostración. Ejercicio.

Se termina esta sección con un teorema relacionado con la teoría de conjuntos. El cual se presenta sin prueba.

Definición. *Sea n un entero positivo. Se dice que el conjunto S tiene n elementos si existe una función biyectiva de S a $\{k \in P : k \leq n\}$. Si $f : S \longrightarrow \{k \in P : k \leq n\}$ y g denota la inversa de f, los elementos de S se denotan por $a_1, \ldots, a_n$ donde $g(i) = a_i$.*

Teorema 22. *Sea S un conjunto, entonces S es finito $\iff$ $S = \emptyset$ ó S tiene n elementos para algún $n \in P$.*

Observación 16. *Recuerde que la definición de un conjunto finito fue dada en términos de subconjuntos de S.*

De ahora en adelante el único sistema de Peano $(P, Sc, +, \bullet, <, 1)$ le llamaremos conjunto de enteros positivos y los elementos de P se denotarán por 1, 2=Sc(1), 3=Sc(2), ..., (1+ n)=Sc(n) y el conjunto P se denotará por $\mathbb{N}$.

Observación 17. *Está más o menos "claro" que el primer elemento 1, puede reemplazarse por cualquier elemento fijo, digamos "0" y el sistema"nuevo" es isomorfo al discutido aquí.*

0.3.7. Ejercicios

1.- Resuelva todos los ejercicios asignados en las notas.

2.- En los siguientes ejercicios $\mathbb{N}$ denotará al conjunto de los enteros positivos, es decir al único sistema de Peano y Sc denotará a la función sucesor. Demuestre que Sc no tiene puntos fijos.

3.- Demuestre que $\mathbb{N}$ y $Sc(\mathbb{N})$ tienen la misma cardinalidad.

4.- Un conjunto S se dice numerable si S tiene la misma cardinalidad que $\mathbb{N}$. Demuestre que todo conjunto numerable es infinito.

5.- Para cada $n \in \mathbb{N}$ sea $I_n = \{m \in \mathbb{N} : m \leq n\}$. Demuestre que I_n es un conjunto finito. A I_n se le llama un intervalo inicial.

6.- Sea $T \subseteq \mathbb{N}$ no vacío. Demuestre que T es un intevalo inicial $\iff$ T satisface las condiciones:

   a) $Sc(n) \in T$ implica $n \in T$.

   b) Existe un $m \in T$ tal que $Sc(m) \notin T$.

7.- Demuestre que dos intervalos iniciales I_m, I_n tienen la misma cardinalidad $\iff$ $m = n$.

8.- Dado $m \in \mathbb{N}$ se define el intervalo terminal $T_m = \{n \in \mathbb{N} : m \leq n\}$. Demuestre que T_m es infinito.

9.- Dado $n \in \mathbb{N}$ entonces se tiene una y solo una de las siguientes posibilidades.

   a) $n = 1$.

   b) Existe un $m \in \mathbb{N}$ tal que $n = 2m$.

   c) Existe un $m \in \mathbb{N}$ tal que $n = 2m + 1$.

10.- Proporcione una definición de la función factorial de n usando el teorema de recursión ó el teorema 13.

11.- Sea $(S, <)$ un conjunto bien ordenado, M un subconjunto acotado. Demuestre que M admite máximo y mínimo.

0.4. Los Enteros

Se ha visto que el sistema $(\mathbb{N}, +, \bullet, <, 1)$ satisface las propiedades de los enteros positivos, la siguiente meta es construir un sistema, llamado sistema de enteros, que satisfaga entre otras propiedades, que la ecuación $m + p = p$ tenga una solución, recuerde que esta ecuación no tiene soluciones en $\mathbb{N}$.

Se tiene que en el sistema $(\mathbb{N}, +, \bullet, <, 1)$ hay elementos que satisfacen $m + q = p + n$ para diferentes valores. Si agrupamos parejas de elementos en $\mathbb{N}$, (m, n) y (p, q) con la condición $m + q = p + n$, entonces se tiene una relación en $\mathbb{N} \times \mathbb{N}$, más concretamente: los elementos $(m, n), (p, q) \in \mathbb{N} \times \mathbb{N}$ están relacionados por $\sim$ si y sólo si $m + q = p + n$ ó $(m, n) \sim (p, q)$ si y sólo si $m + q = n + p$.

Teorema 23. *La relación definida anteriormente es una relación de equivalencia en* $\mathbb{N} \times \mathbb{N}$.

Demostración. i) Está claro que $(m,n) \sim (m,n)$, ya que $m+n = n+m$ i.e. $\sim$ es reflexiva.
ii) Si $(m,n) \sim (p,q)$ entonces $m+q = n+p$ y esto es equivalente a $p+n = q+m$ por lo tanto $(p,q) \sim (m,n)$, simetría.
iii) Si $(m,n) \sim (p,q)$ & $(p,q) \sim (r,s)$ entonces $m+q = n+p$ y $p+s = q+r$, por lo que $m+q+s = p+n+s = p+s+n = r+q+n$, por cancelación en $\mathbb{N}$ se tiene $m+s = r+n$, i.e. $(m,n) \sim (r,s)$ entonces $\sim$ es transitiva. ■

Dado un elemento $(m,n) \in \mathbb{N}\times\mathbb{N}$, la clase de equivalencia de (m,n) se denotará por $[(m,n)]$: $= \{(p,q) \in \mathbb{N} \times \mathbb{N} : (m,n) \sim (p,q)\} = \{(p,q) \in \mathbb{N} \times \mathbb{N} : m+q = p+n\}$.

Definición. *Se define el conjunto de los enteros y se denota por* $\mathbb{Z} := \frac{\mathbb{N}\times\mathbb{N}}{\sim} = \{[(m,n)] : (m,n) \in \mathbb{N} \times \mathbb{N}\}$.

Observación 18. *Suponga* $[(m,n)] = [(m',n')]$ & $[(p,q)] = [(p',q')]$, *entonces* $[(m+p, n+q)] = [(m'+p', n'+q')]$. *En efecto, de lo supuesto se tiene* $m+n' = m'+n$ & $p+q' = p'+q$, *sumando estas ecuaciones se obtiene* $m+p+n'+q' = n+q+m'+p'$ *y esta última ecuación es equivalente a* $[(m+p, n+q)] = [(m'+p', n'+q')]$.

De la observación anterior se concluye que existe una operación en $\mathbb{Z}$ definida a continuación. Dados $[(m,n)], [(p,q)] \in \mathbb{Z}$ se define la **suma** de $[(m,n)]$ & $[(p,q)]$ por $[(m,n)] + [(p,q)] := [(m+p, n+q)]$.

El resultado siguiente proporciona las propiedades básicas de $(\mathbb{Z}, +)$.

Teorema 24. *La operación* $+$ *en* $\mathbb{Z}$ *satisface:*

i) $+$ *es asociativa.*

ii) $+$ *es conmutativa.*

iii) $\mathbb{Z}$ *contiene una identidad única para* $+$ *denotada 0.*

iv) $\forall\, a = [(m,n)] \in \mathbb{Z}$ *existe un único* $a' \in \mathbb{Z}$ *tal que* $a + a' = 0$.

Demostración. i) Se obtiene de la asociatividad en $\mathbb{N}$.
ii) Se obtiene de la conmutatividad en $\mathbb{N}$.
iii) Si $[(m,n)] \in \mathbb{Z}$, entonces $[(m,n)]+[(1,1)] := [(m+1, n+1)] = [(m,n)]$. También se tiene, $[(m,n)] + [(p,q)] = [(m,n)] \Rightarrow p{=}q$, y claramente $[(1,1)] = [(p,p)] \,\forall\, p \in \mathbb{N}$, por lo tanto hay un elemento único en $\mathbb{Z}$ denotado 0 tal que $0 + a = a \;\forall\, a \in \mathbb{Z}$.
iv) Suponga $[(m,n)] + [(x,y)] = [(1,1)]$ entonces $[(m+x, n+y)] = [(1,1)]$ por lo que $x{=}n$ & $y{=}m$ es una solución, se debe mostrar que esta solución es única. Se cambiará un poco la notación. Si $a = [(m,n)]$ y $0 = [(1,1)]$, entonces se tiene que $a{+}a' = 0$ con $a' = [(n,m)]$. Si a'' también satisface $a{+}a'' = 0$ entonces $a' = a' + 0 = a' + (a + a'') = (a' + a) + a'' = 0 + a'' = a''$. ■

Definición. *Sea* G *un conjunto no vacío con una operación binaria denotada por* $\bullet$. *Si* $(G, \bullet)$ *satisface*

i) $\bullet$ *es asociativa.*

ii) Existe $e \in G$ *tal que* $e \bullet g = g \bullet e = g \ \forall\, g \in G$.

iii) $\forall\, g \in G$, *existe* $g' \in G$ *tal que* $g \bullet g' = g' \bullet g = e$.

G se llama un grupo.

Si $(G, \bullet)$ es un grupo y $\bullet$ es conmutativa, G es llamado un grupo abeliano. El nombre abeliano se da después de que Niels Henrik Abel, matemático noruego, probara por primera vez en los años 1820's que si el grupo de permutaciones de las raíces de una ecuación de la forma $f(x) = a_n x^n + \cdots + a_1 x + a_0 = 0$ es conmutativo, entonces la ecuación es "soluble por radicales". Esto significa, de manera un poco imprecisa, que las raíces de un polinomio $f(x) = a_n x^n + \cdots + a_1 x + a_0$ se pueden obtener resolviendo un número finito de ecuaciones del tipo $x^k - A = 0$.

Con la terminología de la teoría de grupos, el teorema 24 establece que $(\mathbb{Z}, +)$ es un grupo abeliano.

0.4.1. Multiplicación en $\mathbb{Z}$

La multiplicación en $\mathbb{Z}$ está motivada por las reglas que involucran la multiplicación de enteros con signo, como muestra el siguiente ejemplo.

$$(+2)(-3) = (6-4)(6-9) = (6 \bullet 6 \ + \ 4 \bullet 9) - (4 \bullet 6 \ + \ 6 \bullet 9)$$

Es necesario traducir la ecuación anterior a la notación usada en los enteros. Antes que todo, el entero 6 - 4 se identifica con [(6, 4)] y similarmente 6 -9 se identifica con [(6, 9)], entonces con esta notación se puede escribir (+2)(-3)=[(6, 4)][(6, 9)]=[(6 $\bullet$6 + 4 $\bullet$9, 4 $\bullet$ 6 + 6 $\bullet$9)]. En general, el entero m - n se identifica con $[(m, n)]$ & p - q con $[(p, q)]$, por lo que una posible definición de multiplicación en $\mathbb{Z}$ que satisfaga las propiedades de multiplicación de enteros con signo es:

$$[(m, n)][(p, q)] = [(mp + nq, mq + np)] \tag{3}$$

Se demostrará que esta definición es independiente de los representantes de las clases $[(m, n)]$ y $[(p, q)]$. Más concretamente, se tiene

Teorema 25. *Si* $[(m, n)] = [(m', n')]$ *y* $[(p, q)] = [(p', q')]$ *entonces* $[(mp + nq, mq + np)] = [(m'p' + n'q', m'q' + n'p')]$.

Demostración. El resultado se obtiene si se demuestra lo siguiente:

$$[(mp + nq, mq + np)] = [(m'p + nq', m'q + n'p)] \tag{4}$$

y

$$[(m'p + nq', m'q + n'p)] = [(m'p' + n'p', m'q' + n'p')] \tag{5}$$

Por hipótesis $m+n' = m'+n$, por lo que usando las propiedades de la adición y multiplicación en $\mathbb{N}$ se tiene $(mp + nq) + (m'q + n'p) = (m + n')p + (n + m')q$=$(m + n')p + (m + n')q = (m + n')(p + q)$. Usando la misma idea tenemos $(m'p + nq') + (mq + np) = (m + n')(p + q)$, de lo anterior se obtiene (4).
Ahora usando la hipótesis $p + q' = p' + q$ y argumentando como antes, se llega a

$$(m'p + nq') + (m'q' + n'p') = (m' + n')(p + q')$$

y

$$(m'p' + n'q') + (m'q + n'p) = (m' + n')(p + q')$$

por lo cual se obtiene (5). ■

Del teorema 25 se tiene que la operación (3) en $\mathbb{Z}$ es independiente de los representantes de las clases de equivalencia definidas en $\mathbb{N} \times \mathbb{N}$. El resultado siguiente muestra las propiedades principales de las operaciones de adición y multiplicación en $\mathbb{Z}$. Una de las siguientes metas es mostrar que el sistema de enteros positivos se puede identificar canónicamente con un subsistema de los enteros.

Teorema 26. *La multiplicación en $\mathbb{Z}$ satisface*

i) $\forall\ a, b, c \in \mathbb{Z}$, $a \bullet (b \bullet c) = (a \bullet b) \bullet c$, *asociatividad.*

ii) $\forall\ a, b \in \mathbb{Z}$, $a \bullet b = b \bullet a$, *conmutatividad.*

iii) Hay un elemento en $\mathbb{Z}$ denotado por $1_{\mathbb{Z}}$ tal que $a \bullet 1_{\mathbb{Z}} = a$, $\forall\ a \in \mathbb{Z}$.

iv) La multiplicación distribuye sobre la suma, i.e.
$\forall\ a, b, c \in \mathbb{Z}$, $a \bullet (b + c) = a \bullet b + a \bullet c = b \bullet a + c \bullet a = (b + c) \bullet a$.

Demostración. i) Sean $a = [(m, n)], b = [(p, q)]$ y $c = [(r, s)]$ enteros, entonces
$(a \bullet b) \bullet c = [(mp+nq, mq+np)][(r, s)] = [(\{mp+nq\}r+\{mq+np\}s, \{mp+nq\}s+\{mq+np\}r)]$.
Por otro lado tenemos $a \bullet (b \bullet c) = [(m, n)][(pr+qs, ps+qr)] = [(m\{pr+qs\}+n\{ps+qr\}, m\{ps+qr\} + n\{pr + qs\})]$. También se tiene $(a \bullet b) \bullet c = a \bullet (b \bullet c) \iff$
$(mp + nq)r + (mq + np)s + m(ps + qr) + n(pr + qs) =$
$(mp + nq)s + (mq + np)r + m(pr + qs) + n(ps + qr)$
Esta ecuación es, en efecto verdadera.
ii) $a \bullet b = [(mp + nq, mq + np)]$ y $b \bullet a = [(pm + qn, pn + qm)]$ de esto se tiene $a \bullet b = b \bullet a$.
iii) Sea $1_{\mathbb{Z}} = [(1 + 1, 1)]$ entonces se verifica que $[(m, n)] \bullet 1_{\mathbb{Z}} = 1_{\mathbb{Z}} \bullet [(m, n)] = [(m, n)]$ para cada $[(m, n)]$.
iv) Ejercicio. ■

Se ha demostrado que la adición y la multiplicación en $\mathbb{Z}$ tienen las propiedades familiares de $+$ y $\bullet$, si para un entero a se denota por $-a$ al elemento único tal que $a + (-a) = 0$, entonces la "regla de los signos" general dice lo siguiente.

i) $(-a) \bullet (b) = a \bullet (-b) = -ab, \ \forall\, a, b \in \mathbb{Z}$.

ii) $(-a) \bullet (-b) = a \bullet b, \ \forall\, a, b \in \mathbb{Z}$.

Demostración. Ejercicio.

0.4.2. Orden en $\mathbb{Z}$

La definición de orden en el conjunto de enteros positivos tuvo por motivo, la idea "natural" de "mayor que", i.e. si $n, m \in \mathbb{N}$ y m es mayor que n, significa que $m = n + u$. En el caso de los enteros, el orden se motiva por la interpretación de que $[(m, n)]$ "significa" $m - n$, entonces se tiene la siguiente

Definición. *Un entero $a = [(m, n)]$ es positivo si $n < m$, aquí $<$ es la relación de orden en $\mathbb{N}$.*

Debido a que la definición anterior está dada en términos de representantes del entero a, se debe mostrar que si $[(m, n)] = [(p, q)]$ entonces $n < m \iff q < p$.

De $[(m, n)] = [(p, q)]$ se tiene $m+q = n+p$, entonces $n < m \iff \exists\, u \in \mathbb{N}$ tal que $m = n+u$, por lo que $n + u + q = n + p$, por la propiedad de cancelación en $\mathbb{N}$ se tiene $p = q + u$, i.e. $q < p$. El argumento anterior puede invertirse, i.e. $n < m \iff q < p$. Con esto se ha mostrado que la definición es independiente de la elección de (m, n).

Teorema 27 (Propiedad de la Tricotomía en $\mathbb{Z}$). *Si $a \in \mathbb{Z}$, entonces una y sólo una de las tres condiciones siguientes se cumple.*

i) a es positivo.

ii) $a = 0$.

iii) $-a$ es positivo.

Demostración. Sea $a = [(m, n)]$, entonces por definición, a es positivo $\iff n < m$. También se tiene que $0 = [(1, 1)]$, por lo tanto $a = 0 \iff m = n$. Por otro lado, $-a = [(n, m)]$, entonces $-a$ es positivo $\iff m < n$. De aquí, la tricotomía se obtiene de la tricotomía en $\mathbb{N}$. ■

Ejercicio. Sean a, b enteros. Suponga que a y b son positivos. Muestre que

i) $a + b$ es positivo.

ii) $a \bullet b$ es positivo.

Se define en $\mathbb{Z}$ la relación siguiente: dados $a, b \in \mathbb{Z}$, se dice que aRb si $b - a$ es positivo.

