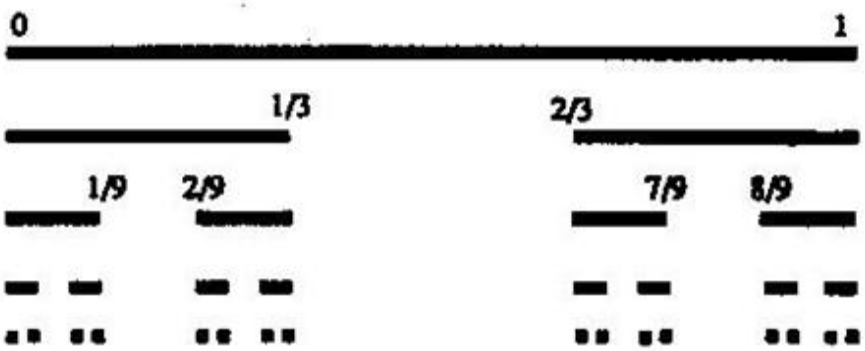
ÁLGEBRA I

Gascón José y Serrano Wladimir

República Bolivariana de Venezuela
Caracas: Universidad Nacional Abierta, 2017
ISBN 978-980-236-747-4

UNIDAD 1

Conjuntos



Conjunto de Cantor

Semana 1

Aplicar el concepto de conjunto en la resolución de problemas, en el modelado matemático y en la demostración de nuevos resultados.

Contenidos a tratar: Conjunto y elemento. Algunas paradojas en la Teoría de Conjuntos de Cantor. Álgebra de conjuntos. Cardinalidad de un conjunto.

(el conjunto de Cantor). Este conjunto, que describiremos recursivamente, tiene propiedades muy interesantes. Fue propuesto por *Georg Ferdinand Ludwig Philipp Cantor* (1845, San Petesburgo, Rusia – 1918, Halle, Alemania) en 1883 en el marco de su estudio sobre el **continuo**. Sin embargo, ya H.J.S. Smith, profesor en la Universidad de Oxford había publicado en 1875 *On the integration of discontinuous functions* un método para construir conjuntos nada-densos. Al parecer es ésta la primera publicación de este tipo de conjuntos. El conjunto de Cantor, *C*, se construye de

la siguiente manera: veamos… consideremos un segmento de longitud uno. Omitamos de éste el tercio central y repitamos este proceso en cada uno de los segmentos resultantes (ver el gráfico anterior). Y así hasta el infinito…! Pensemos entonces… ¿Queda algún punto luego de este proceso infinito? Es decir, ¿el conjunto *C* tiene algún elemento? Observemos que los puntos señalados con 0 y 1 (justo los extremos del segmento) no son omitidos en ninguna de las etapas del proceso infinito, así tanto el 0 como el 1 están en el conjunto *C*. Además de estos, también pertenecen a *C* los puntos $\frac{1}{3}, \frac{2}{3}, \frac{1}{9}, \frac{2}{9}, \frac{7}{9}, \frac{8}{9}, \ldots$ El gráfico nos da la idea de que los extremos de los segmentos resultantes de cada una de las etapas están en *C*. Así, podemos preguntarnos ¿cuántos extremos obtenemos en cada etapa? Fijémonos en que en la etapa 1 (el segmento de longitud 1) hay dos extremos (los puntos 0 y 1), en la dos hay cuatro extremos (los puntos 0, 1, $\frac{1}{3}$ y $\frac{2}{3}$), en la tres, ocho extremos (0, $\frac{1}{9}, \frac{2}{9}, \frac{1}{3}, \frac{2}{3}, \frac{7}{9}, \frac{8}{9}$, 1), en la cuatro hay diez y seis... Con ello listamos las siguientes relaciones:

