Introducción al Algebra

Luis Manuel Reyes de la Luz

Septiembre 2023

Índice general

Parte I

Algebra Superior I

Capítulo 1

Introducción a la Teoría de Conjuntos

La Teoría de Conjuntos es una rama de las matemáticas que estudia los conjuntos, que son colecciones de objetos. La teoría fue desarrollada por Georg Cantor a finales del siglo XIX, quien demostró que los conjuntos pueden ser infinitos y que existen infinitos de diferentes tamaños.

En 1901, Bertrand Russell descubrió una paradoja en la teoría de conjuntos, conocida como la paradoja de Russell. La paradoja plantea que no puede existir un conjunto de todos los conjuntos que no se contienen a sí mismos como elementos.

La paradoja de Russell llevó a una crisis en la teoría de conjuntos, que fue resuelta por Ernst Zermelo, Abraham Fraenkel y Thoralf Skolem. Zermelo propuso un sistema axiomático de conjuntos que evitaba la paradoja de Russell. Este sistema, conocido como la Teoría de Conjuntos de Zermelo-Fraenkel, es la base de la teoría de conjuntos moderna.

A continuación se presenta un resumen de la historia de la Teoría de Conjuntos, desde Cantor, la paradoja de Russell, y la axiomatización de Z-F:

- **Siglo XIX**: Georg Cantor desarrolla la teoría de conjuntos, demostrando que los conjuntos pueden ser infinitos y que existen infinitos de diferentes tamaños.
- **1901**: Bertrand Russell descubre la paradoja de Russell, que plantea que no puede existir un conjunto de todos los conjuntos que no se contienen a sí mismos como elementos.
- **Principios del siglo XX**: Ernst Zermelo propone un sistema axiomático de conjuntos que evita la paradoja de Russell.
- **1920**: Abraham Fraenkel y Thoralf Skolem precisan el sistema axiomático de Zermelo, resultando de ello la Teoría de Conjuntos de Zermelo-Fraenkel.

La Teoría de Conjuntos es una teoría fundamental en matemáticas, que se utiliza en una amplia gama de campos, como la topología, la teoría de la medida, la lógica matemática y la teoría de la computabilidad, entre otros más.

1.1. Axiomas ZF.

Durante estas notas presentaremos los axiomas ZF a medida que se vayan necesitando. Para formular la teoría necesitamos un lenguaje:

Definición 1.1.1 — Lenguaje de la teoría de conjuntos. El lenguaje de la teoría de conjuntos consiste en lo siguiente:

1. **Conjuntos**: Denotamos a los conjuntos como letras mayusculas $A, B, C, \cdots$. Adicionalmente, por convención, definimos la noción de elementos como aquel que pertenece a un conjunto determinado, y podemos denotarlo con letras pequeñas $a, b, c, \cdots$.

2. **Pertenencia**: Denotamos $\in$ como simbolo de pertenencia. Escribimos $x \in X$ para decir que x es un elemento de X y se lee como x pertenece a X.
3. El lenguaje de la lógica proposicional y de primer orden.
4. **Llaves**: $\{,\}$, usados para delimitar los elementos de un conjunto.
5. **Igualdad**: Usado para representar la igualdad de conjuntos.

Y como reglas de inferencia, usaremos las reglas de inferencias de la lógica proposicional y de primer orden. Con ello, solo basta definir y comprender los axiomas. [Del conjunto vacio] Existe un conjunto que no tiene elementos.

$$\exists X,\ (\forall x,\ x \notin X)$$

[De Extensión] Sean A, B conjuntos entonces:

$$A = B \Leftrightarrow ((\forall x \in A,\ x \in B) \wedge (\forall x \in B,\ x \in A))$$

Usando estos axiomas podemos fundamentar lo siguiente:

Proposición 1.1.1 Existe un único conjunto que no tiene elementos.

Definición 1.1.2 Definimos al único conjunto que no tiene elementos como conjunto vacio y lo denotamos como $\emptyset$.

Definición 1.1.3 — Contención. Sean A, B conjuntos, decimos que A está contenido en B, denotado como $A \subseteq B$ si $\forall x \in A$, $x \in B$.

Proposición 1.1.2 Dados A, B conjuntos, las siguientes afirmaciones son equivalentes:

1. $A = B$.
2. $A \subseteq B$ y $B \subseteq A$.

[De comprensión] Sea $P(x)$ una propiedad de x y A un conjunto, entonces existe un conjunto B tal que:

$$x \in B \Leftrightarrow\ (x \in A \wedge P(x))$$

■ **Ejemplo 1.1** Si A y B son conjuntos, entonces existe un conjunto R tal que $x \in R$ si y sólo si $x \in A$ y $x \in B$. ■

■ **Ejemplo 1.2** El conjunto de todos los conjuntos no existe. ■

Proposición 1.1.3 Sea A un conjunto y $P(x)$ una propiedad, entonces hay un único conjunto B tal que $x \in B$ si y sólo si $x \in A$ y $P(x)$ lo satisface.

Definición 1.1.4 — Intersección. Sea A y B conjuntos, el conjunto intersección de A y B es el único conjunto $A \cap B$ que se define como sigue:

$$A \cap B := \{x|\ x \in A \wedge x \in B\}$$

[Del Par] Para cualesquiera a y b, hay un conjunto C tal que $x \in X$ si y sólo si $x = a$ ó $x = b$ El axioma del par asegura que todo conjunto es un elemento de algún conjunto y dos conjuntos cualesquiera son simultaneamente elementos de algún mismo conjunto.

■ **Ejemplo 1.3** $\{\emptyset, \emptyset\} = \{\emptyset\}$. ■

[De Unión] Sea $\mathcal{F}$ una familia de conjuntos, entonces existe un conjunto X tal que $x \in X$ si y sólo si $x \in A$ para algún $A \in \mathcal{F}$.

Proposición 1.1.4 El conjunto anterior es único con dicha propiedad.

Definición 1.1.5 — Unión. Sean A y B conjuntos, el conjunto unión de A y B como el único conjunto $A \cup B$ que se define como sigue:

$$A \cup B := \{x | x \in A \vee x \in B\}$$

[Del conjunto potencia] Sea X un conjunto, entonces existe un conjunto P tal que $A \in P$ si y sólamente si $A \subseteq X$.

Definición 1.1.6 — Conjunto Potencia. Decimos que un conjunto A es subconjunto de B si $A \subseteq B$. El conjunto de todos los subconjuntos de B es denotado como $\mathbf{P}(B)$

[De Regularidad] Para todo conjunto X no vacio, existe y tal que $y \in x$ y $x \cap y = \emptyset$. Gracias a este axioma, podemos evitar las siguientes patologias.

Teorema 1.1.5 Las siguientes afirmaciones son válidas:

1. Para cualquier conjunto X no vacio se tiene $X \notin X$.
2. Para cualquier par de conjuntos no vacios A y B no puede pasar simultaneamente que $A \in B$ y $B \in A$.

1.2. Teoremas de Contención.

Teorema 1.2.1 — Propiedades de Contención. Las siguientes afirmaciones son válidas para conjuntos A, B, C.

1. $A \subseteq A$.
2. Si $A \subseteq B$ y $B \subseteq A$ entonces $A = B$.
3. Si $A \subseteq B$ y $B \subseteq C$ entonces $A \subseteq C$

Demostración. Para el primer punto, sea $x \in A$ entonces $x \in A$ concluyendo por definición que $A \subseteq A$. El segundo punto es un caso particular de 1.1.2. Para el tercer punto, sea $x \in A$, por hipótesis tenemos $A \subseteq B$, entonces $x \in B$, luego por hipótesis tenemos $B \subseteq C$ entonces $x \in C$, concluyendo por definición $A \subseteq C$. ■

Teorema 1.2.2 — Caracterización de la unión. Sean A, B conjuntos entonces las siguientes afirmaciones son válidas:

1. $A \subseteq A \cup B$ y $B \subseteq A \cup B$.
2. Sea P un conjunto tal que satisface las siguientes propiedades:
   a) $A \subseteq P$ y $B \subseteq P$.
   b) Si H es otro conjunto tal que $A \subseteq H$ y $B \subseteq H$ entonces $P \subseteq H$.

   Entonces $P = A \cup B$.

Notemos que el segundo punto nos da una técnica para probar cuando un conjunto es la unión de otros dos. De manera similar tenemos una técnica para probar la intersección y es la que se menciona en el siguiente teorema.

Teorema 1.2.3 — Caracterización de la intersección. Sean A, B conjuntos entonces las siguientes afirmaciones son válidas:

1. $A \cap B \subseteq A$ y $A \cap B \subseteq B$.
2. Sea Q un conjunto tal que satisface las siguientes propiedades:
   a) $Q \subseteq A$ y $Q \subseteq B$.
   b) Si H es otro conjunto tal que $H \subseteq A$ y $H \subseteq B$ entonces $H \subseteq P$.

   Entonces $P = A \cap B$.

Proposición 1.2.4 Sean A, B conjuntos, entonces son equivalentes:

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

1.3. Algebra de Conjuntos.

Teorema 1.3.1 — Algebra de Conjuntos. Sean A, B, C conjuntos, las siguientes afirmaciones son válidas:

1. $A \cap A = A$ y $A \cup A = A$.
2. $A \cap B = B \cap A$ y $A \cup B = B \cup A$.
3. $A \cap (B \cap C) = (A \cap B) \cap C$ y $A \cup (B \cup C) = (A \cup B) \cup C$.
4. $A \cap \emptyset = \emptyset$ y $A \cup \emptyset = A$.
5. $A \cap (B \cup C) = (A \cap B) \cup (A \cap B)$ y $A \cup (B \cap C) = (A \cup B) \cap (A \cup B)$.

Proposición 1.3.2 Sean A, B conjuntos, las siguientes afirmaciones son válidas:

1. $A \cap (A \cup B) = A$.
2. $A \cup (A \cap B) = A$.

Definición 1.3.1 — Diferencia de conjuntos. Sea X un conjunto y A, B subconjuntos de X definimos:

1. **Diferencia de conjuntos:** $A - B := \{x \in X |\ x \in A,\ x \notin B\}$.
2. **Diferencia simétrica de conjuntos:** $A \triangle B := (A - B) \cup (B - A)$.

Proposición 1.3.3 — Propiedades de Diferencia,. Sea X un conjunto y A, B subconjuntos de X, las siguientes afirmaciones son válidas:

1. Si $A \subseteq B$ entonces $X - B \subseteq X - A$.
2. **Leyes de Morgan:** Tenemos las siguientes igualdades:

$$X - (A \cup B) = (X - A) \cap (X - B),\ X - (A \cap B) = (X - A) \cup (X - B)$$

3. $A \cup (X - A) = X$ y $A \cap (X - A) = \emptyset$.
4. $A \triangle B = (A \cup B) - (A \cap B)$.
5. $A \triangle B = \emptyset$ si y sólo si $A = B$.

1.4. Union e intersección albitraria de conjuntos.

Definición 1.4.1 — Union e intersección albitraria. Sea $\mathcal{F}$ una familia de conjuntos definimos:

1. **Unión:** $\bigcup \mathcal{F} = \bigcup_{A \in \mathcal{F}} A := \{x |\ \exists A \in \mathcal{F},\ x \in A\}$.
2. **Intersección:** $\bigcap \mathcal{F} = \bigcap_{A \in \mathcal{F}} A := \{x |\ \forall A \in \mathcal{F},\ x \in A\}$.

Teorema 1.4.1 — Propiedades de la Union e intersección albitraria. Sean $\{A_i\}_{i \in I}$ y $\{B_j\}_{j \in J}$ familias no vacias de conjuntos, entonces las siguientes afirmaciones son válidas:

1. $\left(\bigcap_{i \in I} A_i\right) \cup \left(\bigcap_{j \in J} B_j\right) = \bigcap_{(i,j) \in I \times J} A_i \cup B_j$.
2. $\left(\bigcup_{i \in I} A_i\right) \cap \left(\bigcup_{j \in J} B_j\right) = \bigcup_{(i,j) \in I \times J} A_i \cap B_j$.
3. Si X es un conjunto, entonces se cumplen las **leyes de Morgan**:
   a) $X - \left(\bigcup_{i \in I} A_i\right) = \left(\bigcap_{i \in I} X - A_i\right)$.
   b) $X - \left(\bigcap_{i \in I} A_i\right) = \left(\bigcup_{i \in I} X - A_i\right)$.

1.5. Producto Cartesiano Binario.

Definición 1.5.1 — Par ordenado. Para cualesquiera a y b, definimos el par ordenado como el siguiente conjunto:

$$(a,b) = \{\{a\},\{a,b\}\}$$

Teorema 1.5.1 — Propiedades del par ordenado. Las siguientes afirmaciones son válidas:

1. Para toda a, $(a,a) \neq \{a\}$.
2. Para toda a, b tenemos $(a,b) = (b,a)$ si y sólo si $a = b$.
3. $(a,b) = (c,d)$ si y sólo si $a = c$ y $b = d$.

Definición 1.5.2 — Producto Cartesiano Binario. Dados A y B conjuntos, definimos el Producto Cartesiano Binario como sigue:

$$A \times B = \{(a,b) |\ a \in A, b \in B\}$$

Teorema 1.5.2 — Propiedades del producto cartesiano. Las siguientes afirmaciones son válidas:

1. $A \times B = \emptyset$ si y sólo si $A = \emptyset$ ó $B = \emptyset$.
2. $A \times B \subseteq C \times D$ si y sólo si $A \subseteq C$ y $B \subseteq D$.
3. $A \times (B \cup C) = (A \times B) \cup (A \times C)$.
4. $A \times (B \cap C) = (A \times B) \cap (A \times C)$.

Proposición 1.5.3 Para conjuntos no vacios A, B tenemos $A \times B = B \times A$ si y sólamente si $A = B$.

1.6. Propiedades del conjunto potencia.

Proposición 1.6.1 Si $A \subseteq B$ entonces $\mathbf{P}(A) \subseteq \mathbf{P}(B)$.

Proposición 1.6.2 Sea $\{A_i\}_{i\in I}$ una familia no vacia de conjuntos y B un conjunto entonces tenemos las siguientes identidades:

1. $B \times \left(\bigcup_{i\in I} A_i\right) = \bigcup_{i\in I} B \times A_i$.
2. $B \times \left(\bigcap_{i\in I} A_i\right) = \bigcap_{i\in I} B \times A_i$.

Teorema 1.6.3 — Propiedades del conjunto potencia. Las siguientes afirmaciones son válidas para una familia no vacia de conjuntos $\{A_i\}_{i\in I}$

1. $\bigcap_{i\in I} \mathbf{P}(A_i) = \mathbf{P}\left(\bigcap_{i\in I} A_i\right)$.
2. $\bigcup_{i\in I} \mathbf{P}(A_i) \subseteq \mathbf{P}\left(\bigcup_{i\in I} A_i\right)$.

1.7. Ejercicios

1. ¿Exíste el conjunto $x = \{x, a, b, c\}$? Argumenta.
2. Prueba usando el axioma de regularidad que el conjunto $A = \{0, 1, 2\}$ existe.
3. Aplica el axioma de la unión al conjunto $A = \{8\}$.
4. Demuestre la verdad o falsedad (con un contraejemplo) del siguiente enunciado: Si A $\subseteq$ B y B $\in$ C entonces A $\notin$ C.

5. Sean A, B y C conjuntos. Demuestre que:

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

6. Sean A y B conjuntos no vacíos y $(A \times B) \cup (B \times A) = C \times C$. Demuestre que $A = B = C$.
7. Prueba que $A \triangle B = \emptyset$ si y sólo si $A = B$.
8. Demuestra que $A \subseteq C$ si y sólo si $A \cup (B \cap C) = (A \cup B) \cap C$.
9. Sea X un conjunto que contiene a $A \cup B$.
   a) Demuestra que si $A \cup B = X$ entonces $X - A \subseteq B$.
   b) Demuestra que si $A \cap B = \emptyset$ entonces $A \subseteq X - B$.
   c) Utilizando los incisos anteriores demuestra que $A = X - B$ sí y sólo si $A \cup B = X$ y $A \cap B = \emptyset$.
10. Prueba que $(a, b) \subseteq \mathbf{P}(\{a, b\})$.
11. Considera $A, B \subseteq X$ y $C, D \subseteq Y$ demuestra que $(A \times C) \cap (B \times D) = (A \cap B) \times (C \times D)$.
12. Demuestra que para cualquier conjunto X se tiene que $\bigcap \mathbf{P}(X) = \emptyset$.
13. Sean $\mathcal{F} \neq \emptyset$ y X conjuntos, definamos $\mathcal{E} := \{A \in \mathbf{P}(X) |\ A = X \cap F$ para algún $F \in \mathcal{F}\}$, demuestra que $X \cap \bigcup \mathcal{F} = \bigcup \mathcal{E}$.

Capítulo 2

Relaciones y Fuciones

La historia del concepto de función se remonta a la antigüedad, con los trabajos de los matemáticos griegos. En ese momento, la función se entendía como una relación entre dos cantidades, una independiente y otra dependiente. En el siglo XVI, el matemático francés René Descartes introdujo el concepto de coordenadas cartesianas, que permitió representar funciones geométricamente. Esto condujo a un mayor interés en el estudio de las funciones, y a la aparición de nuevas definiciones y teoremas.

En el siglo XVII, el matemático alemán Gottfried Leibniz acuñó el término "función"para referirse a una relación entre dos variables. Leibniz también introdujo el concepto de función analítica, que es una función que se puede expresar mediante una fórmula matemática. En el siglo XVIII, el matemático suizo Leonhard Euler definió la función como una regla de correspondencia entre dos conjuntos. En el siglo XIX, el matemático francés Augustin-Louis Cauchy introdujo el concepto de función real, que es una función que toma valores reales. Cauchy también introdujo el concepto de límite, que es un concepto fundamental en el estudio de las funciones. En el siglo XX, el matemático alemán David Hilbert desarrolló una teoría axiomática de las funciones reales. Esta teoría proporciona una base sólida para el estudio de las funciones. En la actualidad, el concepto de función es uno de los conceptos más importantes en matemáticas. Las funciones se utilizan en una amplia gama de áreas, como el cálculo, el análisis, la probabilidad y la estadística.

En la actualidad, la definición de función se basa en el concepto de relación. Una relación es una colección de pares ordenados. Una función es una relación en la que cada elemento del primer conjunto, llamado dominio, está asociado con un único elemento del segundo conjunto, llamado codominio. Esta definición es más abstracta que la definición tradicional de función, pero tiene la ventaja de ser más general. Se puede aplicar a cualquier tipo de relación, no solo a las funciones analíticas.

2.1. El concepto conjuntista de Relaciones.

Definición 2.1.1 — Relación. Sean A, B conjuntos, una relación de A en B es un subconjunto $R \subseteq A \times B$. Como notación, a cada elemento $(a, b) \in R$ lo denotamos como aRb.

■ **Ejemplo 2.1 — Igualdad.** La relación de igualdad $a = b$ es la relación $\triangle = \{(x, x) \in X \times X\}$. ■

■ **Ejemplo 2.2 — Inclusión.** Fijando X un conjunto, la relación inclusión es el conjunto $\{(A, B) \in \mathbf{P}(X) \times \mathbf{P}(Y) |\ (\forall x \in A \Rightarrow x \in B)\}$. ■

Definición 2.1.2 — Elementos de una relación. Sea R una relación de A en B, definimos:

1. El dominio de R como el conjunto $dom(R) = \{x \in A |\ \exists y \in B, xRy\}$.
2. El rango de R como el conjunto. $ran(R) = \{y \in B |\ \exists x \in B, xRy\}$.

3. El campo de R como el conjunto $dom(R) \cup ran(R)$.

Notemos que $R \subseteq dom(R) \times ran(R) \subseteq A \times Y$ pero no necesariamente $dom(R) \times ran(R) \subseteq R$, entonces se puede pensar que el producto cartesiano de Dominio y Rango es el producto cartesiano más pequeño donde R está definida.

■ **Ejemplo 2.3** Notemos que $dom(\triangle) = X$ y $ran(\triangle) = X$ pero no pasa que $X \times X \subseteq \triangle$ al menos que X consta de un solo elemento. ■

Definición 2.1.3 — Imagen directa e imagen inversa.. Sea R una relación de A en B, definimos:

1. Para cada $X \subseteq A$, la imagen directa de X bajo R como el conjunto:

$$R(X) = \{y \in B | \ \exists x \in X, \ xRy\}$$

2. Para cada $Y \subseteq B$, la imagen inversa de Y bajo R como el conjunto:

$$R^{-1}(Y) = \{x \in A | \ \exists y \in Y, \ xRy\}$$

Definición 2.1.4 — Relacion Inversa. Sea R una relación de A en B definimos la relación inversa como la relación:

$$R^{-1} = \{(y, x) \in B \times A | \ (x, y) \in R\}$$

Definición 2.1.5 — Composición de Relaciones. Sean $R \subseteq A \times B$ y $S \subseteq B \times C$ dos relaciones. Definimos la composición $S \circ R \subseteq A \times C$ como:

$$S \circ R = \{(x, z) \in A \times B | \ \exists y \in B, (x, y) \in R, \ (y, z) \in S\}$$

Es posible que $S \circ R = \emptyset$, asi que daremos condiciones para que la composición no sea vacía.

Proposición 2.1.1 Sean $R \subseteq A \times B$ y $S \subseteq B \times C$ dos relaciones, entonces $S \circ R$ es distinto del vacio si $ran(R) \cap dom(S) \neq \emptyset$.

Demostración. Sea $x \in ran(R) \cap dom(S)$, entonces por definición de rango de R existe $a \in A$ tal qye aRx, luego por definición de dominio de S entonces existe $c \in C$ tal que xSc y por definición de composición de funciónes $(a, c) \in S \circ R$, mostrando que $S \circ R$ es distinto del vacio. ■

Dentro de las matemáticas existen muchos tipos de relaciones, casi todos ellos caracterizados por algunas de las siguientes propiedades.

Definición 2.1.6 — Propiedades de Relaciones. Sea R una relación de X en si mismo. Definimos las siguientes propiedades que puede tener una relación:

1. **Reflexiva**: Si $\triangle \subseteq R$.
2. **Irreflexiva**: Si $R \subseteq X \times X - \triangle$.
3. **Simétrica**: Si $R = R^{-1}$.
4. **Asimétrica**: Si $R \cap R^{-1} = \emptyset$.
5. **Antisimétrica**: Si $R \cap R^{-1} = \triangle$.
6. **Transitiva**: Si $R \circ R \subseteq R$.

En estas notas, trabajaremos principalmente con 3 tipos de relaciones importantes dados por las siguientes definiciones.

Definición 2.1.7 — Función. Dados A, B conjuntos, una función f de A hacia B, denotado como

$$f : A \to B$$

es una relación $f \subseteq A \times B$ que cumple la siguiente propiedad:
- Si $(x, y) \in f$ y $(x, z) \in f$ entonces $y = z$.

La propiedad de que una relación se llame función nos dice que para cada elemento del dominio le corresponde un único elemento del contradominio (no pide necesariamente lo converso), entonces gracias a esta propiedad podemos usar la notación $f(x) = y$ cada ves que $(x, y) \in f$.

Definición 2.1.8 — Orden parcial. Dado X un conjunto, un orden parcial en X es una relación $\leq \subseteq X \times X$ que satisface las siguientes propiedades:
1. Es reflexiva.
2. Es antisimétrica.
3. Es transitiva.

Definición 2.1.9 — Relacion de Equivalencia.. Dado X un conjunto, una relación de equivalencia en X es una relación $\sim \subseteq X \times X$ tal que satisface las siguientes propiedades:
1. Es reflexiva.
2. Es simétrica.
3. Es transitiva.

Cada tipo de relación tendrá su propio estudio en las siguientes secciones.

Construcciones técnicas. Nos centraremos ahora en dar una técnica de construcción de relaciones que cumplan las mismas propiedades (que puede generalizarse en la teoría de retículas completas). Para ello tomemos $\mathcal{F} \subseteq \mathbf{P}(\mathbf{P}(X \times X))$ una familia de relaciones que satisfacen las mismas propiedades y además pediremos que $\mathcal{F}$ cumpla las siguientes propiedades:
1. Si $\emptyset \neq \mathcal{G} \subseteq \mathcal{F}$ entonces $\bigcap \mathcal{G} \in \mathcal{F}$.
2. $X \times X \in \mathcal{F}$.

Nuestro objetivo es resolver lo siguiente:
- Dado $R \subseteq X \times X$ una relación albitraria, encontrar la menor relación S tal que:
  1. $S \in \mathcal{F}$.
  2. $R \subseteq S$.

Si existe tal relación, a S lo llamaremos la **relación del tipo $\mathcal{F}$ generada por R.**

Proposición 2.1.2 Sea $\mathcal{F}$ que cumple las hipótesis anteriores, y $R \subseteq X \times X$ una relación entonces la relación del tipo $\mathcal{F}$ generada por R es el siguiente conjunto:

$$\langle R \rangle = \bigcap \{Q \in \mathcal{F} |\ R \subseteq S\}$$

■ **Ejemplo 2.4** La simetrización de una relación. Esto se debe pues la familia de relaciones simétricas:

$$\mathcal{F} = \{R \subseteq X \times X |\ R = R^{-1}\}$$

Cumple las hipótesis dadas, entonces por la proposición anterior, para cada R relación en X, es posible generar la menor relación simétrica que contiene a R, véase los ejercicios. ■

■ **Ejemplo 2.5** Si consideramos

$$\mathcal{F} = \{R \subseteq X \times X |\ \triangle \subseteq R\}$$

Notemos que, como $\triangle \subseteq X \times X$ entonces $X \times X \in \mathcal{F}$. Luego si tomamos una subfamilia $\mathcal{G} \subseteq \mathcal{F}$, tenemos que:

$$\triangle \subseteq \bigcap \mathcal{G}$$

esto se ve porque para cada $S \in \mathcal{G}$, cumple por estar tambien en $\mathcal{F}$ que $\triangle \subseteq S$, entonces por propiedades de intersección, implica que $\triangle \subseteq \bigcap \mathcal{G}$. Consecuentemente podemos concluir que $\bigcap \mathcal{G} \in \mathcal{F}$. Mostrando que

la familia $\mathcal{F}$ satisface las hipotesis pedidas, por la proposición anterior existe el menor conjunto reflexivo. Se deja al lector probar que para toda relación R en X, el conjunto reflexivo generado por R es:

$$\langle R \rangle = R \cup \triangle$$

■

2.2. Propiedades generales de Funciones.

Teorema 2.2.1 — Propiedades de funciones. Sea $f\colon X \to Y$ una función, las siguientes afirmaciones son válidas:

1. Dado $A \subseteq X$ entonces $A = \emptyset$ si y sólo si $f(A) = \emptyset$.
2. $f^{-1}(\emptyset) = \emptyset$.
3. $f(\{x\}) = \{f(x)\}$.
4. Si $A \subseteq B \subseteq X$ entonces:
   a) $f(A) \subseteq f(B)$.
   b) $f(B) - f(A) \subseteq f(B - A)$.
5. Si $C \subseteq D \subseteq Y$ entonces:
   a) $f^{-1}(C) \subseteq f^{-1}(D)$.
   b) $f^{-1}(D - C) = f^{-1}(D) - f^{-1}(C)$.
6. Sea $\{A_i\}_{i\in I} \subseteq X$ y $\{B_i\}_{i\in I} \subseteq Y$ entonces:
   a) $f\left(\bigcup_{i\in I} A_i\right) = \bigcup_{i\in I} f(A_i)$.
   b) $f\left(\bigcap_{i\in I} A_i\right) \subseteq \bigcap_{i\in I} f(A_i)$.
   c) $f^{-1}\left(\bigcup_{i\in I} B_i\right) = \bigcup_{i\in I} f^{-1}(B_i)$.
   d) $f^{-1}\left(\bigcap_{i\in I} B_i\right) = \bigcap_{i\in I} f^{-1}(B_i)$.
7. Si $A \subseteq X$ y $B \subseteq Y$ entonces son equivalentes:
   a) $A \subseteq f^{-1}(f(A))$.
   b) $B \cap f(X) = f(f^{-1}(B))$.