Observación 19. *R es transitiva y satisface la propiedad de la tricotomía.*

Demostración. Si $a, b \in \mathbb{Z}$, entonces $b-a = b+(-a) \in \mathbb{Z}$. Aplicando el Teorema 27 se tiene sólo una de las condiciones: $a - b = 0$, $a - b$ es positivo ó $b - a$ es positivo. Suponga que aRb & bRc entonces $b - a$ & $c - b$ son positivos, por el ejercicio anterior $(c - b) + (b - a) = c - a$ es positivo, de esta manera aRc. ■

Definición. *Dados $a, b, \in \mathbb{Z}$, se dice que $a <_{\mathbb{Z}} b$ si $b - a$ es positivo. Denotemos por $\mathbb{Z}^+ = \{a \in \mathbb{Z} : 0 <_{\mathbb{Z}} a\}$.*

Ejercicio. Muestre que

i) $\mathbb{Z}^+ = \{-a : a <_{\mathbb{Z}} 0\}$.

ii) $\mathbb{Z}^+ = \{[(Sc(n), 1)] : n \in \mathbb{N}\}$.

Para mostrar ii) note que $[(Sc(n), 1)] \in \mathbb{Z}^+ \ \forall \ n \in \mathbb{N}$. Si $a = [(p, q)] \in \mathbb{Z}^+$ entonces se tienen dos casos

a) $q = 1 < p \ \Rightarrow \ p = Sc(n)$ para algún n.

b) Si $1 < q < p$ entonces $q = 1 + m$, $p = 1 + m + n$ y $a = [(p, q)] = [(1 + n + m, 1 + m)] = [(Sc(n), 1)]$.

Ejercicio.

i) Si $a, b \in \mathbb{Z}\backslash\{0\}$, muestre que $ab \neq 0$.

ii) Si $ab = ac$ y $a \neq 0$, muestre que $b = c$.

iii) $a < b \iff a + c < b + c \ \forall \ c \in \mathbb{Z}$.

iv) $a < b \iff ac < bc \, \forall \ c \in \mathbb{Z}^+$.

Como se mencionó anteriormente, uno de los objetivos es mostrar que el sistema de enteros positivos es isomorfo a un subsistema de los enteros, para ser más preciso, se mostrará que $(\mathbb{N}, +, \bullet, <, 1) \hookrightarrow (\mathbb{Z}, +_{\mathbb{Z}}, \bullet_{\mathbb{Z}}, <_{\mathbb{Z}}, 0, 1)$. El teorema siguiente es el enunciado exacto de lo anterior.

Teorema 28 (Inclusión de $\mathbb{N}$ en $\mathbb{Z}$). *Sea $\varphi : \mathbb{N} \longrightarrow \mathbb{Z}$ definido por $\varphi(n) = [(Sc(n), 1)] \in \mathbb{Z}^+$, entonces φ satisface:*

i) φ es inyectiva.

ii) $\varphi(m + n) = \varphi(m) +_{\mathbb{Z}} \varphi(n) \ \forall \ m, \ \forall \ n \in \mathbb{N}$.

iii) $\varphi(m \bullet n) = \varphi(m) \bullet_{\mathbb{Z}} \varphi(n)\ \forall\ m,\ \forall\ n \in \mathbb{N}$.

iv) $\varphi(m) <_{\mathbb{Z}} \varphi(n) \iff m < n$.

Demostración. i) Se tiene $[(Sc(n),1)] = [(Sc(m),1)] \iff Sc(n)+1 = Sc(m)+1 \iff m = n$ (por la inyectividad de Sc).
ii) Se tiene $[(Sc(n),1)] +_{\mathbb{Z}} [(Sc(m),1)] = [(Sc(n)+Sc(m), 1+1)] = [(Sc(n+m),1)] = \varphi(n)+\varphi(m)$.
iii) Por la definición de multiplicación en $\mathbb{Z}$ se tiene:
$[(Sc(n),1)][(Sc(m),1)] = [(Sc(n) \bullet Sc(m)+1, Sc(n)+Sc(m))] = [(mn+n+m+1+1, n+m+1+1)] = [(mn+1,1)] = [(Sc(mn),1)] = \varphi(n)\varphi(m)$.
iv) Se tiene $\varphi(m) = [(Sc(m),1)] <_{\mathbb{Z}} [(Sc(n),1)] = \varphi(n) \iff [(Sc(n),1)] - [(Sc(m),1)] = [(Sc(n),1)] + [(1, Sc(m))] = [(Sc(n)+1, Sc(m)+1)] =$
$[(Sc(Sc(n)), Sc(Sc(m)))]$ es positivo y esto último ocurre si y sólo si
$Sc(Sc(m)) < Sc(Sc(n)) \iff m < n$. ■

El teorema anterior permite identificar al elemento $[(Sc(n),1)]$ con n y $\mathbb{N}$ con $\mathbb{Z}^+$.

Definiendo $S_{\mathbb{Z}} : \mathbb{Z}^+ \longrightarrow \mathbb{Z}^+$ por $S_{\mathbb{Z}}(a) := a+1$ se puede demostrar que:

i) $\varphi \circ Sc = S_{\mathbb{Z}} \circ \varphi\ \forall\ n \in \mathbb{N}$.

ii) $(\mathbb{Z}^+, S_{\mathbb{Z}}, 1_{\mathbb{Z}})$ es un sistema de Peano.

0.4.3. Propiedades Aritméticas de los Enteros

En esta sección se establecerán dos teoremas básicos concernientes a la aritmética de los enteros: el algoritmo de la división y el teorema fundamental de la aritmética. El primero habla sobre el hecho de que, no siempre un entero divide a otro, y el segundo dice que cualquier entero se obtiene de bloques "elementales", los números primos. Se tiene que cualquier entero positivo x es de la forma $2n$ ó $2n+1$, y el siguiente resultado extiende este hecho a cualquier entero b, i.e. dados cualesquiera enteros positivos a y $b \in \mathbb{Z}$, existen q y r tales que $a = bq + r$ con $0 \leq r < b$, más precisamente.

Teorema 29 (Algoritmo de la división). *Para cualesquiera $a, b \in \mathbb{Z}$, $b > 0$ existen $q, r, \in \mathbb{Z}$ únicos, tales que $a = bq + r$ con $0 \leq r < b$.*

Demostración. `Caso I` $a \geq 0$. Si $a = 0$ entonces $0 = b \bullet 0 + 0$, de esta manera se puede suponer que $a > 0$. Si $a = 1$ se tienen dos subcasos: si $b = 1$ entonces $1 = 1 \bullet 1 + 0$. Si $b > 1$, entonces $a = b \bullet 0 + a$.
Supongamos $a = bq + r$ con $0 \leq r < b$. Entonces $a+1 = bq + 1 + r$. Como $r < b$, entonces $r+1 \leq b$. Si $r+1 = b$ entonces $a+1 = (b+1)q + 0$. Si $r+1 < b$ entonces $a+1 = bq + (r+1)$ con $0 \leq r+1 < b$. De cualquier forma se tiene $a = bq + r$ con $0 \leq r < b$.

`Caso II` $a < 0$, entonces $-a > 0$. Del caso I, $-a = bq_1 + r_1$, $0 \leq r_1 < b$ entonces $a = b(-q_1) + (-r_1)$. Si $r_1 = 0$ hemos terminado, si $r_1 > 0$ entonces $0 < b < b + r_1$ y $a = b(-q_1 - 1) + (b - r_1)$ con $0 < b - r_1 < b$.

`Unicidad`. Supongamos $a = bq + r = bq' + r'$, entonces $b(q - q') = r' - r$. Si $r' > r$, entonces $q - q' > 0$, i.e. $q - q' \geq 1$, de esta forma $b(q - q') = r' - r \geq b$ y de esto último, $r' \geq b + r$ $\Rightarrow\Leftarrow$.
Si $r > r'$ entonces $q' - q > 0$ y nuevamente se tiene una contradicción, de lo anterior, $r = r'$ y $q - q' = 0$. ■

Observación 20. *El teorema anterior puede mejorarse suponiendo $b \neq 0$. Si $b < 0$ entonces $-b > 0$ y por el teorema se tiene $a = -bq + r = b(-q) + r$ con $0 \leq r < -b$.*

Definición. *Si $a, b \in \mathbb{Z}$ se dice que a divide a b si $\exists\ c \in \mathbb{Z}$ tal que $b = ac$. También se dice que a es un divisor de b.*

Definición. *Un entero $p \in \mathbb{N}\backslash\{1\}$ es primo si los únicos divisores positivos de p son 1 & p.*

Definición. *Dados $a, b \in \mathbb{Z}$, se dice que $d \in \mathbb{Z}^+$ es un máximo común divisor* (gcd) *de a y b si*

i) $d \mid a$ & $d \mid b$.

ii) Si $d_1 \mid a$ & $d_1 \mid b$ entonces $d_1 \mid d$.

Observación 21. *Si d & d_1 satisfacen i) y ii) entonces $d = d_1$. El máximo común divisor de a y b se denota por* $\gcd(a, b)$.

Teorema 30. *Dados dos enteros a, b con al menos uno diferente de cero, entonces el* $\gcd(a, b)$ *existe y* $\gcd(a, b) = d = ax + by$ *para algunos enteros x, y.*

Demostración. Sea $S = \{ax + by | x, y \in \mathbb{Z}\}$ subconjunto de $\mathbb{Z}$. Se tiene $\pm a, \pm b \in S$. Debido a que al menos uno de a ó b no es cero, entonces S tiene elementos positivos, de esta manera $S \cap \mathbb{N} \neq \emptyset$, por el principio del buen orden en $\mathbb{N}$, existe un mínimo elemento $d \in S$.

Afirmación. $d = \gcd(a, b)$. Primeramente se mostrará que d divide a cualquier elemento de S.
Sea $ax + by \in S$, por el algoritmo de la division existen $q, r \in \mathbb{Z}$ tales que $ax + by = qd + r$ con $0 \leq r < d$. También se tiene que $d = ax_0 + by_0$ para algunos $x_0, y_0 \in \mathbb{Z}$, por lo que $ax + by - qd = ax + by - qx_0a - qy_0b = (x - qx_0)a + (y - qy_0)b = r$ y de esto se tiene $r \in S$. La minimalidad sobre d implica $r = 0$. Como $a, b \in S$ entonces $d|a$ y $d|b$.
Si $d_1 \mid a$ & $d_1 \mid b$, entonces $d_1 \mid ax_0 + by_0 = d$, y de ésto se tiene que $d = \gcd(a, b)$. ■

Definición. *Dos enteros a y b son primos relativos si* $\gcd(a, b) = 1$.

Corolario 1. *Dados $a, b \in \mathbb{Z}$, a & b son primos realtivos $\iff$ existen $a_0, b_0 \in \mathbb{Z}$ tales que $1 = aa_0 + bb_0$.*

Demostración. Del teorema anterior se tiene $\gcd(a,b) = d = aa_0 + bb_0$ para algunos enteros a_0, b_0. Si $d = 1$ entonces $1 = aa_0 + bb_0$. Por otro lado, si $1 = aa_0 + bb_0$ & $d > 1$ entonces $d \mid aa_0 + bb_0 = 1 \Rightarrow\Leftarrow$. ■

Corolario 2. *Si* $\gcd(a,c) = 1$ *y* $c \mid ab$, *entonces* $c \mid b$.

Demostración. Ya que $\gcd(a,c) = 1$, entonces del corolario 1, existen $a_0, c_0 \in \mathbb{Z}$ tales que $1 = aa_0 + cc_0$, multiplicando esta ecuación por b se tiene $b = baa_0 + bcc_0$. Por hipótesis $ab = cx$ para algún x, entonces $b = cxa_0 + cbc_0 = c(xa_0 + bc_0)$, i.e. $c \mid b$. ■

Corolario 3. *Si* p *es primo y* $p \nmid a$ *entonces* $\gcd(a,p) = 1$.

Demostración. Ya que p es primo, entonces los únicos divisores positivos de p son 1 y p. Como $p \nmid a$ entonces $\gcd(a,p) = 1$. ■

Corolario 4. *Si* p *es primo y* $p \mid ab$, *entonces* p *divide a alguno de* a *y* b.

Demostración. Si $p \nmid a$ entonces del Corolario 3, $\gcd(a,p) = 1$. Del Corolario 2 se obtiene el resultado con $p = c$. ■

Corolario 5. *Si* $\gcd(a,b) = 1$ & $a \mid c$ *y* $b \mid c$ *entonces* $ab \mid c$.

Demostración. Puesto que $\gcd(a,b) = 1$, entonces $1 = aa_0 + bb_0$, por lo tanto $c = aca_0 + bcb_0 = abxa_0 + abyb_0 = ab(xa_0 + yb_0)$ para algunos $x, y \in \mathbb{Z}$. ■

Teorema 31 (Teorema Fundamental de la Aritmética). *Dado cualquier entero* $a \notin \{\pm 1, 0\}$, *a tiene una representación única (excepto orden) como un producto de primos y signo i.e.* $a = \pm p_1^{e_1} \cdots p_r^{e_r}$, *con* $p_i \neq p_j$ *si* $i \neq j$.

Demostración. Es suficiente demostrar el teorema para $a > 1$.

`Existencia`. Si $a = 2$ no hay nada que probar, entonces se puede suponer que el resultado se cumple para $a > 2$. Si $a+1$ es primo, hemos terminado. Si $a+1 = bc$ con $1 < b, c < a+1$, por la hipótesis inductiva, b & c tienen una factorización en primos, por lo tanto $a+1$ también.

`Unicidad`. Suponga $a = p_1^{e_1} \cdots p_r^{e_r} = q_1^{a_1} \cdots q_s^{a_s}$ con p_i & q_j primos. De la ecuación anterior se tiene $p_i \mid q_1^{a_1} \cdots q_s^{a_s}$, entonces de una generalización obvia del Corolario 4, $p_i \mid q_j$ para alguna j, de esta manera $p_i = q_j$. Después de volver a enumerar, si es necesario, se puede suponer $i = j = 1$, y $e_1 \geq a_1$, de esta manera $p_1^{e_1 - a_1} p_2^{e_2} \cdots p_1^{e_r} = q_2^{a_2} \cdots q_s^{a_s}$. Continuando con este argumento se muestra que $s = r, e_i = a_i$ & $p_i = q_i \; \forall \; i$. ■

0.4.4. El Algoritmo Euclidiano

Euclides, en sus Elementos, indica un algoritmo para encontrar el gcd de a & b. Este algoritmo se basa en el algoritmo de la división, es por eso que algunas veces sus nombres se usan como sinónimos. El algoritmo de la división dice lo siguiente:

Dado $a, b, \in \mathbb{Z}$ con al menos uno $\neq 0$, digamos $b \neq 0$, entonces existen $q, r, \in \mathbb{Z}$ tales que $a = bq + r$ con $0 \leq r < b$, si $b > 0$, ó $0 \leq r < -b$ si $b < 0$.

Por facilidad se supone $b > 0$. Entonces de $a = bq + r$ se tiene $d \mid a$ & $d \mid b \iff d \mid b$ & $d \mid r$ por lo que $\gcd(a, b) = \gcd(b, r)$.

Continuando este proceso con b y r_1, r_1 y r_2, y así sucesivamente, se obtienen las siguientes ecuaciones y condiciones.

$$\begin{array}{cc} a = bq_1 + r_1 & 0 \leq r_1 < b \\ b = r_1q_2 + r_2 & 0 \leq r_2 < r_1 \\ r_1 = r_2q_3 + r_3 & 0 \leq r_3 < r_2 \\ \vdots & \vdots \\ r_{n-2} = r_{n-1}q_n + r_n & 0 \leq r_n < r_{n-1} \end{array}$$

Entonces se ha construído una sucesión decreciente de enteros no negativos $r_n < \cdots < r_2 < r_1$, así, se tiene necesariamente $r_n = 0$ para algún n. Tomando un n mínimo tal que $r_{n-1} \neq 0$ y $r_n = 0$ y de la observación anterior se tiene

$$\gcd(a, b) = \gcd(b, r_1) = \cdots = \gcd(r_{n-2}, r_{n-1}) = r_{n-1} \neq 0.$$

A continuación se presenta un método práctico para encontrar el gcd de dos enteros positivos, así como la combinación lineal tal que $\gcd(a, b) = aa_0 + bb_0$. Este método está estrechamente ligado con el procedimiento para encontrar la forma normal de Smith de una matriz entera. La forma normal de Smith de una matriz entera, se obtiene aplicando operaciones elementales en las filas de una matriz con entradas enteras. Puesto que se estará trabajando en los enteros, se suprimirán los cocientes, y en lugar de éstos, se usará el algoritmo de la división.

Sean a, b enteros, se puede suponer $a, b > 0$, más aún, $a \geq b$, entonces $a = bq_1 + r_1$ con $0 \leq r_1 < b$. Considere la matriz $A_0 = \begin{bmatrix} a & 1 & 0 \\ b & 0 & 1 \end{bmatrix}$, multiplicando la fila 2 por $-q_1$ y sumándola a la fila 1, se tiene $\begin{bmatrix} a & 1 & 0 \\ b & 0 & 1 \end{bmatrix} \sim \begin{bmatrix} r_1 & 1 & -q_1 \\ b & 0 & 1 \end{bmatrix} \sim \begin{bmatrix} b & 0 & 1 \\ r_1 & 1 & -q_1 \end{bmatrix} = A_1$

Pruebe si $r_1 = 0$. Si $r_1 \neq 0$ entonces $b = r_1q_2 + r_2$, de esta manera $\begin{bmatrix} b & 0 & 1 \\ r_1 & 1 & -q_1 \end{bmatrix} \sim \begin{bmatrix} r_2 & -q_2 & 1 + q_1q_2 \\ r_1 & 1 & -q_1 \end{bmatrix} = A_2$

Continuando con el proceso se llega a la siguiente matriz

$A_n = \begin{bmatrix} r_n & * & * \\ r_{n-1} & a_0 & b_0 \end{bmatrix}$

Si $r_n = 0$ entonces $\gcd(a, b) = r_{n-1} = aa_0 + bb_0$.