$$\textit{etapa} \rightarrow \textit{número de extremos}$$

$$1 \rightarrow 2$$

$$2 \rightarrow 4$$

$$3 \rightarrow 8$$

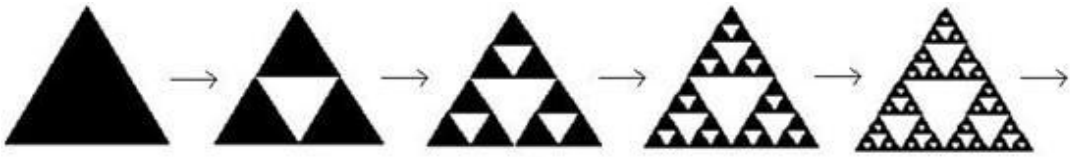
$$4 \rightarrow 16$$

$$5 \rightarrow 32$$

$$\vdots$$

Y podemos concluir que para la etapa *n* habrá 2^n extremos (al menos 2^n puntos que están en *C*). Note que $2=2^1$, $4=2^2$, $8=2^3$… Pero, ¿cuántos puntos hay en el conjunto de Cantor? Más aún, dado un número real cualquiera comprendido entre 0 y 1, digamos $\frac{17}{18}$, ¿cómo sabemos si está o no en *C*? ¿Puede encontrar el lector algún criterio general que permita dar respuesta a esta pregunta?

El conjunto de Cantor es un ejemplo de un conjunto cuya construcción es sencilla pero que posee propiedades muy complejas. Es, además, uno de los fractales más curiosos junto con el famoso triángulo de Sierpinski.

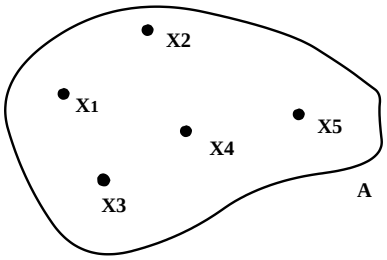


Triángulo de Sierpinski. ¡Este conjunto recibe su nombre del matemático polaco Waclaw Sierpinski (1882-1969) quien lo expuso en 1915 con la intención de mostrar que una curva puede cortarse consigo misma en todos sus puntos!

1.1. Las ideas de conjunto y elemento

La lectura anterior puede seguirse sin necesidad de manejar "significados precisos" para los términos *"conjunto"* y *"elemento"*. Convendremos en que "conjunto" y "elemento", aún cuando se encuentran en la base del álgebra de conjuntos, serán términos no definidos (o primitivos) –manejaremos ideas intuitivas de ellos, aunque más adelante advertiremos sobre algunos cuidados importantes. Ciertos intentos que se han dado en el seno de las matemáticas por definir estos términos han implicado algunas contradicciones en las teorías que se han edificado. Por ejemplo, Cantor dio como definición inicial: "un conjunto es cualquier colección *T* de objetos determinados y bien distintos *x* de nuestra percepción o nuestro pensamiento (que se denominan elementos de *T*), reunidos en un todo". Richard Dedekind visualizó los conjuntos como sacos o bolsas: "un conjunto es un saco lleno de elementos. Dentro del saco puede haber números, letras, plantas, personas, mastodontes… prácticamente cualquier cosa". El mismo Cantor, conocido como el padre de la Teoría de Conjuntos, mostró algunas de las contradicciones que tales definiciones implicaban –lo que al parecer, junto a las duras críticas que recibió por ello, contribuyó a que complicase su estado psicológico en varios momentos importantes de su productiva actividad matemática.

Un conjunto lo entenderemos intuitivamente como una colección de objetos o elementos. Si *x* es un objeto (elemento) de un conjunto *A*, podemos decir que "*x* pertenece a *A*", y podemos escribir $x \in A$. En caso contrario, si *x* no pertenece a *A*, se escribe que $x \notin A$.



El conjunto $A = \{x_1, x_2, x_3, x_4, x_5\}$

Si *A* consta de los elementos x_1, x_2, x_3, x_4 y x_5 entonces escribimos que $A = \{x_1, x_2, x_3, x_4, x_5\}$, o bien, $A = \{x_i : 1 \le i \le 5\}$ (el conjunto *A* consta de los elementos x_i tales que *i* es un número natural comprendido entre 1 y 5, incluidos los extremos). Nótese que para describir un conjunto es posible (a) listar todos sus elementos, o (b) haciendo explícita la o las propiedades que verifican sus elementos. En todo esto vale la aclaratoria que sigue. Los símbolos que hemos usado para elementos y conjuntos son eso: etiquetas que denotan o representan a ciertos objetos mas no los objetos en sí mismos. Los que siguen son ejemplos de conjuntos.