Teorema 2.2.2 — Igualdad de funciones. Sean $f, g\colon X \to Y$ dos funciones, entonces $f = g$ si y sólo si $dom(f) = dom(g)$ y para toda $x \in dom(f)$ se tiene $f(x) = g(x)$.

Debido al teorema anterior, haremos la siguiente convención:

- $f\colon X \to Y$ se entiende como una función en donde $dom(f) = X$.

Proposición 2.2.3 Sean $f\colon A \to B$ y $g\colon B \to C$ dos funciones, las siguientes afirmaciones son válidas:

1. Para todo $A' \subseteq A$ se tiene que $g \circ f(A') = g(f(A'))$.
2. Para todo $C' \subseteq C$ se tiene que $(g \circ f)^{-1}(C') = f^{-1}(g^{-1}(C'))$.
3. Además si $h\colon C \to D$ es otra función entonces tenemos que:

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

Definición 2.2.1 — Funcion identidad. Sea X un conjunto, definimos la función identidad

$$\mathrm{Id}_X\colon X \to X$$

tal que $\mathrm{Id}_X(x) = x$ para toda $x \in X$.

Proposición 2.2.4 Sea $f\colon X \to Y$ una función, entonces:

$$f \circ \mathrm{Id}_X = f,\ \mathrm{Id}_Y \circ f = f.$$

En general cuando f es función, no necesariamente f^{-1} es función.

■ **Ejemplo 2.6** Toda función $f\colon \{1,2,3\} \to \{2,4\}$ se tiene que la relación f^{-1} no es función. ■

Definición 2.2.2 — Inyectividad. Una función $f\colon X \to Y$ se llama inyectivo si cada ves que $x, y \in dom(f)$ satisfacen que $f(x) = f(y)$ entonces $x = y$.

Proposición 2.2.5 Sea $f\colon X \to Y$ una función, entonces f^{-1} es una función si y sólo si f es inyectiva.

Teorema 2.2.6 — Caracterización de funciones inyectivas. Sea $f\colon X \to Y$ una función, entonces son equivalentes:

1. f es inyectiva.
2. Existe $g\colon Y \to X$ tal que $g \circ f = \mathrm{Id}_X$.
3. Para cada par de función $u, v\colon Z \to X$ tal que $f \circ u = f \circ v$ entonces $u = v$.
4. Para todo subconjunto $A \subseteq X$ se cumple $f^{-1}(f(A)) = A$.
5. Para cualesquiera $A \subseteq B \subseteq X$, se cumple que $f(B - A) = f(B) - f(A)$.
6. Para cualesquiera $A, B \subseteq X$, se cumple que $f(A \cap B) = f(A) \cap f(B)$.

Necesitamos una noción de función inversa.

Definición 2.2.3 — Funciones inversas. Sea $f\colon X \to Y$, una función, definimos:

1. Inversa derecha, como una función $g\colon B \to A$ tal que $f \circ g = \mathrm{Id}_B$.
2. Inversa izquierda, como una función $g\colon B \to A$ tal que $g \circ f = \mathrm{Id}_A$.
3. Inversa, si es inversa derecha e izquierda.

Que la relación inversa sea función, no necesariamente es una función inversa.

■ **Ejemplo 2.7** Sea $f\colon \{1,2\} \to \{1,2,3\}$ una función inyectiva. Entonces la relación inversa es $f^{-1}\colon \{f(1), f(2)\} \to \{1,2\}$. Es claro que $f \circ f^{-1} = \mathrm{Id}_{\{1,2,\}}$ pero no pasa que $f^{-1} \circ f = \mathrm{Id}_{\{1,2,3\}}$ ■

Definición 2.2.4 Sea $f\colon X \to Y$ una función, decimos que f es:

1. sobreyectiva si $imf = Y$.
2. biyectiva si es inyectiva y sobreyectiva.

Teorema 2.2.7 — Caracterización de las sobreyectivas. Sea $f\colon X \to Y$ una función, las siguientes afirmaciones son equivalentes:

1. f es sobreyectiva.
2. Para todo subconjunto no vacio $A \subseteq Y$, $f^{-1}(A) \subseteq X$ no es vacio.
3. Para todo par de funciones $u, v\colon Y \to Z$ tal que $u \circ f = v \circ f$ implica que $u = v$.
4. Para todo subconjunto $B \subseteq Y$, se tiene que $B = f(f^{-1}(B))$.

Para lo siguiente necesitamos un axioma más, llamado el Axioma de elección.

Definición 2.2.5 — Función de Elección. Sea A un conjunto, definimos una función de elección como una función:

$$f_A\colon \mathbf{P}(A) - \emptyset \to A$$

tal que para todo $B \subseteq A$ se tiene que $f|_A(B) \in B$.

Proposición 2.2.8 Todo conjunto finito tiene función de elección.

[Axioma de Elección] Todo conjunto no vacio tiene función de elección.

Proposición 2.2.9 Sea $\{X_i\}_{i\in I}$ entonces existe una función:

$$f\colon I \to \bigcup_{i\in I} X_i$$

tal que $f_i(i) \in X_i$

Demostración. Tomemos $A = \bigcup_{i\in I} X_i$ y definamos $\mu\colon I \to \mathbf{P}(A) - \emptyset$ como sigue, para cada $i \in I$, $\mu(i) = X_i$ y por el axioma de elección, construimos una función de elección $f|_A$, por tanto $f := f|_A \circ \mu$ es una función deseada. ■

Con esto en mente, daremos los teoremas de completación de diagramas. Primero definiremos una relación importante.

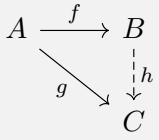
Definición 2.2.6 — Nucleo conjuntista de f. Sea $f\colon A \to B$ una función, definimos el nucleo conjuntista de f como:

$$\ker f := \{(x, y) \in A^2 |\ f(x) = f(y)\}$$

■ **Ejemplo 2.8** Una función $f\colon A \to B$ es inyectiva si y sólo si $\ker f = \triangle$. ■

Teorema 2.2.10 — Primer teorema de completación.. Dados $f\colon A \to B$ y $g\colon A \to C$ dos funciones, entonces las siguientes afirmaciones son equivalentes:

1. $\ker f \subseteq \ker g$.
2. Existe una función $h\colon B \to C$ tal que el siguiente diagrama es conmutativo



Demostración. Supongamos que $\ker f \subseteq \ker g$, fijemos $c_0 \in C$ entonces definamos la siguiente función $h\colon B \to C$:

$$h(b) = \begin{cases} g(a) & b \in im(f) \wedge f(a) = b \\ c_0 & b \in B - im(f) \end{cases}$$

Esta función está bien definida, pues dado $b \in B$ se tiene los siguientes casos:

1. Caso I: $b \in B - im(f)$ entonces es evidente.
2. Caso II: $b \in im(f)$ y supongamos que existen $a, a' \in A$ tales que:

$$f(a) = b = f(a') \Rightarrow\ (a, a') \in \ker(f)$$

pero por hipótesis, esto implica que $(a, a') \in \ker(g)$, obteniendo que $g(a) = g(a')$, por lo tanto $h(b)$ esta bien definida ya que no depende de la elección de preimagenes en $f^{-1}(\{b\})$.

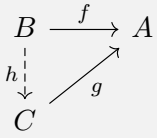
obteniendo que h es función. Luego dado $a \in A$ obtenemos entonces:

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

Por lo tanto $h \circ f = g$. Conversamente, supongamos que existe una función $h\colon B \to C$ tal que $g = h \circ f$, entonces si $(a, a') \in \ker(f)$ obtenemos $f(a) = f(a')$, componiendo con h obtenemos $h \circ f(a) = h \circ f(a')$ es decir $g(a) = g(a')$ por tanto $(a, a') \in \ker(g)$, concluyendo $\ker(f) \subseteq \ker(g)$. ■

Teorema 2.2.11 — Segundo teorema de completación.. Dados $f\colon B \to A$, $g\colon C \to A$, entonces las siguientes afirmaciones son equivalentes:

1. $im(f) \subseteq im(g)$.
2. Existe una función $h\colon B \to C$ tal que el siguiente diagrama es conmutativo



Demostración. Supongamos que $im(f) \subseteq im(g)$, notemos que para cada $b \in B$ se tiene $f(b) \in im(f) \subseteq im(g)$ obteniendo que existe una $c \in C$ tal que $f(b) = g(c)$, luego, para cada $b \in B$ denotemos $X_b := g^{-1}(\{b\})$ y $I = B$, entonces usando 2.2.9, tenemos una única elección de cada $b \in B$ a un único $c_b \in X_b$, definiendo una función $h\colon B \to C$ como sigue:

$$h(b) = c_b \Leftrightarrow \ g(c_b) = f(b)$$

de la construcción obtenemos $g \circ h = f$. Conversamente, supongamos que existe $h\colon B \to C$ una función tal que $g \circ h = f$, dado $a \in im(f)$ entonces existe $b \in B$ tal que $f(b) = a$, pero usando la hipótesis tenemos $a = f(a) = g(h(a))$ y $h(a) \in C$, obteniendo que $a \in im(g)$ por lo tanto $im(f) \subseteq im(g)$. ■

Con lo anterior, podemos ampliar la caracterización de funciones sobreyectivas.

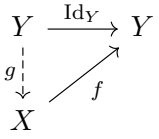
Teorema 2.2.12 — Caracterización Sobreyectiva II. Sea $f\colon X \to Y$ una función, entonces son equivalentes:

1. f es sobreyectiva.
2. Existe una función $g\colon Y \to X$ tal que $f \circ g = \mathrm{Id}_Y$.

Demostración. Supongamos que existe una función $g\colon Y \to X$ tal que $f \circ g = \mathrm{Id}_Y$, tomemos $y \in Y$, aplicando la ecuación anterior obtenemos

$$f(g(y)) = y$$

con $g(y) \in X$, obteniendo $y \in im(f)$, por tanto $im(f) = Y$, es decir f es sobreyectiva. Ahora consideremos a f sobreyectiva, entonces $im(f) = Y$, aplicando 2.2.11, con $im(\mathrm{Id}_Y) = Y = im(f)$



obteniendo $f \circ g = \mathrm{Id}_Y$. ■

Sea $f\colon X \to Y$ una función, entonces son equivalentes:

1. f es biyectiva.
2. f tiene inversa.
3. f tiene inversa y su inversa es biyectiva.

Ahora daremos algunos casos importantes de los teoremas de completación, usando las caracterizaciones de sobreyectivas e inyectivas.

Proposición 2.2.13 Dados $f\colon A \to B$ y $g\colon A \to C$ dos funciones, con f sobreyectivo. Entonces son equivalentes:

1. $\ker f \subseteq \ker g$.

2. Existe una única función $h\colon B \to C$ tal que $g = h \circ f$.

Más aún, las siguientes afirmacione son válidas:

1. Si $\ker f = \ker g$, entonces h es inyectivo.

Proposición 2.2.14 Dados $f\colon B \to A$ y $g\colon C \to A$, con g inyectiva. Entonces las siguientes afirmaciones son equivalentes:

1. $im(f) \subseteq im(g)$.
2. Existe una única función $h\colon B \to C$ tal que $f = g \circ h$.

Más aún, si $im(f) = im(g)$ entonces la función es sobreyectiva.

2.3. Relaciones de Orden.

Proposición 2.3.1 Dado $(P, \leq)$ una relación de orden. Entonces la relación inversa $\leq^{-1}$ es una relación de orden.

Demostración. Primero consideremos los siguientes hechos para una relación en general

1. Si $\Delta \subseteq R$ entonces $\Delta \subseteq R^{-1}$.
2. Si R es antisimétrica, usando que $(R^{-1})^{-1} = R$, entonces R^{-1} tambien es antisimétrica.
3. Si R es transitiva, entonces R^{-1} tambien es transitiva. Esto se ve como sigue, si $(a,b),(b,c) \in R^{-1}$ entonces $(c,b),(b,a) \in R$, pero R es transitiva entonces $(c,a) \in R$ por tanto $(a,c) \in R$.

Con todo lo anterior, se obtiene la afirmación. ■

Definición 2.3.1 — Orden dual. Si $(P, \leq)$ es un orden, definimos el orden dual $(P^d, \leq^d)$ como sigue:

1. $P^d = P$.
2. $\leq = \leq^{-1}$.

A la función $1_P^d\colon (P, \leq) \to (P^d, \leq^d)$ se le llama dualización.

■ **Ejemplo 2.9** Sea $X = \{1, 2, 4, 3, 5, 60\}$ y $\leq$ la relación de divisibilidad. ■

■ **Ejemplo 2.10** El orden lexicográfico en $A \times B$ se define como $(a_1, a_2) \leq_L (b_1, b_2)$ si y solo si $a_1 < b_1$ o $(a_1 = b_1$ y $a_2 \leq b_2)$. ■

Dado una propiedad, definición o teorema, definimos su dual como la propiedad, intercambiando $\leq$ por $\leq^d$.

Proposición 2.3.2 Principio de dualidad, para todo orden $(P, \leq)$ se tiene que:

$$((P^d)^d, (\leq^d)^d) \cong (P, \leq)$$

.

Definición 2.3.2 Dado $(P, \leq)$ un conjunto parcialmente ordenado.

1. Un elemento máximal es un elemento $m \in P$ tal que para cada $p \in P$ con $m \leq p$ implica que $m = p$.
2. Un máximo es un elemento $m \in P$ tal que para todo $p \in P$ implica $p \leq m$. Generalmente lo denotamos como $m = 1$.
3. Un elemento minimal es un elemento $m \in P$ tal que para cada $p \in P$ con $p \leq m$ implica que $p = m$.
4. Un mínimo es un elemento $m \in P$ tal que para todo $p \in P$ implica $m \leq p$. Generalmente lo denotamos como $m = 0$.
5. P es acotado si contiene un $1, 0$.

Definición 2.3.3 — Cota superior y Cota inferior. Sea $(P, \leq)$ un conjunto parcialmente ordenado y $S \subset P$. Definimos:

1. Una cota superior como un elemento $x \in P$ tal que $\forall s \in S$ se tiene que $s \leq x$. El conjunto de cotas superiores es denotado como S^u. Si S^u tiene un elemento minimal, este es llamado como **supremo** de S, y lo denotamos como $\bigvee S$.
2. Una cota inferior como un elemento $x \in P$ tal que $\forall s \in S$ se tiene que $x \leq s$. El conjunto de las cotas inferiores es denotado como S^l. Si S^l tiene un elemento maximal, este es llamado como **ínfimo** de S, y lo denotamos como $\bigwedge S$.

Definición 2.3.4 — Retícula. Un conjunto ordenado $(P, \leq)$ se llama retícula, si para cada pareja $a, b \in P$, existe su supremo e infimo. Denotamos $a \wedge b = inf\{a, b\}$ y $a \vee b = sup\{a, b\}$.

Teorema 2.3.3 — Propiedades de una retícula. Sea L una retícula, entonces las siguientes propiedades se cumplen:

1. $a \wedge a = a$, $a \vee a = a$.
2. $a \wedge b = b \wedge a$ y $a \vee b = b \vee a$.
3. $a \wedge (a \vee b) = a$ y $a \vee (a \wedge b) = a$.
4. $a \wedge (b \wedge c) = (a \wedge b) \wedge c$.

Además $a \leq b$ si y sólo si $a = a \wedge b$.

Vamos a ver como interactúan estos elementos bajo funciones. Primero hay que notar que si $(P, \leq_P)$ y $(Q, \leq_Q)$ son ordenes parciales no toda función $f\colon P \leq Q$ preserva el orden.

■ **Ejemplo 2.11** Consideremos $P = \{1, 2, 3, 4\}$ y $f\colon P \to P$ definido como sigue $f(1) = 1, f(2) = 4, f(3) = 1, f(4) = 1$ ■

Vale la pena, estudiar con funciones que preserven una relación.

Definición 2.3.5 Una función $f\colon (X, R) \to (Y, S)$ se dice que preserva relaciones si cada vez que $(a, b) \in R$ entonces $(f(a), f(b)) \in S$. Si las relaciones son de ordenes, a una función que preserva relaciones se le conoce como función creciente.

Hablemos de propiedades generales.

Proposición 2.3.4 Las siguientes afirmaciones son válidas:

1. Si $f\colon (P, R_P) \to (Q, R_Q)$, $g\colon (Q, R_Q) \to (T, R_T)$ son funciones que preservan en relaciones entonces $g \circ f\colon (P, R_R) \to (T, R_T)$ tambien preserva relaciones.
2. $\mathrm{Id}_P\colon (P, R) \to (P, S)$ preserva relaciones si y sólo si $R \subseteq S$

Proposición 2.3.5 Sea $f\colon (P, \leq_P) \to (Q, \leq_Q)$ una función creciente, entonces son válidos lo siguiente:

1. Si $S \subseteq P$ es un subconjunto vacio, tenemos:
   a) Para cada $p \in P$ cota superior (inferior) de S implica que $f(p) \in Q$ es una cota superior (inferior) de $f(P)$.
   b) Si existe $sup(S)$ y $inf(S)$ entonces:

$$sup(f(S)) \leq f(sup(S)),\ f(sup(S)) \leq sup(f(S)).$$

2.4. Relaciones de Equivalencia y Particiones.

Definición 2.4.1 — Particiones. Sea X un conjunto y $\mathcal{F}$ una familia de subconjuntos de X. Decimos que $\mathcal{F}$ es un subconjunto si:

1. $\bigcup \mathcal{F} = X$.
2. Si $A, B \in \mathcal{F}$ distintos entonces $A \cap B = \emptyset$.
3. Para todo $A \in \mathcal{F}$, $A \neq \emptyset$.

Proposición 2.4.1 Sea X un conjunto y $\sim$ una relación de equivalencia. Para cada $x \in X$ denotamos $[x] = \{a \in X |\ x \sim a\}$, entonces $\{[x] |\ x \in X\}$ es una partición en X. En particular tenemos que $a \sim b$ si y sólo si $[a] = [b]$.

Proposición 2.4.2 Sea X un conjunto y $\mathcal{F}$ una partición, definimos la siguiente relación, $a \sim b$ si y sólo si existe $A \in \mathcal{F}$ tal que $\{a, b\} \subseteq A$. Entonces $\sim$ es una relación de equivalencia.

Teorema 2.4.3 — Particiones y Equivalencias. Sea X un conjunto, definimos $Equi(X)$ el conjunto de todas las relaciones de equivalencia y $Part(X)$ el conjunto de todas las parciciones, entonces hay una biyección $Equi(X) \cong Part(X)$.

Proposición 2.4.4 Sea X un conjunto y R una relación de equivalencia, definimos el conjunto cociente de X módulo R como sigue:

$$X/R = \{[a] |\ a \in X\}$$

y definimos $p_R \colon X \to X/R$ como sigue $p_R(x) = [x]$. Entonces:

1. p_R es una función.
2. p_R es sobreyectivo.
3. $\ker p_R = R$.

Proposición 2.4.5 $p_R \colon X \to X/R$ es biyectivo si y sólo si $R = \triangle$.

Demostración. Si p_R es biyectivo, sabemos por definición que $\triangle \subseteq R$, ahora tomemos $(a, b) \in R$ entonces $p_R(a) = p_R(b)$, pero p_R es biyectivo entonces $a = b$ obteniendo $(a, b) \in \triangle$. Conversamente si $R = \triangle$ entonces claramente p_R es inyectivo, por lo tanto p_R es biyectivo. ■

Proposición 2.4.6 Sea $f \colon (X, R) \to (Y, S)$ una función que preserva relaciones de equivalencia, entonces existe una única función $\hat{f} \colon X/R \to Y/S$ tal que el siguiente diagrama conmuta:

$$\begin{array}{ccc} X & \xrightarrow{f} & Y \\ {\scriptstyle p_R}\downarrow & & \downarrow{\scriptstyle p_S} \\ X/R & \xrightarrow[\hat{f}]{} & Y/S \end{array}$$

Demostración. Sea $(a, b) \in \ker p_R = R$,como f preserva relaciones, entonces $(f(a), f(b)) \in S$, obteniendo $p_S \circ f(a) = p_S \circ f(b)$, es decir $(a, b) \in \ker p_S \circ f$, entonces por 2.2.10 existe una función $\hat{f} \colon X/R \to Y/S$ tal que $p_R \circ f = \hat{f} \circ p_R$, y como p_R es sobreyectiva entonces $\hat{f}$ es único. ■

Teorema 2.4.7 — Teorema conjuntista de Noether. Sea $f \colon X \to Y$ entonces existe una única biyección entre $X/\ker(f) \cong im(f)$ tal que el siguiente diagrama conmuta:

$$\begin{array}{ccc} X & \xrightarrow{f} & Y \\ {\scriptstyle p_R}\downarrow & & \uparrow \\ X/\ker(f) & \xrightarrow[\cong]{} & im(f) \end{array}$$

Demostración. Notemos que f preserva las siguientes relaciones $f\colon (X, \ker(f)) \to (Y, \triangle_Y)$, entonces por la proposición anterior existe una única función $h_1\colon X/\ker(f) \to Y$ tal que el siguiente diagrama conmuta:

$$\begin{array}{ccc} X & \xrightarrow{f} & Y \\ {\scriptstyle p_R}\downarrow & \nearrow_{h_1} & \\ X/\ker(f) & & \end{array}$$

Usando el teorema 2.2.11 tenemos que $im(f) \subseteq im(h_1)$, luego si $a \in im(h_1)$ entonces existe $[x] \in X/\ker(f)$ tal que $h_1([x]) = a$, es decir $f(x) = a$, obteniendo que $a \in im(f)$ y por tanto $im(f) = im(h_1)$, luego como la función inclusión $im(f) \to Y$ es inyectiva, entonces por 2.2.11 existe una única función $\phi\colon X/\ker(f) \to im(f)$ tal que el siguiente diagrama conmuta:

$$\begin{array}{ccc} X & \xrightarrow{f} & Y \\ {\scriptstyle p_R}\downarrow & \nearrow_{h_1} & \uparrow \\ X/\ker(f) & \xrightarrow[\phi]{} & im(f) \end{array}$$

Ahora, notemos que h_1 es inyectiva, pues si $h_1([x]) = h_1([y])$ entonces $f(x) = f(y)$ obteniendo que $(x, y) \in \ker(f)$ y por tanto $[x] = [y]$. Gracias a que h_1 es inyectiva y que $im(f) = im(h_1)$ entonces usando 2.2.11 se tiene que existe una única función $\psi\colon im(f) \to X/\ker(f)$ tal que el siguiente diagrama conmuta:

$$\begin{array}{ccc} X & \xrightarrow{f} & Y \\ {\scriptstyle p_R}\downarrow & \nearrow_{h_1} & \uparrow \\ X/\ker(f) & \xleftarrow[\psi]{} & im(f) \end{array}$$

Entonces por unicidad de las construcciones obtenemos que $\psi \circ \phi = \mathrm{Id}_{X/\ker(f)}$ y $\phi \circ \psi = \mathrm{Id}_{im(f)}$, mostrando la biyección $X/\ker(f) \cong im(f)$. ■

2.5. El producto infinito.

Fijemos $\{A_i\}_{i\in I}$ una familia no vacia de conjuntos. Debido a 2.2.9 podemos definir una noción de coordenadas de tamaño I como sigue. La idea principal es:

$$(a_i)_{i\in I} \Leftrightarrow \ a_i \in A_i$$

Entonces dado $f\colon I \to \bigcup_{i\in I} X_i$ como en 2.2.9, notemos que para cada $i \in I$ $f(i) \in A_i$, entonces f se puede pensar como una coordenada para el producto de las A_i's. Obteniendo la siguiente definición:

Definición 2.5.1 — Producto cartesiano. El producto cartesiano de las $\{A_i\}_{i\in I}$ es el conjunto:

$$\prod_{i\in I} A_i := \left\{ f\colon I \to \bigcup_{i\in I} A_i \mid \ f(i) \in X_i, \ \forall i \in I \right\}$$

Como abuso de notación, dado $f \in \prod_{i\in I} A_i$ denotamos $(a_i)_{i\in I}$ en donde $a_i := f(i)$.