Observación 22 *El método presentado anteriormente se aplica para encontrar el máximo común divisor de elementos que pertenezcan a un dominio entero*[2] *en el cual se cumpla el algoritmo eucliadno, por ejemplo el anillo de polinomios con coeficientes en un campo.*

Ejemplos.

1. Encuentre $\gcd(32, 28)$ y la combinación lineal tal que $\gcd(32, 28) = 32x + 28y$.

   $$\begin{bmatrix} 32 & 1 & 0 \\ 28 & 0 & 1 \end{bmatrix} \sim \begin{bmatrix} 4 & 1 & -1 \\ 28 & 0 & 1 \end{bmatrix} \sim \begin{bmatrix} 28 & 0 & 1 \\ 4 & 1 & -1 \end{bmatrix} \sim \begin{bmatrix} 0 & -7 & 8 \\ 4 & 1 & -1 \end{bmatrix}$$

   De aquí se tiene

   $4 = 32 - 28$.

2. Encuentre $\gcd(47, 5) = 47x + 5y$.

   $$\begin{bmatrix} 47 & 1 & 0 \\ 5 & 0 & 1 \end{bmatrix} \sim \begin{bmatrix} 2 & 1 & -9 \\ 5 & 0 & 1 \end{bmatrix} \sim \begin{bmatrix} 5 & 0 & 1 \\ 2 & 1 & -9 \end{bmatrix} \sim \begin{bmatrix} 1 & -2 & 19 \\ 2 & 1 & -9 \end{bmatrix} \sim \begin{bmatrix} 2 & 1 & -9 \\ 1 & -2 & 19 \end{bmatrix} \sim \begin{bmatrix} 0 & 5 & -47 \\ 1 & -2 & 19 \end{bmatrix}$$

   De esto se tiene $\gcd(47, 5) = 1 = 47(-2) + 5(19)$.

Ejercicio. Escriba un programa para encontrar $\gcd(a, b) = ax_0 + by_0$.

Nota. Si $\gcd(a, b) = 1$, entonces las entradas *, * de A_n son a y b permutados y con signo.

0.4.5. Representación de los Enteros en Base b

El sistema decimal significa que se usan 10 símbolos $0, 1, \cdots, 9$ y una representación de un número a en la forma $a_0 + a_1 10 + \cdots + a_k 10^k = a$ con $0 \leq a_i \leq 9$, a_i entero para cada i. Es menos común la representación de un número entero en base 2, i.e., cualquier a se puede representar como $a = a_0 + a_1 2 + a_2 2^2 + \cdots + a_k 2^k$, donde a_i es cero o uno para cada i.

Por ejemplo 133 se representa como $133 = 3 + 3 \bullet 10 + 1 \bullet 10^2$ en base 10 y $133 = 1 + 2^2 + 2^7$ en base 2. En notación posicional se tiene $133 = (3 + 3 \bullet 10 + 1 \bullet 10^2)_{10}$ en base 10 y $(1 + 2^2 + 2^7)_2 = 10000101$ en base 2.

Desde un punto de vista aritmético, algunas veces es más eficiente hacer cálculos usando base 2, especialmente para hacer cálculos con una computadora.

El siguiente resultado garantiza que cualquier entero positivo $b > 1$ se puede usar para representar números enteros[3]. Antes, se da la definición precisa de lo que entendemos por notación posicional.

[2] Ver definición después de la Observación 25

[3] Cualquier real se puede representar en base b

Definición. *Dados dos enteros positivos a y b, $b > 1$. Se dice que a admite una representación en base b si existen enteros $n, c_0, \cdots, c_n$ no negativos tales que $a = c_0 + c_1 b + \cdots + c_n b^n$ con $0 \leq c_i < b \ \forall \ i$ y $c_n \neq 0$. La representación posicional de a en base b, denotada $(a)_b$ es $(a)_b = c_n c_{n-1} \cdots c_0$.* A los enteros $c_0, \ldots, c_n$ se les llama los dígitos de a en base b.

Teorema 32. *Sea $b > 1$ un entero, entonces cualquier otro entero positivo a admite una representación única en base b.*

Demostración. Antes de empezar la demostración se hará la convención $b^0 := 1$.
Sea $a \in \mathbb{N}$, si $a = 1$ entonces $a = 1 \bullet b^0$ y esta representación es claramente única.
Suponga que $a > 1$ y el resultado verdadero para todo $a_1 < a$. Por la propiedad de tricotomía se tiene $a < b$ ó $a \leq b$.
Si $a < b$ entonces $a = a \bullet 1 = a \bullet b^0$, claramente ésta es una representación de a en base b. Si $a = \sum_{k=0}^{n} c_k b^k$ es otra representación con $n > 0$, y $c_n \neq 0$, entonces $a = c_n b^n + \sum_{k=0}^{n-1} c_k b^k$, esto claramente contradice $a < b$.
Si $b \leq a$, entonces del algoritmo de la división existen $q, r \in \mathbb{Z}$ tales que

$$a = bq + r \qquad \text{con} \qquad 0 \leq r < b \tag{6}$$

De la hipótesis $b \leq a$ y la condición anterior sobre r se tiene $0 < a - r = bq$, así $q > 0$. Ya que $1 < b$ entonces $q < qb \leq a$, de aquí, por la hipótesis de inducción, q admite una representación única en base b, i.e. existe una única $m \geq 0$ y enteros $d_0, \ldots, d_m$ con $0 \leq d_i < b$ y $d_m \neq 0$ tales que $q = \sum_{i=0}^{m} d_i b^i$ Sustituyendo en (6) se tiene:

$$a = b \sum_{i=0}^{m} d_i b^i + r = \sum_{i=0}^{m} d_i b^{i+1} + r$$

Esto muestra que a tiene una representación en base b.
Si $a = \sum_{k=0}^{l} c_k b^k$ es otra representación de a, entonces se debe tener que $l > 0$, pues de otra forma $a = c_k < b \Rightarrow\Leftarrow$. De aquí, se tiene $a = c_0 + \sum_{k=1}^{l} c_k b^k = c_0 + (\sum_{k=1}^{l} c_k b^{k-1})b$. Ya que $0 \leq c_0 < b$, entonces la unicidad en la representación de a por medio del algoritmo de la división implica $c_0 = r$ & $q = \sum_{k=1}^{l} c_k b^{k-1}$. Ahora la hipótesis de inducción garantiza la unicidad de la representación de a. ■

Corolario. *Con la notación anterior, n es el mínimo entero tal que $b^n \leq a < b^{n+1}$.*

Demostración. La representación de a implica $b^n \leq a$, ya que $a = c_n b^n + \sum_{k=0}^{n-1} c_k b^k$. Se tiene también $c_k < b$, así $c_k \leq b-1$, por lo tanto $a \leq \sum_{k=0}^{n}(b-1)b^k = b^{n+1} - 1 < b^{n+1}$. ■

Ejercicio. Obtenga el algoritmo para sumar enteros cuando se representan en base b. ¿Podría obtener el algoritmo de la multiplicación?

0.5. Congruencias módulo m y Clases de Residuos

En la vida diaria, algunos hechos son periódicos, por ejemplo para saber qué día será Navidad en 1999 se debe resolver un problema "mod 7". Hay muchos ejemplos donde se usa la aritmética mod m. En esta sección se precisará que significa resolver un problema mod m.

0.5.1. Aritmética en $\frac{\mathbb{Z}}{m\mathbb{Z}}$

Definición. *Sea m un entero positivo, dados $a, b \in \mathbb{Z}$ se dice que a es congruente a b módulo m, en símbolos $a \equiv b \pmod{m}$ si $m \mid a-b$.*

Observación 23. *$\equiv$ es una relación de equivalencia*

i) $a \equiv a \pmod{m}$ $\forall\, a \in \mathbb{Z}$.

ii) $a \equiv b \pmod{m} \Rightarrow b \equiv a \pmod{m}$.

iii) $a \equiv b \pmod{m}$ *&* $b \equiv c \pmod{m}$ *entonces* $a \equiv c \pmod{m}$.

Dados $m \geq 1$ y $a \in \mathbb{Z}$ se denota por $[a]_m$ o simplemente $[a]$, a la clase de equivalencia de a bajo la relación de congruencia módulo m, i.e., $[a]_m = \{r : a \equiv r \pmod{m}\} = \{r : m \mid (a-r)\} = \{r : a = mq + r, q \in \mathbb{Z}\}$.

Ejercicio. Verifique que dado $m \geq 1$, hay exactamente m clases de equivalencia mod m, dichas clases de equivalencia son $[0], [1], \ldots, [m-1]$.

Si $m \geq 1$, el conjunto de clases de equivalencia se denota por $\frac{\mathbb{Z}}{m\mathbb{Z}} = \{[0], \cdots, [m-1]\}$.

Dados $[a], [b] \in \frac{\mathbb{Z}}{m\mathbb{Z}}$ se definen las operaciones siguientes

i) $[a] + [b] := [a+b]$.

ii) $[a][b] := [ab]$.

Observación 24. *Las operaciones anteriores están bien definidas.*

i) Si $[a] = [a']$ *&* $[b] = [b']$ *entonces* $a = a' + qm$ *&* $b = b' + q_1 m$, *de donde* $a + b = a' + b' + (q + q_1)m$, *i.e.* $[a + b] = [a' + b']$.

ii) De las ecuaciones anteriores se tiene $ab = a'b' + mr$ *para algún* r, *entonces* $[ab] = [a'][b']$

Las definiciones siguientes no son realmente necesarias, sin embargo proporcionan una terminología coherente.

Definición. *Sea* R *un conjunto no vacío en el cual están definidas dos operaciones binarias* $+$ *y* $\bullet$ *que satisfacen:*

i) $(R, +)$ *es un grupo abeliano con identidad 0.*

ii) $(R, \bullet)$ *satisface*

a) $(x \bullet y) \bullet z = x \bullet (y \bullet z),\ \forall\ x, y, z, \in R$, *asociatividad de* $\bullet$

b) $x \bullet y = y \bullet x,\ \forall\ x, y \in R$, *conmutatividad de* $\bullet$

c) $x \bullet (a + b) = x \bullet a + x \bullet b$, *distributividad izquierda de* $\bullet$ *con respecto a* $+$.

d) Existe $1 \in R \backslash \{0\}$ *tal que* $x \bullet 1 = 1 \bullet x = x\ \ \forall\ x \in R$.

La estructura $(R, +, \bullet, 0, 1)$ con las propiedades anteriores es llamada un anillo conmutativo con identidad. Si no hay confusión se dice que R es un anillo ó un anillo conmutativo con 1.

Observación 25. *En la definición general de anillo, se suprimen las condiciones b) y d) y se agrega la propiedad distributiva de* $\bullet$ *respecto a* $+$ *por la derecha. En la definición anterior esta propiedad se obtiene de b) y c).*

Definición. *Si* R *es un anillo conmutativo con 1 y satisface* $ab = 0 \Rightarrow a$ *ó* b *es cero,* R *es llamado un dominio entero. Si adicionalmente,* $\forall\ a \in R \backslash \{0\}$ *existe* a' *tal que* $aa' = 1$, R *se llama un campo.*

De la definición de adición y multiplicación en $\dfrac{\mathbb{Z}}{m\mathbb{Z}}$ se muestra fácilmente que $[0]$ y $[1]$ son identidades para $+$ y $\bullet$ respectivamente.
En el teorema siguiente están contenidas las propiedades principales de las operaciones en $\dfrac{\mathbb{Z}}{m\mathbb{Z}}$.

Teorema 33. $\left(\dfrac{\mathbb{Z}}{m\mathbb{Z}}, +, \bullet, [0], [1]\right)$ *es un anillo conmutativo con identidad. Adicionalmente,* $\dfrac{\mathbb{Z}}{m\mathbb{Z}}$ *es un campo* $\iff$ m *es un número primo.*

Demostración. i) $\left(\dfrac{\mathbb{Z}}{m\mathbb{Z}}, +\right)$ es un grupo abeliano. Ejercicio

ii) a) La asociatividad de $\bullet$ se obtiene de la asociatividad de $\bullet$ en $\mathbb{Z}$.

b) Se obtiene de la conmutatividad en $\mathbb{Z}$.

c) Se obtiene de la distributividad de $\bullet$ respecto a $+$ en $\mathbb{Z}$.

d) Claramente $[1][a] = [a]\ \forall\ [a] \in \dfrac{\mathbb{Z}}{m\mathbb{Z}}$.

De lo anterior se tiene que $\dfrac{\mathbb{Z}}{m\mathbb{Z}}$ es un anillo.

Si $\dfrac{\mathbb{Z}}{m\mathbb{Z}}$ es un campo y m no es primo, entonces existen $r, s \in \mathbb{Z}$ tales que $m = rs$, y $[r], [s] \neq [0]$. También se tiene $[r][s] = [0]$, ya que $\dfrac{\mathbb{Z}}{m\mathbb{Z}}$ es un campo, entonces existe $[s']$ tal que $[s][s'] = [1]$, así $[r][s][s'] = [r] = [0] \Rightarrow\Leftarrow$, de aquí se debe tener que $m = p$, un número primo. Recíprocamente, si $m = p$ es primo y $[a] \neq [0]$, entonces $(p, a) = 1$, de aquí existen $x, y \in \mathbb{Z}$ tales que $1 = ax + py$, por lo tanto $[1] = [ax] = [a][x]$.
De lo anterior se tiene que todo $[a]$ no cero tiene inverso, si $[a], [b] \neq 0$ entonces $[a][b] \neq 0$, pues existe $[b']$ tal que $[b][b'] = 1$, si $[a][b] = [0]$, entonces $[a] = [a][b]\ [b'] = [0]$. ■

Ejercicio. Sea D un anillo conmutativo con identidad y finito. Muestre que, D es un dominio entero $\iff$ D es un campo.

Observación 26. *Si* $\dfrac{\mathbb{Z}}{m\mathbb{Z}} = \{[a_1], \ldots, [a_m]\}$ *y* $\gcd(k, m) = 1$, *entonces* $\dfrac{\mathbb{Z}}{m\mathbb{Z}} = \{[ka_1], \ldots, [ka_m]\}$.

Demostración. Es suficiente mostrar que $[ka_i] = [ka_j] \Rightarrow i = j$. Suponga que $[ka_i] = [ka_j]$, entonces $m \mid k(a_i - a_j)$, ya que $gcd(k, m) = 1$ entonces $m \mid (a_i - a_j)$ i.e. $[a_i] = [a_j]$, por lo tanto $i = j$. ■

Definición. *Dado* $m \geq 1$, *la función de Euler* φ *se define como sigue* $\varphi(m) = |\{[k] \in \dfrac{\mathbb{Z}}{m\mathbb{Z}} : (k, m) = 1\}|$.

Observación 27. *Una reformulación de la definición de* $\varphi(m)$ *es* $\varphi(m) = |\{k \in \mathbb{N} : k \leq m, \gcd(k, m) = 1\}|$.

Ejercicio. Si $m = p^e$, p un primo muestre que $\varphi(p^e) = p^{e-1}(p - 1)$.

En el siguiente ejercicio se enuncia una de las propiedades fundamentales de la función φ de Euler. Para una demostración ver el apéndice al final de las notas.

Ejercicio. Si $\gcd(m, n) = 1$ entonces $\varphi(mn) = \varphi(m)\varphi(n)$.

Teorema 34 (Euler). *Sean* $m \geq 1$ *y* $a \in \mathbb{Z}$ *tales que* $gcd(a, m) = 1$, *entonces* $a^{\varphi(m)} \equiv 1$ (mód m).

Demostración. Sea $[a_1], \ldots, [a_{\varphi(m)}]$ el conjunto de elementos cuyos representantes son primos relativos con m. De la observación anterior
$\{[aa_1], \ldots, [aa_{\varphi(m)}]\} = \{[a_1], \ldots, [a_{\varphi(m)}]\}$. También se tiene que
$\gcd(m, a_1 \cdots a_{\varphi(m)}) = 1$. El siguiente producto se toma en el anillo $\dfrac{\mathbb{Z}}{m\mathbb{Z}}$. $[aa_1] \cdots [aa_{\varphi(m)}] = [a_1] \cdots [a_{\varphi(m)}]$, de aquí $a^{\varphi(m)} a_1 \cdots a_{\varphi(m)} \equiv a_1 \cdots a_{\varphi(m)} \pmod{m}$. Ya que $\gcd(m, a_1 \cdots a_{\varphi(m)}) = 1$ entonces $a^{\varphi(m)} \equiv 1 \pmod{m}$. ■

Corolario (Teorema Chico de Fermat). *Sea p un número primo, $a \in \mathbb{Z}$, entonces $a^p \equiv a \pmod{p}$.*

Demostración. Si $p \mid a$, claramente se tiene $a^p \equiv a \pmod{p}$. Si $p \nmid a$ entonces $gcd(p, a) = 1$ y $\varphi(p) = p - 1$, por lo tanto del teorema de Euler $a^{p-1} \equiv 1 \pmod{p}$, $\Rightarrow a^p = a \, mod \, p$. ■

Ejercicio

a) Demuestre que el producto de n enteros positivos consecutivos es divisble por $n!$ Concluya de aquí que si p es un número primo, entonces p divide a los coeficientes binomiales[4]

$$\binom{p}{1}, \binom{p}{2}, \ldots, \binom{p}{p-1}$$

b) Use el ejercicio anterior para mostrar que $(x_1 + \cdots + x_n)^p \equiv x_1^p + \cdots + x_n^p \pmod{p}$, si $x_i \in \mathbb{Z}$.

c) Si $m \equiv 1 \pmod{p^\alpha}$ entonces $m^p \equiv 1 \pmod{p^{\alpha+1}}$ $\forall \, \alpha > 0$.