1. $\{x : x \text{ es una medida de longitud antigua y antropométrica de Venezuela}\}$.

   Algunos de sus elementos son: brazada, cuarta, codo, dedo, hasta donde llega la vista, jeme, paso, pie, pulgada, toesa y tranco. Aunque es difícil hacer una lista exhaustiva de los objetos de este conjunto.
2. **(costo del agua en Latinoamérica).** El precio del m^3 de agua en Bogotá 2.0 US$, en Quito 1.2 US$, en Brasilia 1 US$, en Montevideo 0.89 US$, en Lima

0.51 US$, en México DF 0.35 US$, en San Salvador 0.3 US$, y en Caracas 0.23 US$ (en este último caso el costo incluye la recolección de aguas servidas). En este caso el conjunto queda descrito por un par ordenado (Ciudad, costo del agua). Conjuntos como este resultan importantes en el análisis de temas como el acceso de la población al agua, las políticas de no-privatización (recordemos el impulso de la semi-privatización del agua en Venezuela desde fines de la década de 1980 a través de la figura de contratistas, o la Guerra del Agua en Bolivia en el año 2000) y la contaminación.

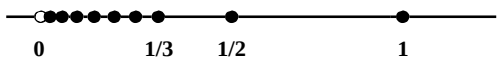
3. $P = \{x \in \mathbb{N} : x \text{ tiene sólo dos divisores}\}$ es el conjunto de los números primos (Aquí $\mathbb{N}$ representa al conjunto de los números naturales). Observe que el 1 no es un número primo pues sólo tiene un divisor. Así que existen números naturales que son primos, otros son compuestos y números como el 1 que no es ni primo ni compuesto. Haciendo un abuso de notación podemos escribir que

$$P = \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, ...\}.$$

   Es un hecho importante en matemáticas que el conjunto *P* tiene infinitos elementos. La prueba de este hecho se debe a Euclides y la expondremos en el Módulo II.

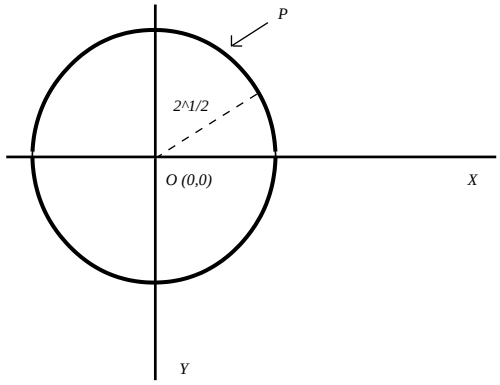
4. La colección de los números naturales $\mathbb{N}$ es un ejemplo de conjunto. Así como también: $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ *y* $\mathbb{C}$, los enteros, racionales, reales y complejos, respectivamente.

5. $P = \{\frac{1}{n} : n \in \mathbb{N}^*\}$ donde $\mathbb{N}^*$ es el conjunto de los números naturales exceptuando al cero. Observemos que $P = \{1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \frac{1}{5}, ...\}$. Una representación en la recta real de *P* es



Gráfica de los racionales de la forma $\frac{1}{n}$

6. Sea $P = \left\{ x \in \mathbb{R}^2 : d\left(x, O\right) = \sqrt{2} \right\}$ es el conjunto de los puntos del Plano $\mathbb{R}^2$ cuya distancia euclídea con respecto al punto origen es igual a $\sqrt{2}$. En este caso el gráfico de *P* es



Los puntos del Plano cuya distancia con respecto a O es $\sqrt{2}$

7. Sea $P = \left\{ x \in \mathbb{Z} : x \middle| 20 \right\}$ es el conjunto de los enteros *x* tales que *x* es un divisor de 20. Así, $P = \left\{1, 2, 4, 5, 10, 20\right\}$. ¡Y este es el tercer conjunto que exponemos con una cantidad finita de elementos!
8. **(total de residuos sólidos).** Con los datos del total de residuos sólidos recolectados por entidad federal en nuestro país entre 2006 y 2008 se determinan varios conjuntos de interés. Tal es el caso del conjunto que consta de los datos correspondientes a las entidades costeras para algunos de estos años; o incluso, aquel que reúne las proporciones entre estos datos y el número de habitantes para esa fecha –lo que permitiría ver qué entidades poseen mayor índice de desechos sólidos por habitante (como advertirá, sólo con los datos de la tabla es imposible responder la cuestión anterior).