■ **Ejemplo 2.12** Dados A_1, A_2, A_3 conjuntos, entonces un elemento $f \in \prod_{i\in I} A_i$ es una función de la forma

$$f\colon \{1, 2, 3\} \to A_1 \cup A_2 \cup A_3$$

con la propiedad de que $a_1 = f(1) \in A_1$, $a_2 = f(2) \in A_2$ y $a_2 \in A_3$ y con esto dandole sentido a la terna ordenada (a_1, a_2, a_3) como la función f. Se deja al lector comparar esto con la definición de producto cartesiano binario y encontrar similitudes. ∎

∎ **Ejemplo 2.13** Sean A, B conjuntos, consideremos $I := \{1, 2\}$, denotemos $A_1 = A$ y $A_2 = B$ entonces existe una biyección:

$$\prod_{i \in I} A_i \to A \times B$$

con la propiedad $f \leftrightarrow (f(1), f(2)) = (a, b)$. ∎

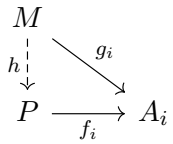
Vamos ahora a dar una caracterización alternativa al producto cartesiano. Para cada $i_0 \in I$ definimos la i_0-ésima proyección canónica como sigue

$$\pi_{i_0} \colon \prod_{i \in I} A_i \to A_{i_0}, \ \pi_{i_0}(f) = f(i_0)$$

Con esta familia de funciones obtenemos una caracterización del producto cartesiano, tambien llamada **propiedad universal del producto**.

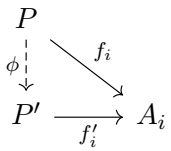
Definición 2.5.2 — Propiedad universal del producto. Sea P un conjunto y $\{f_i \colon P \to A_i\}_{i \in I}$ una familia de funciones indexadas por I. Decimos que la pareja $(P, \{f_i\}_{i \in I})$ satisface la propiedad universal del producto de las $\{A_i\}_{i \in I}$ si cumple lo siguiente:

- Para todo conjunto M y familia de funciones $\{g_i \colon M \to A_i\}$ existe una única función $h \colon M \to P$ tal que para toda $i \in I$, el siguiente diagrama conmuta:



Una cualidad de la definición anterior es que si dos parejas satisfacen la propiedad universal del producto para las mismas $\{A_i\}_{i \in I}$ entonces son .ªencialmente"lo mismo.

Proposición 2.5.1 La propiedad universal del producto es única salvo biyecciones. Es decir si $(P, \{f_i\}_{i \in I})$ y $(P', \{f'_i\}_{i \in I})$ satisfacen la propiedad universal del producto para la familia de conjuntos $\{A_i\}_{i \in I}$ entonces existe una única biyección $\phi \colon P \to P'$ tal que para toda $i \in I$ el siguiente diagrama conmuta:



Teorema 2.5.2 — Caracterización Categórica del producto cartesiano. La pareja $(\prod_{i \in I} A_i, \{\pi_i\}_{i \in I})$ satisface la propiedad universal del producto.

∎ **Ejemplo 2.14** Consideremos los conjuntos A, B, C, sea $P := (A \times B) \times C$, y las siguientes funciones:

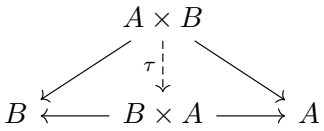
1. $\pi_A((a, b), c) = a$.
2. $\pi_B((a, b), c) = b$.
3. $\pi_C((a, b), c) = c$.

Entonces $(P, \{\pi_A, \pi_B, \pi_C\})$ satisface la propiedad universal del producto de las A, B, C y por lo tanto existe una única biyección entre P y $\prod_{i \in \{1,2,3\}} A_i$. En donde $A_1 = A$, $A_2 = B$ y $A_3 = C$. Mostrando que:

$$A \times B \times C \cong (A \times B) \times C$$

■

■ **Ejemplo 2.15** Hay que dar una advertencia ante esta caracterización, pues la caracterización es que un conjunto con una familia puede ser biyectivamente el producto cartesiano. Pero no necesariamente son lo mismo. Por ejemplo, con la propiedad universal se garantiza que existe una única biyección $\tau\colon A \times B \to B \times A$ tal que el siguiente diagrama conmuta:



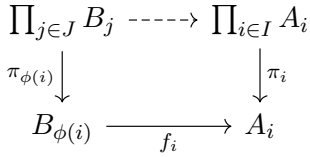
¿Que hace esta biyección? Esta función invierte las parejas ordenadas, de hecho está definido como sigue:

$$\tau(a, b) = (b, a)$$

Pero, en terminos de la igualdad de conjuntos, se sabe que $A\times B$ y $B\times A$ son completamente distintos cuando $A \neq B$, ver 1.5.3. Por razones como esta, la propiedad universal del producto es una caracterización salvo biyecciones, o coloquialmente te dice cuales conjuntos se pueden organizar para verse .[es]cencialmenteçomo un producto. ■

A continuación realizaremos algunas construcciones adicionales relacionados con el producto cartesiano y su propiedad universal.

Funciones inducidas por la propiedad universal del producto Fijemos $\{A_i\}_{i\in I}$ y $\{B_j\}_{j\in J}$ dos familias no vacias de conjuntos y $\phi\colon I \to J$ una función entre los índices. Para cada $i \in I$ tenemos una función $f_i\colon B_{\phi(i)} \to A_i$, aplicando la propiedad universal del producto de las $\{A_i\}_{i\in I}$ para la pareja $(\prod_{j\in J} B_j, \{f_i \circ \pi_{\phi(i)}\}_{i\in I})$ entonces induce una única función $\prod_{j\in J} B_j \to \prod_{i\in I} A_i$ tal que para toda $i \in I$ el siguiente diagrama conmuta:



Dicha función lo denotaremos como $\prod_{i\in I}^{\phi} f_i$, usando el diagrama conmutativo anterior, podemos deducir que esta función se define como sigue:

$$\left(\prod_{i\in I}^{\phi} f_i\right)(b_j)_{j\in J} = (f_i(b_{\phi(i)}))_{i\in I}.$$

Ademas cuando $I = J$ y $\phi = \mathrm{Id}_I$ entonces simplemente lo denotamos como $\prod_{i\in I} f_i$, más aún si $I = \{1, \cdots, n\}$ es finito entonces podemos denotarlo como $\prod_i f_i = f_1 \times \cdots \times f_n$.

Proposición 2.5.3 Las siguientes afirmaciones son válidas:

1. $\prod_{i\in I} \mathrm{Id}_{A_i} = \mathrm{Id}_{\prod_{i\in I} A_i}$.
2. Si $\phi\colon I \to J$, $\psi\colon J \to T$, $\{f_i\colon B_{\phi(i)} \to A_i\}_{i\in I}$, $\{g_j\colon C_{\psi(j)} \to B_j\}_{j\in J}$ son funciones, entonces

$$\prod_{i\in I}^{\psi\circ\phi} (f_i \circ g_{\phi(i)}) = \prod_{i\in I}^{\phi} f_i \circ \prod_{j\in J}^{\psi} g_j.$$

3. En particular si ϕ es una biyección y las f_i son biyecciones, se tiene la biyección canónica:

$$\prod_{i\in I}^{\phi} f_i \colon \prod_{i\in I} A_i \to \prod_{j\in J} B_j$$

■ **Ejemplo 2.16** Con la afirmación anterior, podemos dar una demostración alternativa a que hay una biyección canonica $A \times B \cong B \times A$. Para ello, definimos $\phi\colon \{1,2\} \to \{2,1\}$ como $\phi(1) = 2$ y $\phi(2) = 1$, denotamos $A_1 = A$, $A_2 = B$, $B_1 = B$ y $B_2 = A$, entonces definimos $f_1 = \mathrm{Id}_A$ y $f_2 = \mathrm{Id}_B$, entonces como ϕ, f_1, f_2 son biyecciones obtenemos por la afirmación anterior, la biyección canónica:

$$A \times B \cong B \times A$$

Este razonamiento se puede generalizar como sigue:

- Sea $\sigma\colon I \to I$ una biyección entre un conjunto no vacio, entonces existe una biyección canónica:

$$\prod_{i\in I} A_i \cong \prod_{i\in I} A_{\sigma(i)}.$$

  Denominando a esta propiedad como la **conmutatividad generalizada** del producto.

■

2.6. Ejercicios

2.6.1. Relaciones

1. Para cada relación R, encuentra su dominio, rango y campo.
   a) $X = \{1,2,3,4,5,6\}$ y R es la pareja de números cuya suma dan 7.
   b) X un conjunto no vacio y $R = \triangle$.
   c) A el conjunto de alumnos y B los números del 1 al 10 y R la relación es asignar una nota de alumnos en la materia.
   d) R asignar el valor de un producto. ¿Quienes son los conjuntos A y B adecuados?.
   e) A el conjunto de almuerzos preparados en una casa especifica y B el conjunto de hijos de una familia especifica. R es darle el almuerzo al hijo.
   f) R el precio de una casa en una zona de la ciudad de México. ¿Quienes son los conjuntos A y B adecuados?-
2. Del ejercicio anterior ¿Qué relaciones son funciones? Argumenta.
3. Sea R una relación en $A \times B$ y X_1, X_2 subconjuntos de A. Demuestra que:
   a) $R(X_1 \cup X_2) = R(X_1) \cup R(X_2)$.
   b) $R(X_1 \cap X_2) \subseteq R(X_1) \cap R(X_2)$.
   c) $R(X_1) - R(X_2) \subseteq R(X_1 - X_2.)$
4. Consideremos $C = \{(x,y) \in \mathbb{R} \times \mathbb{R} |\ x^2 + y^2 = 1\}$, pensado como relación. Responde:
   a) ¿Es Reflexiva?
   b) ¿Es simétrico?
   c) ¿Es transitivo?
   d) Calcula la menor relación de equivalencia que contiene a C y describelo.
5. Sea $R \subseteq X \times Y$, demuestra que $(R^{-1})^{-1} = R$.
6. Sea $\{R_i\}_{i\in I}$ una familia de relaciones, demuestra que $(\bigcap_{i\in I} R_i)^{-1} = \bigcap_{i\in I} R_i^{-1}$.
7. Fija X un conjunto, estudiaremos relaciones en X, es decir subconjuntos de la forma $R \subseteq X \times X$.
   a) Demuestra que si $\{R_i\}_{i\in I}$ es una familia de relaciones simétricas, demuestra que $\bigcap_{i\in I} R_i$ es una relación simétrica.

b) Sea $A \subseteq X \times X$ una relación, definimos la simetrización (Usando el teorema visto en clase) de A como sigue:

$$S(A) := \bigcap \{R |\ R \text{ es simétrico, } A \subseteq R\}$$

Encuentra $S(A)$ en donde $X = \{a, b, c, d\}$ y $A = \{(a, b), (a, c), (b, d)\}$.

2.6.2. Funciones.

1. Sea $A \subseteq X$ y $f\colon X \to Y$ una función y $i\colon X \to Y$ la función inclusión. Demuestra que:
   a) $f|_A = f \circ i$.
   b) Denotemos $g = f|_A$. Muestra que para todo $B \subseteq Y$, se cumple que $g^{-1}(B) = A \cap f^{-1}(B)$.
2. Consideremos $X = \mathbb{R} = Y$ y sea C una curva suave sin autointersecciones (por ejemplo una circunferencia). ¿Porque es imposible definir subconjuntos de X y Y tales que C pensado como relación pueda ser una función? ¿Porque con una parabola horizontal si se puede? Argumenta.
3. Sea $\{[-n, n]\}_{n\in\mathbb{N}}$ una familia de subintervalos. Resuelve:
   a) Demuestra que $\bigcap_{n\in\mathbb{N}}[-n, n] = \{0\}$.
   b) Considera $f\colon \mathbb{R} \to \mathbb{R}$ dado como $f(x) = \sin(2kx)$. Muestra que la función asi como es definida no es inyectiva ni sobreyectiva.
   c) Calcula $f\left(\bigcap_{n\in\mathbb{N}}[-n, n]\right)$.
   d) Calcula $\bigcap_{n\in\mathbb{N}} f([-n, n])$. ¿El conjunto coincide con el conjunto anterior?
4. Consideremos $f\colon X \to Y$ una función, demuestra lo siguiente:
   a) Si $A \subseteq B \subseteq X$ entonces $f(B) - f(A) \subseteq f(B - A)$.
   b) Si $C \subseteq D \subseteq Y$ entonces $f^*(D) - f^*(C) = f^*(D - C)$.
   c) Si $\{B_i\}_{i\in I}$ son subconjuntos de Y entonces $f^*\left(\bigcap_{i\in I} B_i\right) = \bigcap_{i\in I} f^*(B_i)$.
   d) Si $A \subseteq X$ entonces $A \subseteq f^*(f(A))$.
   e) Si $B \subseteq Y$ entonces $B \cap f(X) = f(f^*(B))$.
5. Consideremos $f\colon A \to B$ y $g\colon B \to C$ funciones. ¿Cierto o falso?
   a) Si $g \circ f$ es sobreyectiva entonces g es sobreyectiva.
   b) Si $g \circ f$ es inyectiva entonces f es inyectiva.
   c) Si f es inyectiva entonces $g \circ f$ es inyectiva.
   d) Si $g \circ f$ es biyectiva entonces f y g es inyectiva.
6. ¿Porqué para cualquier función $f\colon \{a, b, c\} \to \{1, 2, 3, 4, 5\}$ no puede tener una inversa derecha? Argumenta tu respuesta.
7. Considera $f\colon \{1, 2\} \to \{1, 2, 3\}$ una función inyectiva. ¿Es posible que la inversa izquierda de f coincida con la relación inversa? Argumenta.
8. Asumiendo el axioma de elección. Consideremos a $f\colon X \to Y$ como una función. Resuelve:
   a) Muestra que si existe su inversa derecha y su inversa izquierda entonces estos son iguales. Dicho de manera coloquial, solo tiene un inverso.
   b) Da un contra ejemplo de una función que solo tenga inversas izquierdas y no sean únicas. (Hint: Usa una función inyectiva de la forma $f\colon \{a, b\} \to \{1, 2, 3\}$)
   c) Muestra que si f tiene inversa derecha e izquierda entonces f es biyectiva.
9. Sea $f\colon X \to Y$ una función, demuestra que f es inyectiva si y sólo si para todo A, B subconjuntos de X se cumple que $f(A \cap B) = f(A) \cap f(B)$.
10. Sea $f\colon X \to Y$ una función, demuestra que f es inyectiva si y sólo si $\ker = \triangle_X$.

2.6.3. Relaciones de orden

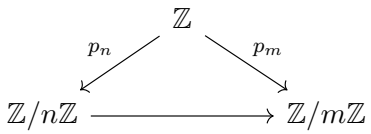
1. Sea P un orden parcial con supremos e infimos. Para $x, y \in P$ demuestra que son equivalentes:
   a) $x \leq y$.

   b) $x = x \wedge y$.
   c) $y = x \vee y$.
2. Sean $(X, \leq_X), (Y, \leq_Y)$ dos relaciones de orden. Construye la menor relación de orden $\leq$ en $X \times Y$ tal que las proyecciones $\pi_X \colon X \times Y \to X$ y $\pi_Y \colon X \times Y \to Y$ son crecientes.
3. Sea $X = \{a, b, c, d\}$, resuelve:
   a) Determina todos los órdenes en donde a y b no sean comparables.
   b) ¿Cuantos órdentes totales tiene X?
4. Sea $A = \mathbb{N} \times \mathbb{N}$ junto al orden lexicográfico. Determina si son ciertas o falsas:
   a) $(2, 15) \leq (3, 2)$.
   b) $(16, 1) \leq (15, 112)$.
   c) $(3, 12) \leq (3, 10)$.
5. Sea P un conjunto ordenado con supremos y tomemos $a, b, c \in P$ demuestra que $\sup\{a, b, c\} = (a \vee b) \vee c$.

2.6.4. Relaciones de Equivalencia

.

1. Consideremos $f \colon X \to Y$ una función. Resuelve:
   a) Demuestra que $\ker f$ es una relación de equivalencia. A cada clase le llamaremos la fibra de f.
   b) Decimos que f tiene fibras iguales si toda fibra tiene el mismo número de elementos. Muestra que una función sobreyectiva de la forma $f \colon \{1, 2, 3, 4, 5\} \to \{1, 2\}$ nunca puede tener dicha propiedad.
   c) Supongamos que X tiene n elementos y Y tiene m elementos, si $f \colon X \to Y$ tiene fibras iguales entonces m divide a n.
2. Consideremos $\mathbb{Z}$ el conjunto de todos los numeros enteros. Resuelve:
   a) Fija $n \in \mathbb{Z}^+$ un numero natural. Definimos la siguiente relación en $\mathbb{Z}$, $x \sim y$ si existe $c \in \mathbb{Z}$ tal que $x - y = nc$. Demuestra que esta relación es de equivalencia.
   b) Denotemos al conjunto cociente como $\mathbb{Z}/n\mathbb{Z}$. Demuestra que es un conjunto finito. Más precisamente ¿Cuantás clases de equivalencia tiene?.
   c) Dados $n, m \in \mathbb{Z}^+$. Demuestra que existe una función $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ tal que el siguiente diagrama conmuta:



      Si y sólamente si $n \leq m$.
3. Consideremos $X = [0, 1]$ el intervalo cerrado. Resuelve
   a) Definimos en X la siguiente relación, $x \sim y$ si $|x - y| = 1$ ó $x = y$. Demuestra que la relación es de equivalencia.
   b) Sea $Y = \{(x, y) \in \mathbb{R}^2 |\ x^2 + y^2 = 1\}$ la circunferencia. Demuestra que $f \colon X \to Y$ definido como $f(t) = (\cos(2\pi t), \sin(2\pi t))$ es una función sobreyectiva.
   c) Describe $\ker f$.
   d) Demuestra, usando la tecnica de completación de diagramas que $X/\sim$ esta en correspondencia biyectiva con Y. (Hint: Completa el diagrama usando f del ejercicio y p la proyección canonica de la relación.)
4. Determine si la relación es de equivalencia y en caso de serlo describir la partición.
   a) $n \sim m$ en $\mathbb{Z}$ si $nm \geq 0$.
   b) $n \sim m$ en $\mathbb{Z}$ si $x^2 + y^2 = 9$.

c) $n \sim m$ en $\mathbb{Q}$ si nm es un entero.

5. Sea X un conjunto no vacio, demuestra que si R es una relación de equivalencia de X entonces $R = \ker f$ para alguna función.
6. Fijemos X un conjunto no vacio. Demuestra que hay una biyección entre el conjunto de las funciones sobreyectivas de $f\colon X \to Y$ y el conjunto de las relaciones de equivalencia de X. ¿Cuántas relaciones de equivalencia tiene $X = \{a, b, c\}$?.
7. Sea $X = \{a, b, c, d, e, f\}$ y consideremos las particiones $\{\{a\}, \{c, b\}, \{d, e, f\}\}$ y $\{\{a, b, c, d\}, \{e, f\}\}$ y sean R_1, R_2 sus relaciones de equivalencia inducidas. Si R es la relación de equivalencia generada por $R_1 \cup R_2$, descibre su partición.

Capítulo 3

Los números naturales, sus estructuras y aplicaciones.

La historia de la axiomatización y construcción de los números naturales se remonta a la antigua Grecia, con los trabajos de Euclides en su libro .Elementos". En este libro, Euclides establece un conjunto de axiomas y postulados a partir de los cuales deduce toda la geometría.

En el siglo XIX, los matemáticos comenzaron a buscar una axiomatización similar para la aritmética. Uno de los primeros intentos fue el de Richard Dedekind, quien en 1888 definió los números naturales como los subconjuntos de los conjuntos enteros que tienen un elemento inicial y un sucesor.

En 1889, Giuseppe Peano publicó su obra .Arithmetices Principia Nova Methodo Exposita", en la que presenta una axiomatización de los números naturales basada en cinco axiomas y un símbolo indefinido. Los axiomas de Peano son los siguientes:

- 0 es un número natural.
- Si n es un número natural, entonces n + 1 es un número natural.
- Si n es un número natural, entonces n + 1 es distinto de 0.
- Si n y m son números naturales, entonces n + m es igual a m + n.
- Si n es un número natural, entonces n + 0 es igual a n.

El símbolo indefinido de Peano es el símbolo "S", que representa la operación de sucesor. Los axiomas de Peano se pueden utilizar para demostrar todos los teoremas de la aritmética básica.

En la actualidad, la axiomatización de Peano es la más aceptada por los matemáticos. Sin embargo, existen otras axiomatizaciones posibles, como la de Zermelo-Fraenkel, que se utiliza en la teoría de conjuntos.

La construcción de los números naturales a partir de los axiomas de Peano se puede realizar de la siguiente manera:

- Se define el número 0 como un número natural.
- Se define el número 1 como el sucesor de 0.
- Se define el número 2 como el sucesor de 1.
- Se define el número 3 como el sucesor de 2.
- Recursivamente

De esta manera, se puede construir un conjunto infinito de números naturales, cada uno de los cuales es el sucesor del anterior. La axiomatización y construcción de los números naturales es un hito importante en la historia de las matemáticas. Gracias a ella, la aritmética se ha convertido en una teoría sólida y consistente. La axiomatización de los naturales usando los axiomas ZF es una construcción más abstracta que la axiomatización de Peano. Sin embargo, tiene la ventaja de ser más general, ya que no requiere la existencia de un conjunto inicial, como el número 0. Además, la axiomatización de los naturales usando

los axiomas ZF es más consistente que la axiomatización de Peano. Esto se debe a que los axiomas ZF no permiten la construcción de conjuntos infinitos de conjuntos, que podrían conducir a paradojas.

3.1. Cardinalidad.

Para estas notas, nosotros usaremos la axiomatización de los números naturales usando ZF y daremos además una construcción de las operaciones usando una versión moderna de los axiomas de Peano, llamada Sistemas de Peano.

Definición 3.1.1 — Cardinalidad. Sean X, Y dos conjuntos, decimos que X tiene la misma cardinalidad que Y (tambien suelen decirse que X es equipotente a Y o que los conjuntos X, Y son equipotentes) si existe una función biyectiva $f\colon X \to Y$. En esta situación, lo denotamos como $|X| = |Y|$.

Proposición 3.1.1 Sean X, Y, Z conjuntos, entonces las siguientes afirmaciones son ciertas:

1. $|X| = |X|$.
2. Si $|X| = |Y|$ entonces $|Y| = |X|$.
3. Si $|X| = |Y|$ y $|Y| = |Z|$ entonces $|X| = |Z|$.

Demostración. Para la primera parte, consideremos $\mathrm{Id}_X\colon X \to X$, esta función claramente es biyectiva, por tanto $|X| = |X|$. Para la segunda parte, por hipótesis, existe una función biyectiva $f\colon X \to Y$, entonces por 2.2 tenemos que su inversa $g\colon Y \to X$ es biyectiva, por tanto $|Y| = |X|$. Por último, se tiene por hipótesis que existen funciones biyectivas $f\colon X \to Y$ y $g\colon Y \to Z$, entonces $g \circ f\colon X \to Z$ es biyectiva, concluyendo que $|X| = |Z|$. ■

Vamos a empezar a ver bases para çontar". Primero por los axiomas de Z.F. tenemos que existen los siguientes conjuntos de manera recursiva

1. $A_0 := \emptyset$
2. Si A_n está definido, entonces $A_{n+1} = A_n \cup \{A_n\}$.

Definición 3.1.2 — Los números naturales.

1. Denotamos $\mathbb{N}$ como el conjunto de todas las A_n definidas anteriomente.
2. Decimos que un conjunto X es finito si existe un $A_n \in \mathbb{N}$ tal que X es equipotente a A_n. Más aún, denotamos $n = |X|$. En caso contrario decimos que X es un conjunto infinito.

La existencia "formal"de los conjuntos naturales se debe al axioma de comprensión y el axioma de infinitud. Cosa que no demostraremos en estas notas. Sin embargo enfatizaremos el siguiente hecho:

1. Si A es un número natural, entonces al número natural $A \cup \{A\}$ lo denominamos como el sucesor de A y se puede escribir como $S(A)$. Por ejemplo $S(0) = 1$, $S(1) = 2$.

Definición 3.1.3 — Conjunto inductivo.. Un conjunto A se le llama inductivo si satisface las siguientes propiedades:

1. $0 \in A$.
2. Si $x \in A$ entonces $S(x) \in A$.

Como consecuencia:

Proposición 3.1.2 Si A es un conjunto inductivo, entonces $\mathbb{N} \subseteq A$.

Demostración. Sea $n \in \mathbb{N}$ por construcción, se tiene la cadena de numeros naturales:

$$0 \subseteq 1 \subseteq \cdots \subseteq n$$

por definición de conjunto inductivo, se tiene $0 \in A$, y luego $1 \in A$, recursivamente, llegamos a que $n \in A$, por lo tanto $\mathbb{N} \subseteq A$. ■

Teorema 3.1.3 — Principio de Inducción. Sea $P(x)$ una propiedad con valores en los números naturales, tales que:

1. $P(0)$ se satisface.
2. Si $P(n)$ se satisface entonces $P(S(n))$ tambien se satisface.

Por lo tanto $P(n)$ se satisface para todos los números naturales.

Demostración. Esto se sigue de que $A = \{n \in \mathbb{N} |\ P(n) \text{ se satisface}\} \subseteq \mathbb{N}$ es un conjunto inductivo. ■

Proposición 3.1.4 Para todo número natural, se tiene que $n \notin n$.

Proposición 3.1.5 Si $S(n) = S(m)$ entonces $n = m$.

Proposición 3.1.6 Para todo natural $n \in \mathbb{N}$ se tiene que $S(n) = \{0, 1, \cdots, n\}$.

Demostración. Procesdemos por inducción, para $n = 0$ se tiene $S(0) = 0 \cup \{\emptyset\} = \{0\}$. Supongamos por hipótesis de inducción que $S(n) = \{0, 1, 2, \cdots, n\}$ para alguna $n \in N$, sea $m = S(n)$ entonces por definición $S(m) = m \cup \{m\} = \{0, 1, \cdots, n\} \cup \{m\}$ obteniendo

$$S(m) = \{0, \cdots, m\}$$

Como $m = S(n)$ tambien satisface la afirmación, por principio de inducción concluyes que la afirmación se cumple para toda $n \in \mathbb{N}$. ■

Usando la descripción anterior tenemos el siguiente resultado interesante que cumplen solo los conjuntos finitos.