0.5.2. Ejercicios

1.- Resuelva todos los ejercicios asignados en las notas.

2.- Defina el máximo común divisor de $a_1, \ldots, a_k$ elementos de $\mathbb{Z}$ y demuestre que es combinación lineal de ellos.

3.- Defina el mínimo común múltiplo de a y b y denotándole por $[a, b]$ demuestre que $[a, b] = \frac{ab}{\gcd(a,b)}$.

4.- Se definen los números de Fermat por $F_n = 2^{2^n} + 1$. Demuestre que $\gcd(F_n, F_m) = 1$ si $n \neq m$. Concluya de esto que hay infinidad de primos.

5.- Sean a, n enteros mayores que uno. Si $a^n - 1$ es primo, entonces $a = 2$ y n es primo.

[4]Dados dos enteros positivos m y n se define el coeficiente binomial de m y n por $\binom{m}{n} = \dfrac{m!}{(m-n)!n!}$

6.- Sean m, n enteros positivos, suponga que $\gcd(m, n) = 1$. Si $a, b \in \mathbb{Z}$ entonces existe x tal que $x \equiv a \pmod{m}$ y $x \equiv b \pmod{n}$.

7.- Sea $a_1 = 1$, $a_2 = 1$ y $a_n = a_{n-1} + a_{n-2}$ para todo $n \geq 3$. Los a_n se llaman los números de Fibonacci. Demuestre que $\gcd(a_n, a_{n+1}) = 1$ para toda n.

8.- Sean m, n enteros positivos tales que $\gcd(n, m) = 1$. Demuestre que $m^{\varphi(n)} + n^{\varphi(m)} \equiv 1 \pmod{nm}$, con φ denotando la función de Euler.

9.- Si φ es como en el problma 8 determine los $n \in \mathbb{N}$ tales que:

1.- $\varphi(n) = n - 1$.

2.- $\varphi(n) = \varphi(2n)$.

3.- $\varphi(n)$ divide a n.

10.- Sea p un primo y $n \in \mathbb{N}$. Demuestre que

$$1^n + 2^n + \cdots + (p-1)^n \equiv \begin{cases} -1 \pmod{p} & \text{si } p-1 | n \\ 0 \pmod{p} & \text{si } p-1 \nmid n \end{cases}$$

11.- Demuestre el teorema de Wilson, es decir si m es un entero positivo, m es primo $\iff$ $(m-1)! \equiv -1 \pmod{m}$.

12.- Sea $n \in \mathbb{N}$ el cual no es divisible por ningún primo p con $p^3 \leq n$. Demuestre que n admite a lo más dos factores primos.

13. Sea $f(x) \in \mathbb{Z}[x]$ un polinomio no constante. Demuestre que $f(n)$ no es primo para una infinidad de $n \in \mathbb{N}$. ¿Conoce un polinomio $f(x)$ tal que $f(n)$ es primo para al menos 10 valores consecutivos de n?

14.- Sea $n \in \mathbb{N}$. Demuestre:

a) $n^4 + 4$ no es primo si $n > 1$.

b) $8^n + 1$ no es primo para todo $n \in \mathbb{N}$.

15.- Sean a, b enteros tales que $gcd(a, b) = 1$. Demuestre $gcd(a^k, b^n) = 1$ para todo $k \geq 1$ y para todo $n \geq 1$.

16.- ¿Es verdadero el siguiente enunciado? Para todo $n > 1$ existe un primo p tal que $n < p < 2n$.

17.- Demuestre que hay infinidad de primos de la forma $4n + 1$, $n \in \mathbb{N}$. Sean $a, b \in \mathbb{N}$ fijos ¿que condiciones deben satisfacer a y b para que $an + b$ sea primo, con $n \in \mathbb{N}$? Investigar cual es el teorema de Dirichlet para sucesiones de primos.

18.- Demuestre que $2^{32} + 1$ no es primo.

19.- Demuestre que la ecuación $x^n = n$ no tiene solución en $\mathbb{Q}$ para todo $n \in \mathbb{N} \setminus \{1\}$.

20.- Sea n un natural. Demuestre que n es divisible por 3 (9) $\iff$ la suma de sus dígitos en base 10 es divisible por 3 (9).

21.- Encuentre un criterio para divisivilidad por 11 y por 2^k.

22.- Sean $a, b, c \in \mathbb{Z}$. Demuestre que la ecuación $ax + by = c$ tiene solución en $\mathbb{Z}$ $\iff$ $\gcd(a, b)$ divide a c.

23.- Sean $a, b \in \mathbb{Z}$ primos relativos. Demuestre que $\gcd(a + b, a - b)$ es 1 ó 2.

24.- Con las hipótesis del ejercicio anterior, si ab es un cuadrado, entonces a y b también son cuadrados.

25.- Si $a^n + 1$ es un primo mayor que 2, demuestre que a es par y n es una potencia de 2.

26. Sea $\mathbb{Z}[\sqrt{-2}] := \{a + b\sqrt{-2} : \ a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$. Demuestre que con las operaciones de suma y producto en $\mathbb{C}$, $\mathbb{Z}[\sqrt{-2}]$ es un dominio entero. Un elemento u en un anillo conmutativo R se dice una unidad si $uv = 1$ para algún $v \in R$. Determine las unidades de $\mathbb{Z}[\sqrt{-2}]$. ¿Se cumple el teorema fundamental de la aritmética en $\mathbb{Z}[\sqrt{-2}]$?

27.- Demuestre que la ecuación $3x^2 + 2 = y^2$ no tiene soluciones enteras. ¿Cuál es la interpretación geométrica de este hecho? ¿Tiene soluciones enteras la ecuación $x^2 + y^2 = 3$.

28.- Determine todas las soluciones enteras de la ecuación $x^2 + y^2 = z^2$. Sugerencia: encuentre todos los puntos racionales en el círculo unitario.

29.- ¿Tiene soluciones en $\mathbb{Z} \setminus \{0\}$ la ecuación $x^4 + y^4 = z^2$?

30.- ¿Es un entero la suma $1 + \frac{1}{2} + \cdots + \frac{1}{n}$?

31.- Demuestre que $\mathbb{Z}$ y $\mathbb{N}$ tienen la misma cardinalidad.

32.- Determine cuales primos se pueden representar como suma de dos cuadrados. Conteste lo mismo para un entero positivo. ¿Que enteros pueden ser representados como suma de tres cuadrados? Compare con la segunda parte del ejercicio 27.

33.- Demuestre que en un campo finito todo elemento se representa como suma de dos cuadrados, en particular el -1. ¿En que campos finitos el -1 es un cuadrado?

34.- Sea C una cónica con coeficientes en los racionales. Suponga que C tiene un punto racional. Demuestre que C tiene infinidad de puntos racionales.

35.- Si p es un primo y $a \equiv b \pmod{p}$ entonces $a^{p^{n-1}} \equiv b^{p^{n-1}} \pmod{p^n}$.

36.- Demuestre que para cada $n \in \mathbb{N}$ se pueden encontrar n enteros consecutivos que no son primos.

0.6. El Campo de los Números Racionales

Se sabe que el cociente de enteros no es siempre un entero, por ejemplo $\frac{5}{3}$ no es un entero , esto se puede formular diciendo que el inverso multiplicativo de 3, por 5 no es un entero, sin embargo, $\frac{5}{3}$ es un número racional, intuitivamente el campo de los números racionales está constituído por enteros, y los inversos multiplicativos de aquellos diferentes de cero. Esta idea se precisará a continuación

Nota. *Un número racional es un cociente de dos enteros* $\frac{a}{b}, b \neq 0$, *y* $\frac{a}{b} = \frac{c}{d} \iff ad - bc = 0$. *Este hecho sugiere tomar parejas de enteros* (a, b) *y* (c, d) *con* $bd \neq 0$ *y declarar que estas parejas representan el mismo número racional si y sólo si* $ad - bc = 0$.

En otras palabras, se tiene una relación $S = \mathbb{Z} \times (\mathbb{Z}\backslash\{0\})$ definida como sigue.

Dados $(a, b), (c, d) \in S$, $(a, b) \sim (c, d)$ si y sólo si $ad - bc = 0$.

Observación 28. $\sim$ *es una relación de equivalencia en S.*

i) $(a, b) \sim (a, b)$ *claro.*

ii) $(a, b) \sim (c, d)$ *entonces* $ad - bc = 0 \Rightarrow bc - ad = 0 = cb - da$, *por lo tanto* $(c, d) \sim (a, b)$.

iii) Si $(a, b) \sim (c, d)$ *y* $(c, d) \sim (e, f)$ *entonces* $ad - bc = 0$ *y* $cf - de = 0$. *Multiplicando la primera ecuación por* f *y la segunda por* b *y sumando se tiene* $adf - bde = 0$. *Ya que* $d \neq 0$, *entonces* $af - be = 0$, *i.e.* $(a, b) \sim (e, f)$.

Dado $(a, b) \in S$, la clase de equivalencia de (a, b) se denota por $[(a, b)]$.

Definición. *El conjunto de los números racionales se define como* $\mathbb{Q} = \frac{S}{\sim} := \{[(a, b)] : a \in \mathbb{Z}, b \in \mathbb{Z}\backslash\{0\}\}$.

Notación. *Si* $[(a, b)] \in \mathbb{Q}$ *se escribe* $[(a, b)] = \frac{a}{b}$.

Usando esta notación, se puede intuir como definir la suma y multiplicación de racionales.

Dados $\frac{a}{b}, \frac{c}{d} \in \mathbb{Q}$, se define $\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$ y $\frac{a}{b} \bullet \frac{c}{d} = \frac{ac}{bd}$.

Enseguida se muestra que estas definiciones son independientes de los representantes, más precisamente:

Supongamos que $\frac{a}{b} = \frac{a'}{b'}$ y $\frac{c}{d} = \frac{c'}{d'}$ entonces

$$ab' - a'b = 0 \tag{7}$$

y

$$cd' - c'd = 0 \tag{8}$$

De estas ecuaciones se tiene $ab'dd' - a'bdd' = 0$ & $cd'bb' - c'dbb' = 0$; sumándolas obtenemos $adb'd' - a'bdd' + cd'bb' - c'dbb' = 0$ y de aquí se tiene $(ad + bc)b'd' = (a'd' + b'c')bd$ ó

$$\frac{ad + bc}{bd} = \frac{a'd' + b'c'}{b'd'} \tag{9}$$

Multiplicando (7) por cd' y (8) por $a'b$ se tiene

$$ab'cd' - a'bcd' = 0$$

$$cd'a'b - c'da'b = 0$$

Sumando estas ecuaciones se llega a $ab'cd' - c'da'b = 0$, equivalentemente

$$\frac{ac}{bd} = \frac{a'c'}{b'd'} \tag{10}$$

Las ecuaciones (9) y (10) muestran que la suma y la multiplicación de racionales está bien definida.

De las definiciones de suma y producto en $\mathbb{Q}$ se tiene que $\frac{0}{1}$ y $\frac{1}{1}$ son identidades para la suma y producto respectivamente; la notación para estas identidades son 0 y 1 como siempre.

Las principales propiedades de $\mathbb{Q}$ con las operaciones definidas se encuentran contenidas en el siguiente teorema.

Teorema 35. *$(\mathbb{Q}, +, \bullet, 0, 1)$ es un campo.*

Demostración. Mostrar que $\mathbb{Q}$ es un campo, es equivalente a mostrar que

i) $(\mathbb{Q}, +, 0)$ es un grupo abeliano.

ii) $(\mathbb{Q}\backslash\{0\}, \bullet, 1)$ es un grupo abeliano.

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

i) La adición en $\mathbb{Q}$ es asociativa. Si $\frac{a}{b}, \frac{c}{d}, \frac{e}{f} \in \mathbb{Q}$, entonces
$\left(\frac{a}{b} + \frac{c}{d}\right) + \frac{e}{f} = \frac{ad + bc}{bd} + \frac{e}{f} = \frac{(ad + bc)f + bde}{bdf}$ y
$\frac{a}{b} + \left(\frac{c}{d} + \frac{e}{f}\right) = \frac{a}{b} + \frac{cf + de}{df} = \frac{adf + b(cf + de)}{bdf}$, de las ecuaciones anteriores se concluye que
$\left(\frac{a}{b} + \frac{c}{d}\right) + \frac{e}{f} = \frac{a}{b} + \left(\frac{c}{d} + \frac{e}{f}\right)$.
La existencia de 0 se obtiene de $\frac{0}{1} + \frac{a}{b} = \frac{0 \bullet b + a \bullet 1}{b \bullet 1} = \frac{a}{b}$. El inverso aditivo de $\frac{a}{b}$ es $\frac{-a}{b}$ y la conmutatividad se obtiene de la conmutatividad en $\mathbb{Z}$.

ii) Está claro que $\bullet$ es asociativa, es decir $\left(\frac{a}{b}\bullet\frac{c}{d}\right)\bullet\left(\frac{e}{f}\right)=\frac{a}{b}\bullet\left(\frac{c}{d}\bullet\frac{e}{f}\right)$. También se tiene que $\frac{a}{b}\bullet\frac{1}{1}=\frac{a}{b}\bullet\frac{c}{c}=\frac{a}{b}\ \forall\ c\neq 0$, de esta forma $\frac{1}{1}$ es una identidad. Si $\frac{a}{b}\neq 0$ entonces $[(a,b)]\neq[(0,1)]$ ó $a\neq 0$, de aquí, el elemento $[(b,a)]=\frac{b}{a}\in\mathbb{Q}$, y $\frac{b}{a}\bullet\frac{a}{b}=\frac{1}{1}$, esto se obtiene de $ba-ab=0$.
También se tiene que $\frac{a}{b}\bullet\frac{c}{d}=\frac{c}{d}\bullet\frac{a}{b}$, ya que $acdb-bdca=0$. De aquí se concluye que $(\mathbb{Q}\backslash\{0\},\bullet,1)$ es un grupo abeliano.
iii) Distributividad: $\frac{a}{b}\bullet\left(\frac{c}{d}+\frac{e}{f}\right)=\frac{a}{b}\bullet\frac{cf+de}{df}=\frac{a(cf+de)b}{bdfb}=$
$\frac{acbf+bdae}{(bd)bf}$.
Por otro lado $\frac{ac}{bd}+\frac{ae}{bf}=\frac{acbf+bdae}{(bd)(bf)}$ y de estas ecuaciones la igualdad
$\frac{a}{b}\bullet\left(\frac{c}{d}+\frac{e}{f}\right)=\frac{ac}{bd}+\frac{ae}{bf}$ se obtiene. ■

0.6.1. Orden en el Campo de los Números Racionales

Se puede decir que, tener un campo ordenado, es la mínima condición para empezar con cálculo o más general, análisis. En esta sección se define el orden en el campo de los números racionales, y se empieza la construcción del único campo que es arquimediano, ordenado y completo: **los números reales**.

Antes de empezar el trabajo de construir el sistema de los números reales se presentan algunas consideraciones sobre los dominios enteros ordenados.

Definición. *Sea D un dominio entero. Un subconjunto no vacío P en D es llamado un conjunto de elementos positivos si*

i) P es cerrado bajo adición y multiplicación.

ii) Dado $a\in D$, exactamente una de las siguientes condiciones se cumple: $a\in P$, $a=0$ ó $-a\in P$ (tricotomía).

Si P es un conjunto de elementos positivos en D, $-P=\{-a:a\in P\}$ y $D=\{0\}\cup P\cup(-P)$. Por ii), es claro que la unión anterior es disjunta.

Si D tiene un conjunto de elementos positivos P, se dice que D es ordenado por P. El conjunto $P\cup\{0\}$ es llamado el conjunto de elementos no negativos en D.

Observación 29. *Si D es un dominio entero ordenado, el conjunto de elementos no negativos induce un orden parcial como se muestra a continuación:*
Dados $a,b\in D$, $a\leq b$ si $b-a\in P\cup\{0\}$.

Primeramente, note que el conjunto de elementos no negativos en D es cerrado bajo adición y multiplicación.

i) Claramente $a \leq a$, $\forall\, a$.

ii) Si $a \leq b$ & $b \leq c$, entonces $b-a$, $c-b \in P \cup \{0\}$, de esta manera $(c-b)+(b-a) = c-a \in P \cup \{0\}$ por lo tanto $a \leq c$.

iii) Si $a \leq b$ & $b \leq a$ entonces, $b-a, a-b \in P \cup \{0\}$ por lo tanto $a = b$.

Se tiene que el orden en D inducido por los elementos no negativos satisface la propiedad de la tricotomía. Si D es un campo con un conjunto de elementos positivos se dirá que D es un campo ordenado.

Recuerde que un número racional x es una clase de equivalencia $x = [(a,b)]$ con $b \neq 0$. Sea $\mathbb{Q}^+ = \{x \in \mathbb{Q} : ab >_{\mathbb{Z}} 0\}$.
Supongamos $[(a,b)] = [(c,d)]$, entonces $ab >_{\mathbb{Z}} 0 \iff cd >_{\mathbb{Z}} 0$.
En efecto, $[(a,b)] = [(c,d)] \iff ad - bc = 0$ ó $ad = bc$, entonces

$$adbc = b^2c^2 \tag{11}$$

Si $ad >_{\mathbb{Z}} 0$, entonces $ad \neq 0$, de esto $bc \neq 0$, y de (11) se tiene $ad >_{\mathbb{Z}} 0 \iff bc >_{\mathbb{Z}} 0$.