	2006	2007	2008
Total	**22.909.172**	**24.416.785**	**21.738.872**
Distrito Capital	-	750	-
Amazonas	50.500	88.480	97.500
Anzoátegui	1.172.500	436.777	1.791.600
Apure	632.100	328.808	172.182
Aragua	973.012	1.680.000	1.776.460
Barinas	257.480	673.000	622.500
Bolívar	1.345.740	1.421.996	1.212.900
Carabobo	2.001.796	2.650.287	1.536.030
Cojedes	306.708	365.500	-
Delta Amacuro	88.598	124.400	100.100
Falcón	769.680	475.628	442.600
Guárico	452.000	493.752	597.504
Lara	1.154.696	1.382.124	828.890
Mérida	76.000	546.336	-
Miranda	3.305.400	3.452.120	3.894.080
Monagas	106.227	379.300	210.000
Nueva Esparta	384.600	233.200	367.500
Portuguesa	570.015	586.971	629.853
Sucre	1.164.800	1.476.772	1.507.773
Táchira	2.052.200	2.168.966	1.053.700
Trujillo	546.251	581.900	669.500
Vargas	311.039	149.930	400.000
Yaracuy	570.558	854.700	320.400
Zulia	4.617.272	3.865.088	3.507.800
Dep. Federales	-	-	-

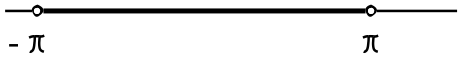
Total de residuos sólidos recolectados en la República Bolivariana de Venezuela (2006-2008).

Ciertas decisiones que afecten positiva o negativamente al ambiente y a la población en sí misma pueden basarse en el estudio de tales conjuntos; que van desde las decisiones en el seno de la familia y la comunidad hasta las que involucran a los organismos del Estado y la economía.

9. **(encuesta).** La compilación de los datos de una encuesta determina un conjunto. En este caso el conjunto puede ser o no numérico.
10. **(monóxido de Carbono).** Los datos sobre el nivel de CO en cierto punto de la ciudad y en un determinado intervalo.
11. **(fósiles en la Guajira venezolana).** La reunión de los fósiles de moluscos y mamíferos encontrados en la Guajira venezolana en junio de 2010 por parte de investigadores del IVIC, UBV y UCV (en el marco de un estudio sobre erosión costera) es un ejemplo de conjunto. Éste muestra que "comunidades indígenas seminómadas vivieron en la Guajira venezolana entre 4000 a 6000 años antes de Cristo!, con formas de organización social que les permitieron construir casas, cementerios y dejar depósitos de alimentos y desechos conocidos como conchales" (Correo del Orinoco, 8-10-2010).

Una muestra de los conchales encontrados en junio de 2010 en la Guajira venezolana (que datan entre 4000 y 6000 años antes de Cristo). Foto: Lenín Parra (UBV)

12. $P = \{x \in \mathbb{R} : |x| < \pi\} = \{x \in \mathbb{R} : -\pi < x < \pi\}$ tiene por gráfica



Los puntos de R comprendidos entre $-\pi$ *y* π

13. **(primos gemelos).** $P=\{(x,y): x \text{ y } y \text{ sean primos gemelos}\}$ es el conjunto de las parejas, o pares ordenados, de primos gemelos, es decir, de aquellos primos cuya diferencia es 2. Tal es el caso de $(3,5)$, $(5,7)$, $(11,13)$, $(17,19)$, $(29,31)\ldots$ ¿Cuántos primos gemelos hay?. Nadie conoce si este conjunto es finito o infinito.
14. **(funciones reales).** La colección *F* de todas las funciones reales de variable real es un conjunto importante, en este caso podemos escribir $F=\{f \mid f:\mathbb{R}\to\mathbb{R}\}$.