Proposición 3.1.7 Si $f : n \to n$ es inyectiva entonces f es biyectiva

Demostración. Supongamos que es válido para $n = 1$ entonces si $f : 1 \to 1$ es una función, por definición de función esta función en particular es inyectiva y sobreyectiva por lo tanto f es biyectiva. Supongamos por hipótesis de inducción que la afirmación es válida para alguna $n \in \mathbb{N}$, ahora para $m = S(n)$, y consideremos $f : m \to m$ una función inyectiva, basta ver que es sobreyectiva. Tenemos dos casos importantes:

1. Caso I $f(n) \subseteq n$, es este caso me permite definir una función $\hat{f} : n \to n$ tal que el siguiente diagrama conmuta:

$$\begin{array}{ccc} m & \xrightarrow{f} & m \\ \uparrow & & \uparrow \\ n & \xrightarrow[\hat{f}]{} & n \end{array}$$

   Esto implica que $\hat{f}$ es inyectiva, pero por hipótesis de inducción, tenemos que $\hat{f}$ es sobreyectiva. Pero ya que para toda $k \leq n$ se cumple que

$$f(k) = \hat{f}(k)$$

   y que $f(m) = m$ por hipótesis del caso I, entonces f es biyectiva.
2. Caso II $f(n) \not\subseteq n$, entonces existe una $k \leq n$ tal que $f(k) = m$, como f es inyectiva, se tiene que $f(m) = w$ para alguna $w \in n$

■

Sea X un conjunto finito y $f : X \to X$ una función inyectiva, entonces f es biyectiva.

Demostración. Como X es finito, entonces existe un conjunto natural n tal que $X \cong n$ y entonces existe una única función $\hat{f}\colon n \to n$ tal que el siguiente diagrama conmuta:

$$\begin{array}{ccc} X & \xrightarrow{f} & X \\ {\scriptstyle\cong}\downarrow & & \downarrow{\scriptstyle\cong} \\ n & \xrightarrow[\hat{f}]{} & n \end{array}$$

Ahora si $f\colon X \to X$ es inyectiva, entonces $\hat{f}$ es inyectiva y por la afirmación anterior $\hat{f}$ es biyectiva, concluyendo que f es biyectiva. ■

Dicho resultado anterior se puede reformular como sigue:

Proposición 3.1.8 Sea X un conjunto finito y $f\colon X \to X$ una función, entonces son equivalentes:
1. f es inyectiva.
2. f es sobreyectiva.

Demostración. Si f es inyectiva, por la afirmación anterior entonces f es biyectiva, en particular f es sobreyectiva. Conversamente si f es sobreyectiva, por la caracterización de funciones sobreyectivas 2.2.12, tenemos que existe $g\colon X \to X$ tal que $f \circ g = \mathrm{Id}_X$ y por la caracterización de funciones inyectivas 2.2.6 tenemos que g es inyectiva y por la afirmación anterior se tiene que g es biyectiva y entonces f es también biyectiva, en particular f es inyectiva. ■

Si $f\colon X \to X$ es una función inyectiva con $im(f) \subset X$ como subconjunto propio, entonces X es infinito.

Demostración. Supongamos por contradicción que X es finito y existe una función $f\colon X \to X$ inyectiva con $im(f)$ como subconjunto propio de X, entonces f no es sobreyectiva, pero eso contradice la afirmación anterior, completando la prueba. ■

Por ultimo presentaremos variantes del principio de Inducción que son útiles para demostraciones.

Proposición 3.1.9 — Principio de Inducción sobre k. Sea $P(n)$ una propiedad sobre los naturales, fijemos $k \in \mathbb{N}$, y supongamos que las siguientes afirmaciones se cumplen:
1. $P(k)$ lo satisface.
2. Si para alguna $n \geq k$ $P(n)$ se satisface entonces $P(S(n))$ se satisface.

Entonces para toda $n \geq k$, se satisface $P(n)$.

Proposición 3.1.10 — Principio de Inducción modificado.. Sea $P(n)$ una propiedad sobre los naturales tales que:
1. $P(0)$ se satisface.
2. Si para alguna $n \in\in \mathbb{N}$, se tiene que $P(k)$ se satisface para toda $k \in \{0, 1, \cdots, n\}$ entonces $P(n+1)$ se satisface.

Entonces para toda $n \in \mathbb{N}$, se satisface $P(n)$.

3.2. El buen orden.

Definición 3.2.1 — Conjunto bien ordenado. Sea $(P, \leq)$ un orden, decimos que esta bien ordenado si para todo subconjunto no vacio $B \subseteq P$ tiene mínimo.

Proposición 3.2.1 Sea P un conjunto bien ordenado. Entonces:
1. P tiene un orden lineal, es decir para todo $x, y \in P$, entonces solo se cumple una de las siguientes afirmaciones:

   a) $x < y$.
   b) $x = y$.
   c) $y < x$.
2. Para todo $x \in P$ existe un elemento $s(x) \in P$ con la siguientes propiedades:
   a) $x \neq s(x)$ y $x < s(x)$.
   b) Si $y \in P$ es tal que $x \leq y \leq s(x)$ entonces $x = y$ ó $y = s(x)$.

   A este elemento lo llamamos el elemento sucesor de x con respecto al orden de P.
3. Para toda función creciente e inyectiva $f\colon P \to P$ es la identidad, es decir $f = \mathrm{Id}_P$.

Definición 3.2.2 Definimos el siguiente orden en los naturales $\mathbb{N}$ como sigue: $n \leq m$ si y sólo si $n \in m$ ó $n = m$.

Proposición 3.2.2 Las siguientes afirmaciones son equivalentes:
1. $(\mathbb{N}, \leq)$ esta bien ordenado.
2. El principio de inducción se cumple.

Teorema 3.2.3 — El orden de los naturales. El conjunto $(\mathbb{N}, \leq)$ es un buen orden. Además para todo natural n, el sucesor $s(n)$ es el elemento sucesor de n con respecto al orden definido.

3.3. Sistemas de Peano.

Con toda la construcción de las secciones anteriores podemos axiomatizar las operaciones de los naturales y mostrar que los naturales son caracterizados por las propiedades de la definición de un sistema de Peano, es decir, axiomatizar la existencia de los números naturales.

Definición 3.3.1 — Sistemas de Peano.. Un sistema de Peano es una terna (N, a, s) en donde N es un conjunto $a \in N$ y $s\colon N \to N$ una función tal que:
1. $a \notin im(s)$.
2. s es inyectiva.
3. (Principio de Inducción Abstracto) Para cada $T \subseteq N$, si:
   a) $a \in T$.
   b) Para toda $n \in N$, si $n \in T$ implica $s(n) \in T$.

   Entonces $T = N$.

Teorema 3.3.1 — El modelo principal. $(\mathbb{N}, 0, S)$ es un sistema de Peano.

Definición 3.3.2 — Isomorfismo de sistemas de Peano. Dados (N, a, s) y (N', a', s') dos sistemas de Peano decimos que son isomorfos si existe una función biyectiva $\psi\colon N \to N'$ tal que:
1. $\psi(a) = a'$.
2. El siguiente diagrama conmuta:

$$\begin{array}{ccc} N & \xrightarrow{s} & N \\ {\scriptstyle\psi}\downarrow & & \downarrow{\scriptstyle\psi} \\ N' & \xrightarrow[s']{} & N' \end{array}$$

Como se mencionó al principio, el objetivo de los sistemas de Peano, usando las definiciones dadas es mostrar que todo sistema de Peano es isomorfo al sistema de los números naturales definido anteriormente. Para ello necesitamos los siguientes resultados técnicos.

Teorema 3.3.2 — Teorema de Recursión. Sea (N, a, s) un sistema de Peano, X un conjunto, $x_0 \in X$ y $f\colon X \to X$ una función, entonces existe una única funcion $\psi\colon N \to X$ tal que:

1. $\psi(a) = x_0$.
2. El siguiente diagrama conmuta:

$$\begin{array}{ccc} N & \xrightarrow{s} & N \\ {\scriptstyle\psi}\downarrow & & \downarrow{\scriptstyle\psi} \\ X & \xrightarrow[f]{} & X \end{array}$$

Proposición 3.3.3 Dos sistemas de Peano son isomorfos.

Con esto podemos concluir la caracterización de los números naturales, junto al cero y al principio de inducción como el sistema de Peano principal. Ahora procedemos a construir sus operaciones básicas.

Teorema 3.3.4 — Construcción de la Suma. Sea $(N, 0, s)$ un sistema de Peano, entonces existe una única función $\psi\colon N \times N \to N$ tal que:

1. Para cada $m \in N$, $\psi(m, 0) = m$.
2. Para toda $m, n \in N$, $\psi(m, s(n)) = s(\psi(m, n))$.

Definición 3.3.3 Definimos $m + n := \psi(m, n)$

Proposición 3.3.5 — Propiedades de la suma. Para todo $m, n, r \in \mathbb{N}$ tenemos las siguientes afirmaciones validas:

1. **Sucesión** $s(n) = n + 1$.
2. **Asociatividad** $(m + n) + r = m + (n + r)$.
3. **Neutro** $m + 0 = m = 0 + m$.
4. **Conmutatividad** $m + n = n + m$.
5. **Ley de cancelación** Si $m + r = n + r$ entonces $m = n$.
6. **Es ordenado** Si $m \leq n$ entonces $m + r \leq n + r$.

Teorema 3.3.6 — Construcción de la multiplicación. Sea $(N, 0, s)$ un sistema de Peano, entonces existe una única función $\phi\colon N \times N \to N$ tal que para todo $m, n \in N$:

1. $\phi(m, 0) = 0$.
2. $\phi(m, s(n)) = \phi(m, n) + m$.

Definición 3.3.4 Definimos $m * n := \phi(m, n)$

Proposición 3.3.7 — Propiedades de la multiplicación. Para todo $m, n, r \in \mathbb{N}$ tenemos las siguientes afirmaciones validas:

1. **Asociatividad** $(m * n) * r = m * (n * r)$.
2. **Neutro** $m * 1 = m = 1 * m$.
3. **Conmutatividad** $m * n = n * m$.
4. **Ley de cancelación** Si $m * r = n * r$ y $r \neq 0$ entonces $m = n$.
5. **Es ordenado** Si $m \leq n$ entonces $m * r \leq n * r$.
6. **Es distributivo** $r * (m + n) = r * m + r * n$.
7. **No tiene divisores cero** Si $m \neq 0 \neq n$ entonces $mn \neq 0$.

3.4. Fundamentos del conteo.

Definición 3.4.1 — Conjuntos Disjuntos. Sea A, B conjuntos, decimos que son disjuntos si $A \cap B = \emptyset$. Ademas si $\mathcal{F}$ es un familia no vacia de conjuntos, decimos que son disjuntos por pares si para todo par de conjuntos distintos $A, B \in \mathcal{F}$ son disjuntos.

Proposición 3.4.1 Sean A, B una pareja de conjuntos disjuntos finitos, entonces:

$$|A| + |B| = |A \cup B|$$

Notemos que si $f\colon X \to Y$ es una función inyectiva entonces por 2.4.7 se tiene el siguiente diagrama conmutativo:

$$\begin{array}{ccc} X & \xrightarrow{\quad f \quad} & Y \\ & {\scriptstyle\cong}\searrow \quad \nearrow{\scriptstyle\subset} & \\ & f(X) & \end{array}$$

Mostrando que la cardinalidad de $|X|$ puede ser menor o igual a la cardinalidad de $|Y|$, motivando la siguiente definición.

Definición 3.4.2 — Orden en la cardinalidad.. Sean X, Y conjuntos, decimos $|X| \leq |Y|$ si existe una función inyectiva $f\colon X \to Y$.

Proposición 3.4.2 Sea $B \subseteq A$ con A finito entonces:

$$|B - A| + |A| = |B|$$

Proposición 3.4.3 Sean A, B conjuntos finitos, entonces:

$$|A \cup B| = |A| + |B| - |A \cap B|$$

Proposición 3.4.4 Sean A, B conjuntos finitos, entonces:

$$|A \times B| = |A| * |B|$$

Definición 3.4.3 — Función Característica.. Fijemos X un conjunto no vacio. Para cada $A \subseteq X$ definimos:

$$\chi_A^X\colon X \to \{0,1\},\ \chi_A^X(x) = \begin{cases} 1 & x \in A \\ 0 & x \in X - A \end{cases}$$

Ademas, si X está claro, podemos escribir $\chi_A := \chi_A^X$.

Proposición 3.4.5 Para todo subconjunto $A \subseteq X$, la función caracteristica χ_A es en efecto una función.

Proposición 3.4.6 Sea X un conjunto no vacio, entonces existe una biyección natural:

$$\epsilon_X\colon \mathbf{P}(X) \to \mathrm{Hom}_{\mathbf{C}}(X, \{0,1\})$$

En donde la naturalidad se entiende como sigue; si $f\colon X \to Y$ es una función, entonces el siguiente diagrama conmuta:

$$\begin{array}{ccc} \mathbf{P}(Y) & \xrightarrow{\epsilon_Y} & \mathrm{Hom}_{\mathbf{C}}(Y, \{0,1\}) \\ {\scriptstyle f^*(-)}\downarrow & & \downarrow{\scriptstyle \mathrm{Hom}_{\mathbf{C}}(f, \{0,1\})} \\ \mathbf{P}(X) & \xrightarrow[\epsilon_X]{} & \mathrm{Hom}_{\mathbf{C}}(X, \{0,1\}) \end{array}$$

Proposición 3.4.7 Sean X, Y dos conjuntos finitos, entonces:

$$|\mathrm{Hom}_{\mathbf{Set}}(X,Y)| \cong |X|^{|Y|}$$

Si X es un conjunto finito entonces:

$$|\mathbf{P}(X)| = 2^{|X|}$$

Teorema 3.4.8 — Interpretaciones de los arreglos con repetición.. Existe una biyección entre los siguientes conjuntos:

1. $Fun(n,m)$.
2. El conjunto de palabras de longitud n es un alfabeto de m-letras.
3. El conjunto de cadenas de n-elementos escogidos de un conjunto de m objetos.
4. El conjunto de las maneras de distribuir n-objetos en m-cajas.

Principio de Dirichlet. Si $f\colon X \to Y$ es una función, tenemos los siguientes hechos que el lector puede verificar:

1. $\mathcal{F} = \{f^*(\{y\}) |\ y \in im(f)\}$ es una partición de X.
2. $\mathcal{F}$ le corresponde a la relación $\ker f$.
3. Si f es inyectiva entonces $\ker f = \triangle_X$, entonces $|f^*(\{y\})| = 1$ para todo punto en la imagen.

Proposición 3.4.9 — Principio del Palomar. Sea $f\colon m \to n$ una función sobreyectiva con $m > n$ entonces f no puede ser inyectivo.

Se puede precisar el principio de Dirichlet y darle una formulación combinatoria.

Teorema 3.4.10 — Principio de Dirichlet. Sean $n = km + 1$ objetos, entonces cualquier asignación de n objetos a m cajas, existe una caja con al menos $k+1$ objetos.

3.5. Combinaciones y Permutaciones.

Proposición 3.5.1 Sea X un conjunto finito de n elementos, entonces el conjunto de funciones biyectivas tiene la cardinalidad:

$$|Biy(x)| = n(n-1)(n-2)\cdots 3*2*1$$

Definición 3.5.1 — Permutaciones. Sea X un conjunto de n elementos, una permutación es una biyección $f\colon X \to X$. Entonces el número de permutaciones de X es denotado como $n!$. Usando la proposición anterior, imponemos $0! = 1$.

Proposición 3.5.2 — El principio de la división.. Sean X, Y conjuntos finitos no vacios y $f\colon X \to Y$ con la siguiente propiedad; para cada $y \in Y$ el conjunto $|f^{-1}(y)| = k$ entonces $|X| = k|Y|$.

Demostración. Se sigue de la partición:

$$X = \bigcup_{y \in Y} f^*(\{y\})$$

Entonces:

$$|X| = \sum_{y \in Y} k = k|Y|.$$

■

Definición 3.5.2 — El número $P(n,m)$. Sea X, Y conjuntos de n y m elementos con $n \leq m$, el numero de n permutaciones sobre m es el número de funciones inyectivas de la forma $f\colon X \to Y$.

Proposición 3.5.3 Sea X, Y conjuntos finitos de tamaño n y m elementos con $n \leq m$ entonces el número de funciones inyectivas es:

$$P(n,m) = \frac{n!}{(n-m)!}$$

Demostración. Primero supongamos que $X \subseteq Y$ Consideremos la función:

$$\psi\colon Biy(Y) \to Iny(X,Y)$$

definida como $\psi(f) := f \circ i_X$. Esta función es sobreyectiva y cumple que $|Y - f(X)| = n - m$ elementos, asi que para cada $f\colon X \to Y$, por el principio de multiplicación, es posible encontrar $(n-m)!$ funciones biyectivas $\hat{f}\colon Y \to Y$ tales que $f = \hat{f} \circ i_X$. Entonces por el principio de la división, tenemos:

$$|Biy(Y)| = (n-m)!P(n,m) \Rightarrow \ P(n,m) = n!/(n-m)!$$

■

Teorema 3.5.4 — Interpretación de las permutaciones. Existe una biyección:

1. $Iny(n,m)$.
2. El conjunto de palabras de longitud n en un alfabeto de m letras con la condición de que las letras sean distintas.
3. El conjunto de sucesiones de n-elementos distintos escogidos de un conjunto de m-elementos.
4. El conjunto de las maneras de distribuir n objetos en m cajas con la condición de que ninguna caja tiene más de un objeto.

Teorema 3.5.5 — Coeficiente binomial. Sea X un conjunto finito de n elementos y $m \leq n$, entonces el número de subconjuntos de m elementos es:

$$C(n,m) = \frac{n!}{m!(n-m)!}$$

Demostración. Denotemos $A_m = \{A \subseteq X |\ |A| = m\}$ entonces definimos la función:

$$\chi\colon Iny(m,n) \to A_m$$

Definido como $\chi(f) = f_*(m)$. Si $A \subseteq X$ es de cardinalidad m y fiemos $f \in Iny(m,n)$ tal que $f_*(m) = A$, entonces tenemos una biyección

$$Biy(m) \cong \{f \in Iny(m,n) |\ f_*(m) = A\}$$

Obteniendo que $\chi^*(A)$ tiene $m!$ elementos, por el principio de división obtenemos:

$$P(n,m) = m!C(n,m)$$

Por lo tanto $C(n,m) = \frac{n!}{m!(n-m)!}$. ■

Proposición 3.5.6 — Propiedades del número combinatorio. Las siguientes afirmaciones son válidas:

1. Sean $k_1 + k_2 = n$ entonces $C(n,k_1) = C(n,k_2)$.

2. **Teorema de Pascal**: $C(n,k)+C(n,k+1)=C(n+1,k+1)$.
3. Tenemos la siguiente identidad:
$$\sum_{k=0}^{n} C(n,k) = 2^n$$

Demostración. Para el primer punto tenemos que:
$$C(n,k_1) = \frac{n!}{k_1!(n-k_1)!} = \frac{n!}{(n-k_2)!k_2!} = C(n,k_2)$$

Para el segundo punto tenemos:
$$\begin{aligned} C(n,k)+C(n,k+1) &= \frac{n!}{k!(n-k)!} + \frac{n!}{(k+1)!(n-k-1)!} \\ &= \frac{(k+1)n!}{(k+1)!(n-k)!} + \frac{(n-k)n!}{(k+1)!(n-k)!} = \frac{(n+1)!}{(k+1)!(n-k)!} \end{aligned}$$

Para el último punto, tenemos la partición:
$$\mathbf{P}(X) = \bigcup_{k=1}^{n} A_k$$

Donde $|A_k| = C(n,k)$ obteniendo la igualdad deseada. ■

Teorema 3.5.7 — Teorema del Binomio. Sea $x \in \mathbb{N}$ entonces tenemos la siguiente identidad para cada $n \in \mathbb{N}$:
$$(x+y)^n = \sum_{k=0}^{n} C(n,k)x^k y^{n-k}$$

Demostración. Por inducción, para $n=1$ se tiene
$$(x+y)^1 = x+y = C(1,0)x + C(1,1)y$$

Supongamos válido para $n=m$ entonces:
$$\begin{aligned} (x+y)^{m+1} &= (x+y)^m(x+y) \\ &= \left(\sum_{k=0}^{m} C(m,k)x^k y^{m-k}\right)(x+y) \\ &= \sum_{k=0}^{m} C(m,k)x^{k+1}y^{m-k} + C(m,0)x^0y^{m+1} + \sum_{k=1}^{m} C(m,k)x^k y^{m-k+1} \\ &= \sum_{k=0}^{m} C(m,k)x^{k+1}y^{m-k} + x^0y^{m+1} + \sum_{k=0}^{m-1} C(m,k+1)x^{k+1}y^{m-k} \\ &= x^{m+1}y^0 + \sum_{k=0}^{m-1} C(m,k)x^{k+1}y^{m-k} + x^0y^{m+1} + \sum_{k=0}^{m-1} C(m,k+1)x^{k+1}y^{m-k} \\ &= x^{m+1}y^0 + \sum_{k=0}^{m-1} (C(m,k)+C(m,k+1))x^{k+1}y^{m-k} + x^0y^{m+1} \\ &= \sum_{k=0}^{m+1} C(m+1,k)x^k y^{m+1-k} \end{aligned}$$

■

Teorema 3.5.8 — Interpretaciones de Combinatoria. Los siguientes conjuntos son sobreyectivos:
1. A_k.
2. El conjunto de maneras de poner n objetos en dos cajas B_1 y B_2 tales que B_1 tiene k elementos y B_2 tiene $n-k$ elementos.

3.5.1. Conteo con repetición

Definición 3.5.3 — Multiconjuntos formal. Sea A un conjuto, definimos:
1. Un multiconjunto como una pareja (A, m) en donde $m\colon A \to \mathbb{N}$. Para cada $a \in A$, se le entiende a $m(a)$ como la cantidad de veces que a se repite en el multiconjunto.
2. El soporte de un multiconjunto (A, m) es el conjunto $sup(A) := \{x \in A | m(x) \neq 0\}$. Decimos ademas que (A, m) es finito si su soporte es un conjunto finito.
3. Para un multiconjunto (A, m) finito, definimos la cardinalidad de (A, m) como en número:
$$|(A, m)| := \sum_{x \in sup(A)} m(x).$$
4. Si $|A| = n$, el número de multiconjuntos de cardinalidad k es denotado $\left(\binom{n}{k}\right)$. Es tambien llamado combinaciones con repetición.
5. Si (A, m) es un multiconjunto, una d-permutación es una d-tupla (x_i) donde $x_i \in A$ y x se puede repetir a lo más $m(x)$-veces en la d-tupla.

Definición 3.5.4 — Coeficiente Multinomial. Sea n definimos lo siguiente:
1. Una colección $\{k_i\}$ se llama particion de n si $k_1 + k_2 + \cdots + k_r = n$.
2. Dado n y una partición $k_1, \cdots, k_r$ definimos el coeficiente multinomial:
$$C(n : k_1, \cdots, k_r)$$
Como el número de maneras de poner n objetos en r cajas B_i tales que B_i tiene k_i elementos. Este número es llamado también permutaciones con repetición.

Teorema 3.5.9 Se tiene que:
$$C(n : k_1, \cdots, k_r) = \frac{n!}{k_1! \cdot \cdots \cdot k_r!}$$

Proposición 3.5.10 — Una identidad importante.
$$C(n, k_1, \cdots, k_r) = C(k_1, k_r)C(k_1 + k_2, k_2)C(k_1 + \cdots + k_r)k_r$$

Teorema 3.5.11 — Teorema del Multinomio. Sean $x_1, \cdots, x_r$ elementos en un anillo conmutativo R, entonces:
$$(x_1 + \cdots + x_r)^n = \sum_{k_1 + \cdots + k_r = n} C(n : k_1, \cdots, k_r) x_1^{k_1} \cdots x_r^{k_r}$$

Proposición 3.5.12 Los siguientes conjuntos son biyectivos:
1. El numero de maneras de distribuir n objetos en r-cajas con B_i que contenga k_i elementos.
2. Dado r elementos, donde cada elemento se repite k_i veces, el número de n-tuplas donde se distribuye los r elementos con las repeticiones dadas.

Proposición 3.5.13 Sea M un multiconjunto de n elementos, donde cada elemento $a \in M$ se tiene que $m(a) = \infty$, el número de m permutaciones con repetición es n^m.

Ahora consideremos conteos donde el orden no cuenta.

Teorema 3.5.14 — Interpretaciones. Los siguientes conjuntos son biyectivos:

1. El número de multiconjuntos de cardinalidad k tomados de un conjunto de n elementos.
2. El número de soluciones enteras positivas de la ecuación:

$$x_1 + \cdots + x_n = k$$

3. El número de monoides de n variables de grado k.

Teorema 3.5.15 El número de soluciones de enteros positivos de la ecuación:

$$x_1 + \cdots + x_n = r$$

es $C(n + r - 1, r)$

Proposición 3.5.16 — Propiedades del coeficiente de multiconjuntos. Las siguientes afirmaciones son válidas:

1. $\left(\binom{n}{k}\right) = C(n + k - 1, k)$.
2. $\left(\binom{n}{k}\right) = \left(\binom{n+1}{k-1}\right)$.
3. $\left(\binom{n}{k}\right) = \left(\binom{n}{k-1}\right) + \left(\binom{n-1}{k}\right)$

Proposición 3.5.17 Los siguientes conjuntos son biyectivos:

1. El número de sucesiones crecientes de longitud k de r números.
2. El conjunto de todas las maneras de poner k objetos identicos en r cajas distintas.
3. El conjunto de todos los multiconjuntos de cardinalidad k de un conjunto de r elementos.

Proposición 3.5.18 El numero de maneras de poner k objetos idéntidcos en $r$cajas distintas, de manera que cada caja tenga almenos un objeto es $C(r - 1, k - 1)$.

Proposición 3.5.19 El número de particiones en de un conjunto de n elementos, en k_i objetos, es

$$S(n; k_1, \cdots, k_r) = \frac{n!}{k_1! \cdots k_r!(1!)^{k_1} \cdots (r!)^{k_r}}$$

3.6. Ejercicio.

3.6.1. Principio de Inducción.

1. Demuestra por principio de inducción:
   a) La suma de 3 cubos consecutivos es divisible entre 3.
   b) Todo número natural se puede expresar como una suma de potencias de 2.
   c) Para todo real $r \in \mathbb{R}$ se cumple para cada $n \in \mathbb{N}$:

$$\sum_{k=0}^{n} r^k = \frac{1 - r^{n+1}}{1 - r}$$

2. **Ordenamiento de la burbuja.** Fijemos n como conjunto natural, una sucesión de $n + 1$ numeros reales es una función $a \colon n \to \mathbb{R}$. Decimos que una sucesión a está ordenada si cada ves que $m \leq n$

entonces $a_m \leq a_n$. Decimos que una sucesión a tiene un ordenamiento si existe una función biyectiva $b\colon n \to n$ tal que $a \circ b$ es una sucesión ordenada. El pseudocódigo es el siguiente:

a) Empieza con $n = 0$
b) Si $a(n) \leq a(n^+)$ entonces:
  1) Avanza a n^+.
  2) De lo contrario, reordena intercambiando de lugar $a(n) \leftrightarrow a(n^+)$. Luego avanza a n^+
c) Repite el proceso anterior, hasta llegar a $n - 1$.
d) Vuelve a poner $n = 0$, repite el proceso desde (b) tantas veces como $n - 1$.