Teorema 36. $\mathbb{Q}^+$ *es un conjunto de elementos positivos para* $\mathbb{Q}$.

Demostración. i) Se debe probar que $\mathbb{Q}^+$ es cerrado bajo adición y multiplicación pues claramemte es no vacío. Sean $x, y \in \mathbb{Q}^+$ digamos $x = \dfrac{a}{b}$, $y = \dfrac{c}{d}$, entonces $x+y = \dfrac{ad+bc}{bd} >_{\mathbb{Z}} 0 \iff (ad+bc)bd = abd^2 + cdb^2 >_{\mathbb{Z}} 0$, en efecto esto es verdadero.
Por otro lado, $x \bullet y = \dfrac{ac}{bd}$, por lo tanto $x \bullet y >_{\mathbb{Z}} 0 \iff acbd >_{\mathbb{Z}} 0 \iff (ad)(bc) >_{\mathbb{Z}} 0$. Como $ad, bc >_{\mathbb{Z}} 0$, entonces $x \bullet y >_{\mathbb{Z}} 0$.
ii) Sea $x \in \mathbb{Q}\backslash\{0\}$, entonces $x = \dfrac{a}{b}$ con $a \neq 0$, de esta manera $ba >_{\mathbb{Z}} 0$ ó $ba <_{\mathbb{Z}} 0$, por tricotomía en $\mathbb{Z}$. Si $ba >_{\mathbb{Z}} 0$, entonces $\dfrac{a}{b} \in \mathbb{Q}^+$. Si $ba <_{\mathbb{Z}} 0$, entonces $-ab >_{\mathbb{Z}} 0$ por lo tanto $\dfrac{-a}{b} = -\dfrac{a}{b} \in \mathbb{Q}^+$. ■

Del teorema anterior, se tiene que $\mathbb{Q}$ es un campo ordenado, el conjunto de elementos no negativos en $\mathbb{Q}$ induce un orden parcial en $\mathbb{Q}$ que satisface la propiedad de la tricotomía. Si se considera el orden en $\mathbb{Q}$ inducido por $\mathbb{Q}^+$ entonces se tiene, como se muestra en el siguiente resultado, que $\mathbb{Z} \hookrightarrow \mathbb{Q}$ (inclusión) y la inclusión conserva, tanto operaciones como el orden, más precisamente:

Teorema 37. *Sea* $\varphi : \mathbb{Z} \to \mathbb{Q}$ *dado por* $\varphi(a) = [(a,1)] = \dfrac{a}{1}$. *Entonces* φ *satisface*

i) $\varphi(a+b) = \varphi(a) + \varphi(b),\ \forall\ a, b \in \mathbb{Z}$.

ii) $\varphi(a \bullet b) = \varphi(a) \bullet \varphi(b),\ \forall\ a, b \in \mathbb{Z}$.

iii) $\varphi(a) > 0 \iff a >_{\mathbb{Z}} 0$.

Demostración. i) Claramente $[(a+b,1)] = [(a,1)] + [(b,1)]$, así $\varphi(a+b) = \varphi(a) + \varphi(b)$.
ii) $[(a,1)][(b,1)] = [(ab,1)]$, entonces $\varphi(a \bullet b) = \varphi(a) \bullet \varphi(b)$.
iii) $[(a,1)] > 0 \iff a \bullet 1 = a >_{\mathbb{Z}} 0$. ■

Definición. *Sea* F *un campo, se dice que* F *tiene característica* $p > 0$, *si* p *es el mínimo entero positivo, tal que* $p \bullet x = \underbrace{x + \cdots + x}_{\text{p veces}} = 0\ \forall\ x \in F$. *Si* $px \neq 0\ \forall\ p > 0$, *entonces se dice que* F *tiene característica cero.*

Ejercicios.

1. Si F es un campo, entonces F tiene característica cero o primo.
2. Suponga que F es un campo ordenado, entonces F tiene característica cero.
3. Si F & K son campos, una función $\varphi : K \to F$ se llama un homomorfismo si $\varphi(a+b) = \varphi(a) + \varphi(b)$ y $\varphi(a \bullet b) = \varphi(a) \bullet \varphi(b)\ \forall\ a, b \in K$. Muestre que φ es cero o inyectiva. Si K y F son campos ordenados y φ no es cero, entonces φ conserva el orden $\iff$ φ transforma elementos positivos en elementos positivos.

Suponga que F es un campo ordenado, entonces la función $\mathbb{Z} \xrightarrow{f} F$ definida por $f(n) = n \bullet 1_F$ es un homomorfismo inyectivo; la inyectividad se obtiene de 2, ejercicio anterior, esta función se puede extender a $\mathbb{Q}$ en una forma natural, por lo tanto F contiene un subcampo isomorformo a $\mathbb{Q}$.

Anteriormente se vió que $\mathbb{Q}$ es un campo ordenado, el orden es inducido por $\mathbb{Q}^+$; con el orden en $\mathbb{Q}$ se definirá uno de los conceptos básicos en cálculo: el valor absoluto de un número racional. Puesto que se trabajará en un contexto más general, se definirá el valor absoluto en un campo ordenado.

Definición. *Si* F *es un campo ordenado, el valor absoluto en* F, *se define, como una función* $|\ | : F \to F$ *dada por* $|x| := \max\{x, -x\}$.

Teorema 38. *Si* F *es un campo ordenado, entonces:*

i) $0 \leq |-x| = |x|,\ \forall\ x \in F$.

ii) $x \leq |x|\ \&\ -x \leq |x|,\ \forall\ x \in F$.

iii) $|x| = 0 \iff x = 0$.

iv) $|x + y| \leq |x| + |y|,\ \forall\, x, y \in F$.

v) $|xy| = |x||y|$ & $|x| - |y| \leq ||x| - |y|| \leq |x - y|,\ \forall\, x, y \in F$.

Demostración. i) De la definición de valor absoluto se tiene $|x| = |-x|$. Si $x \neq 0$, entonces $x \in P$ ó $-x \in P$, con P el conjunto de elementos positivos en F. Si $x \in P$, se tiene $x > 0 > -x$ por lo que $|x| = x \geq 0$. Si $-x \in P$ uno obtiene $-x \geq 0 \geq x$ por lo tanto $|x| = -x \geq 0$.
ii) Si $x \in P$, entonces $|x| = x$. Si $x \notin P$, se obtiene $-x \in P$, así que $|x| = -x \geq 0 \geq x$; de cualquier forma, $|x| \geq x$. También $-x \leq |x|$.
iii) Si $|x| = \max\{x, -x\} = 0$ y $x \neq 0$, entonces $|x| \in P$ $\Rightarrow\Leftarrow$.
iv) Si $x + y \in P$ entonces $|x + y| = x + y \leq |x| + |y|$ de ii), si $(x + y) \notin P$ obtenemos $|x+y| = -(x+y) = -x+(-y) \leq |x|+|y|$ también de ii). Finalmente, si $x+y = 0$ entonces $|x + y| = 0 \leq |x| + |y|$.
v) Si $xy \in P$, entonces $|xy| = xy = (-x)(-y)$, de esta manera $|xy| = |x||y|$. Se tiene $|x| = |x + y - y| \leq |x - y| + |y|$, así $|x| - |y| \leq |x - y|$; análogamente $|y| = |y - x + x| \leq |y-x|+|x| \Rightarrow |y|-|x| \leq |y-x| = |x-y|$, por lo que $\max\{|x|-|y|, |y|-|x|\} =| |x|-|y| |\leq |x-y|$. $|x| =| |x| - |y| + |y| |\leq| |x| - |y| | + |y|$ por lo tanto $|x| - |y| \leq| |x| - |y| |$. De aquí, se tiene el resultado deseado. ■

0.6.2. Campos Ordenados Arquimedianos

En física, es bien conocido el postulado de Arquímedes que dice lo siguiente:

> *Dame una palanca lo suficientemente larga y un punto de apoyo y moveré al mundo.*

Este postulado es conocido como el *principio arquimediano* para los números reales, por supuesto, debe ser traducido a un lenguaje preciso; el postulado exacto es:

Definición (Principio Arquimediano). *Sea F un campo ordenado. Si $<$ denota el orden en F, $<$ se llama arquimediano si para cada dos $a, b \in F$ con $b > 0$, existe $n \in \mathbb{N}$ tal que $a \leq nb$.*

Definición *Sea F un campo ordenado por $<$. Se dice que $<$ es denso en F, si para todos $a, b \in F$ con $a < b$, existe $c \in F$ tal que $a < c < b$.*

Observación 30. *Si $(F, <)$ es un campo ordenado, entonces $<$ es denso.*

Demostración. Sea $a < b$, como F es ordenado, entonces $1_F + 1_F = 2 > 0$, de esta manera $a + a < a + b < b + b$, por lo tanto $a < \dfrac{a+b}{2} < b$. ■

Corolario. *El orden en* $\mathbb{Q}$ *es denso.*

Teorema 39. $(\mathbb{Q}, <)$ *es un campo arquimediano.*

Demostración. Sean $a, b \in \mathbb{Q}$ con $b > 0$. Si $a \leq b$ hemos terminado, por lo tanto se puede suponer que $0 < b < a$, entonces $b = \frac{m}{n}, a = \frac{p}{q}$ con m, n, p, q enteros positivos, de ésto, $a = \frac{p}{q} \leq p \leq pm = pn\frac{m}{n} = pnb$. ■

0.7. El Sistema de los Números reales

En esta sección se presenta la construcción del sistema de los números reales, ésta se inicia en un contexto más general, es decir, varios de los conceptos y términos necesarios se establecen en forma general en un campo ordenado, así lo haremos, y particularizando a $\mathbb{Q}$, se obtiene el campo de los números reales denotado por $\mathbb{R}$.

0.7.1. Sucesiones en un Campo Ordenado

Por una sucesión $\{a_n\}$ en un conjunto X se entiende una función $f : \mathbb{N} \to X$ con $f(n) := a_n$. Recordemos que dada una sucesión $\{a_n\}$ se define el concepto de subsucesión de $\{a_n\}$ como la función $f \circ g : \mathbb{N} \to X$ con $g : \mathbb{N} \to \mathbb{N}$ creciente. En notación, si $g(k) = n_k$ entonces la subsucesión $f \circ g$ se representa por $\{a_{n_k}\}$.

Si F es un campo ordenado y $\{a_n\} \subseteq F$ es una sucesión, se dice que $\{a_n\}$ es acotada, si existe $a \in F$ tal que $|a_n| \leq a \ \forall \ n \in \mathbb{N}$. $\{a_n\}$ se llama una sucesión de Cauchy, si $\forall \ e \in F, e > 0$ existe $N \in \mathbb{N}$ tal que $|a_n - a_m| < e, \quad \forall \ n, m \geq N$. Una sucesión $\{a_n\}$ se llama creciente (decreciente) si $a_n \leq a_{n+1}$ $(a_{n+1} \leq a_n)$ para todo n. Una sucesión es monótona, si es creciente o decreciente. Una sucesión $\{a_n\}$ tiene un límite $a \in F$, si para cada $e > 0$ en F existe $N \in \mathbb{N}$ tal que $|a_n - a| < e$ para todo $n \geq N$. Si la sucesión tiene límite se escribe $\lim\limits_{n\to\infty} a_n = a$.

Ejercicio. Si $\{a_n\}$ es una sucesión de Cauchy en un campo ordenado F, entonces $\{a_n\}$ es acotada.

Dadas dos sucesiones $\{a_n\}$ y $\{b_n\}$ en un campo F, se define la suma y el producto en la forma usual, i.e.

i) $\{a_n\} + \{b_n\} := \{a_n + b_n\}$.

ii) $\{a_n\} \bullet \{b_n\} := \{a_n b_n\}$.

Teorema 40. *Sea* F *un campo ordenado. Si* $\{a_n\}$ *y* $\{b_n\}$ *son sucesiones de Cauchy, entonces también lo son* $\{a_n + b_n\}$ *y* $\{a_n b_n\}$.

Demostración. Sea $e > 0$, entonces $\frac{e}{2} > 0$. Puesto que $\{a_n\}$ y $\{b_n\}$ son sucesiones de Cauchy existen $N_1, N_2 \in \mathbb{N}$ tales que $|a_n - a_m| < \frac{e}{2}$, $\forall\, n, m \geq N_1$ & $|b_n - b_m| < \frac{e}{2}$ $\forall\, n, m \geq N_2$. Si $N = \max\{N_1, N_2\}$ entonces $|(a_n + b_n) - (a_m + b_m)| \leq |a_n - a_m| + |b_n - b_m| < e$ $\forall\, n, m \geq N$. Se tiene $|a_n b_n - a_m b_m| = |a_n b_n - a_m b_m - a_n b_m + a_n b_m| = |a_n(b_n - b_m) + b_m(a_n - a_m)| \leq |a_n||b_n - b_m| + |b_m||a_n - a_m|$. Por el ejercicio anterior se tiene que $\{a_n\}$ y $\{b_n\}$ son acotadas, entonces existe $M \in F$ tal que $|a_n|, |b_n| < M$ $\forall\, n$, por lo tanto $|a_n b_n - a_m b_m| \leq M(|b_n - b_m| + |a_n - a_m|)$. Puesto que $\{a_n\}$ y $\{b_n\}$ son sucesiones de Cauchy, entonces existe $N \in \mathbb{N}$ tal que $|b_n - b_m| < \frac{\varepsilon}{2(M+1)}$ y $|a_n - a_m| < \frac{\varepsilon}{2(M+1)}$, por lo tanto $|a_n b_n - a_m b_m| \leq M(\frac{\varepsilon}{2(M+1)} + \frac{\varepsilon}{2(M+1)}) = \frac{M\varepsilon}{M+1} < \varepsilon$. ■

Ejercicio. Si $\{a_n\}$ es una sucesión en un campo ordenado F, entonces $\{a_n\}$ tiene a lo más un límite.

Observación 31. *Si $\{a_n\}$ tiene un límite, entonces $\{a_n\}$ es una sucesión de Cauchy.*

Demostración. Dado $e > 0$ existe N tal que $|a_n - a| < \frac{e}{2}$, entonces $|a_n - a_m + a - a| \leq |a_n - a| + |a_m - a| < e$ $\forall\, n, m \geq N$. ■

El recíproco de la observación anterior no es verdadero, en general, este hecho motiva la construcción del sistema de los números reales pues hay sucesiones de Cauchy de racionales que no tienen límite en $\mathbb{Q}$.

Ejercicios.

1. Si $\{a_n\}$ es una sucesión convergente en F que satisface $|a_n| \leq b$ $\forall\, n$ entonces $\lim_{n\to\infty} |a_n| = |a| \leq b$, donde $a = \lim_{n\to\infty} a_n$.
2. Si $\lim_{n\to\infty} a_n = a$ y $\lim_{n\to\infty} b_n = b$, entonces $\lim_{n\to\infty} (a_n + b_n) = a + b$, $\lim_{n\to\infty} (a_n b_n) = ab$.
3. Si $\lim_{n\to\infty} a_n = a \neq 0$, entonces $\lim_{n\to\infty} \frac{1}{a_n} = \frac{1}{a}$.

Teorema 41. *Sea F un campo ordenado, $\{a_n\}$ es una sucesión de Cauchy, tal que $\lim_{n\to\infty} a_n \neq 0$, entonces existe una sucesión de Cauchy $\{b_n\}$ tal que $\lim_{n\to\infty} (a_n b_n) = 1$.*

Demostración. Como $\lim_{n\to\infty} a_n \neq 0$, entonces existe $e_1 > 0$ tal que $\forall\, n \in \mathbb{N}$ existe $k \geq n$ con $|a_k| \geq e_1$. También se tiene que $\{a_n\}$ es una sucesión de Cauchy, por lo tanto existe $N_1 \in \mathbb{N}$ tal que $|a_m - a_n| < \frac{e_1}{2}$ $\forall\, m, n \geq N_1$. Sea $k > N_1$ entonces $|a_n| = |a_k - a_k + a_n| \geq |a_k| - |a_k - a_n| > e_1 - \frac{e_1}{2} = \frac{e_1}{2}$ $\forall\, n \geq N_1$, es decir $a_n \neq 0$ $\forall\, n \geq N_1$.

Definamos $b_n = \begin{cases} 1 & \text{Si } n < N_1 \\ \dfrac{1}{a_n} & \text{Si } n \geq N_1 \end{cases}$

$\{b_n\}$ es una sucesión de Cauchy, en efecto, si $e > 0$ entonces existe N_2 tal que $|a_n - a_m| < \frac{e_1^2}{4} e \ \forall\ n, m \geq N_2$, así $|b_n - b_m| = \dfrac{|a_m - a_n|}{|a_m||a_n|} < \dfrac{e_1^2}{4} \bullet \dfrac{4e}{e_1^2} = e \ \ \forall\ n, m \geq \max\{N_1, N_2\}$. También $a_n b_n = 1 \ \forall\ n \geq N_1$, de lo cual $\lim\limits_{n\to\infty} a_n b_n = 1$. ■

Sea $R_F = \{\{a_n\} : \{a_n\}$ una sucesión de Cauchy en $F\}$, con F un campo ordenado. Del Teorema 40 se tiene que $(R_F, +, \bullet, \{0\}, \{1\})$ es un anillo conmutativo. Definamos en R_F la relación siguiente: $\{a_n\} \sim \{b_n\}$ si $\lim\limits_{n\to\infty} (a_n - b_n) = 0$.