Definición. Si *B* es un conjunto y sus elementos también son elementos del conjunto *A*, entonces se dice que *B* es *subconjunto* de *A* o que *B* es *parte* de *A*, y se simboliza por $B\subset A$, o bien, $A\supset B$.

Del concepto de subconjunto podemos derivar una condición para la igualdad entre conjuntos *A,B.* Tenemos *A=B* si, y sólo si, $B\subset A$ y $A\subset B$ esto es, si cada uno es subconjunto del otro (lo cual es equivalente a decir que tienen exactamente los mismos elementos).

La *intersección* de los conjuntos *A* y *B es un conjunto que consta de los elementos que son comunes a A y a B,* se denota por $A\cap B$. Y la *unión* de los conjuntos *A* y *B es el conjunto que consta de los elementos que están en A o que están en B,* se denota por $A\cup B$. Estas nociones pueden generalizarse como sigue. Sea $A_i\subset A$ para cada *i* entre 1 y *n*, o bien, para $i\in\mathbb{N}^*$. $(A_i)_{i\in\mathbb{N}^*}$ se denomina *una familia de subconjuntos* de *A.* Ahora,

$$\bigcap_{i=1}^{n} A_i$$

$$\bigcap_{i=1}^{\infty} A_i$$

denotan, respectivamente, a la intersección de cantidad finita e infinita de conjuntos A_i, es decir, de la familia A_i. Este último caso se ilustra en el ejemplo 3. Y para la unión

$$\bigcup_{i=1}^{n} A_i$$

$$\bigcup_{i=1}^{\infty} A_i .$$

Si un conjunto no tiene elementos se denomina vacío y se le designa con el símbolo $\varnothing$. Además, convendremos en que el vacío es parte o es un subconjunto de cualquier conjunto *A*, es decir, $\varnothing \subset A$. Y, dado un conjunto *A*, podemos definir el conjunto partes de *A* (también llamado conjunto potencia), $P(A)$, que consta de todos los subconjuntos de *A*.

1. Consideremos al conjunto que consta de las soluciones reales de la ecuación $-x^2 - 1 = 0$. En este caso, debido a que esta ecuación no tiene soluciones reales escribimos que $\{x \in \mathbb{R} : -x^2 - 1 = 0\} = \{x \in \mathbb{R} : x^2 = -1\} = \varnothing$.
2. Si $A = \{x \in \mathbb{R} : 0 \le x \le 1\}$ y $B = \{x \in \mathbb{R} : 0 \le x \le \frac{1}{3} \text{ ó } \frac{2}{3} \le x \le 1\}$, entonces

$$A \cap B = B \text{ y}$$
$$A \cup B = A .$$

En este caso, $B \subset A$.

3. **("Último" "Teorema" de Fermat).** El conjunto que consta de las soluciones *x*, *y*, y *z* enteras positivas no triviales de la ecuación

$$x^n + y^n = z^n, \ con \ \ n > 2$$

es vacío. Por no triviales entendemos soluciones distintas a $x=y=z=0$ o $x=z=1, y=0$ o cosas afines.

Este resultado es conocido como el *Último Teorema de Fermat* cuya demostración se dio casi trescientos años luego de su formulación. Y representó uno de los problemas abiertos más importantes de todas las Matemáticas resuelto hacia finales del siglo XX por Andrew Wiles.