Demuestra por inducción que el ordenamiento por burbuja ordena correctamente a una lista de n elementos con $n > 0$.

3. **Numeros de fibonacci**. Definimos la sucesión de fibonacci $f\colon \mathbb{N} \to \mathbb{N}$ mediante la siguiente regla recursiva:

$$f_0 = 0,\ f_1 = 1,\ f_{n+2} = f_{n+1} + f_n$$

Demuestra por inducción las siguientes propiedades de los números de fibonacci:

a) Para toda $n \in \mathbb{N}$ se tiene:

$$f_n = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^n - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^n$$

b) f_n divide a f_{2n}.
c) $f_{n+1}f_{n-1} - f_n^2 = (-1)^n$.
d) $f_{n+2}^2 - f_n^2 = f_{2n+2}$.

4. Prueba por inducción que la siguiente identidad matricial se cumple:

$$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^n = \begin{pmatrix} f_{n-1} & f_n \\ f_n & f_{n+1} \end{pmatrix}$$

5. Demuestra que $x + 1$ divide a $x^{2n+1} + 1$.
6. Consideremos $G = (V, E)$ un grafo simple, tenemos los siguientes conceptos intuitivos:

a) Un paseo en G es una sucesión $v_0, v_1, \cdots, v_n$ tal que $(v_k, v_{k+1}) \in E$ es un vértice.
b) Decimos que un paseo es cerrado si $v_0 = v_n$.
c) El tamaño de un pase es la cantidad de lados que paso, es decir n.
d) Un camino es un paseo donde no se repite los vértices.
e) Un ciclo es un camino cerrado.

Demuestra que todo paseo cerrado contiene un ciclo de tamaño impar.

7. Usando los conceptos anteriores, muestra que en un grafo simple G, dados dos vértices distintos u, v, demuestra que cada paseo que inicia en u y termina en v, contiene un camino que inicia en u y termina en v. Hint: Usa principio de inducción sobre el tamaño del paseo.
8. Muestra que $1 + 3 + \cdots + (2n - 1) = n^2$.
9. Prueba por principio de inducción que el número de subconjuntos de un conjunto de n elementos es 2^n.
10. **Preparativos para las matemáticas del Cubo de Rubik**. Sea X un conjunto finito no vacio de n-elementos, decimos que una permutación $f\colon X \to X$ es un m-ciclo si existe una $a \in X$ tal que:

a) $\{a = f^0(a), f(a), f^2(a), \cdots, f^{m-1}(a)\}$ son todos distintos.
b) $f^m(a) = a$.

Muestra que todo m-ciclo es la composición de 2-ciclos.

3.6.2. Propiedades de los números naturales.

1. Consideremos n, m conjuntos naturales. Demuestra que si $n^+ = m^+$ entonces $m = n$.
2. Sea B un conjunto finito, y $A \subseteq B$, demuestra que A es finito.
3. ¿Cierto o falso? Si B es conjunto finito y $B \subseteq C$ entonces C es finito.
4. ¿Cierto o falso? Si B es un conjunto inifito y $B \subseteq C$ entonces C es infinito.
5. Considerando la estructura algebraica de $\mathbb{N}$, deducida de los axiomas de Peano, muestra que para todo $a, b \in \mathbb{N}$ se cumple que $(a + b)^2 \leq 2a^2 + 2b^2$.
6. Muestra que si $a, b, c, d \in \mathbb{N}$ tales que $a \leq b$ y $c \leq d$ entonces $ac \leq bd$.
7. ¿Cierto o falso? La siguiente identidad $m + (nq) = (m + n)(m + q)$. Argumenta.

3.6.3. Fundamentos de combinatoria.

1. Demuestra por inducción que si $A_1, \cdots, A_n$ son conjuntos finitos entonces:

$$|A_1 \times \cdots \times A_n| = |A_1| \cdot \cdots \cdot |A_n|$$

2. ¿De cuántas maneras pueden colocarse una torre blanca y una torre negra en un tablero de ajedrez de modo que se ataquen?
3. En un acto deben hablar Daniel, Rubi, Angel, Pablo y Valeria. ¿De cuántas maneras se puede confeccionar la lista de oradores con la condición de que Daniel hable antes que Angel? ¿Y si la condición es que Rubi hable inmediatamente después que Daniel? ¿Y si deben alternarse oradores de distintos géneros?
4. ¿De cuántas maneras pueden colocarse un alfil blanco y uno negro en un tablero de ajedrez de modo que se ataquen mutuamente (es decir, que estén en una misma diagonal)?
5. En un campeonato de béisbol jugado por el sistema de eliminatorias se enfrentan n equipos. En cada ronda los equipos perdedores salen del torneo. Al formar los pares de equipos que se van a enfrentar puede eventualmente quedar un equipo sin jugar, éste descansa y pasa a la ronda siguiente. Se desea saber cuántos juegos se realizarán durante el campeonato.

3.6.4. Combinaciones y Permutaciones.

1. ¿Cuántas banderas con tres franjas horizontales del mismo ancho y distintos colores pueden formarse, si se dispone de tela amarilla, azul, verde, blanca y roja?
2. En el alfabeto Morse, usado en telegrafía, se emplean solamente dos signos: el punto y la raya. ¿Cuántas palabras distintas pueden formarse compuestas de uno, dos, tres, cuatro o cinco signos? Generalice.
3. ¿Cuántas palabras diferentes pueden formarse con las letras de la palabra UNICORNIO?
4. En un plano hay n puntos, k de los cuales están alineados. A excepción de ellos no hay tres en línea recta. ¿Cuántas líneas rectas diferentes resultan si se unen los n puntos dos a dos?

Capítulo 4

Estructuras Algebraicas.

El álgebra universal es una rama de la matemática que estudia las estructuras algebraicas en sí, no los ejemplos ("modelos") de estructuras algebraicas. Esto significa que el álgebra universal se preocupa por las propiedades generales de las estructuras algebraicas, independientemente de su aplicación específica.

La historia del álgebra universal se remonta a la antigüedad, con el estudio de las estructuras algebraicas básicas, como los grupos, los anillos y los campos. Sin embargo, el álgebra universal como campo formal de estudio no se desarrolló hasta el siglo XIX.

En 1847, George Boole publicó su libro "The Laws of Thought", que introdujo la lógica simbólica. La lógica simbólica se basó en el estudio de las operaciones binarias, que son operaciones que toman dos elementos como entrada y producen un elemento como salida.

En 1890, Alfred North Whitehead y Bertrand Russell publicaron su libro "Principia Mathematica", que estableció las bases de la lógica matemática. "Principia Mathematicaütilizó operaciones binarias para definir conceptos matemáticos básicos, como la suma, la multiplicación y la igualdad.

En 1914, Emil Post publicó su artículo Ïntroduction to a General Theory of Elementary Propositions", que introdujo las operaciones n-arias. Las operaciones n-arias son operaciones que toman n elementos como entrada y producen un elemento como salida.

En 1928, Garrett Birkhoff publicó su libro "Lattices", que introdujo el concepto de retículos. Los retículos son estructuras algebraicas que se pueden utilizar para modelar una variedad de sistemas, como la lógica, la teoría de la decisión y la teoría de la computación.

El álgebra universal se ha desarrollado rápidamente en los últimos años. Se ha utilizado para estudiar una variedad de estructuras algebraicas, como los grupos, los anillos, los campos, los módulos, los espacios vectoriales y las álgebras de Lie.

Las operaciones n-arias son importantes en el álgebra universal porque permiten definir estructuras algebraicas más complejas. Por ejemplo, un grupo es un conjunto con una operación binaria que satisface ciertas propiedades. Un anillo es un conjunto con dos operaciones binarias que satisfacen ciertas propiedades. Un espacio vectorial es un conjunto con una operación binaria (suma) y una operación unitaria (multiplicación por escalares).

Las operaciones n-arias también son importantes porque permiten estudiar sistemas con más de dos elementos. Por ejemplo, un sistema de tres ecuaciones lineales se puede modelar como un álgebra con tres operaciones binarias.

El álgebra universal tiene una amplia gama de aplicaciones en otras áreas de las matemáticas, la informática y la ciencia. Por ejemplo, el álgebra universal se utiliza para estudiar:

- La lógica simbólica
- La teoría de la decisión
- La teoría de la computación

- La geometría algebraica
- La teoría de números
- La física
- La química
- La biología

En particular, el álgebra universal se utiliza para:

- Definir nuevos conceptos matemáticos
- Probar teoremas matemáticos
- Desarrollar nuevos algoritmos informáticos
- Modelar sistemas físicos y biológicos

4.1. Estructuras algebraicas.

Para lo siguiente, conviene realizar la siguiente notación, si X es un conjunto, denotamos $X^n := \prod_{i=1}^n X$ con sus respectivos proyecciones coordenados $\{\pi_i^X\}_{i=1}^n$. Notemos además que si $f\colon X \to Y$ es una función, por la propiedad universal del producto, f se levanta al producto en una única función denotada $f^{(n)}\colon X^n \to Y^n$ tal que el siguiente diagrama conmuta:

$$\begin{array}{ccc} X^n & \xrightarrow{f^{(n)}} & Y^n \\ {\scriptstyle \pi_i^X}\downarrow & & \downarrow{\scriptstyle \pi_i^Y} \\ X & \xrightarrow[f]{} & Y \end{array}$$

Algunas observaciones directas:

1. Por naturalidad, f es biyectiva implica que $f^{(n)}$ es biyectiva.
2. Si f es sobreyectiva (o inyectiva) entonces $f^{(n)}$ lo es, pues en particular $()^{(n)}$ levanta inversos derechos e izquierdos.

Definición 4.1.1 — Operaciones n-arias. Sea X un conjunto, una operación n-aria(cerrada) es una función de la forma $\mu\colon X^n \to X$. Denotamos (X, μ) a la estructura n-aria de X y lo llamamos una estructura algebraica n-aria.

Nos centraremos en operaciones binarias, para dar ejemplos satisfactorios y clasificarlos, definimos las propiedades que puede tener una operacion binaria.

Definición 4.1.2 — Propiedades de una operación binaria. Sea $m\colon A \times A \to A$ una operación binaria. Decimos que m es:

1. Indepotente, si para toda $a \in A$ se cumple que $m(a, a) = a$.
2. Asociativo, si para todo $a, b, c \in A$ se cumple que $m(a, m(b, c)) = m(m(a, b), c)$.
3. Conmutativo, si para todo $a, b \in A$ se cumple que $m(a, b) = m(b, a)$.
4. Cancelable por la derecha, si para cada ecuación $m(a, x) = m(b, x)$ implica que $a = b$.
5. Cancelable por la izquierda, si para cada ecuación $m(x, a) = m(x, b)$ implica que $a = b$.
6. Tiene neutro, si existe $e \in A$ tal que para toda $a \in A$ se cumple $m(a, e) = a = m(e, a)$.
7. Tiene inversos, si para todo $a \in A$ existe $b \in B$ tal que $m(a, b) = e = m(b, a)$.

■ **Ejemplo 4.1** Si $(P, \leq)$ es un orden tal que para toda $a, b \in P$ el supremo $a \vee b$ existe, entonces podemos definir una operación binaria $\vee\colon P \times P \to P$. Esta operación satisface:

1. Es indepotente.
2. Es asociativo,
3. Es conmutativo.

4. Es cancelable por la derecha y por la izquierda.
5. Si tiene objeto 0 (elemento mínimo) entonces es el neutro de la operación.
6. No necesariamente tiene inversos.

■

■ **Ejemplo 4.2** Sea X un conjunto vacio. Entonces a $A = Biy(X)$ le inducimos la operación dado por la composición, obteniendo las siguientes propiedades:

1. Es asociativo.
2. En general no es indepotente.
3. En general no es conmutativo.
4. Tiene a Id_X como su identidad.
5. Tiene inversos.

■

■ **Ejemplo 4.3** Los $\mathbb{N}$ con la suma, tiene las propiedades:

1. Es asociativo.
2. En general no es indepotente.
3. Es conmutativo.
4. Tiene a 0 como su identidad.
5. No tiene inversos en general.

Una situación análoga sucede con los naturales con la multiplicación. ■

■ **Ejemplo 4.4** Las simetrías del cuadrado. Consideremos un cuadrado en el plano, con vértices dentro de la circunferencia unitaria. El grupo de las simetrias del cuarado es denotado como $D4$ y se denomina el grupo diédrico. Este satisface:

1. Es asociativo.
2. No es conmutativo.
3. Tiene neutro.
4. Tiene inversos.

Ilustrar todos los subgrupos de $D4$. ■

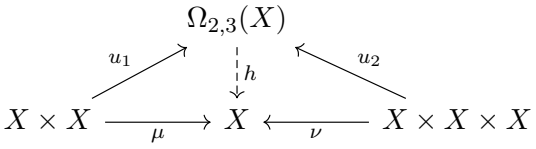
Tambien exiten estructuras donde trabajan mas de una operación y se relacionan entre si.

Definición 4.1.3 — Propiedad distributiva. Sea X un conjunto, $\mu\colon X \times X \to X$ y $\nu\colon X \times X \to X$ dos operaciones. Decimos que μ distribuye a ν si para toda $a, b, c \in X$ se cumple:

$$\mu(a, \nu(b, c)) = \nu(\mu(a, b), \mu(a, c).$$

■ **Ejemplo 4.5** Los naturales $\mathbb{N}$ con la suma y producto, tenemos que el producto distribuye a la suma. ■

Para poder estudiar las propiedades generales que cualquier tipo de estructura algebraica, necesitamos una construcción que nos ayude a juntar la información de un conjunto, junto a sus estructuras. Por ejemplo, supongamos que X tiene dos operaciones, uno binario $\mu\colon X \times X \to X$ y uno ternario $\nu\colon X \times X \times X \to X$, entonces es posible construir un conjunto y una función que junte la información de ambos. Consideremos la unión disjunta $\Omega_{2,3}(X) := (X \times X) \coprod (X \times X \times X)$, entonces usando la propiedad universal de la unión disjunta existe una única función $h\colon \Omega_{2,3}(X) \to X$ tal que el siguiente diagrama conmuta:



Entonces h está definido como sigue:

$$h(a) = \mu(a), \text{ si } a \in X \times X, \; h(A) = \nu(a), \text{ si } a \in X \times X \times X$$

Además $\Omega_{2,3}(X)$ cumple las siguientes propiedades:

1. Si $f\colon X \to Y$ es una función, esto induce dos funciones $f^{(2)}\colon X^2 \to Y^2$ y $f^{(3)}\colon X^3 \to Y^3$ y usando la propiedad universal de la union disjunta, existe una única función $\Omega_{2,3}(f)\colon \Omega_{2,3}(X) \to \Omega_{2,3}(Y)$ tal que:

$$\begin{array}{ccc} X^{n_i} & \xrightarrow{f^{(n_i)}} & Y^{n_i)} \\ \downarrow{\scriptstyle u_i} & & \downarrow{\scriptstyle v_i} \\ \Omega(X) & \xrightarrow[\Omega(f)]{} & \Omega(Y) \end{array}$$

2. Si $f\colon X \to Y$ y $g\colon Y \to Z$ entonces $\Omega(g \circ f) = \Omega(g) \circ \Omega(f)$.
3. Si $f = \mathrm{Id}_X$ entonces $\Omega(\mathrm{Id}_X) = \mathrm{Id}_{\Omega(f)}$.

Esta construcción se extiende para cada sucesión $n := (n_i)_{i\in I} \in \mathbb{N}^I$. Obteniendo las asignaciones:

1. $\Omega_n(X) = \coprod_{i\in I} X^{n_i}$.
2. Para cada $f\colon X \to Y$ función, $\Omega_n(f) = \coprod_{i\in I} f^{(n_i)}$

Dichas asignaciones cumplen propiedades similares. Cuando no haya confusión denotamos $\Omega = \Omega_n$.

Proposición 4.1.1 La asignación Ω_n cumple las siguientes propiedades para una función $f\colon X \to Y$.

1. Si f es inyectiva entonces $\Omega(f)$ tambien lo es.
2. Si f es sobreyectiva entonces $\Omega(f)$ también lo es.

Demostración. Para la primera parte, se tiene que existe $g\colon Y \to X$ tal que $f \circ g = \mathrm{Id}_X$ entonces $\Omega(f) \circ \Omega(g) = \mathrm{Id}_{\Omega(X)}$, por tanto $\Omega(f)$ es inyectiva. La segunda parte se hace de manera análoga. ■

Definición 4.1.4 — Ω-algebra. Dado n una sucesión de naturales, una Ω-algebra consiste en la pareja (X, μ) en donde $\mu\colon \Omega_n(X) \to X$. A la función μ lo denominaremos como la estructura algebraica de X.

Definición 4.1.5 — Homomorfimos de Algebras. Sean $(X, \mu), (Y, \nu)$ Ω-algebras, una función $f\colon X \to Y$ se llama homomorfismo de algebras si el siguiente diagrana conmuta:

$$\begin{array}{ccc} \Omega(X) & \xrightarrow{\Omega(f)} & \Omega(Y) \\ {\scriptstyle \mu}\downarrow & & \downarrow{\scriptstyle \nu} \\ X & \xrightarrow[f]{} & Y \end{array}$$

En tal caso lo denotaremos como $f\colon (X, \mu) \to (Y, \nu)$.

Proposición 4.1.2 Las siguientes afirmaciones son válidas.

1. Sean μ, μ' estructuras de X entonces $\mathrm{Id}_X\colon (X, \mu) \to (X, \mu')$ es homomorfismo de algebras si y sólamente si $\mu = \mu'$. En tal caso lo denotaremos como $\mathrm{Id}_{(X,\mu)}$.
2. Si $f\colon (X, \mu) \to (Y, \nu)$ y $g\colon (Y, \nu) \to (Z, \zeta)$ son homomorfismos de algebras entonces $g \circ f\colon (X, \mu) \to (Z, \zeta)$ tambien lo es.

Demostración. Ejercicio al lector. ■

Definición 4.1.6 — Subalgebra. Dado (X, μ) una Ω-algebra, y $Y \subseteq X$ un subconjunto, decimos que Y es subalgebra si existe una estructura algebraica μ_Y tal que la función inclusión $i\colon (Y, \mu_Y) \to (X, \mu)$ es un homomorfismo de algebras.

Notemos que en general si $f : Y \to X$ es una función inyectiva, dados ν, ν' dos estructuras en Y que hacen a f una estructura algebraica, entonces $\nu = \nu'$, es decir:

Proposición 4.1.3 Si (Y, ν) es una estructura algebraica y $f\colon X \to Y$ es inyectiva. Si existe una estructura algebraica μ en X tal que f es homomorfismo de algebras, entonces esta es única.

Demostración. Si $\mu, \mu'\colon \Omega(X) \to X$ son Ω-estructuras tales que hacen a f un homomorfismo, entonces:

$$f \circ \mu = \nu \circ \Omega(f) = f \circ \mu'$$

Como f es inyectiva, entonces es cancelable por la izquierda, esto implica $\mu = \mu'$. ■

Con esta propiedad tenemos que si (W, μ_W) es una subálgebra de (X, μ), notemos que $\Omega(i)$ cumple del diagrama conmutativo para cada $i \in I$:

$$\begin{array}{ccc} W^{n_i} & \xrightarrow{i^{n_i}} & X \\ {\scriptstyle u_i}\downarrow & & \downarrow{\scriptstyle v_i} \\ \Omega(W) & \xrightarrow[\Omega(i)]{} & \Omega(X) \end{array}$$

Si $w \in W^{n_i}$ entonces $\Omega(i)(w) = i^{n_i}(w) = w$, entonces usando que i es homomorfismo de algebras, tenemos del diagrama conmutativo:

$$\begin{array}{ccc} \Omega(W) & \xrightarrow{\Omega(i)} & \Omega(X) \\ {\scriptstyle \mu_W}\downarrow & & \downarrow{\scriptstyle \mu} \\ W & \xrightarrow[i]{} & X \end{array}$$

que $\mu_W(w) = i \circ \mu_W(w) = \mu \circ \Omega(i)(w) = \mu(w)$, es decir que de la proposición anterior, la restricción $\mu_W = \mu|_W$ es la única estructura posible para que W sea una subálgebra.

■ **Ejemplo 4.6** Si G es una estructura con una operación binaria μ entonces un subconjunto $H \subseteq G$ es una subálgebra si y sólamente si $\mu(H \times H) \subseteq H$, es decir para toda $a, b \in H$ entonces $\mu(a, b) \in H$. ■

Sea (X, μ) una Ω-algebra del tipo $n = (n_i)$ y $W \subseteq X$, para cada $i \in I$ denotemos $\mu_i := \mu \circ u_i\colon X^{n_i} \to X$ la n_i-operación de la estructura μ. Entonces $W \subseteq X$ es una subálgebra si y sólamente si para toda $i \in I$ se cumple la siguiente propiedad:

$$\forall w_1, \cdots, w_{n_i} \in W \Rightarrow \ \mu_i(w_1, \cdots, w_{n_i}) \in W$$

Proposición 4.1.4 Si (X, μ) es una estructura algebraica y $f\colon X \to Y$ es sobreyectiva. Si existe una estructura algebraica ν en Y tal que f es homomorfismo de algebras, entonces esta es única.

Demostración. Si $\nu, \nu'\colon \Omega(Y)$ son estructuras tales que hacen a f un homomorfismo, entonces:

$$\nu \circ \Omega(f) = f \circ \mu = \nu' \circ \Omega(f)$$

Como $\Omega(f)$ es una sobreyectividad entonces $\nu = \nu'$. ■

Proposición 4.1.5 Sea $f\colon (X, \mu) \to (Y, \nu)$ un homomorfismo de algebras, entonces son equivalentes:

1. f es monomorfismo.
2. f es inyectivo.

Está claro que no todo subconjunto de una Ω-algebra es una sub-algebra, sin embargo podemos construir la subalgebra generada por dicho subconjunto. Para ello definiremos una propiedad similar al 2.1.2.

Proposición 4.1.6 Sea $\mathcal{F} \subseteq \mathbf{P}(X)$ tales que:
1. $X \in \mathcal{F}$.
2. Si $\emptyset \neq \mathcal{G} \subseteq$ entonces $\bigcap \mathcal{G} \in \mathcal{F}$

Entonces para todo $A \subseteq X$ tenemos que el conjunto:

$$\langle A \rangle = \bigcap \{W \in \mathcal{F} |\ A \subseteq W\}$$

Satisface las siguientes propiedades:
1. $\langle A \rangle \in \mathcal{F}$ tal que $A \subseteq \langle A \rangle$.
2. Es el menor objeto en $\mathcal{F}$ con dicha propiedad.

Demostración. Por el punto 2 de la proposición tenemos que $\langle A \rangle \in \mathcal{F}$ y por construcción se tiene que $A \subseteq \langle A \rangle$, luego si $W \in \mathcal{F}$ es tal que $A \subseteq W$ entonces $W \in \{W \in \mathcal{F} |\ A \subseteq W\}$ obteniendo que por propiedades de intersección $\langle A \rangle \subseteq W$. ■

Denotemos $Sub(X, \mu) := \{A \subseteq X |\ (A, \nu) \to (X, \mu)\}$.

Proposición 4.1.7 $Sub(X, \mu)$ cumple las siguientes propiedades:
1. $(X, \mu) \in Sub(X, \mu)$.
2. Si $\mathcal{G} \subseteq Sub(X, \mu)$ entonces $\bigcap \mathcal{G} \in Sub(X, \mu)$.
3. Para todo $S \subseteq X$ existe la menor subalgebra $c(S)$ tal que $S \subseteq c(S)$. Dicha subalgebra se llama la subálgebra generada por S.
4. $Sub(X, \mu)$ es una retícula completa con infimo la intersección y supremo:

$$\bigvee \mathcal{G} := c\left(\bigcup \mathcal{G}\right)$$

Demostración. Notemos que la inclusión de (X, μ) en (X, μ) es la $\mathrm{Id}_{(X,\mu)}$ y por 4.1.2 tenemos que es homomorfismo de algebras, por lo tanto $(X, \mu) \in Sub(X, \mu)$. Luego si $a \in \Omega(\bigcap \mathcal{G}) \subseteq \Omega(W)$ con $W \in \mathcal{G}$ entonces $\mu|_W(a) \in W$, esto implica que $\mu|_{\bigcap \mathcal{G}}(a) = \mu_W(a) \in W$ para toda $W \in \mathcal{G}$ por lo tanto $\mu|_{\bigcap \mathcal{F}}(a) \in \bigcap \mathcal{G}$ mostrando que $\bigcap \mathcal{G}$ es una subálgebra. Para los siguientes puntos se deducen de 4.1.6. ■

■ **Ejemplo 4.7** Sea $(\mathbb{N}, +)$ entonces:
1. La subalgebra generada por $\{1\}$ es $\mathbb{N} - \{0\}$.
2. La subálgebra generada por $\{2, 5\}$ es $\{n \in \mathbb{N} |\ n = 2x + 5y,\ x, y \in \mathbb{N}\}$

■

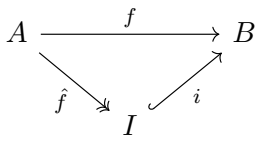
■ **Ejemplo 4.8** Consideremos $(\mathbb{R}^2, +, *)$ entonces:
1. Para cada $m \in \mathbb{R}$ el conjunto $l_m := \{(x, y) \in \mathbb{R}^2 |\ (x, y) = t(m, 1),\ t \in \mathbb{R}^2\}$ es una subalgebra.
2. El conjunto $l_\infty := \{(x, y) \in \mathbb{R}^2 |\ y = 0\}$ es una subalgebra.
3. El conjunto $\{0\}$ es una subalgebra.