Observación 32. *$\sim$ es una relación de equivalencia.*

i) Es claro que $\{a_n\} \sim \{a_n\}$, ya que $\lim\limits_{n\to\infty} (a_n - a_n) = 0$.

ii) Si $\{a_n\} \sim \{b_n\}$ entonces $\lim\limits_{n\to\infty} (a_n - b_n) = -\lim\limits_{n\to\infty} (b_n - a_n) = 0$, por lo tanto $\{b_n\} \sim \{a_n\}$.

iii) Si $\{a_n\} \sim \{b_n\}$ y $\{b_n\} \sim \{c_n\}$ entonces $\lim\limits_{n\to\infty} (a_n - b_n) = 0$ & $\lim\limits_{n\to\infty} (b_n - c_n) = 0$, por lo tanto $\lim\limits_{n\to\infty} (a_n - b_n + b_n - c_n) = \lim\limits_{n\to\infty} (a_n - c_n) = 0$.

Dado un elemento $\{a_n\} \in R_F$ la clase de equivalencia a la cual $\{a_n\}$ pertenece se denota por $[\{a_n\}]$.

Para definir al sistema de los números reales tomamos $F = \mathbb{Q}$, más precisamente.

Definición. *El conjunto de los números reales denotado por $\mathbb{R}$ se define como sigue* $\mathbb{R} := \frac{R_{\mathbb{Q}}}{\sim} = \{[\{a_n\}] : \{a_n\}$ *es una sucesión de Cauchy en* $\mathbb{Q}\}$.

0.7.2. Adición y Multiplicación en $\mathbb{R}$

Afirmación. *Si $\{a_n\} \sim \{a'_n\}$ y $\{b_n\} \sim \{b'_n\}$ entonces $\{a_n + b_n\} \sim \{b'_n + a'_n\}$ y $\{a_n b_n\} \sim \{a'_n b'_n\}$. Se tiene $\lim\limits_{n\to\infty} (a_n - a'_n) = 0$ y $\lim\limits_{n\to\infty} (b_n - b'_n) = 0$, de esta manera $\lim\limits_{n\to\infty} (a_n - a'_n + (b_n - b'_n)) = \lim\limits_{n\to\infty} ((a_n + b_n) - (a'_n + b'_n)) = 0$, demostrando $\{a_n + b_n\} \sim \{a'_n + b'_n\}$.*
Se tiene $|a_n b_n - a'_n b'_n| = |(a_n - a'_n)b_n + (b_n - b'_n)a'_n| \leq |a_n - a'_n||b_n| + |b_n - b'_n||a'_n|$. Puesto que $\{b_n\}$ y $\{a'_n\}$ son acotadas y $\lim\limits_{n\to\infty} |a_n - a'_n| = \lim\limits_{n\to\infty} |b_n - b'_n| = 0$ entonces $\lim\limits_{n\to\infty} (a_n b_n - a'_n b'_n) = 0$.

De la afirmación anterior, se tiene que la adición y multiplicación en $\mathbb{R}$ definidas anteriormente no dependen de los representantes.

i) $[\{a_n\}] + [\{b_n\}] := [\{a_n + b_n\}]$.

ii) $[\{a_n\}] \bullet [\{b_n\}] := [\{a_n b_n\}]$.

Con estas operaciones, es fácil verificar que $[\{0\}]$ & $[\{1\}]$ son identidades para la adición y multiplicación en $\mathbb{R}$.

Teorema 42. $(\mathbb{R}, +, \bullet, [\{0\}], [\{1\}])$ *es un campo.*

Demostración. Trabaje los detalles, use los teoremas 40 y 41.

Con lo hecho anteriormente se tiene que $\mathbb{R}$ es un campo, propiedad importante. Lo que haremos en lo sucesivo es mostrar que $\mathbb{R}$ es un campo ordenado, arquimediano y completo. Dos de estos conceptos han sido enunciados, el tercero es el siguiente

Definición. *Suponga que F es un campo ordenado, F se dice completo, si cada sucesión de Cauchy en F converge en F.*

El orden en $\mathbb{R}$ se dará en términos de elementos positivos, por lo cual es necesario precisar estas ideas. Dado que los elementos de $\mathbb{R}$ son clases de equivalencia de sucesiones de Cauchy la siguiente definición es necesaria.

Definición. *Sea F un campo ordenado. Una sucesión $\{a_n\}$ en F se dice positiva, si existen $e > 0$ & $k \in \mathbb{N}$ con $a_n > e \ \ \forall\, n \geq k$.*

Teorema 43. *Sea F un campo ordenado, $\{a_n\}$ una sucesión de Cauchy, entonces exactamente uno de los siguientes enuciados es verdadero.*

a) $\lim\limits_{n\to\infty} a_n = 0$.

b) $\{a_n\}$ *es positiva.*

c) $\{-a_n\}$ *es positiva.*

Demostración. Primero se muestra que una de las condiciones se cumple. Si $\lim\limits_{n\to\infty} a_n \neq 0$, entonces existe $e > 0$ tal que $\forall\, m \in \mathbb{N}$ existe $k \geq m$ con $|a_k| > e$. Para $\dfrac{e}{2}$ existe $m_1 \in \mathbb{N}$ tal que $|a_n - a_m| < \dfrac{e}{2} \ \ \forall\, n, m \geq m_1$.
De aquí, para m_1 existe $k \geq m_1$, tal que $|a_k| > e$, entonces si $n \geq m_1$ se tiene $|a_n| = |a_n - a_k + a_k| \geq |a_k| - |a_n - a_k| > e - \dfrac{e}{2} = \dfrac{e}{2}$. De esta desigualdad y de la hipótesis sobre $\{a_n\}$ se tiene que $a_n \geq \dfrac{e}{2}$ ó $-a_n \geq \dfrac{e}{2} \ \ \forall\, n \geq m_1$, i.e. $\{a_n\}$ ó $\{-a_n\}$ es positiva. Se verifica directamente que solamente una de las condiciones anteriores se cumple. ■

Observación 33. *Suponga que $\{a_n\}$ es una sucesión de Cauchy positiva, entonces cada sucesión de Cauchy $\{a'_n\} \in [\{a_n\}]$ es positiva.*

Demostración. Puesto que $\{a_n\}$ es positiva, entonces existen $e \in F, e > 0$ y $k \in \mathbb{N}$ con $a_n \geq e \ \ \forall\, n \geq k$. La hipótesis $\{a'_n\} \in [\{a_n\}]$ implica $|a'_n - a_n| < \dfrac{e}{2} \ \ \forall\, n \geq k_1$, o equivalentemente $-\dfrac{e}{2} < a'_n - a_n < \dfrac{e}{2}$, por lo tanto $\dfrac{e}{2} = e - \dfrac{e}{2} < a_n - \dfrac{e}{2} < a'_n$ i.e. $\{a'_n\}$ es positiva. ■

Definición. *Dado $x = [\{a_n\}] \in \mathbb{R}$, se dice que x es positivo, si $\{a_n\}$ es positiva, y se escribe $x >_{\boldsymbol{\mathcal{R}}} 0$. Se denota por $\mathbb{R}^+ = \{x \in \mathbb{R} : x >_{\boldsymbol{\mathcal{R}}} 0\}$.*

Teorema 44. *$\mathbb{R}^+$ es un conjunto de elementos positivos para $\mathbb{R}$.*

Demostración. Es claro que $\mathbb{R}^+$ es no vacío, puesto que $\{[1]\} = 1 \in \mathbb{R}^+$.

i) $\mathbb{R}^+$ es cerrado bajo adición y multiplicación.
Si $x, y \in \mathbb{R}^+$ entonces existen $\{a_n\} \in x$ y $\{b_n\} \in y$ con $\{a_n\}$ y $\{b_n\}$ positivas, por lo tanto $\{a_n + b_n\}$ es positiva. Análogamente se muestra que $\{a_n b_n\}$ es positiva.

ii) Dado $x \in \mathbb{R}$ se debe mostrar que exactamente uno de $x = 0, x > 0, -x > 0$ se cumple. Esto sigue del Teorema 43 y la Observación 33. ■

Dados $x, y \in \mathbb{R}$ se dice que $x \leq y$ Si $y - x \in \mathbb{R}^+ \cup \{0\}$.
Así como se hizo para $\mathbb{N}$ y $\mathbb{Z}$, se demostrará que $\mathbb{Q}$ está inyectado en $\mathbb{R}$ y la inyección conserva las operaciones y el orden, más precisamente.

Teorema 45. *Sea $\varphi : \mathbb{Q} \to \mathbb{R}$ la función dada por $\varphi(x) = [\{x\}]$. Entonces φ satisface:*

i) $\varphi(x + y) = \varphi(x) + \varphi(y)$,

ii) $\varphi(x \bullet y) = \varphi(x) \bullet \varphi(y)$,

iii) $\varphi(x) >_{\boldsymbol{\mathcal{R}}} 0 \iff x >_{\boldsymbol{\mathcal{Q}}} 0$.

Demostración. i) y ii) son claros.
iii) $[\{x\}] >_{\boldsymbol{\mathcal{R}}} 0 \iff \{x\} > 0 \iff x >_{\boldsymbol{\mathcal{Q}}} 0$, entonces $\varphi(x) >_{\boldsymbol{\mathcal{R}}} 0 \iff x >_{\boldsymbol{\mathcal{R}}} 0$. ■

Con lo anterior, se mostró que $\mathbb{R}$ es un campo ordenado que contiene un subcampo isomorfo a $\mathbb{Q}$, una de las siguientes metas es mostrar que $\mathbb{R}$ es completo y arquimediano, y cualquier otro campo F que es ordernado, arquimediano y completo es isomorfo a $\mathbb{R}$.

De ahora en adelante se identificará a $\mathbb{Q}$ con $\varphi(\mathbb{Q})$ y el elemento $x \in \mathbb{Q}$ con $[\{x\}]$.

Se ha visto que $\mathbb{R}$ es un campo ordenado, por lo tanto $\mathbb{R}$ tiene un valor absoluto, puede verificarse que el valor absoluto en $\mathbb{R}$ satisface $|x|_{\boldsymbol{\mathcal{R}}} = [\{|a_n|_{\boldsymbol{\mathcal{Q}}}\}]$ donde $x = [\{a_n\}]$. De esta observación es fácil verificar que cuando se identifica una sucesión $\{a_n\} \subseteq \mathbb{Q}$ con una sucesión en $\mathbb{R}$, $\{a_n\}$ es una sucesión de Cauchy en $\mathbb{Q} \iff \{a_n\}$ es una sucesión de Cauchy en $\mathbb{R}$.

Observación 34. *Si $\varepsilon \in \mathbb{R}$ satisface $0 < \varepsilon$, entonces existe $e \in \mathbb{Q}$ tal que $0 < e < \varepsilon$.*

Demostración. Sea $\varepsilon = [\{a_n\}]$ con $\{a_n\}$ positiva, entonces existen $e_1 \in \mathbb{Q}, e_1 > 0$ y $n_1 \in \mathbb{N}$ tales que $a_n \geq e > 0 \ \forall\, n \geq n_1$. Por la densidad del orden en $\mathbb{Q}$, $\exists\, e \in \mathbb{Q}$ tal que $0 < e < e_1$, ahora el elemento $e = [\{e\}]$ satisface $0 < e < \varepsilon$. ■

En el trayecto para demostrar que $\mathbb{R}$ es completo, se deberá demostrar que cualquier sucesión de Cauchy en $\mathbb{Q}$ converge en $\mathbb{R}$. Aquí se debe tener cuidado con el enunciado; se enfatiza que $\mathbb{Q}$ se identifica con su imagen en $\mathbb{R}$.

Teorema 46. *Si* $\{a_n\}$ *es una sucesión de Cauchy en* $\mathbb{Q}$ *y* $\{a_n\} \in \xi$ *es un número real, entonces* $\lim_{n\to\infty} a_n = \xi$ *(el límite se toma en* $\mathbb{R}$*).*

Demostración. Se debe mostrar que, dado $\varepsilon > 0$ en $\mathbb{R}$ existe $n_0 \in \mathbb{N}$ tal que $|a_n - \xi| < \varepsilon$ en $\mathbb{R}$ $\forall\, n \geq n_0$.

Dado $\varepsilon > 0$ en $\mathbb{R}$, de la observación anterior, existe $e \in \mathbb{Q}$ tal que $0 < e < \varepsilon$. La hipótesis en $\{a_n\}$ garantiza que existe $n_e \in \mathbb{N}$ tal que $|a_m - a_n| < \dfrac{e}{2}$ $\forall\, m, n \geq n_e$, de esta desigualdad se tiene $\dfrac{e}{2} < e - |a_n - a_m|$ $\forall\, n, m \geq n_e$. Para cada $n \geq n_e$ considere la sucesión $\{b_m^{(n)}\}$ definida por $b_m^{(n)} = e - |a_n - a_m|$.

Por construcción, $\{b_m^{(n)}\}$ es una sucesión positiva de Cauchy en $\mathbb{R}$ $\forall\, n \geq n_e$. De la definición de orden en $\mathbb{R}$ se tiene $[\{b_m^{(n)}\}] = [\{e - |a_n - a_m|\}] > 0\ \forall\, n \geq n_e$ o $e = [\{e\}] > [\{|a_n - a_m|\}]$. También se tiene que $|a_n - \xi| = |[\{a_n\}] - [\{a_m\}]| = [\{|a_n - a_m|\}]$, entonces $|a_n - \xi| < e < \varepsilon$ $\forall\, n \geq n_e$. ■

Corolario 1. *Si* $\xi \in \mathbb{R}$ *y* $\varepsilon > 0$ *en* $\mathbb{R}$*, existe* $a \in \mathbb{Q}$ *tal que* $|\xi - a| < \varepsilon$ *en* $\mathbb{R}$.

Demostración. Del teorema anterior, $\lim_{n\to\infty} a_n = \xi$ para cada $\{a_n\} \in \xi$, por lo tanto, dado $\varepsilon > 0$ en $\mathbb{R}$ existe $n_1 \in \mathbb{N}$ tal que $|\xi - a_n| < \varepsilon$ $\forall\, n \geq n_1$. Tome $a = a_{n_1}$ ■

Corolario 2. *Si* $\xi < \eta$ *en* $\mathbb{R}$*, entonces existe* $a \in \mathbb{Q}$ *tal que* $\xi < a < \eta$.

Demostración. Se tiene que el orden en $\mathbb{R}$ es denso, entonces existe $c \in \mathbb{R}$ tal que $\xi < c < \eta$. Sea $\varepsilon = \min\{c - \xi, \eta - c\}$, por el corolario anterior existe $a \in \mathbb{Q}$ tal que $|a - c| < \varepsilon$; esta desigualdad equivale a $-\varepsilon < a - c < \varepsilon$. De esto y la definición de ε uno tiene $\xi \leq c - \varepsilon < a < c + \varepsilon \leq \eta$. ■

Corolario 3. $\mathbb{R}$ *es arquimediano.*

Demostración. Sean $x, y \in \mathbb{R}$ con $y > 0$. Si $x \leq y$, no hay nada que probar entonces se puede suponer que $0 < y < x$, de aquí $0 < y < x < x + y$. Se sabe que existen $a, b \in \mathbb{Q}$ tales que $0 < a < y < x < b < x + y$. Aplicando el principio arquimediano a $\mathbb{Q}$ se tiene $b \leq na$ para algún n. El resultado sigue, i.e. $ny \geq x$. ■

Teorema 47. $\mathbb{R}$ *es completo.*

Demostración. Se deberá mostrar que una sucesión de Cauchy en $\mathbb{R}$ converge en $\mathbb{R}$. Sea $\{\xi_n\}$ una sucesión de Cauchy en $\mathbb{R}$. Por el corolario 1, dados $\xi \in \mathbb{R}, \varepsilon > 0$ existe $a \in \mathbb{Q}$ tal que $|\xi - a| < \varepsilon$, en particular para $\varepsilon = \dfrac{1}{n}$ y $\xi = \xi_n$, existe $a_n \in \mathbb{Q}$ tal que $|\xi_n - a_n| < \dfrac{1}{n}$. De este procedimiento se tiene una sucesión $\{a_n\} \subseteq \mathbb{Q}$.

Afirmación. $\{a_n\}$ es una sucesión de Cauchy. Primeramente, note que la sucesión $\dfrac{1}{n} \to 0$ en $\mathbb{R}$, entonces dado $\varepsilon > 0$ en $\mathbb{R}$ existe $n_1 \in \mathbb{N}$ tal que $|\xi_n - a_n| < \dfrac{1}{n} < \dfrac{\varepsilon}{3}$ $\forall\, n \geq n_1$. Ahora, usando

la hipótesis sobre $\{\xi_n\}$, se tiene que existe $n_2 \in \mathbb{N}$ tal que $|\xi_n - \xi_m| < \frac{\varepsilon}{3}$ para todo $n, m \geq n_2$, de esta manera $|a_m - a_n| = |a_m - \xi_m + \xi_m - \xi_n + \xi_n - a_n| \leq |a_m - \xi_m| + |\xi_m - \xi_n| + |\xi_n - a_n| < \frac{\varepsilon}{3} + \frac{\varepsilon}{3} + \frac{\varepsilon}{3} = \varepsilon \ \ \forall\, n, m \geq \max\{n_1, n_2\}$.