4. Podríamos escribir al conjunto de Cantor en términos de la intersección de infinitos conjuntos. Veamos: denotemos con C_0 al intervalo $[0,1]$. De acuerdo con el proceso de construcción de este peculiar conjunto debemos dividir al intervalo $[0,1]$ en tres intervalos iguales, a saber, $\left[0, \frac{1}{3}\right]$, $\left(\frac{1}{3}, \frac{2}{3}\right)$ y $\left[\frac{2}{3}, 1\right]$. Ahora suprimimos el tercio central, es decir, $\left(\frac{1}{3}, \frac{2}{3}\right)$. Etiquetemos $C_1 = \left[\frac{2}{3}, 1\right] \cup \left[\frac{2}{3}, 1\right]$. De la misma manera obtenemos que $C_2 = \left[0, \frac{1}{9}\right] \cup \left[\frac{2}{9}, \frac{3}{9}\right] \cup \left[\frac{6}{9}, \frac{7}{9}\right] \cup \left[\frac{8}{9}, 1\right]$ y así sucesivamente… Con ello se define a *C* como la intersección de todos los C_n

$$C = \bigcap_{n=0}^{\infty} C_n \, .$$

5. Sea $A = \{a, b\}$. Como *a* y *b* son elementos de *A*, entonces $\{a\}$ y $\{b\}$ son subconjuntos de *A*, por la definición de subconjunto de un conjunto. También el mismo *A* es subconjunto de sí mismo pues como $a, b \in A$ se tiene que

$\{a, b\} \in P(A)$. Y $\varnothing \in P(A)$ ya que $\varnothing \subset A$. Entonces, $P(A) = \{\varnothing, \{a\}, \{b\}, A\}$.

1.2. Algunas paradojas en la Teoría de Conjuntos de Cantor

La definición inicial de Cantor de lo que es un conjunto conllevó algunas paradojas, es decir, algunos problemas en el seno de la teoría matemática que construyó. Una de ellas es la denominada *paradoja de Russell*. Para ilustrarla consideremos el conjunto $R = \{x : x \notin x\}$ (el conjunto *R* consta de los objetos *x* que no pertenecen a sí mismos). Por ejemplo, un pájaro está en *R* pero el conjuntos de las ideas no está en *R.* Pero al preguntarnos si el mismo *R* está o no en *R* surge la paradoja. Veamos: si $R \in R$ entonces $R \notin R$, pues debe cumplir con la propiedad de los objetos *x* que están en *R*, lo cual es contradictorio. Por otra parte, si suponemos que $R \notin R$, entonces *R* verifica la propiedad de los elementos que están en *R*, en consecuencia $R \in R$, y de nuevo esto es contradictorio. Agregamos como comentario que existen muchas versiones de la *paradoja de Russell*, una de ellas, quizás con un valor didáctico importante, la asocia con el siguiente planteamiento: consideremos a *R* el catálogo que reseña a todos los libros de cierta biblioteca, ¿debe *R* reseñarse a sí mismo o no?

Esta paradoja nos muestra que este tipo de objetos no pueden considerarse conjuntos, más aún, el problema proviene de considerar válidas a expresiones como $x \in x$, o bien, $x \notin x$. Vemos entonces que nuestra idea intuitiva de conjunto debe manejarse con mucho cuidado.

Otro de los problemas que se detectaron en la Teoría de Conjuntos de Cantor fue avistado por su mismo creador. La *paradoja de Cantor* tiene que ver con el "conjunto Universo *U* (o Universal)". Para entonces se entendía al conjunto Universo como el conjunto de todos los conjuntos (lo cual se asocia con una de las ideas clásicas sobre el Universo físico como un espacio infinito). Cantor había probado que dado un con-

junto *A* de *n* elementos (con *n* finito o infinito), el conjunto formado por todas las partes (subconjuntos) de *A*, $P(A)$, tenía mayor número de elementos que *n*. La paradoja surge al considerar al conjunto Universo: *U* debe contener a $P(U)$ pues *U* es el conjunto de todos los conjuntos. Pero, de acuerdo con lo probado por Cantor, el conjunto de partes del conjunto Universo $P(U)$ debe tener más elementos que *U*, pero desdice de la noción de *U* como conjunto Universo.

Así, la idea de considerar un conjunto de todos los conjuntos, o conjunto Universo, también implicó serios problemas en la teoría de Cantor. Es por esta razón que tal objeto no es considerado un conjunto. Posteriormente consideraremos la noción de cardinal de un conjunto la cual formalmente requiere del *axioma de elección* para ser formulada pero este axioma no será usado en este curso ya que nuestro concepto de cardinal será manejado de manera intuitiva y el caso de cardinal numerable no requiere del mismo.