Se puede demostrar que $Sub(\mathbb{R}^2)$ consiste en $\mathbb{R}^2$ o en alguna subálgebra de los mencionados anteriormente. De aqui se tiene que:

$$l_\infty \vee l_0 = \mathbb{R}^2,\ l_\infty \wedge l_0 = \{0\}$$

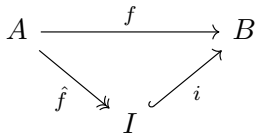
■

Recordemos que dado una función $f\colon A \to B$ este se descompone canónicamente bajo su imagen:

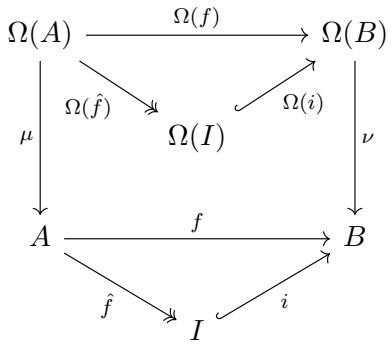


En donde $I = \{b \in B |\ \exists a \in A,\ f(a) = b\}$ es la imagen de f.

Proposición 4.1.8 Sea $f\colon (A, \mu) \to (B, \nu)$ un homomorfismo de algebras, entonces existe una única estructura $\xi\colon \Omega(I) \to I$ tal que el siguiente diagrama de homomorfismos de algebras conmuta:



Demostración. Aplicando Ω tenemos el diagrama conmutativo:



Supongamos que $x, y \in \Omega(A)$ tal que $\Omega(\hat{f})(x) = \Omega(\hat{f})(y)$ entonces $\nu \circ \Omega(f)(x) = \nu \circ \Omega(f)(y)$ entonces $f \circ \mu(x) = f \circ \mu(y)$ entonces $\hat{f} \circ \mu(x) = \hat{f} \circ \mu(y)$, entonces existe un única función $\delta\colon \Omega(I) \to I$ tal que:

$$\delta \circ \Omega(\hat{f}) = \hat{f} \circ \mu$$

Usando que $\Omega(\hat{f})$ es sobreyectivo:

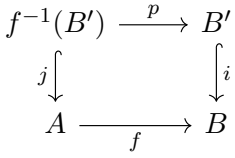
$$\nu \circ \Omega(i) = i \circ \delta$$

■

Si $A' \leq A$ es una subalgebra y $f\colon A \to B$ es un homomorfismo de algebras entonces $f(A')$ es una subalgebra. Ahora para demostrar que la imagen inversa de una subalgebra es tambien una subalgebra, tenemos que probar la siguiente propiedad.

Proposición 4.1.9 Sea $f\colon A \to B$ una función y $B' \subseteq B$ entonces las siguientes afirmaciones son válidas:

1. Existe una única función $p\colon f^{-1}(B') \to B'$ tal que el siguiente diagrama conmuta:



2. Si tenemos el cuadrado conmutativo:

$$\begin{array}{ccc} P & \xrightarrow{a} & B' \\ {\scriptstyle b}\downarrow & & \downarrow{\scriptstyle i} \\ A & \xrightarrow[f]{} & B \end{array}$$

Entonces existe una única función $h\colon P \to f^{-1}(B')$ tal que el siguiente diagrama conmuta:

$$\begin{array}{ccccc} & & P & & \\ & {\scriptstyle b}\swarrow & \downarrow{\scriptstyle h} & \searrow{\scriptstyle a} & \\ A & \xleftarrow[j]{} & f^{-1}(B') & \xrightarrow[p]{} & B' \end{array}$$

Proposición 4.1.10 Sea $B' \leq B$ una subalgebra y $f\colon (A, \mu_A) \to (B, \mu_B)$ un homomorfismo de algebras entonces $f^{-1}(B')$ es una subalgebra de A.

Demostración. Usando el cuadrado conmutativo

$$\begin{array}{ccc} f^{-1}(B') & \xrightarrow{p} & B' \\ {\scriptstyle j}\downarrow & & \downarrow{\scriptstyle i} \\ A & \xrightarrow[f]{} & B \end{array}$$

Entonces aplicando Ω tenemos el cuadrado conmutativo:

$$\begin{array}{ccc} \Omega(f^{-1}(B')) & \xrightarrow{\Omega(p)} & \Omega(B') \\ {\scriptstyle \Omega(j)}\downarrow & & \downarrow{\scriptstyle \Omega(i)} \\ \Omega(A) & \xrightarrow[\Omega(f)]{} & \Omega(B) \\ {\scriptstyle \mu_A}\downarrow & & \downarrow{\scriptstyle \mu_B} \\ A & \xrightarrow[f]{} & B \end{array}$$

Por la proposición anterior existe una única función $\zeta\colon \Omega(f^{-1}(B')) \to f^{-1}(B')$ tal que p y j son homorfismos de Ω-algebras. ■

■ **Ejemplo 4.9** Sea $X = \{a, b, c\}$ y $Y = \{a, b\}$, definimos $f\colon P(X) \to P(Y)$ donde $f(B) = B - \{c\}$ entonces f es un homomorfismo de algebras (en este caso retículas). Consideremos $\mathbf{B} = \{\{a\}, \{a, b\}\}$ entonces $f^{-1}(\mathbf{B}) = \{\{a\}, \{a, c\}, \{a, b\}, \{a, b, c\}\}$ es una subalgebra. ■

Proposición 4.1.11 Sea $\{(X_i, \mu_i)\}_{i\in I}$ una familia de algebras entonces existe una única estructura $\mu\colon \Omega(\prod_{i\in I} X_i) \to \prod_{i\in I} X_i$ tal que las $\pi_i\colon \prod_{i\in I} X_i \to X_i$ son homomorfismos de algebras.

Demostración. Consideremos la familia $\{\mu_i \circ \Omega(\pi_i)\}_{i\in I}$ entonces por la propiedad universal del producto existe una única función $\mu\colon \Omega(\prod_{i\in I} X_i) \to \prod_{i\in I} X_i$ tal que el siguiente diagrama conmuta:

$$\begin{array}{ccc} \Omega(\prod_{i\in I} X_i) & \xrightarrow{\Omega(\pi_i)} & \Omega(X_i) \\ {\scriptstyle \mu}\downarrow & & \downarrow{\scriptstyle \mu_i} \\ \prod_{i\in I} X_i & \xrightarrow[\pi_i]{} & X_i \end{array}$$

■

Teorema 4.1.12 — Completación de Diagramas. Consideremos $f\colon (A,\mu_A) \to (B,\mu_B)$ y $g\colon (A,\mu_A) \to (C,\mu_C)$ homomorfismos de algebras con f sobreyectivo. Entonces son equivalentes:

1. $\ker f \subseteq \ker g$.
2. Existe un único homomorfismo de algebras $h\colon (B,\mu_B) \to (C,\mu_C)$ tal que $h \circ f = g$.

Demostración. Esta afirmación se puede deducir del 2.2.10, solo basta probar que si $h\colon B \to C$ es una función tal que $h \circ f = g$ entonces h es homomorfismo. Para ello consideremos el siguiente diagrama:

$$\begin{array}{ccccc} \Omega(A) & \xrightarrow{\Omega(f)} & \Omega(B) & \xrightarrow{\Omega(h)} & \Omega(C) \\ \downarrow{\scriptstyle \mu_A} & & \downarrow{\scriptstyle \mu_B} & & \downarrow{\scriptstyle \mu_C} \\ A & \xrightarrow[f]{} & B & \xrightarrow[h]{} & C \end{array}$$

tal que $\mu_C \circ \Omega(g) = g \circ \mu_A$ y $\mu_B \circ \Omega(f) = f \circ \mu_A$ entonces $\mu_C \circ \Omega(h) \circ \Omega(f) = h \circ \mu_B \circ \Omega(f)$ pero $\Omega(f)$ es sobreyectiva entonces $\mu_C \circ \Omega(h) = h \circ \mu_B$, mostrando que h es un homomorfismo de álgebras. ■

Ahora vamos a considerar las construcciones en donde los cocientes son algebras. Sea X un conjunto y R una relación de equivalencia entonces:

- $\pi\colon X \to X/R$ es una función sobreyectiva en donde $\ker \pi = R$.

Conversamente, si $f\colon X \to Y$ es una función sobreyectiva entonces $\ker f$ es una relación de equivalencia de X y además tenemos el diagrama conmutativo:

$$\begin{array}{ccc} X & \xrightarrow{\quad f \quad} & Y \\ & {\scriptstyle p}\searrow \quad \nearrow{\scriptstyle \cong} & \\ & X/\ker f & \end{array}$$

Dado que toda relación de equivalencia en un conjunto X es el núcleo de una función sobreyectiva, tenemos que:

1. Si $f\colon (X,\mu) \to (Y,\nu)$ es un homomorfismo de algebras entonces $Im\ f$ tiene una única estructura de algebra y entonces existe una única estructura de algebra en $X/\ker f$ tal que $p\colon X \to X/\ker f$ es un homomorfismo de algebras.
2. Si $R \subseteq (X,\mu)$ es una relación de equivalencia tal que X/R tiene una estructura de Ω-algebra y la proyección canónica $\pi_R\colon (X,\mu) \to (X/R,\zeta)$ es un homomorfismo de Ω-algebras entonces esta estructura coincide con la estructura inducida por $\ker \pi_R$ ya que $R = \ker \pi_R$. Esto ultimo dice que el siguiente diagrama de funciones se puede completar:

$$\begin{array}{ccc} \Omega(X) & \xrightarrow{\Omega(\pi_R)} & \Omega(X/R) \\ \downarrow{\scriptstyle \mu} & & \vdots{\scriptstyle \zeta} \\ X & \xrightarrow[\pi_R]{} & X/R \end{array}$$

y esto último equivale a pedir la siguiente afirmación:

$$\Omega(\pi_R)(a) = \Omega(\pi_R)(b) \Rightarrow\ \mu(a) R \mu(b)$$

Definición 4.1.7 — Congruencia. Decimos que una relación R en una algebra (X,μ) es de congruencia si existe un homomorfismo de algebras $f\colon (X,\mu) \to (Y,\nu)$ tal que $\ker f = R$.

Proposición 4.1.13 Sea (X, μ) una algebra del tipo binario, y $R \subseteq X \times X$ una relación de equivalencia. Entonces R es de congruencia si y solo si satisface la siguiente propiedad, para cada $a, b, c, d \in R$ tal que $a \sim b$ y $c \sim d$ entonces $\mu(a, c) \sim \mu(b, d)$.

Demostración. Usando que $\Omega(X) = X \times X$, entonces R es de equivalencia si y sólamente R satisface la siguiente propiedad:

$$\Omega(\pi_R)(a, b) = \Omega(\pi_R)(c, d) \Rightarrow \ \mu(a, c) R \mu(b, d)$$

Y esta última es equivalente a la propiedad de la proposición. ■

4.2. Propiedades básicas y ejemplos de Monoides, Grupos, Anillos y Campos.

Definición 4.2.1 — Monoide. Un monoide es una estructura algebrica $\mu\colon X \times X \to X$ tal que cumple las siguientes propiedades:

1. Asociativa.
2. Tiene neutro.

■ **Ejemplo 4.10** La estructura $(\mathbb{N}, +)$ es un monoide cuyo neutro es 0. ■

■ **Ejemplo 4.11** La estructura $(\mathbb{N} - \{0\}, *)$ es un monoide cuyo neutro es 1. ■

Proposición 4.2.1 Las siguientes afirmaciones son válidas para monoides.

1. Si M es un monoide y $S \leq M$ es una subálgebra, entonces S es un monoide.
2. Si $f\colon M \to N$ es un homomorfismo de monoides, entonces $f(M)$ es un monoide.
3. Si M, N son monoides entonces $M \times N$ son monoides.
4. Si M es un monoide y X una estructura algebraica tal que existe un isomorfismo $M \cong X$ entonces X es monoide.

Definición 4.2.2 — Grupo. Un grupo es una estructura algebraica $\mu\colon X \times X$ tal que cumple las siguientes propiedades:

1. Asociativa.
2. Tiene Neutro.
3. Tiene inversos.

Ademas decimos que un grupo es abeliano si es además conmutativo.

Consideremos la clase de la Ω-álgebra del tipo $n = (2, 1, 0)$. Sea X un conjunto y $\mu\colon \Omega(X) \to X$ una función, denotemos a sus operaciones inducidas:

$$\mu_2\colon X \times X \to X, \ \mu_1\colon X \to X, \ \mu_0\colon \ :\{*\} \to X$$

asi que para cada $(X, *)$ operación binaria que satisface los axiomas de grupo, podemos asociar;

1. $* = \mu_2$ como la multiplicación del grupo.
2. μ_1 como la función que envia cada elemento a a su elemento inverso a^{-1}.
3. μ_0 como la función $\mu_0(*) = e$, donde e es el neutro del grupo.

de esta manera podemos estudiar a los grupos y sus construcciones algebraicas. Por ejemplo podemos caracterizar de manera práctica los homomorfismos de grupos $f\colon G \to P$.

Proposición 4.2.2 Sea G y T grupos, una función $f\colon G \to T$ es un homomorfismo de grupos si y sólamente si para toda $a, b \in G$ se tiene $f(a *_G b) = f(a) *_T f(b)$.

Demostración. Si f es un homomorfismo de grupos, en particular se tiene la propiedad deseada. Conversamente si f tiene la propiedad deseada, entonces se tiene el diagrama conmutativo:

$$\begin{array}{ccc} G \times G & \xrightarrow{f \times f} & T \times T \\ {\scriptstyle \mu_2}\downarrow & & \downarrow{\scriptstyle \nu_2} \\ G & \xrightarrow[f]{} & T \end{array}$$

Basta ver la conmutatividad $\nu_1 \circ f = f \circ \mu_1$ y $\nu_0 \circ Id_{\{*\}} = f \circ \mu_0$, es decir probar:

1. Para toda $a \in G$ $f(a^{-1}) = (f(a))^{-1}$.
2. $f(e_G) = e_T$.

Para el segundo, tenemos que $f(e_G) = f(e_G * e_G) = f(e_G) * f(e_G)$ entonces al multiplicar por el inverso tenemos, $e_T = f(e_g)$. Para el primero usando las igualdades:

$$a * a^{-1} = e_G = a^{-1} * a$$

aplicamos la propiedad de f entonces:

$$f(a) * f(a^{-1}) = f(e_G) = e_T = f(a^{-1}) * f(a)$$

obteniendo por unicidad de los inversos que $f(a^{-1}) = (f(a))^{-1}$. ■

Proposición 4.2.3 Las siguientes afirmaciones son válidas para grupos.

1. Subalgebras de grupos son grupos. Más aún un subconjunto $H \subseteq G$ de un grupo es un subgrupo si y sólamente si $0 \in H$ y para toda $x, y \in H$ se tiene que $xy^{-1} \in H$.
2. Si $f\colon G \to P$ es un homomorfismo de grupos, entonces $f(G)$ es un subgrupo.
3. Si G, P son grupos entonces $G \times P$ son grupos.
4. Si G es un grupo y X es una estructura binaria tal que existe un isomorfismo $G \cong X$ entonces X es un grupo.

Vamos a explorar un poco más sobre los cocientes en grupos.

Proposición 4.2.4 Sea $f\colon G \to T$ un homomorfismo de grupos, entonces $(a, b) \in \ker f$ si y sólamente si $f(ab^{-1}) = e_T$.

Demostración. Si $(a, b) \in \ker f$ entonces $f(a) = f(b)$ entonces $f(ab^{-1}) = f(a)(f(b))^{-1} = f(a)(f(a))^{-1} = e_T$. Conversamente si $a, b \in G$ son tales que $f(ab^{-1}) = e_T$ entonces al multiplicar por $f(b)$ por la izquierda tenemos:

$$f(ab^{-1})f(b) = f(b) \Rightarrow \ f(ab^{-1}b) = f(b) \Rightarrow \ f(a) = f(b)$$

concluyendo que $(a, b) \in \ker f$. ■

Gracias a esta proposición, denotamos (por abuso de notación) al siguiente conjunto:

$$\ker f := \{g \in G |\ f(g) = e_T\}$$

Notemos que $\ker f$ es un subgrupo pues $\ker f = f^{-1}(\{e_T\})$ y $\{e_T\}$ es un subgrupo. Conversamente con el subgrupo $\ker f$ podemos recuperar la relación de equivalencia $\ker f$ diciendo $(a, b) \in \ker f$ si y sólamente si $ab^{-1} \in \ker f$. Con esto es natural preguntarse ¿Que subgrupos pueden definir una relación de congruencia?

Definición 4.2.3 — Relacion de congruencia. Dado $H \leq G$ un subgrupo, definimos la relación $\cong$ mód H como sigue:

$$a \cong b \mod H \Leftrightarrow ab^{-1} \in H$$

Proposición 4.2.5 $\cong$ mód H es una relación de equivalencia.

Demostración. Como ejercicio al lector. ■

Proposición 4.2.6 Son equivalentes para un subgrupo $H \leq G$:

1. $\cong$ mód H es una relación de congruencia.
2. $H = \ker f$ para algún morfismo de grupos sobreyectivo f.
3. Para toda $a \in G$ se tiene $aHa^{-1} \subseteq H$.
4. Para toda $a \in G$ se tiene $aHa^{-1} = H$.

Definición 4.2.4 — Subgrupo normal. Decimos que un subgrupo $H \leq G$ es normal si satisface alguna de las condiciones equivalentes de la proposición anterior.

Definición 4.2.5 — Anillo. Un anillo con 1 consiste en un conjunto R con dos estructuras $+\colon R \times R \to R$ y $*\colon R \times R \to R$ tal que:

1. $(R, +)$ es un grupo abeliano.
2. $(R - \{0\}, *)$ es un monoide.
3. El producto distribuye a la suma.

Proposición 4.2.7 Las siguientes afirmaciones son válidas para anillos:

1. Subalgebras de un anillo es un anillo.
2. Si $f\colon R \to T$ es un homomorfismo de anillos, entonces $f(R)$ es un anillo.
3. Si R, T son anillos entonces $R \times T$ son anillos.

Definición 4.2.6 — Tipos de anillos. Sea R un anillo con 1, diremos que es:

1. conmutativo si $(R - \{0\}, *)$ es un monoide conmutativo.
2. un anillo con división si $(R - \{0\}, *)$ es un grupo.
3. un campo si $(R - \{0\}, *)$ es un grupo abeliano.

4.3. Espacios vectoriales.

Definición 4.3.1 — Operación Externa. Sean X, Y conjuntos, una operación binaria externa es una función de la forma $\lambda\colon Y \times X \to X$.

Definición 4.3.2 — Espacio Vectorial. Sea K un campo. Un espacio vectorial sobre K consiste en un grupo abeliano $(V, +)$ junto a una operación externa $*\colon K \times V \to V$ (llamado producto escalar) tal que satisface las siguientes propiedades:

1. $\lambda * (\kappa * v) = (\lambda\kappa)v$.
2. $\lambda(v + w) = \lambda v + \lambda w$.
3. $(\kappa + \lambda)v = \kappa v + \lambda v$.
4. $1 * v = v$.

La clase de espacios vectoriales puede verse como una subclase del siguiente Ω-algebra. Para cada conjunto X, denotamos

1. $\Omega(X) = X \times X \coprod X \coprod \{*\} \coprod K \times X$.
2. Si $f\colon X \to Y$ es una función entonces $\Omega(f) = (f \times f) \coprod f \coprod \mathrm{Id}_{\{*\}} \coprod (\mathrm{Id}_K \times f)$.

Asi que dado una función $\mu\colon \Omega(X) \to X$ tenemos asignado sus operaciones:

$$\mu_2\colon X \times X \to X,\ \mu_1\colon X \to X,\ \mu_0\colon \{*\} \to X,\ \mu^e\colon K \times X \to X$$

Asi que cuando V es un K-espacio vectorial, tenemos que con las asignaciones:

1. μ_2 la suma de V.
2. μ_1 el inverso aditivo de V.
3. μ_0 el neutro aditivo de V.
4. μ^e la multiplicación escalar de K

Entonces V se puede ver como una Ω-algebra. Conviene dar unas primeras propiedades:

Proposición 4.3.1 Sea V un K-espacio vectorial entonces:

1. Para toda $v \in V$ se tiene $0_K * v = 0_V$.
2. Para toda $v \in V$ se tiene $(-1) * v = -v$.

Demostración. Ejercicio al lector. ■

Proposición 4.3.2 Sean V, W dos K-espacios vectoriales y $f\colon V \to W$ una función, entonces f es un homomorfismo de algebras si y sólamente si f satisface la siguiente propiedad:

$$\forall v, w \in V,\ \forall \lambda \in K,\ f(v + \lambda w) = f(v) + \lambda * f(w)$$

Demostración. Si f es homomorfismo de algebras entonces claramente satisface la propiedad de la proposición. Ahora para el converso si f satisface la propiedad de la proposición entonces poniendo $\lambda = 1$ obtenemos:

$$\forall v, w \in V,\ f(v + w) = f(v) = f(w)$$

y usando la caracterización para grupos, tenemos entonces que f preserva las sumas, inverso aditivo y neutros aditivos correspondientes. Luego, usando $v = 0$ tenemos que f preserva las multiplicaciones escalares correspondientes. ■

Proposición 4.3.3 Las siguientes afirmaciones son válidas:

1. Las subalgebras de un K-espacio vectorial es un K-espacio vectorial.
2. Si $f\colon V \to W$ es un homomorfismo de K-espacios vectoriales entonces $f(V)$ es un K-espacio vectorial.
3. Si V, W son espacios vectoriales entonces $V \times W$ es un espacio vectorial.

4.4. Ejercicios

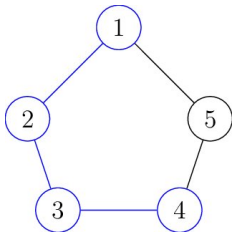
4.4.1. Estructuras Algebraicas.

1. Consideremos la estructura $(\mathbb{N}, +)$ y $n \in \mathbb{N}$, demuestra que el algebra subgenerada de $\{n\}$ es $\{m \in \mathbb{N} |\ m = nx,\ x \in \mathbb{N}\}$.
2. Consideremos la estructura $(\mathbb{N}, *)$ y $n \in \mathbb{N}$, demuestra que el algebra subgenerada de $\{n\}$ es $\{m \in \mathbb{N} |\ m = n^x,\ x \in \mathbb{N}\}$.
3. Consideremos la estrucutras $(\mathbb{N}, +)$ y $(\mathbb{N}, *)$ ¿En cuál de las dos estructuras, se puede ver a $Y = \{1\}$ como subálgebra y en cúal no? Explica.
4. Sea (X, μ) una estructura binaria que tiene elementro neutro $e \in X$, y sea $f\colon (X, \mu) \to (Y, \nu)$ un homomorfismo de algebras. Responde, demostrando si es cierto o dando un contraejemplo si es falso:
   a) ¿Es $Y = f(\{e\})$ una subálgebra?.
   b) ¿El único elemento de Y, denotado como n, será neutro de Y?.
   c) Misma pregunta pero ahora suponiendo que f es sobreyectivo.

5. Consideremos la estructura $(\mathbb{R}^2, +)$ (únicamente con la suma), ¿Cierto o falso? Demuestra en caso de ser cierto o dar un contraejemplo en caso de ser falso.
   a) El conjunto $l_m := \{(x, y) \in \mathbb{R}^2 |\ (x, y) = t(m, 1)\ t \in \mathbb{R}\}$ es una subalgebra de $(\mathbb{R}^2, +)$.
   b) El conjunto $q_m := \{(x, y) \in \mathbb{R}^2 |\ (x, y) = n(m, 1)\ n \in \mathbb{N}\}$ es una subalgebra de $(\mathbb{R}^2, +)$.
   c) El conjunto $W = \{(x, y) \in \mathbb{R}^2 |\ (x, y) \in \mathbb{N}^2\} \cup \{(-1, -1)\}$ es una subalgebra de $(\mathbb{R}^2, +)$.

4.4.2. Propiedades y ejemplos de estructuras binarias.

1. Consideremos el siguiente polígono denotado como P.



   Una simetría de P es una función entre sus vértices $f\colon v(P) \to v(P)$ tal que si ij es una arista en P entonces $f(i)f(j)$ es una arista en P. Resuelve:
   a) Encuentra todas las simetrías que se pueden hacer. Denotamos al conjunto de sus simetrías como $Sym(P)$.
   b) Consideremos a $Sym(P)$ junto a la composición. Muestra que esta estructura binaria satisface los axiomas de grupo. ¿Quien es el neutro?.
   c) Denotemos $\sigma \in Sym(P)$ a la simetria con la siguiente regla de correspondencia:

$$1 \to 2,\ 2 \to 3,\ 3 \to 4, 4 \to 5, 5 \to 1$$

   ¿Cierto o falso? El subgrupo generado de $\{\sigma\}$ es $Sym(P)$.
2. Sea $X := \{1, 2, \cdots, n\}$, denotamos a S_n como el conjunto de todas las permutaciones de X. Resuelve:
   a) Muestra que S_n junto a la composición de funciones, es un grupo. ¿Quien es el neutro?.
   b) Muestra que $Sym(P)$ se puede ver como un subgrupo de S_5.
   c) Da un ejemplo de un elemento de S_5 que no pueda estar en $Sym(P)$.
   d) Usando combinatoria, muestra que $|Sym(P)|$ divide a $|S_5|$. ¿Cuánto vale $|S_5|/|Sym(P)|$.
3. Sea (X, μ) una estructura binaria que es asociativa. Sean $e, f \in X$ tales que cada uno satisface el axioma del neutro, muestra que $e = f$. (Con esto se prueba que en cualquier monoide y cualquier grupo, los elementos neutros son únicos).
4. Sea $(G, *, e)$ un grupo y $a \in G$. Dados $v, w \in G$ tales que cada uno satisface el axioma de inverso para a, muestra que $v = w$. (Con esto se prueba que en cualquier grupo, los inversos son únicos y por tanto podemos denotar al único inverso como a^{-1}).
5. Sea $(G, *, e)$ un grupo muestra las siguientes identidades:
   a) Para toda $a \in G$, $(a^{-1})^{-1} = a$.
   b) Para toda $a, b \in G$, $(a * b)^{-1} = b^{-1}a^{-1}$. OJO: En los axiomas del grupo no se asume la conmutatividad.