Sea $\xi = [\{a_n\}]$, el siguiente paso es mostrar que $\lim_{n\to\infty} \xi_n = \xi$. Se ha probado, Teorema 46, que $\lim_{n\to\infty} a_n = \xi$, entonces existe $n_0 \in \mathbb{N}$ tal que $|a_n - \xi| < \frac{2}{3}\varepsilon \ \ \forall\ n \geq n_0$, así $|\xi_n - \xi| = |\xi_n - a_n + a_n - \xi| \leq |\xi_n - a_n| + |a_n - \xi| < \frac{\varepsilon}{3} + \frac{2}{3}\varepsilon \ \ \forall\, n \geq \max\{n_0, n_1\}$. ■

Se ha definido el concepto de orden denso en un campo ordenado, i.e. se dice que $<$ es denso, si $\forall\ a < b$ exite $c \in F$ tal que $a < c < b$. La siguiente definición precisa el concepto de densidad para subconjuntos de campos ordenados.

Definición. *Sea F un campo ordenado, $A \subseteq F$, A se dice denso en F, si para $x, y \in F$ tales que $x < y$, existe $a \in A$ con $x < a < y$.*

Observación 35. *Uno de los corolarios anteriores, prueba que $\mathbb{Q}$ es denso en $\mathbb{R}$, este es un caso especial de un resultado más general .*

Teorema 48. *Suponga que F es un campo ordenado. Entonces F es arquimediano $\iff$ $\mathbb{Q}_F$ es denso en F. Aquí $\mathbb{Q}_F$ es el subcampo de F isomorfo a $\mathbb{Q}$.*

Demostración. ($\Longrightarrow$ Suponga que $a < b$, entonces $0 < b - a$; como F es arquimediano, existe $n \in \mathbb{N}$ tal que $1 < n(b - a)$, lo que equivale a $0 < \frac{1}{n} < b - a$, de aquí se tiene $a < a + \frac{1}{n} < b$. Nuevamente, por el principio arquimediano existe $m \in \mathbb{N}$ tal que $b \leq \frac{m}{n}$. Sea m el elemento mínimo en $\mathbb{N}$ con esta condición, por lo tanto $\frac{m-1}{n} < b$.

De $a < a + \frac{1}{n} < b$ y $\frac{m-1}{n} < b$ se obtiene $a < \frac{m-1}{n} < b$, mostrando que $\mathbb{Q}_F$ es denso.

$\Longleftarrow$) Suponga ahora $0 < a < b$ en F, entonces existen $x, y \in \mathbb{Q}_F$ tales que $0 < x < a < b < y < b + a$. Puesto que $\mathbb{Q}_F$ es arquimediano, entonces existe $n \in \mathbb{N}$ tal que $nx \geq y$ por lo tanto $na \geq nx \geq y > b$. ■

Ejercicios.

1. Si F es un campo ordenado, y $a \in F\backslash\{0\}$ entonces $a^2 > 0$, en particular $1 > 0$.
2. Si F es un campo finito entonces, F no es un campo ordenado.
3. El campo de los números complejos no es ordenado.
4. Sea F un campo ordenado, F es arquimediano $\iff$ la sucesión $\left\{\frac{1}{n}\right\}$ converge a cero en F.

0.7.3. Unicidad del Sistema de los Números Reales

Ya se demostró la existencia del sistema de números reales, el cual es campo arquimediano, ordenado y completo. En esta última parte se demostrará que $\mathbb{R}$ es único, i.e., si F es cualquier otro campo arquimediano, ordenado y completo, entonces F es isomorfo a $\mathbb{R}$.

Antes de demostrar que $\mathbb{R}$ es isomorfo a cualquier campo ordenado, arquimediano y completo es necesario presentar algunos conceptos que están estrechamente ligados a los conceptos presentados en cálculo. Los conceptos de cota superior e inferior para conjuntos, están relacionados intrínsecamente con la propiedad de complitud de los reales.

Definición. *Sea F un campo ordenado, $A \subseteq F$.*

i) Se dice que A es acotado superiormente, si existe $M \in F$ tal que $a \leq M$ para todo $a \in A$. M se llama cota superior para A.

ii) Se dice que A es acotado inferiormente, si existe $m \in F$ tal que $m \leq a$ para todo $a \in A$. m se llama cota inferior para A.

iii) Se dice que A es acotado, si A tiene tanto una cota superior como inferior.

iv) Un elemento $a \in F$ se llama una cota superior mínima o supremo de A si

a) a es una cota superior para A, y

b) $a \leq u$ para toda cota superior u de A.

v) Un elemento $b \in F$ se llama una cota inferior máxima o ínfimo de A si

a) b es una cota inferior para A, y

b) $v \leq b$ para toda cota inferior v de A.

Observación 36. *Si $A \subseteq F$, F es un campo ordenado, entonces A tiene a lo más un supremo y un ínfimo.*

De Hecho si a & a' son supremos de A, entonces de la definición anterior iv b) se tiene que $a \leq a'$ & $a' \leq a$, de esta manera $a = a'$. Análogamente para ínfimos.

Si F es un campo ordenado, por un intervalo $I \subseteq F$ se entiende, uno de los siguientes conjuntos: $I = \{x \in F : a \leq x \leq b\} = [a, b]$, (intervalo cerrado); $I = \{x \in F : a < x < b\} =]a, b[$, (intervalo abierto); $I = \{x \in F : a \leq x < b\} = [a, b[$, (cerrado por la izquierda, abierto por la derecha); $I = \{x \in F : a < x \leq b\} =]a, b]$, (abierto por la izquierda, cerrado por la derecha). El elemento $b - a$ es llamado la longitud o volumen del intervalo.

Se necesita una definición más.

Definición. *Sea F un campo ordenado, $A, B \subseteq F$ no vacíos, tales que*

i) $A \cap B = \emptyset$.

ii) $A \cup B = F$.

iii) *Si* $a \in A$ *y* $b \in B$, *entonces* $a < b$.

La pareja (A, B) es llamada una **cortadura** de F. Una cortadura (A, B) se llama un "hoyo" si A no tiene un elemento máximo y B no tiene un elemento mínimo.

Si A es un subconjunto de un campo ordenado F, se dice que $p \in F$ es un punto de acumulación de A si $A \cap (]a, b[\backslash\{p\}) \neq \emptyset \quad \forall\ a, b \in F$ tales que $a < p < b$. Un punto $p \in A$ se dice punto aislado de A si existe un intervalo abierto $]a, b[$ que contiene a p tal que $A \cap]a, b[= \{p\}$. El conjunto A se dice abierto en F si para cada $a \in A$ existen $x, y \in F$ tales que $a \in]x, y[\subseteq A$. $B \subseteq F$ es cerrado, si B^c es abierto.

De cálculo se sabe que la complitud de los números reales es equivalente a otras propiedades, por ejemplo al principio de Bolzano-Weierstrass, principio de Cauchy, los cuales se precisarán a continuación.
Antes de presentar la formulación de los principales enunciados que satisfacen los campos isomorfos a $\mathbb{R}$ presentamos dos hechos que son de tipo general, se cumplen en un campo ordenado y serán usados en la demostración del siguiente teorema.

Hecho 1. *Sea* $\{a_n\}$ *una sucesión de Cauchy en* F. *Suponga que* $\{a_n\}$ *tiene una subsucesión* $\{a_{n_k}\}$ *con límite* a *en* F, *entonces* $\lim_{n\to\infty} a_n = a$.

Demostración. Sea $e > 0$ en F, como $\{a_n\}$ es una de sucesión de Cauchy, entonces existe $N_1 \in \mathbb{N}$ tal que $|a_n - a_m| < e$ para cada $n, m \geq N_1$. Si $\lim_{k\to\infty} a_{n_k} = a$ entonces existe $N_2 \in \mathbb{N}$ tal que $|a_{n_k} - a| < \dfrac{e}{2}$ para todo $k \geq N_2$, por lo tanto $|a_n - a| = |a_n - a_{n_k} + a_{n_k} - a| \leq |a_n - a_{n_k}| + |a_{n_k} - a| < e$ para toda $n \geq N_1, N_2$. Note que $n_k \geq k$ pues $n_1 < n_2 \cdots < n_k \cdots$. ■

Hecho 2. *Sea* $\{a_n\}$ *una sucesión en* F, *entonces* $\{a_n\}$ *contiene una subsucesión monótona.*

Demostración. Para $k \in \mathbb{N}$, a_k se llama un pico de $\{a_n\}$ si $a_k \geq a_n \quad \forall\ n \geq k$. Si $\{a_n\}$ no tiene picos, entonces para cada k existe $n_k > k$ tal que $a_{n_k} > a_k$, de aquí, se tiene $a_1 < a_{n_1} < a_{n_2} < \cdots < \cdots$ con $n_1 < n_2 < \cdots <$ y $\{a_{n_k}\}$ es la subsucesión deseada.
Suponga que $\{a_n\}$ tiene picos. Si para algún $k \in \mathbb{N}$ existen infinidad de índices k_j tales que $a_{k_j} = a_k \quad j = 1, \cdots, m, \cdots$ entonces $\{a_{k_j}\}$ es la subsucesión que se busca, por lo que se puede suponer que $\{a_n\}$ tiene un número finito de picos. Sea k tal que a_k es el último pico. Poniendo $m = k + 1$, entonces la sucesión $\{a_{m+i}\}$, $i = 1, 2 \ldots$, no tiene picos y estamos en el primer caso ya considerado. ■

Sea F un campo ordenado, consideremos los siguientes enunciados.

I. (Cauchy)

   a) F es arquimediano, y

   b) F es completo.

II. Todo subconjunto no vacío de F acotado superiormente, tiene un supremo en F.

III. (Dedekind) F no tiene hoyos.

IV. Todo subconjunto no vacío de F acotado inferiormente, tiene un ínfimo.

V. (Heine-Borel) Si X es subconjunto cerrado y acotado de F y $\mathcal{F}$ es una familia de intervalos abiertos cubriendo a X, entonces $\mathcal{F}$ tiene una subfamilia finita que también cubre a X.

VI. (Bolzano-Weierstrass) Todo subcojunto acotado e infinito de F tiene un punto de acumulación en F.

VII. a) F es arquimediano, y

b) Si $\{I_n\}$ es una familia de intervalos cerrados tal que $I_{n+1} \subset I_n$ entonces $\cap_{n\in\mathcal{N}} I_n \neq \emptyset$.

Teorema 49. *Sea F un campo ordenado, entonces los enunciados anteriores son equivalentes.*

Demostración. I $\Rightarrow$ II Sea A un subconjunto de F no vacío y acotado superiormente, entonces existe $x \in A$ & $b \in F$ tales que $a \leq b \ \forall\, a \in A$.
Dado $n \in \mathbb{N}$, por la propiedad arquimediana de F, existe $m \in \mathbb{N}$ tal que $b - x \leq \dfrac{m}{n}$, de esta manera, el conjunto $B_n = \{m \in \mathbb{N} : x + \dfrac{m}{n}$ es una cota superior de $A\} \neq \emptyset$. Sea m_n el elemento mínimo de B_n, de aquí $z_n = x + \dfrac{m_n}{n}$ es una cota superior para A, pero $z_n - \dfrac{1}{n} = x + \dfrac{m_n - 1}{n}$ no lo es. Sea $b_n = z_n - \dfrac{1}{n}$, entonces $\exists\ a \in A$ tal que $b_n \leq a$. Para otro entero $m \neq n$ y argumentando como antes, existe un mínimo entero k_m tal que $b - x \leq \dfrac{k_m}{m}$, de lo que se obtiene que $z_m = x + \dfrac{k_m}{m}$ es cota superior de A y $x + \dfrac{k_m - 1}{m}$ no lo es. Definiendo $b_m = z_m - \dfrac{1}{m}$ se tiene $b_m < a < z_n$ para algún $a \in A$, por lo tanto $b_m - b_n < z_n - (z_n - \dfrac{1}{n}) = \dfrac{1}{n}$ y $b_n - b_m < z_m - (z_m - \dfrac{1}{m}) = \dfrac{1}{m}$, así $|b_n - b_m| \leq max\{\dfrac{1}{n}, \dfrac{1}{m}\}$. Usando nuevamente la hipótesis arquimediana en F se concluye que $\{b_n\}$ es una sucesión de Cauchy, puesto que F es completo, entonces $\lim\limits_{n\to\infty} b_n = \omega$.
`Afirmación`. $\omega = \sup A$. ω es una cota superior para A, pues de otra forma $\exists\ x \in A$ tal que $0 < x - \omega$, entonces $\exists\ n \in \mathbb{N}$ tal que $b_n - \omega \leq |b_n - \omega| < \dfrac{x - \omega}{2}$ y $\dfrac{1}{n} < \dfrac{x - \omega}{2}$, así $z_n = b_n + \dfrac{1}{n} < (\omega + \dfrac{x - \omega}{2}) + \dfrac{x - \omega}{2} = x$, contradiciendo que z_n es una cota superior para A.
Si c es una cota superior para A y $c < \omega$ entonces para algún $n \in \mathbb{N}$, $\omega - b_n \leq |\omega - b_n| < \omega - c$ y de ésto $c < b_n$, pero b_n no es una cota superior para A, i.e. $c < b_n \leq x$ para algún $x \in A$ $\Rightarrow\Leftarrow$.

II $\Rightarrow$ III Sea (A, B) una cortadura en F, ya que A & B son no vacíos y todo elemento en b es una cota superior para A, entonces por hipótesis A tiene un supremo. Sea $a = \sup A \in F = A \cup B$. Si $a \in A$, entonces A tiene un elemento máximo, si $a \in B$ entonces B tiene un elemento mínimo, así, de cualquier forma (A, B) no es un hoyo.

III $\Rightarrow$ IV Sea B un subconjunto de F no vacío y acotado inferiormente. Sea $X = \{x \in F : x \leq b \ \forall\, b \in B\}$, $Y = F \backslash X$.

`Afirmación`. (X, Y) es una cortadura en F. Por hipótesis $X \neq \emptyset$, también Y es no vacío, puesto que $b + 1 \in Y$ para cada $b \in B$. También por construcción se tiene $F = X \cup Y$ & $X \cap Y = \emptyset$.
Dados $x \in X$, $y \in Y$ entonces $x < y$, pues de otra forma $y \leq x \leq b \ \forall\, b \in B$, por lo tanto $y \in X \Rightarrow\Leftarrow$. Por hipótesis F no tiene hoyos, por lo cual X tiene un elemento máximo, ó Y tiene un elemento mínimo.
Si $X \cap B \neq \emptyset$, entonces $X \cap B = \{x_0\}$ y $x_0 = \text{ínf } B = \max X$.
Si $X \cap B = \emptyset$, entonces $B \subseteq Y = X^c$, ahora, si Y tiene un elemento mínimo digamos y_0 entonces $y_0 \leq y \ \forall\ y \in Y$ en particular $y_0 \leq b \ \forall\ b \in B$, por lo tanto $y_0 \in X \Rightarrow\Leftarrow$. De esta manera, si $X \cap B = \emptyset$, Y no tiene elemento mínimo, entonces X tiene elemento máximo, y este es en el ínfimo de B.

IV $\Rightarrow$ V Primeramente se probará la siguiente afirmación. Sea $I = [a, b]$ un intervalo cerrado en F. Suponga que $\mathcal{F}$ es una familia de intervalos abiertos que cubre a I, entonces $\mathcal{F}$ contiene una subfamilia finita, que también cubre a I.
Sea $B = \{x \in I : [x, b]$ es cubierto por un número finito de elementos de $\mathcal{F}\}$. Claramente $b \in B$, es decir B es no vacío y por construcción a es una cota inferior para B, entonces la hipótesis garantiza la existencia de $x_0 = \text{ínf } B$.
$x_0 \in B$, en efecto, $x_0 \in I$ por lo que existe $\mathcal{U}_0 \in \mathcal{F}$ tal que $x_0 \in \mathcal{U}_0 =]c, d[$, de esto se tiene $c < x_0 < d$. Ya que $x_0 = \text{ínf } B$ y el orden en F es denso, existe $\omega \in F$ tal que $x_0 < \omega < d$, de esta manera $[\omega, b]$ es cubierto por $\mathcal{U}_1, \cdots, \mathcal{U}_n \in \mathcal{F}$, así $\{\mathcal{U}_0, \mathcal{U}_1, \cdots, \mathcal{U}_n\}$ cubre $[x_0, b]$, demostrando que $x_0 \in B$.
$x_0 = a$. Si $a < x_0$, entonces $a, c < x_0 < d$, otra vez por la densidad de $<$, existe z con $a, c, < z < x_0$; igual que antes $[z, b]$ es cubierto por $\{\mathcal{U}_0, \mathcal{U}_1, \cdots, \mathcal{U}_n\}$, por lo tanto $z \in B$, entonces $x_0 \leq z \Rightarrow\Leftarrow$. Probando la afirmación.
Ahora suponga que X es subconjunto cerrado y acotado de F el cual es cubierto por la familia $\mathcal{F}$ consistiendo de intervalos abiertos.
Ya que X es acotado, entonces $X \subseteq [a, b] = I$ para algún I; también se tiene que X es cerrado, entonces X^c es abierto, de esto se tiene que para todo $x \in I \setminus X$, existe un intervalo abierto J_x tal que $J_x \cap X = \emptyset$. Sea $\mathcal{F}_1 = \{J_x : x \in I \setminus X$ y $J_x \cap X = \emptyset\}$, entonces $\mathcal{F} \cup \mathcal{F}_1$ es una cubierta abierta de I, por la afirmación anterior, existe una subfamilia finita $\{\mathcal{U}_1, \cdots, \mathcal{U}_n\} \subseteq \mathcal{F} \cup \mathcal{F}_1$ que cubre a I, en particular cubre a X. Ahora, la construcción de $\mathcal{F}_1$ garantiza que $\mathcal{F} \cap \{\mathcal{U}_1, \cdots, \mathcal{U}_n\}$ cubre a X.