Un conjunto no puede tenerse a sí mismo como elemento. Esto es, un objeto como

$$A = \{A, x_1, x_2, x_3, ...\}$$

no es un conjunto.

Además, no existe el conjunto de todos los conjuntos ya que eso contradice lo anterior, ¿porqué?.

Colecciones como la de los ordinales, noción en la que incursionaremos más adelante, tampoco podían considerarse conjuntos. Vemos entonces que las nociones de conjunto como una colección cualquiera de objetos (Cantor) o como un saco lleno de elementos (Dedekind), entre otras que no hemos mencionado (aunque no con ello desmerecemos su enorme valor histórico para el desarrollo de esta teoría), conllevan

paradojas como las de Cantor o Russell. Existen varias soluciones a estas paradojas –radicales o no, como la *teoría de los Tipos* de Russell (1903), la axiomática de Zermelo (1908), los aportes de Fraenkel (la axiomática de Zermelo-Fraenkel), von Newmann (axiomática de Bernays-Gödel-von Neumann), entre otras. Convendremos aquí, como señalamos antes, en que, un conjunto no puede ser elemento de sí mismo y que no existe un conjunto Universo con la intención de evitar tales paradojas.

1.3. Álgebra de conjuntos

Ya con las ideas que se han construido podemos iniciar el esbozo de la *teoría de Conjuntos*. En este sentido, probaremos algunas de las propiedades medulares de esta teoría apoyados en herramientas lógicas que suponemos conocidas por el lector; a saber: negación ($\neg$), conjunción ($\wedge$), disyunción ($\vee$), implicación ($\Rightarrow$), doble implicación o bicondicional ($\Leftrightarrow$) y disyunción exclusiva ($\bar{\vee}$), así como en los cuantificadores "para todo" ($\forall$) y "existe" ($\exists$). Otras propiedades se propondrán al lector como ejercicios/problemas. Consideraremos entonces un conjunto S que contiene a los conjuntos mencionados de seguida.

Proposición 1. Sea A un conjunto cualquiera, entonces

1. El conjunto vacío es único.
2. $A \subset A$

Demostración. (1) Supongamos, por *reducción al absurdo*, que no existe un único conjunto $\varnothing$; esto es, podemos decir que $\varnothing^*$ es otro conjunto vacío que verifica $\varnothing \neq \varnothing^*$. Pero, por definición [$\varnothing \subset A$ para cualquier conjunto A] se tiene en particular que

$$\varnothing \subset \varnothing^*$$

y además

$$\varnothing^* \subset \varnothing$$

Y de acuerdo con la definición de igualdad de conjuntos, se tiene que $\varnothing = \varnothing^*$, lo cual es absurdo, pues habíamos supuesto que $\varnothing \neq \varnothing^*$. El absurdo parte de suponer que no hay un único conjunto vacío. Concluimos entonces que existe un único conjunto vacío. (2) Resta probar la parte dos. Como

$$\forall x : x \in A \Rightarrow x \in A$$

(para todo *x* de *A* se verifica que *x* pertenece a *A*), entonces $A \subset A$. ■

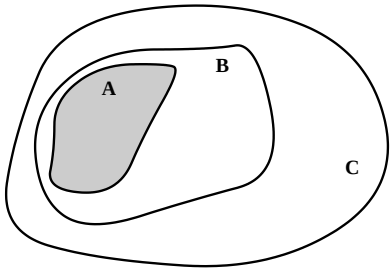
Proposición 2. Sean *A*, *B* y *C* conjuntos cualesquiera, si $A \subset B$ y $B \subset C$ entonces $A \subset C$.

Demostración. Supongamos que $A \subset B$ y $B \subset C$, entonces se tiene por la definición de subconjunto de un conjunto que:

$$\forall x \mid \ x \in A \Rightarrow x \in B \text{ y además } \forall x \mid \ x \in B \Rightarrow x \in C,$$

Así, por silogismo hipotético, puede concluirse que $\forall x \mid \ x \in A \Rightarrow x \in C$. Esto completa la prueba.