   Hint: Muestra que el elemento propuesto, satisface el axioma de inverso del elemento entre paréntesis, y por el ejercicio anterior obtienes la igualdad.
6. Sea $(G, *, e)$ un grupo y $a \in G$, muestra que:
   a) El subgrupo generado de a es $\{\cdots, a^{-2}, a^{-1}, e, a, a^2, a^3, \cdots\}$.
   b) Si G es finito, muestra que existe alguna $n \in \mathbb{N}$ tal que $a^n = e$. Hint: Supon por contradicción de que no existe tal n, usa el inciso anterior y que G es finito para llegar a una contradicción,

7. Sea G un grupo finito, siguiendo el ejercicio anterior, para cada $a \in G$ denotamos $ord(a) := \min\{n \in \mathbb{N} | a^n = e\}$ y es llamado el orden de a. Demuestra:
   a) Para $a \in G$, muestra que la función $f_a \colon G \to G$ definida como $f_a(x) = a * x$ es biyectiva. Hint: Como G es finito, basta ver que f_a es inyectiva.
   b) Si $h = |G|$, muestra que $a^h = e$.
   c) Muestra que $ord(a)$ divide a h. Concluye de que si G tiene orden 7, entonces todo elemento $a \neq e$ satisface $ord(a) = 7$.
   d) Si $f \colon G \to P$ es un homomorfismo de grupos entonces $ord(f(a))$ divide a $ord(a)$.
   e) Si G es de tamaño 7, P es de tamaño 5, $a \in G$ de orden 7 y $b \in P$ de orden 5, muestra que $ord(a, b) = 35$. Hint: Considera los homomorfismo de proyecciones coordenadas $G \times P \to P$ y $G \times P \to G$ y el inciso anterior.

4.4.3. Propiedades y ejemplos de estructuras con más de una operación.

1. Consideremos el anillo de polinomios $F[x]$ con F un campo. Denotemos $F_n[x] := \{p(x) \in F[x] | \ \partial p \leq n\}$. Muestra que si $n \neq 0$ entonces $F_n[x]$ no es un subanillo pero si es un subespacio vectorial sobre F.
2. Considera X un conjunto con al menos dos elementos. ¿$(\mathbf{P}(X), \cap, \cup)$ es un anillo? Si no es asi, ¿Que propiedades no cumple para ser anillo?
3. Un cuadrado mágico es una matriz cuadrada $M = (a_{ij})_{1 \leq i,j \leq n}$ con la propiedad de que la suma de una fila es igual a la suma de una columna y también es igual a la suma de sus diagonales, es decir satisface las siguientes ecuaciones para $(a_{ij})_{1 \leq i,j \leq n}$:

$$\sum_{s=1}^{n} a_{is} = \sum_{s=1}^{n} a_{sj} = \sum_{s=1}^{n} a_{ss} = \sum_{s=1}^{n} a_{s,n-s+1}$$

   entonces a cada cuadrado mágico M denotamos c_M a la suma $\sum_{s=1}^{n} a_{ss}$. Denotamos $MS_n := \{(M, c_M) | \ M$ es cuadrádo mágico de suma $c_M\}$. Resuelve:
   a) Muestra que MS_n es un $\mathbb{R}$-espacio vectorial. ¿Quién es el neutro?.
   b) Muestra que $f \colon MS_n \to \mathbb{R}$ definido como $f(M, c_M) = c_M$ es $\mathbb{R}$-lineal.
   c) Muestra que la siguiente matriz es un cuadrado mágico tal que está en el $\ker f$.

$$\begin{pmatrix} 0 & 1 & -1 \\ -1 & 0 & 1 \\ 1 & -1 & 0 \end{pmatrix}$$

   d) Construye 10 cuadrados mágicos distintos de números naturales cuya suma sea 15. Argumenta como lo obtuviste.
4. Definimos $V := \{f \colon \mathbb{R} \to \mathbb{R} | \ f(-x) = -f(x), \ \forall x \in \mathbb{R}\}$, muestra que V es un $\mathbb{R}$-espacio vectorial.
5. Demuestra lo siguiente:
   a) Sea R un anillo, decimos que un elemento $a \in R - \{0\}$ es un divisor cero si existe $b \in R - \{0\}$ tal que $ab = 0$. Muestra que si $1 \neq 0$ entonces ningun divisor cero es invertible.
   b) Sea F un anillo con división, muestra que $F \times F$ no puede ser un anillo con división.
6. Decimos que un anillo conmutativo R es un dominio entero si no tiene divisores cero. Muestra lo siguiente.
   a) Sea R un anillo conmutativo y $a \in R$ no cero, denotamos $f_a \colon R \to R$ la función definido como sigue $f_a(x) = a * x$. Muestra que a no es divisor cero si y sólo si f_a es inyectivo.
   b) Demuestra que si D es un dominio entero finito, muestra que D es un campo. Hint: Prueba que $f_a \colon D \to D$ es una función biyectiva para toda $a \neq 0$.

7. Definamos $\mathbb{Q}[i] := \{a + bi |\ a, b \in \mathbb{Q}\}$, encuentra las operaciones de suma y multiplicación de tal manera que extienda las operaciones de $\mathbb{Q} \subseteq \mathbb{Q}[i]$.

Capítulo 5

Teoria de Ecuaciones Lineales

De aqui en adelante asumiremos que K es un campo y V es un K-espacio vectorial

5.1. Bases y Matriz de rerepsentación

Proposición 5.1.1 Sea $S \subseteq V$, entonces:

$$\langle S\rangle = \{\sum_{k=1}^{n} \lambda_k v_k |\ \lambda_k \in K,\ v_k \in S,\ n \in \mathbb{N}\}$$

Demostración. Consideremos $W = \{\sum_{k=1}^{n} \lambda_k v_k |\ \lambda_k \in K,\ v_k \in S,\ n \in \mathbb{N}\}$, vamos a mostrar primero que W es subespacio vectorial. Notemos que $0 \in W$ pues:

$$0 = \sum_{k=1}^{n} 0 * v_k$$

Luego si $v, v' \in W$ descritos como:

$$v = \sum_{k=1}^{n} \lambda_k v_k \tag{5.1}$$

$$v' = \sum_{k=1}^{n'} \lambda'_k v_k \tag{5.2}$$

Entonces para cada $\lambda \in K$:

$$v - \lambda * v' = \sum_{k=1}^{\max n,n'} (\lambda_k - \lambda * \lambda'_k) v_k$$

asi que obtenemos $v - \lambda * v' \in W$ por tanto W es subespacio vectorial, y además para cada $v \in S$ entonces $v = 1 * v \in W$ obteniendo $S \subseteq W$. Ahora si W' es otro subespacio vectorial tal que $S \in W$, entonces para cada $\sum_{k=1}^{n} \lambda_k v_k \in W$, como cada $v_k \in S \subseteq W'$ y W' es un subespacio vectorial entonces $\sum_{k=1}^{n} \lambda_k v_k \in W'$, obteniendo $W \subseteq W'$ y por la definición de subespacio obtenemos que $\langle S\rangle = W$ ■

■ **Ejemplo 5.1** Si $V = \mathbb{R}^2$ entonces:
1. $\langle\{(1,0),(0,1)\}\rangle = \mathbb{R}^2$.
2. $\langle\{(2,3),(-1,1)\}\rangle = \mathbb{R}^2$.

3. $\langle\{(1,1),(2,2)\}\rangle = \{(x.x)|\ x \in \mathbb{R}\}$.
4. $\langle\{(1,1),(2,3),(6,-1)\rangle = \mathbb{R}^2$,
5. $\langle\{(2,4),(-1,-2),(10,20)\}\rangle = \{(t,2t)|\ t \in \mathbb{R}\}$

■

Notemos que es posible encontrar conjuntos distintos que generan el mismo espacio vectorial. Una pregunta natural ¿Que propiedades debe tener un conjunto de tal manera de que cada elemento sea importante para generar dicho conjunto?.

Proposición 5.1.2 Sea $S \subseteq V$ entonces son equivalentes:

1. $\langle S\rangle = \langle S - \{x_0\}\rangle$, para algún $x_0 \in S$.
2. Existen $v_1, \cdots, v_n \in S$ tales que existen $\lambda_1, \cdots, \lambda_n$ no todos cero con la propiedad:

$$\sum_{k=1}^{n} \lambda_k v_k = 0$$

Demostración. Si para algún $x_0 \in S$ se cumple que $\langle S\rangle = \langle S - \{x_0\}\rangle$, entonces existen $x_1, \cdots, x_n \in S - \{x_0\}$ tales que:

$$x_0 = \sum_{i=1}^{n} \alpha_i x_i,\ \ \alpha_i \in K$$

con α_i no todos cero. Conversamente, tenemos que $\langle S - \{x_0\}\rangle \subseteq \langle S\rangle$ para todo $x_0 \in S$, por hipótesis, existen $v_1, \cdots, v_n \in S$ tales que existen $\lambda_1, \cdots, \lambda_n$ no todos cero con la propiedad:

$$\sum_{k=1}^{n} \lambda_k v_k = 0$$

supongamos sin pérdida de generalidad que $\lambda_1 \neq 0$ entonces:

$$v_1 = \sum(-\frac{\lambda_k}{\lambda_1})v_k$$

esto implica que para cada $v \in \langle S\rangle$ tal que:

$$v = \alpha_1 v_1 + \sum_{v \neq v_0} \lambda_i v_i$$

entonces:

$$v = \sum_{v \in S - \{v_1\}} \delta_v v$$

por lo tanto $\langle S\rangle = \langle S - \{v_1\}\rangle$. ■

Definición 5.1.1 — Dependencia e Independencia Lineal. Decimos que un subconjunto $S \subseteq V$ es linealmente dependendiente si satisface alguna de las condiciones equivalentes de (5.1.2). En caso contrario diremos que S es linealmente independiente.

■ **Ejemplo 5.2** Tenemos la lista de los siguientes subconjuntos: ■

Ahora vamos a determinar la importancia en los conjuntos linealmente independientes.

Definición 5.1.2 — Suma interna. Sean $W_1, W_2 \leq V$ dos subespacios, entonces definimos el espacio suma interna como:

$$W_1 + W_2 = \langle W_1 \cup W_2 \rangle$$

Sabemos que todo elemento $w \in W_1 + W_2$ por (5.1.1) se puede escribir de la forma $w = w_1 + w_2$, en donde $w_1 \in W_1$ y $w_2 \in W_2$. Una pregunta es ¿Dicha descomposición lineal es única?

Proposición 5.1.3 Sean $W_1, W_2 \leq V$ dos subespacios vectoriales, entonces son equivalentes:

1. $W_1 \cap W_2 = 0$.
2. Si $w_1 + w_2 = w_1' + w_2' \in W_1 + W_2$ entonces $w_1 = w_1'$ y $w_2 = w_2'$.

Demostración. Supongamos que $W_1 \cap W_2 = 0$, entonces supongamos que $w_1 + w_2 = w_1' + w_2' \in W_1 + W_2$ donde $w_1, w_1' \in W_1$ y $w_2, w_2' \in W_2$, entonces:

$$w_1 - w_1' = w_2' - w_2 \in W_1 \cap W_2$$

pero por hipótesis obtenemos $w_1 = w_1'$ y $w_2 = w_2'$. Conversamente, supongamos que $w \in W_1 \cap W_2$ entonces como $w \in W_1 + W_2$ existen $v_1 \in W_1$ y $v_2 \in W_2$ tal que:

$$0 + w = w + 0 = w = v_1 + v_2$$

y por hipótesis obtenemos $v_1 = 0$ y $v_2 = 0$ es decir $W_1 \cap W_2 = 0$. ■

Una consecuencia interesante de esto es lo siguiente

Definición 5.1.3 — Suma directa. Dados $W_1, W_2, \cdots, W_n \leq V$ subespacios vectoriales, decimos que la suma interna $W_1 + W_2 + \cdots + W_n$ es una suma directa (interna) si todo elemento $w \in W_1 + W_2 + \cdots + W_n$ se puede escribir de manera única como elementos:

$$w = w_1 + w_2 + \cdots + w_n, \ w_i \in W_i$$

En tal caso denotamos a la suma interna como $W_1 \oplus W_2 \oplus \cdots \oplus W_n$.

Proposición 5.1.4 Sean $W_1, \cdots, W_n \leq V$ subespacios, entonces son equivalentes:

1. La suma interna de las W_i's es directa.
2. Para toda $i = 1, \cdots, n$, se tiene que $W_i \cap (\sum_{j \neq i} W_j) = 0$.

Demostración. Supongamos (1) válido, entonces si $w \in W_i \cap (\sum_{i \neq j} W_j)$ entonces existe una combinación lineal:

$$w = \sum_{j=1, i \neq j}^{n} w_j + 0 w_i, \ w_j \in W_j$$

Pero por otro lado

$$w = \sum_{j=1, i \neq j}^{n} 0 * w_j + 1 w, \ w_j \in W_j$$

Entonces por definición de suma interna, implica que $w_i = 0$ para toda i, obteniendo que $w = 0$. Conversamente, supongamos que w tiene descripciones:

$$\sum_{i=1}^{n} w_i = w = \sum_{i=1}^{n} w_i'$$

Entonces para cada j fija:

$$w_j - w'_j = \sum_{i \neq j}^{n} (w_i - w'_i) \in W_i \cap (\sum_{i \neq j} W_j)$$

por hipótesis, implica que $w_j = w'_j$ para cada $j = 1, \cdots, n$. ■

Proposición 5.1.5 Sean $W_1, \cdots, W_n \leq V$ un subespacios tales que $W_i = \langle S_i \rangle$ con S_i linealmente indepen-diente, entonces son equivalentes:

1. La suma interna de las W_i es directa.
2. La unión de las S_i es un conjunto linealmente independiete.

Demostración. Supongamos válido (1) entonces tomemos una combinación lineal:

$$\sum_{i=1}^{m_1} \lambda_i^{(1)} s_i^{(1)} + \cdots + \sum_{i=1}^{m_n} \lambda_i^{(n)} s_i^{(n)} = 0$$

como la suma interna es directa esto implica que $\lambda_i^(j) = 0$ para toda i, j, por tanto la union de las $S'_i s$ es linealmente independiente. Conversamente supongamos que para alguna $w \in \sum_{i=1}^{n} W_n$ se tiene descripciones:

$$\sum_{i=1}^{n} w_i = w = \sum_{i=1}^{n} w'_i$$

Entonces:

$$\sum_{i=1}^{n} (w_i - w'_i) = 0$$

Escribiendo $w_i - w'_i \in W_i = \langle S_i \rangle$ obtenemos una combinación lineal del 0 en $\langle \bigcup_{i=1}^{n} S_i \rangle$ pero por hipótesis eso implica que $w_i = w'_i$ para cada $i = 1, \cdots, n$, por lo tanto la suma interna es directa. ■

Una consecuencia directa de lo anterior es:

Proposición 5.1.6 Si $S = \{v_1, \cdots, v_n\}$ entonces son equivalentes:

1. S es linealmente independiente.
2. $\langle S \rangle = \bigoplus_{v \in S} \langle v \rangle$.

Proposición 5.1.7 Denotemos $\mathcal{L}, \mathcal{D}$ como la familia de conjuntos linealmente independietes y linealmente dependientes de V respectivamente. Las siguientes afirmaciones son válidas:

1. Si $S \in \mathcal{L}$ y $S' \subseteq S$ entonces $S' \in \mathcal{L}$.
2. Si $S \in \mathcal{D}$ y $S \subseteq S'$ entonces $S' \in \mathcal{D}$.
3. Sea $\{S_i\}_{i \in I} \subseteq \mathcal{L}$ tal que $S_i \subseteq S_j$ ó $S_j \subseteq S_i$ para toda $i, j \in I$, entonces $\bigcup S_i \in \mathcal{L}$.

Demostración. Para (1), consideremos la siguiente combinación lineal en S':

$$\sum_{v \in S'} \lambda_v v = 0$$

entonces se tiene la combinación lineal:

$$\sum_{v \in S'} \lambda_v v + \sum_{v \in S - S'} 0 * v = 0$$

pero S es linealmente independiente, entonces :

$$\lambda_v = 0, \ \forall v \in S'$$

por lo tanto S' es l.i. Para (2), como S es l.d., entonces existe $x \in S$ tal que $\langle S\rangle = \langle S - \{x\}\rangle$, tomemos $v \in \langle S\rangle$ tal que tiene combinación lineal con x, digamos:

$$v = \lambda_x x + \sum_{v \neq x} \lambda_v v$$

Pero existen $v \in S - \{x\}$ tales que:

$$x = \sum_{v \in S',\ v \neq x} \delta_v v$$

obteniendo

$$v = \sum_{w \in S, w \neq v} \alpha_w w + \sum_{w \in S' - S} \alpha_w w$$

por lo tanto $\langle S'\rangle = \langle S' - \{v\}\rangle$. Para el (3) punto, tomemos $v_1, \cdots, v_n \in \bigcup_{i\in I} S_i$, entonces existen $i_1, \cdots, i_n \in I$ tales que $v_j \in S_{i_j}$, por hipótesis existe $i = i_{j'}$ tal que $S_{i_k} \subseteq S_i$ para toda $i_1, i_2, \cdots, i_n$, y entonces $\{v_1, \cdots, v_n\} \subseteq S_i$, pero como S_i es l.i. entonces $v_1, \cdots, v_n$ tiene como unica combinación lineal del 0, coeficientes cero, por lo tanto $\bigcup_{i\in I} S_i$ es l.i. ■

Lo anterior nos describe que podemos encontrar un subconjunto S con las siguientes propiedades:

1. S es linealmente independiete.
2. $V = \langle S\rangle$.

De esta manera, tenemos que todo elemento de v se puede escribir de manera única como una combinación lineal de S, a esta propiedad será llamado base del espacio vectorial.

Definición 5.1.4 Un subconjunto $S \subseteq V$ se llama base de V si satisface las siguientes propiedades:

1. S es linealmente independiete.
2. $V = \langle S\rangle$.

Para asegurar la existencia, requerimos el siguiente lema de conjuntos:

Proposición 5.1.8 — Lema de Zorn. Si P es un conjunto ordenado tal que para todo subconjunto $S \subseteq P$ que sea un orden lineal (tambien llamado una cadena), cumple la propiedad de que S tiene una cota superior, entonces P tiene un elemento maximal.

La prueba es un poco más general, y se menciona en el siguiente teorema sin demostración.

Proposición 5.1.9 Las siguientes afirmaciones son equivalentes:

1. El lema de Zorn se satisface.
2. El axioma de elección se satisface.

Una vez establecido, podemos demostrar la existencia de las bases:

Proposición 5.1.10 Todo espacio vectorial V tiene una base.

Demostración. Sea $\mathbf{L}$ la colección de todos los subconjuntos linealmente independientes, por una proposición anterior, probamos que toda cadena en $\mathbf{L}$ tiene una cota superior, entonces por el Lema Zorn, existe un $S \in \mathbf{L}$ que es un elemento maximal. Vamos a probar que S es una base, tenemos que $\langle S\rangle \subseteq V$, ahora supongamos que es una contención estricta, es decir existe una $v \in V - \langle S\rangle$, entonces $\langle S\rangle \subset \langle S \cup \{v\}\rangle$, entonces $S \cup \{v\}$ es l.i. pero eso contradice que a que S sea el elemento maximal, por lo tanto $\langle S\rangle = V$. ■

Proposición 5.1.11 Las siguientes afirmaciones son validas:

1. Si S es linealmente independiente y S' es linealmente dependiente entonces $|S| \leq |S'|$.
2. Todas las bases tienen la misma cardinalidad.

La afirmación la dejaremos sin prueba.

Definición 5.1.5 — Dimensión de un espacio vectorial.. Dado V un espacio vectorial sobre K definimos la dimensión como $\dim_K V = |S|$ donde S es una base de V.

Por las proposiciones anteriores tenemos que la dimensión está bien definida.

Proposición 5.1.12 Sea V un espacio vectorial de dimensión con cardinalidad $|I|$, entonces tenemos el isomorfismo K-lineal:

$$V \cong \{f\colon I \to K|\ \sup(f) \text{ es finito}\}$$

Sabemos que $\prod_I K$, el producto de $|I|$-copias de K es canónicamente biyectivo a $Fun(I,V)$, a $Fun(I,V)$ le dotamos de estructura de K-espacio vectorial mediante la estructura del producto de algebras y se lo heredamos mediante la biyección canonica, entonces tenemos una función K-lineal e inyectiva:

$$\{f\colon I \to K|\ \sup(f) \text{ es finito}\} \to \prod_I K$$

que es un isomorfismo cuando I es finito (gracias a que la propiedad de que $\sup(f)$ sea finito, lo cumple toda función $f\colon I \to K$ cuando I es finito), entonces en general se puede entender (como estructura de espacio vectorial) todo espacio V de dimensión finita si se entiende la estructura del espacio K^n. En este capítulo estudairemos únicamente espacios vectoriales de dimensión finita. Ahora, sea V un espacio vectorial de dimensión finita (digamos n), tenemos que el isomorfismo (pasando por el isomorfismo de 5.1.12):

$$\gamma_S\colon V \to K^n$$

Depende de la elección de la base. Más especificamente, si $S = \{v_1, \cdots, v_n\}$ es una base ordenada de V, el isomorfismo está dado como:

$$\gamma_S\left(\sum_{i=1}^n \lambda_i v_i\right) = (\lambda_1, \cdots, \lambda_n)$$

denominamos al valor $\gamma_S(v)$ como la **matriz (o el vector) de representación de v en la base S.** Ahora si $P = \{w_i\}_{i=1}^n$ es otra base de V, usando la biyección $S \cong P$ entonces existe un isomorfismo lineal $\nu_S^P\colon K^n \to K^n$ construido como sigue:

1. Si $\sum_{i=1}^n \lambda_i v_i = v = \sum_{i=1}^n \theta_i w_i$ son sus únicas descripciones de v en cada base. En particular para cada $j = 1, \cdots, n$ existen únicos escalares $\theta_i^{(j)}$ tales que:

$$v_j = \sum_{i=1}^n \theta_i^{(j)} w_i$$

2. Entonces en general se tiene:

$$\sum_{i=1}^n \theta_i w_i = v = \sum_{j=1}^n \lambda_j v_j = \sum_{j=1}^n \lambda_j \left(\sum_{i=1}^n \theta_i^{(j)} w_i\right)$$

3. Esto anterior usando sus matrices de representación, definamos la matriz cuadrada $A = (a_{ij})$ como $a_{ij} := \theta_i^{(j)}$ y entonces se tiene:

$$\begin{pmatrix} \theta_1 \\ \vdots \\ \theta_n \end{pmatrix} = \begin{pmatrix} \theta_1^{(1)} & \cdots & \theta_1^{(n)} \\ \vdots & & \vdots \\ \theta_n^{(1)} & \cdots & \theta_n^{(n)} \end{pmatrix} \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix}$$

Es decir $\nu_S^P(\gamma_S(v)) = \gamma_P(v)$.

Basta probar que es un isomorfismo.

Proposición 5.1.13 Para todo par de bases finitas S, P en V se cumple:

$$\nu_S^P \circ \nu_P^S = \mathrm{Id}_{K^n} = \nu_P^S \circ \nu_S^P$$

Para acompletar, tenemos el siguiente lema técnico.

Proposición 5.1.14 Sea K^n con la base canónica, entonces para toda función lineal $f\colon K^n \to K^m$ le corresponde una única matriz $A \in \mathbf{M}_{n\times m}(K)$ tal que para toda $v \in K^n$ se cumple:

$$f(v) = A \cdot v$$

Esta manera de pensar en representaciones matriciales se puede extender para todo morfismo lineal, como sigue.

Teorema 5.1.15 — Representación matricial. Sean V, W dos espacios de dimensión finita, fijemos las bases $S_V \subseteq V$ y $S_W \subseteq W$ y sea $f\colon V \to W$ una función K-lineal, entonces existe una única matriz T_f cuya única función lineal asociada $\hat{f}(v) = T_f \cdot v$ satisface el siguiente diagrama conmutativo de funciones K-lineales:

$$\begin{array}{ccc} V & \xrightarrow{\gamma_{S_V}} & K^n \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle \hat{f}} \\ W & \xrightarrow[\gamma_{S_W}]{} & K^m \end{array}$$

en donde $n = \dim_K V$ y $m = \dim_K W$.

■ **Ejemplo 5.3** Consideremos $f\colon K_{n+1}[x] \to K_n[x]$ definido como $f(p(x)) = \frac{dp}{dx}(x)$ la derivación formal, entonces: ■

5.2. Teoría general de Ecuaciones Lineales.

Muchos problemas en matemáticas se pueden modelar en un problema lineal.

■ **Ejemplo 5.4 — Los cuadrados mágicos.** ■

■ **Ejemplo 5.5 — Sistema de Ecuaciones Lineales.** ■

■ **Ejemplo 5.6 — Corrientes electricas.** ■

■ **Ejemplo 5.7 — Interpolación lineal.** ■

Cada uno de estos problemas se puede presentar como sigue:

- Dado $f\colon V \to W$ una función lineal y $b \in W$, resolver la ecuación:

$$f(x) = b.$$

Primero estudiaremos la unicidad.

Proposición 5.2.1 Sea $f\colon V \to W$ una función lineal y $b \in W$, supongamos que existe una $x_0 \in V$ tal que $f(x_0) = b$ entonces el conjunto solución del problema anterior es:

$$x_0 + \ker f = \{y \in W |\ y = x_0 + h,\ \ f(h) = 0\}$$

Esto me dice en particular que la solución es única si y sólamente si $\ker f = 0$.

Gracias a la afirmación anterior, tenemos que para resolver el problema, se puede resumir en dos pasos:

1. La parte **homogénea**, es decir resolver la ecuación $f(x) = 0$, de esta manera describirás $\ker f$. Luego si $\ker f = 0$, esto es lo mismo que decir que la única solución de la ecuación $f(x) = 0$ es $x = 0$.
2. La parte **no homogénea**, es decir basta encontrar una solución particular de $f(x) = b$ y entonces toda solución será de la forma $y = x_0 + h$ donde h es la solución de la parte homogénea, al menos que la solución sea única.

5.2.1. Teorema del Rango-Nulidad.

Es posible decir sobre la solución de un problema lineal en algunos casos con solo conocer las dimenciones del problema.

Definición 5.2.1 — Rango y Nulidad. Sea $f\colon V \to W$ una función K-lineal entre espacios de dimensión finita. definimos:

1. El rango de f como $Ran(f) = \dim_K f(V)$.
2. La nulidad de f como $null(f) = \dim_K \ker(f)$.

Proposición 5.2.2 Sea $f\colon V \to W$ una función K-lineal sobreyectiva con V de dimensión finita, entonces la dimensión de W es finita.