V $\Rightarrow$ VI Sea X un conjunto acotado infinito, si X no tiene puntos de acumulación, entonces los puntos de X son aislados y esto implica que X es cerrado, para todo $x \in X$ existe un intervalo abierto J_x tal que $J_x \cap X = \{x\}$, y la familia $\mathcal{F} = \{J_x : x \in X\}$ es una cubierta de X, el cual es cerrado y acotado, entonces $\mathcal{F}$ tiene una subfamilia finita que lo cubre, por lo tanto X debe ser finito $\Rightarrow\Leftarrow$.

VI $\Rightarrow$ VII a) F es arquimediano, pues de otra forma existen $a, b \in F$ con $0 < a < b$ y $0 < a \leq na < b \ \ \forall\, n \in \mathbb{N}$. Es claro que $X = \{na : n \in \mathbb{N}\}$ es infinito y no tiene puntos de acumulación, una contradicción.
b) Para cada n sea $J_n = [a_n, b_n]$ un intervalo cerrado tal que $J_{n+1} \subset J_n$, así $a_n \leq a_{n+1} \leq b_{n+1} \leq b_n$, en particular $a_1 \leq a_n \leq b_1 \ \forall\, n$, i.e. el conjunto $X = \{a_n : n \in \mathbb{N}\}$ es acotado.

Si para algún $n_0 \in \mathbb{N},\ a_m = a_{n_0} \ \ \forall\, m \geq n_0$ entonces $a_{n_0} \in J_m \ \ \forall\, m \geq 1$, de lo cual $a_{n_0} \in \cap J_n$.

Si para todo n existe m tal que $a_m \neq a_n$ entonces X es infinito. Por hipótesis X tiene un punto de acumulación, digamos a.

Afirmación. $a_n \leq a \leq b_n \ \ \forall\, n$.
Si $a < a_n$ para algún n, entonces $a < a_n \leq a_m \ \ \forall\, m \geq n$.
Si $0 < \varepsilon < a_n - a$ entonces $]a - \varepsilon, a + \varepsilon[\cap X$ es finito, por lo tanto a no es un punto de acumulación.
Si $b_n < a$ para algún n entonces $a_m \leq b_n < a \ \ \forall\, m \geq n$. Argumentando como antes, se concluye que a no es un punto de acumulación para X. Así $a \in \cap J_n$.
VII $\Rightarrow$ I Es necesario mostrar que cualquier sucesión de Cauchy en F converge en F. Sea $\{a_n\}$ una de sucesión de Cauchy en F.
De los hechos 1 y 2 probados con anterioridad, puede suponerse que $\{a_n\}$ es monótona, decreciente y acotada. Se construirá una sucesión de intervalos anidados $J_n = [c_n, d_n]$ tal que c_n es una cota inferior de $\{a_m\}$ para todo n y d_n no lo es.
Ya que $\{a_n\}$ es acotada inferiormente sea c_1 una cota inferior para $\{a_n\}$ y d_1 tal que $a_k < d_1$ para algún k. Puesto que $\{a_n\}$ es decreciente entonces $a_n \in [c_1, d_1] \ \ \forall\, n \geq k$. Sea $e_1 = \dfrac{c_1 + d_1}{2}$ y definamos $c_2 = e_1$, si e_1 es una cota inferior para $\{a_n\}$ y $d_2 = d_1$, en otro caso sean, $c_2 = c_1$ y $d_2 = e_1$. En general se puede suponer que $J_n = [c_n, d_n]$ se ha construído y defina $e_n = \dfrac{c_n + d_n}{2}$. Sea $c_{n+1} = e_n$ si e_n es una cota inferior para $\{a_n\}$ y $d_{n+1} = d_n$; en otro caso, $c_{n+1} = c_n$ y $d_{n+1} = e_n$. Por la construcción de J_n se tiene $J_{n+1} \subset J_n$ y $\text{vol}(J_n) = \dfrac{d_1 - c_1}{2^{n-1}}$ para todo $n \geq 1$. Por hipótesis $\cap_{n=1}^{\infty} J_n \neq \emptyset$. Si $a \in \cap_{n=1}^{\infty} J_n$, entonces la hipótesis sobre $\{a_n\}$ y la condición $\text{vol}(J_n) = \dfrac{d_1 - c_1}{2^{n-1}}$ junto con la condición arquimediana en F implica directamente que $\lim\limits_{n\to\infty} a_n = a$.
Con esto se ha terminado la demostración del teorema. ■

Teorema 50. *Sea F un campo ordenado arquimediano, entonces F es isomorfo a un subcampo de $\mathbb{R}$.*

Demostración. Se sabe que F contiene un subcampo $F_{\mathbb{Q}}$ isomorfo a $\mathbb{Q}$. También se tiene que F es arquimediano $\iff$ todo elemento $a \in F$ es el límite de una sucesión en $F_{\mathbb{Q}}$ (Teorema 48), i.e. $a = \lim\limits_{n\to\infty} \{\tilde{a}_n\}$ donde $\{a_n\}$ es una sucesión en $\mathbb{Q}$.
Definamos $\psi(a) = \lim\limits_{n\to\infty} a_n \in \mathbb{R}$. Está claro que la definición de ψ es independiente de la sucesión $\{\tilde{a}_n\}$, puesto que el isomorfismo que identifica a $\mathbb{Q}$ con $F_{\mathbb{Q}}$ preserva sucesiones de

Cauchy. Las propiedades de límites garantizan que ψ es un homomorfismo. Si $a > 0$, entonces $\{\tilde{a}_n\}$ es positiva, lo cual implica que $\{a_n\}$ es positiva, así $\lim_{n\to\infty} a_n = \psi(a) > 0 \in \mathbb{R}$, por lo tanto ψ preserva el orden, y esto implica que ψ es inyectiva. ■

Teorema 51. *Todo campo F ordenado, arquimediano y completo es isomorfo a $\mathbb{R}$.*

Demostración. Se tiene que todo $x \in \mathbb{R}$ satisface $x = \lim_{n\to\infty} a_n$ con $\{a_n\} \subseteq \mathbb{Q}$, por lo tanto $\{\tilde{a}_n\}$ tiene un límite en F, digamos $a = \lim_{n\to\infty} \tilde{a}_n$ así $\psi(a) = x$, (ψ como en el teorema anterior), de esta manera ψ es sobre, i.e. $F \cong \mathbb{R}$. ■

Corolario. *Hay solamente un campo que satisface los enunciados I-VII del Teorema 49.* ■

Se ha empezado la construcción del sistema de los números reales con un sistema de Peano, y siguiendo un procedimiento paso a paso se ha llegado obtener el sistema de los reales, $\mathbb{R}$. Tomando por hecho la existencia de los números racionales, la construcción usa como piedra angular, las sucesiones de Cauchy de números racionales. Existe otro enfoque, que es más algebraico, pero se puede decir que en esencia son el mismo, se trata de las cortaduras de Dedekind, cuya definición se da a continuación.

Definición. *Por una cortadura de Dedekind de $\mathbb{Q}$ se entiende una pareja (A, B) de subconjuntos de $\mathbb{Q}$ que satisfacen*

D1 $\mathbb{Q} = A \cup B$ *y* $A \cap B = \emptyset$.

D2 A *y* B *son no vacíos.*

D3 $a < b \ \forall\, a \in A$ *y* $\forall\, b \in B$.

D4 A *no tiene máximo.*

Como se mencionó en la introducción, hay otro enfoque para construir el sistema de los números reales, presentado por Conway [2] cuyo método es, suprimir el procedimiento paso a paso que anteriormente se mencionó. La base del método de Conway, es la reformulación de los postulados de Dedekind mediante cortaduras. El Método de Conway, es sin duda, de mayor alcance, pues su formulación se hace en términos muy generales, de hecho la construcción de Conway da como resultado un campo "Universal"[4, página 352] en donde están "contenidos" todos los campos ordenados. Esto puede ser de interés especialmente para los interesados en la contrucción de los *hiper-reales* y en el *análisis no estándar*.

0.7.4. Ejercicios

1.- Resuelva todos los ejercicios asignados en las notas.

2.- Sea F un campo ordenado. Por una sección superior en F se entiende un $U \subseteq F$ el cual satisface:

a) $U \neq F, \emptyset$,

b) Si $a \in U$ y $a < b$ entonces $b \in U$, y

c) Si $a \in U$ entonces existe $b < a$ tal que $b \in U$.

Un campo ordenado F se dice continuamente ordenado si para toda sección superior U, $F \setminus U$ tiene máximo elemento.

a) Defina sección inferior en un campo ordenado.

b) Si F es un campo continuamente ordenado y B es una sección inferior, demuestre que $F \setminus B$ contiene un mínimo.

3.- ¿Es $\mathbb{Q}$ continuamente ordenado?

4.- Sea F un campo ordenado. Demuestre que F no tiene mínimo elemento y tampoco máximo.

5.- Sea F un campo ordenado, L un subcampo denso en F. Suponga que toda sucesión de Cauchy $\{a_n\} \subseteq L$ converge en F. Demuestre que F es completo.

6.- Sea $r \in \mathbb{R}^+$, demuestre que existe un único $n \in \mathbb{N}$ tal que $n < r \leq n + 1$. Extienda el resultado a cualquier $r \in \mathbb{R}$, salvo que el n ahora es un entero.

7.- Defina la parte entera y fraccionaria de un real r.

8.- Sea b un entero mayor que 1. Demuestre que todo real $r > 0$ admite una representación única en base b de la forma $r = \sum_{i=0}^{\infty} c_i b^{-i}$, con c_i enteros no negativos y $0 \leq c_i < b$ para todo $i \geq 1$. Sugerencia: escriba a r como su parte entera mas su parte fraccionaria.

9.- Sea F un campo ordenado, $\mathbb{Q}_F$ el subcampo de F isomorfo a $\mathbb{Q}$. Se dice que F admite elememtos irracionales si $F \neq \mathbb{Q}_F$. Suponga que F tiene elementos irracionales, demuestre que el conjunto de elementos irracionales es denso en F.

10.- Sea $\mathbb{Q}[x]$ el conjunto de los polinomios con coeficientes en $\mathbb{Q}$. Con la suma y producto usual de polinomios, $\mathbb{Q}[x]$ forma un dominio entero.

a) Imite la construcción de $\mathbb{Q}$ a partir de $\mathbb{Z}$ para obtener un campo a partir de $\mathbb{Q}[x]$. Este campo se llama el campo de las funciones racionales sobre $\mathbb{Q}$ y es denotado por $\mathbb{Q}(x)$; los elementos de $\mathbb{Q}(x)$ son cocientes de polinomios.

b) Sea $P = \{p(x)/q(x) \in \mathbb{Q}(x) : p(x)q(x)$ tiene coeficiente principal positivo$\}$. Demuestre que P es un conjunto de elementos positivos. ¿Es $\mathbb{Q}(x)$ un campo arquimediano?

11.- Sea F el conjunto de las series formales de Laurent $\sum_{-\infty}^{\infty} r_j x^j$ con $r_j \in \mathbb{Q}$ y $r_j = 0$ para todo $j < -m$ para algún $m \in \mathbb{N} \cup \{0\}$. Se define una suma y producto en F como sigue

$$\sum_{-\infty}^{\infty} r_j x^j + \sum_{-\infty}^{\infty} s_j x^j = \sum_{-\infty}^{\infty} (r_j + s_j) x^j$$

$$(\sum_{-\infty}^{\infty} r_j x^j)(\sum_{-\infty}^{\infty} s_j x^j) = \sum_{-\infty}^{\infty} c_j x^j \qquad \text{con } \; c_j = \sum_{p=0}^{j} r_{j-p} s_p.$$

Con las operaciones anteriores F es un campo. Se define un orden en F como sigue:

$$\sum_{-\infty}^{\infty} r_j x^j < \sum_{-\infty}^{\infty} s_j x^j$$

si existe un k tal que $r_j = s_j$ para todo $j < k$ y $r_k < s_k$. Demuestre que F es un campo ordenado el cual no es arquimediano. ¿Hay alguna relación entre los campos de los ejercicios 10 y 11? De hecho F es un campo completo. Este es un ejemplo para mostrar que la condición de ser arquimediano en los enunciados I-VII del teorema 49 es necesaria.

.1. Teorema Chino del Residuo

Teorema A (Teorema Chino del Residuo) *Dados* $m, n \in \mathbb{Z}$, *tales que* $\gcd(m,n) = 1$ *entonces*

i) $\left(\frac{\mathbb{Z}}{mn\mathbb{Z}}\right) \cong \frac{\mathbb{Z}}{m\mathbb{Z}} \times \frac{\mathbb{Z}}{n\mathbb{Z}}$.

ii) $\left(\frac{\mathbb{Z}}{mn\mathbb{Z}}\right)^* \cong \left(\frac{\mathbb{Z}}{m\mathbb{Z}}\right)^* \times \left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^*$.

En donde $\left(\frac{\mathbb{Z}}{m\mathbb{Z}}\right)^* = \{[a] : \gcd(a,m) = 1\}$.

Demostración. i) Definamos $\Psi : \left(\frac{\mathbb{Z}}{mn\mathbb{Z}}\right) \to \left(\frac{\mathbb{Z}}{m\mathbb{Z}}\right) \times \left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)$ como sigue $\Psi([a]_{mn}) := ([a]_m, [a]_n)$. Ψ está bien definida, pues $[a]_{mn} = [b]_{mn} \Rightarrow a - b = mnt$ para algún t, de aquí $[a]_n = [b]_n$ & $[a]_m = [b]_m$. Es directo verificar, que $\Psi([a]_{mn}+[b]_{mn}) = \Psi([a]_{mn})+\Psi([b]_{mn})$. También se tiene que Ψ es inyectiva ya que $\Psi([a]_{mn}) = ([a]_m, [a]_n) = (0,0)$ implica $m \mid a$ & $n \mid a$, de esto y la hipótesis $\gcd(m,n) = 1$ se tiene $mn \mid a$, de esta manera $[a]_{mn} = [0]_{mn}$. Ψ es sobre, en efecto, mostrar que Ψ es sobre es equivalente a mostrar que las congruencias $x \equiv a \pmod{m}$ y $x \equiv b \pmod{n}$ tienen una solución común. Por hipótesis $\gcd(m,n) = 1$, esto implica que existen $m_0, n_0 \in \mathbb{Z}$ tales que $1 = mm_0 + nn_0$. Multiplicando esta ecuación por a y b respectivamente, se obtiene $a = mm_0a + nn_0a$ & $b = mm_0b + nn_0b$. Definamos $x = mm_0b + nn_0a$, entonces se tiene $x \equiv nn_0a \pmod{m}$ y $a \equiv nn_0a \pmod{m}$, de lo cual $x \equiv a \pmod{m}$. Análogamente, $x \equiv mm_0b \pmod{n}$ & $b \equiv mm_0b \pmod{n}$, de esta forma $x \equiv b \pmod{n}$, por lo tanto $\Psi(x) = \Psi([mm_0b + nn_0a]_{mn}) = ([a]_m, [b]_n)$.

ii) Si $[a]_{mn} \in \left(\frac{\mathbb{Z}}{mn\mathbb{Z}}\right)^*$ entonces $\gcd(a, mn) = 1 \Rightarrow \gcd(a,m) = \gcd(a,n) = 1$, por lo tanto $\Psi\left(\left(\frac{\mathbb{Z}}{mn\mathbb{Z}}\right)^*\right) \subseteq \left(\frac{\mathbb{Z}}{m\mathbb{Z}}\right)^* \times \left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^*$.

De la construcción de x en el caso anterior se tiene que si $\gcd(a,m) = \gcd(b,n) = 1$ por lo que $\gcd(x, mn) = 1$. En efecto $x \equiv a \pmod{m} \Rightarrow x - a = tm$. Si $\gcd(x,m) > 1$, entonces existe p primo tal que $p \mid m$ & $p \mid x \Rightarrow p \mid a \Rightarrow \gcd(a,m) > 1 \Rightarrow\Leftarrow$.

Análogamente, si $x \equiv b \pmod{n}$ con $\gcd(b,n) = 1$ entonces $\gcd(x,n) = 1$. Por lo tanto $\gcd(x, mn) = 1$ y $\Psi(x) = ([a]_m, [b]_n) \in \left(\frac{\mathbb{Z}}{m\mathbb{Z}}\right)^* \times \left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^*$. ■

Corolario. *Si* $\gcd(m,n) = 1$ *entonces* $\Psi(mn) = \Psi(m)\Psi(n)$.

Demostración. Sea Ψ como en el teorema anterior, entonces Ψ es una biyección de $\left(\frac{\mathbb{Z}}{mn\mathbb{Z}}\right)^*$ en $\left(\frac{\mathbb{Z}}{m\mathbb{Z}}\right)^* \times \left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^*$, el resultado se obtiene tomando cardinalidad. ■

Bibliografía

[1] Cohen, L.W. and Ehrlich, G., *The estructure of the real number system*. Princeton, D. Van Nostrand Co. Inc. 1963

[2] Conway, J.H., *On Numbers and Games*. Academic Press 1976, 1979

[3] Dedekind, R., *Was sind und was sollen die Zahlen*? Braunschweig 1888

[4] Ebbinghaus, H.D., et. al, *Numbers*. Springer-Verlag, readings in Mathematics, 1991

[5] Feferman, S. *The number systems*, Addison- Wesley 1964

[6] Hardy G.H. and E.M. Wright, *An introduction to the theory of numbers*, Oxford at the clarendon press 1979, fifth edition

[7] Knuth, D.E., *Surreal Numbers*, Addison-Wesley 1974

[8] Landau, E. *Foundations of Analysis*, translated by F. Steinhardt, New York, Chelsea 1951

[9] Peano, G., *Arihtmetices principia nova exposita*, en: Opere scelte Bd. II, Rome 1958, 20-55

Índice alfabético