Proposición 5.2.3 Sea $f\colon V \to W$ una función K-lineal entre espacios de dimensión finita, entonces:

$$\dim_K(V/\ker f) = \dim_K V - \dim_K \ker(f)$$

Como consecuencia directa de estas dos afirmaciones, tenemos el teorema de Rango-Nulidad.

Teorema 5.2.4 — Teorema del Rango-Nulidad. Sea $f\colon V \to W$ una función K-lineal entre espacios de dimensión finita. Entonces:

$$\dim_K V = Ran(f) + Null(f)$$

He aquí algunos resultados interesantes:

■ **Ejemplo 5.8** Sea $f\colon V \to K$ una función K-lineal con $n = \dim_K V$ mayor que 1. Si f no es cero, entonces existe alguna $x \in V$ tal que $f(x) = 1$, entonces $\langle f(x)\rangle = K$ por tener la misma dimensión, esto me dice que f es sobreyectivo y por lo tanto $f(V) = K$ es decir $Ran(f) = 1$, concluyendo por el teorema del Rango-Nulidad:

$$Null(f) = n - 1$$

¿Y qué me dice esto? Me dice en particular que para toda función lineal $f\colon K^n \to K$:

1. Si $c \in K$ entonces la ecuación $f(x) = c$ siempre tiene solución.
2. Dicha solución no es única, pues como $n > 1$ entonces $Null(f) = n - 1 > 0$, es decir que $\ker f \neq 0$ y por tanto toda solución es de la forma $y = x_0 + h$ para alguna solución x_0 particular y todas las homogéneas $h \in \ker f$. ¿Cuantas? Esta pregunta se resuelve usando que $\ker f$ es de dimensión finita, digamos $r > 0$ entonces $|\ker f| = |K|^r$. En particular para campos infinitos, como $\mathbb{R}$, nos dice que la solución de la ecuación lineal en $\mathbb{R}$:

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = c$$

existe y hay una infinidad de soluciones distintas.

■

■ **Ejemplo 5.9** ¿Bajo que condiciones un problema lineal $f\colon K^n \to K^m$ tiene solución única? En este problema, buscamos que $Null(f) = 0$, por el teorema de Rango-Nulidad tenemos que $n = Ran(f)$ pero

como $f(V) \leq K^m$ entonces:

$$n \leq m$$

Obteniendo que las condiciones necesarias y suficientes son:

1. $n \leq m$.
2. Existan n soluciones linealmente independientes.

■

■ **Ejemplo 5.10** Sea $f\colon K^n \to K^m$ y $c \in K^m$ entonces el problema $f(x) = c$ siempre tiene solución si y sólamente si existen $n - m$ soluciones homogéneas linealmente independientes. ■

■ **Ejemplo 5.11** Sea $f\colon K^4 \to K^3$ tal que $Ran(f) = 2$, entonces si $(c_1, c_2, c_3) \in f(K)$, tenemos que la solución del sistema:

$$\begin{cases} a_{11}x + a_{12}y + a_{13}z + a_{14}w &= c_1 \\ a_{21}x + a_{22}y + a_{23}z + a_{24}w &= c_2 \\ a_{31}x + a_{32}y + a_{33}z + a_{34}w &= c_1 \end{cases}$$

es de la forma $y = y_p + \lambda_1 v_1 + \lambda_2 v_2$ en donde v_1, v_2 son soluciones homogéneas linealmente independientes.

■

■ **Ejemplo 5.12** Sea $f\colon K^3 \to K^7$, entonces existen al menos 5 vectores linealmente independientes w_1, w_2, w_3, w_4, w_5 tales que ninguno de los problemas individuales:

$$f(x) = w_1,\ f(x) = w_2,\ f(x) = w_3,\ f(x) = w_4,\ f(x) = w_5$$

Tiene solución. ■

5.3. Método de Gauss-Jordan para la solucion de sistemas lineales.

Parte II

Algebra Superior II

Capítulo 6

Anillos conmutativos y números enteros

6.1. La construcción de Grothendieck.

Sea $(M, *, 1)$ un monoide conmutativo (ejemplo $(\mathbb{N}, +, 0)$) deseamos construir un grupo adecuado que extienda a M y admita inversos.

Definición 6.1.1 — El grupo abeliano asociado a un monoide conmutativo. Sea $(G, *, \hat{1})$ un grupo abeliano, decimos que es el grupo asociado a M si existe un homomorfismo $j\colon M \to G$ tal que para todo homomorfismo $f\colon M \to T$ con T un grupo abeliano, existe un único homomorfismo $\hat{f}\colon G \to T$ tal que el siguiente diagrama conmuta:

$$\begin{array}{ccc} M & \xrightarrow{j} & G \\ & \searrow^{f} & \downarrow \hat{f} \\ & & T \end{array}$$

■ **Ejemplo 6.1** Si G es un grupo abeliano, entonces en particular es un monoide conmutativo, asi que $\mathrm{Id}_G\colon G \to G$ es el grupo abeliano asociado a G. ■

Proposición 6.1.1 Si existe el grupo abeliano asociado a M entonces este es único salvo isomorfismos.

Demostración. Primero notemos lo siguiente: Sea $j\colon M \to G$ el grupo abeliano asociado a M ey $f\colon G \to G$ un homomorfismo de grupos tal que el siguiente diagrama conmuta:

$$\begin{array}{ccc} M & \xrightarrow{j} & G \\ & \searrow^{j} & \downarrow f \\ & & G \end{array}$$

usando la definición (6.1.1) se tiene que $f = \mathrm{Id}_G$.

Ahora tomemos $j\colon M \to G$ y $j'\colon M \to G'$ dos grupos abelianos asociados a M, por definición de j existe un único homomorfismo $f\colon G \to G$ tal que el siguiente diagrama conmuta:

$$\begin{array}{ccc} M & \xrightarrow{j} & G \\ & \searrow^{j'} & \downarrow f \\ & & G' \end{array}$$

de manera similar, por definición de j' existe un único homomorfismo $g\colon G' \to G$ tal que:

$$\begin{array}{ccc} M & \xrightarrow{j'} & G' \\ & \searrow^{j} & \downarrow g \\ & & G \end{array}$$

Esto implica el siguiente diagrama conmutativo

$$\begin{array}{ccc} M & \xrightarrow{j} & G \\ & \searrow^{j} & \downarrow g\circ f \\ & & G \end{array}$$

pero sabemos que implica que $g \circ f = \mathrm{Id}_G$, de manera análoga $f \circ g = \mathrm{Id}_{G'}$ por lo tanto $G \cong G'$. ■

■ **Ejemplo 6.2** Si G es un grupo abeliano y $\gamma\colon G \to T$ es un isomorfismo , entonces se puede ver que es el grupo abeliano asociado a G y directamente es claro (comparando con el último ejemplo) que son isomorfos $G \cong T$. ■

Ahora resta asegurar la existencia con la construcción de algún grupo asociado a un monoide conmutativo, dicha construcción se llama **construcción de Grothendieck** y se hace como sigue: Consideremos el monoide $M \times M$ y definimos la siguiente relación

$$(m,n) \sim (m',n') \;\Leftrightarrow\; m * n' * k = m' * n * k, \quad \text{para algún } k \in M$$

Proposición 6.1.2 La relación definida anteriormente es de equivalencia.

Demostración. Tomemos $(m,n) \in M \times M$, como $m * n * 1 = m * n * 1$ entonces $(m,n) \sim (m,n)$. Luego si $(m,n) \sim (m',n')$ entonces $m * n' * k = m' * n * k$, por conmutatividad de la igualdad (ya que $\triangle$ es de equivalencia) tenemos $m' * n * k = m * n' * k$, es decir $(m',n') \sim (m,n)$. Por último, consideremos que $(m,n) \sim (m',n')$ y $(m',n') \sim (m'',n'')$, asi que por definición se tiene las ecuaciones

$$m * n' * k = m' * n * k \tag{6.1}$$

$$m' * n'' * k' = m'' * n' * k' \tag{6.2}$$

Con lo anterior, notemos que

$$\begin{aligned} m * n'' * (m' * k' * k) &= m * (m' * n'' * k') * k, \text{ por asociatividad y conmutativad} \\ &= m * (m'' * n' * k') * k, \text{ por 6.2} \\ &= m'' * (m * n' * k) * k', \text{ por conmutatividad y asociatividad} \\ &= m'' * (m' * n * k) * k', \text{ por 6.2} \\ &= m'' * n' * (m' * k' * k), \text{ por asociatividad y conmutatividad.} \end{aligned}$$

por lo tanto $(m,n) \sim (m'',n'')$ concluyendo que $\sim$ es de equivalencia. ■

Ahora denotamos:

$$G_M := M \times M/\sim$$

Una nota importante. En la construcción anterior al definir $\sim$ como

$$(m,n) \sim (m',n') \Leftrightarrow m * n' * k = m' * n * k, \quad \text{para algún } k \in M$$

es importante la k como se muestra en la prueba ya que un monoide en general no puede tener la propiedad de cancelación (considera por ejemplo X un conjunto con 3 elementos y el monoide $Fun(X,X)$). De hecho, si el monoide tiene la propiedad de cancelación, entonces se puede definir $\sim$ simplemente como

$$(m,n) \sim (m',n') \Leftrightarrow m * n' = m' * n$$

queda como ejercicio para el lector probar que esta relación, define la misma relación que en el caso de que M no tiene la propiedad de cancelación. El ejemplo importante de monoide que si tiene propiedad de cancelación es $(\mathbb{N}, +, 0)$, como se vio en el capítulo 3.

■ **Ejemplo 6.3** Si lo aplicamos para el monoide $(\mathbb{N}, +, 0)$ tenemos que cada elemento de $G_{\mathbb{N}}$ es de la forma $[(m,n)]$. ¿Qué interpretación se le puede dar? pues como la intención de la construcción dice, en $G_{\mathbb{N}}$ estamos construyendo los números que actuarán como inversos negativos de $+$. De hecho tenemos por ejemplo

$$[(0,4)] = [(9,13)]$$

si denotamos por abuso de notación $[(a,b)] := a - b$ y $[(0,b)] := -b$ entonces la igualdad anterior dice que:

$$-4 = 9 - 13$$

permitiendo construir conjuntistamente los números negativos apartir de los números naturales y los elementos de $G_{\mathbb{N}}$ se conocerán como los enteros que intuitivamente son los números naturales, añadiendo los números negativos. ■

Una vez construido G_M, ahora falta probar que G_M tiene una estructura de grupo y un homomorfismo $M \to G_M$. Denotemos $p_M \colon M \times M \to G_M$ como la proyección canónica.

Proposición 6.1.3 Existe una única estructura binaria μ en G_M tal que p_M es un homomorfismo. Más aún (G_M, μ) es un grupo con $[(1,1)]$ como el neutro.

Demostración. Escribimos ν como la operación usual de $M \times M$, es decir la operación definida como

$$\nu((m,n),(m',n')) = (m * m', n * n')$$

y consideremos el diagrama:

$$\begin{array}{ccc} (M \times M) \times (M \times M) & \xrightarrow{p_M \times p_M} & G_M \times G_M \\ \downarrow{\scriptstyle \nu} & & \\ M \times M & \xrightarrow[p_M]{} & G_M \end{array}$$

notemos que $p_M \times p_M$ es sobreyectiva pues p_M lo es.

Ahora supongamos que para algunos $(m,n),(m',n'),(x,y),(x',y') \in M \times M$ son tales que

$$p_M \times p_M((m,n),(x,y)) = p_M \times p_M((m',n'),(x',y')) \tag{6.3}$$

es decir $[(m,n)] = [(m',n')]$ y $[(x,y)] = [(x',y')]$, entonces por definición de $\sim$ existen $k, k' \in M$ tal que

$$m * n' * k = m' * n * k, \; x * y' * k' = x' * y * k' \tag{6.4}$$

entonces juntando las ecuaciones de (6.4), usando la asociatividad y conmutatividad obtenemos

$$(m * x) * (n' * y') * (k * k') = (m' * x') * (n * y) * (k * k') \tag{6.5}$$

así que

$$\begin{aligned} p_M \circ \nu((m,n),(x,y)) &= p_M(m * x, n * y) \\ &= [(m * x, n * y)] \\ &= [(m' * x', n' * y')], \text{ por 6.5} \\ &= p_M \circ \nu((m',n'),(x',y')) \end{aligned}$$

entonces por 2.2.10 existe una única función $\mu\colon G_M \times G_M \to G_M$ tal que el siguiente diagrama conmuta

$$\begin{array}{ccc} (M \times M) \times (M \times M) & \xrightarrow{p_M \times p_M} & G_M \times G_M \\ \downarrow{\scriptstyle \nu} & & \downarrow{\scriptstyle \mu} \\ M \times M & \xrightarrow[p_M]{} & G_M \end{array}$$

explícitamente la operación está dado por la fórmula

$$\mu([(m,n)],[(x,y)]) := [(m * x, n * y)].$$

Se le deja al lector probar que (G_M, μ) satisface:

1. Asociatividad.
2. Conmutatividad.
3. El $[(1,1)]$ es el neutro.

Solo falta probar que para todo $[(m,n)] \in G_M$ tiene un inverso. Primero notemos que para todo $x \in M$ se tiene

$$[(x,x)] = [(1,1)]$$

esto porque $x * 1 = x = x * 1$. Ahora tomemos $[(m,n)] \in G_M$ entonces

$$\mu([(m,n)],[(n,m)]) = [(m * n, n * m)] = [(m * n, m * n)] = [(1,1)]$$

y como G_M es conmutativo, entonces $[(n,m)]$ es el inverso de $[(m,n)]$ completando la prueba. ■

Definimos $u_M\colon M \to M \times M$ como sigue:

$$u_M(m) = (m,1), \forall m \in M$$

se deja al lector probar que u_M es un homomorfismo de monoides.

Teorema 6.1.4 — Existencia del grupo abeliano asociado.. Sea M un monoide conmutativo, denotamos $j_M := p_M \circ u_M$ entonces (G_M, j_M) es el grupo abeliano asociado a M. Más aún si M es un monoide conmutativo con cancelación entonces j_M es inyectivo.

Demostración. Es claro que j_M es un homomorfismo de monoides. Ahora consideremos $f\colon M \to T$ un homomorfismo de monoides con $(T, *, e)$ un grupo abeliano, definimos $\hat{f}\colon M \times M \to T$ como sigue:

$$\hat{f}(m,n) := f(m) * (f(n))^{-1} \in T$$

notemos que $\hat{f}$ es un homomorfismo de monoides pues

$$\hat{f}(1,1) := f(1) * (f(1))^{-1} = e * e^{-1} = e * e = e$$

y para cada $(m,n),(m',n') \in M \times M$

$$\begin{aligned}
\hat{f}(\nu((m,n),(m',n'))) &= \hat{f}(m * m', n * n') \\
&= f(m * m')(f(n * n'))^{-1}, \text{ esto es por definición de } \hat{f} \\
&= f(m)f(m')(f(n)f(n'))^{-1}, \text{ esto es por definición de homomorfismo} \\
&= f(m)f(m')f(n')^{-1}f(n)^{-1}, \text{ por propiedades de grupos} \\
&= \hat{f}(m,n)\hat{f}(m',n'), \text{ asociatividad y conmutatividad.}
\end{aligned}$$

Luego notemos que el diagrama de homomorfismos conmuta

$$\begin{array}{ccc} M & \xrightarrow{u_M} & M \times M \\ & \searrow^{f} & \downarrow \hat{f} \\ & & T \end{array}$$

pues para todo $m \in M$ se tiene

$$\hat{f} \circ u_M(m) = \hat{f}(m,1) = f(m)(f(1))^{-1} = f(m) * e = f(m).$$

Ahora probaremos que $\ker p_M \subseteq \ker \hat{f}$, consideremos $(m,n) \sim (m',n')$ en $M \times N$ entonces existe $k \in K$ tal que:

$$m * n' * k = m' * n * k$$

aplicando f usando que es homomorfismo, tenemos

$$f(m)f(n')f(k) = f(m')f(n)f(k)$$

como T es grupo abeliano multiplicamos por $f(k)^{-1}$ y reordenando obtenemos

$$f(m)(f(n))^{-1} = f(m')(f(n'))^{-1}$$

es decir

$$\hat{f}(m,n) = \hat{f}(m',n')$$

concluyendo que si $((m,n),(m',n')) \in \ker p_M$ entonces $((m,n),(m',n')) \in \ker \hat{f}$, por 4.1.12 existe un único homomorfismo de algebras $\phi_f \colon G_M \to T$ tal que el siguiente diagrama de homomorfismos, conmuta

$$\begin{array}{ccc} M \times M & \xrightarrow{p_M} & G_M \\ & \searrow^{\hat{f}} & \downarrow \phi_f \\ & & T \end{array}$$

obteniendo que

$$\phi_f \circ j_M = \phi_f \circ p_M \circ u_M = f.$$

Para la unicidad, notemos que si $\psi \colon G_M \to T$ es un homomorfismo de algebras tal que $\psi \circ j_M = f$ entonces para cada $[(m,n)] \in G_M$ se tiene:

$$\psi[(m,n)] = \psi([(m,1)][(1,n)]) = \psi(u_M(m))\psi(u_M(n)^{-1}) = f(m)(f(n))^{-1} = \hat{f}[(m,n)].$$

Mostrando que (G_M, j_M) es el grupo abeliano asociado. Para la última parte, supongamos que $j_M(m) = j_M(n)$ entonces $[(m,1)] = [(n,1)]$ y existe una $k \in M$ tal que

$$m * 1 * k = n * 1 * k \ \Rightarrow m * k = n * k$$

así que cuando M tiene la propiedad de cancelación, la igualdad anterior implica que $m = n$ concluyendo que j_M es inyectiva. ■

6.2. El anillo de los números enteros.

Definición 6.2.1 — Los números enteros. Definimos el conjunto de los números enteros como:

$$\mathbb{Z} := G_{(\mathbb{N},+,0)}$$

además denotamos

1. Los naturales $n := [(n, 0)]$.
2. Los números negativos $-n := [(0, n)]$.
3. El cero (entero) $0 := [(0, 0)]$.

En la sección anterior se probó que $\mathbb{Z}$ tiene una operación de $+$ que extiende la operación de $\mathbb{N}$ en la suma. Vamos a probar que también extiende la operación de multiplicación y además que $\mathbb{Z}$ es un anillo.

Proposición 6.2.1 Todo número en $\mathbb{Z}$ es uno de los siguientes casos:

1. Un número natural.
2. Un número negativo.

Demostración. Sea $[(n, m)] \in \mathbb{Z}$, usando que $\mathbb{N}$ es un conjunto bien ordenado entonces tenemos 3 casos.

1. $n < m$, entonces existe una $c \in \mathbb{N}$ tal que $n + c = m$, esto implica que $[(n, m)] = [(0, c)]$ y entonces es un número negativo.
2. $n = m$, entonces $[(n, m)] = [(0, 0)]$ y es el número natural cero.
3. $n > m$, entonces existe una $c \in \mathbb{N}$ tal que $n = m + c$, esto implica que $[(n, m)] = [(c, 0)]$ y entonces es un número natural.

■

Proposición 6.2.2 Existe una única operación $*\colon \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ tal que:

1. $*$ mediante $j_{\mathbb{N}}$, extiende la operación de multiplicación de los naturales.
2. $(\mathbb{Z}, *, 1)$ es un monoide conmutativo.
3. $(\mathbb{Z}, +, 0, *, 1)$ es un anillo conmutativo y j_M es un homomorfismo de anillos.

Proposición 6.2.3 Si X es numerable entonces $X \times X$ es numerable.

Proposición 6.2.4 El anillo de los enteros $\mathbb{Z}$ es numerable.

6.3. Propiedades de Anillos Conmutativos.

Proposición 6.3.1 Para todo anillo R con uno, existe un único homomorfismo de anillos $f\colon \mathbb{Z} \to R$.

6.4. El orden de los números enteros.

Proposición 6.4.1 Sea $(M, *, 1)$ es un monoide ordenado, es decir cada ves que $m \leq n$ entonces $a * m \leq a * n$ para toda $a \in M$. Entonces G_M es un grupo ordenado.

Proposición 6.4.2 Existe un único orden en $\mathbb{Z}$ que extiende el orden en $\mathbb{N}$.

Capítulo 7

Teoría de Números.

7.1. Divisibilidad.

Definición 7.1.1 — Divisibilidad. Sean $a, b \in \mathbb{Z}$ decimos que a divide a b (denotandolo como $a|b$) si existe una $c \in \mathbb{Z}$ tal que $b = c * a$.

Proposición 7.1.1 Las siguientes afirmaciones son válidas para números enteros.

1. $a|a$ para toda $a \in \mathbb{Z}$.
2. $1|a$ para toda $a \in \mathbb{Z}$.
3. $a|0$ para toda $a \in \mathbb{Z}$.
4. Si $a|b$ y $b|c$ entonces $a|c$.
5. Si $a|b$ y $b|a$ entonces $a = \pm b$.
6. Si $a|b$ y $c|d$ entonces:
   a) $ac|bd$.
   b) Si $a = c$ entonces $a|bx + dy$ para toda $x, y \in \mathbb{Z}$.

Ejercicio 7.1 Demostrar los incisos de la proposición 7.1.1. ■

Ejercicio 7.2 Prueba las siguientes propiedades:

1. Si $x|a$ para toda $a \in \mathbb{Z}$ entonces $x = \pm 1$.
2. Si $x|1$ entonces $x = \pm 1$.

■

Ejercicio 7.3 Sea R un anillo y $u \in R$ una unidad, es decir, existe $v \in R$ tal que $uv = 1$. Muestra que la función $f_u \colon R \to R$ dado por $f_u(x) = ux$ es una biyección. ■

Proposición 7.1.2 El conjunto de unidades $U(\mathbb{Z}) = \{1, -1\}$

Demostración. Sea $u \in \mathbb{Z}$ una unidad, entonces existe $v \in \mathbb{Z}$ tal que $uv = 1$, por definición (7.1.1) tenemos $u|1$ y por ejercicio (7.2) implica que $u = \pm 1$, completando la prueba. ■

Denotamos $\mathbb{Z}^+$ a la imagen de $\mathbb{N}$ bajo $j_{\mathbb{N}} \colon \mathbb{N} \to \mathbb{Z}$.

Proposición 7.1.3 El conjunto $(\mathbb{Z}^+, |)$ es un orden parcial.

Definición 7.1.2 — Máximo comun divisor y mínimo común multiplo. Sean $a, b \in \mathbb{Z}$ y $a' = |a|, b' = |b| \in \mathbb{N}$, definimos:

- El máximo común divisor de a y b como $\inf\{a', b'\}$ en $(\mathbb{Z}^+, |)$ y lo denotamos como $mcd(a, b)$ o simplemente (a, b).
- El mínimo común múltiplo de a y b como $\sup\{a', b'\}$ en $(\mathbb{Z}^+, |)$ y lo denotamos como $mcm(a, m)$ o simplemente $[a, b]$.

Una consecuencia de la proposición (7.1.3) y la definición del supremo (2.3.3) obtenemos:

Proposición 7.1.4 Sean $a, b \in \mathbb{Z}$ y $m > 1$ tal que:

1. $m|a$ y $m|b$.
2. Si $n > 1$, es tal que $n|a$ y $n|b$ entonces $n|m$.

Entonces $m = mcd(a, b)$.

Proposición 7.1.5 Para todo par $a, b \in \mathbb{Z}$ se cumple:

$$mcd(a, b) \cdot mcm(a, b) = |a| \cdot |b|.$$

Demostración. Tenemos que

$$a|ab, \ \ b|ab \tag{7.1}$$

por definición de mínimo común múltiplo (7.1.2)

$$mcm(a, b)|ab \tag{7.2}$$

por definición de divisibilidad (7.1.1), se tiene

$$mcm(a, b) * c' = ab \tag{7.3}$$

Sea $c = |c'|$, entonces de la ecuación (7.3) tenemos

$$c||a|, \ \ c||b| \tag{7.4}$$

Ahora, sea $n > 1$ tal que $n||a|$ y $n||b|$ ■

Definición 7.1.3 — Números primos y primos relativos.. Sean $p, a, b \in \mathbb{Z}$ definimos:

1. Un número primo $p > 1$, como aquel tal que si $x|p$ entonces $x = 1$ ó $x = p$.
2. Decimos que dos números son primos relativos si $mcd(a, b) = 1$.

■ **Ejemplo 7.1** Para toda $n \in \mathbb{Z}$, los números n y $n + 1$ son primos relativos.

Demostración. Sea x un divisor común de n y $n+1$, es decir $x|n$ y $x|n+1$, por definición (7.1.1), tenemos las ecuaciones:

$$xa = n, \ \ xb = n + 1, \ \ a, b \in \mathbb{Z} \tag{7.5}$$

Sustituyendo las ecuaciones de (7.5) tenemos:

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

Entonces $x|1$ y por (7.2) se tiene que $x = \pm 1$, esto quiere decir que $\{1, -1\}$ es el conjunto de divisores y por definición (7.1.1) obtenemos que $mcd(n, n + 1) = 1$, concluyendo que n y $n + 1$ son primos relativos. ■

■

Proposición 7.1.6 — Lema de Euler. Sea p un primo y supongamos que $p|ab$ entonces $p|a$ ó $p|b$.

Corolario 7.1.7 Si p es un primo y $p = ab$, con $a, b > 0$ entonces $a = p$ ó $b = p$.

Demostración. Tenemos por hipótesis $p|ab$ entonces por (7.1.6) implica que $p|a$ ó $p|b$, supongamos sin pérdida de generalidad que $p|a$ entonces por definición (7.1.1) se tiene:

$$p * c = a \tag{7.6}$$

Sustituyendo (7.6) en la hipótesis, tenemos $p = pca$, obteniendo $1 = ca$, es decir $a|1$ y por (7.2) tenemos que $a = 1$, entonces $b = p$. ■

Teorema 7.1.8 — Algoritmo de División Euclidiana. Sean $a, b \in \mathbb{Z}$ entonces existen únicos $q, r \in \mathbb{Z}$ tales que satisfacen:

$$b = aq + r,\ 0 \leq |r| < a \tag{7.7}$$

Demostración. Consideremos $A = \{x \in \mathbb{Z}^+ |\ b - aq > 0\}$ ■

7.2. Ecuaciones lineales diofánticas.

7.3. Aritmética modular.

7.4. Algunas aplicaciones de la Aritmética modular.

Apéndice A

Generalidades de lógica matemática

A.1. Semántica de la Lógica Proposicional.

A.2. Sintática de la Lógica Proposicional.

A.3. Lógica de Primer orden.