Dadas tres proposiciones matemáticas *p*, *q* y *r* para las que se sabe que $(p \Rightarrow q)\, y\, (q \Rightarrow r)$ entonces $p \Rightarrow r$. Este es el silogismo hipotético al que se hizo referencia.



Si A es parte de B y B es parte de C, entonces A es parte de C

Proposición 3. Para cualesquiera conjuntos *A* y *B*, se tiene que:

1. $A \subset B$ si y sólo si $A \cap B = A$ y
2. $A \subset B$ si y sólo si $A \cup B = B$.

Demostración. (2) Para probar que $A \cup B = B$, procederemos verificando las inclusiones implicadas. Si $x \in B$ entonces de acuerdo con la ley lógica $p \Rightarrow p \vee q$, $x \in B \vee x \in A$, por tanto $x \in A \vee x \in B$, esto es, $x \in A \cup B$ (por definición de *A unido con B*). Por lo anterior $B \subset A \cup B$. Probemos ahora que $A \cup B \subset B$. Si $x \in A \cup B$ se tiene que

$$x \in A \vee x \in B$$

Y como $A \subset B$ (por hipótesis), todo *x* de *A* está en *B*, entonces $x \in B \vee x \in B$; con lo cual $x \in B$. Luego, ambas inclusiones implican, por definición de igualdad de conjuntos, que $A \cup B = B$. ■

 La parte (1) se deja a los lectores. Piense el problema antes de verificar la respuesta que sigue a continuación.

 Supongamos ahora que

$$A \subset B$$

entonces

$$A = A \cap A \subset A \cap B,$$

de donde se tiene que

$$A \cap B = A.$$

Ya que claramente

$$A \cap B \subset A$$

Entonces

$$A \cap B = A$$

Dejamos la otra implicación al estudiante UNA.

Proposición 4. Sean *A, B* y *C* conjuntos cualesquiera, entonces se tiene que:

1. $A \cup B = B \cup A$
2. $A \cap B = B \cap A$
3. $A \cup A = A$
4. $A \cup \varnothing = A$
5. $A \cap A = A$
6. $A \cap \varnothing = \varnothing$
7. $(A \cup B) \cup C = A \cup (B \cup C)$
8. $(A \cap B) \cap C = A \cap (B \cap C)$
9. $(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$
10. $(A \cap B) \cup C = (A \cup C) \cap (B \cup C)$

Demostración. (1) $A \cup B = \{x \mid x \in A \vee x \in B\} = \{x \mid x \in B \vee x \in A\} = B \cup A$, por definición de *A unido con B*, ley lógica $p \vee q \Leftrightarrow q \vee p$ y definición de $B \cup A$, respectivamente [Esto también se puede probar verificando la *doble inclusión*: $A \cup B \subset B \cup A$ y $A \cup B \supset B \cup A$]. (2) $A \cap B = \{x \mid x \in A \wedge x \in B\} = \{x \mid x \in B \wedge x \in A\} = B \cap A$, por definición de la inter-

sección de conjuntos, conmutatividad de la conjunción de proposiciones y, nuevamente, por la definición de intersección de conjuntos. (3) $A \cup A = \{x \mid x \in A \vee x \in A\} = \{x \mid x \in A\} = A$, por definición de unión de conjuntos, ley lógica $p \Leftrightarrow p \vee p$ (las proposiciones *p* y $p \vee p$ son equivalentes), y definición de *A*. (4) Por definición tenemos que $\varnothing \subset A$, y por la parte (2) de la proposición anterior se tiene que $A \cup \varnothing = A$.■

 El resto se deja como ejercicios al lector.

(4) Es claro que siempre se tiene que $A \subset A \cup B$ independiente de que es el conjunto *B*, luego $A \subset A \cup \varnothing$. Por otro lado $\varnothing \subset A \Rightarrow A \cup \varnothing \subset A \cup A = A$ por (3) y luego se tiene que $A = A \cup \varnothing$ como queríamos demostrar.

(5) Es claro que $A \cap B \subset A$ para cualquier conjunto *B*, luego $A \cap A \subset A$. Por otro lado, si tomo un *x* en A es claro que *x* pertenece a $A \cap A$, luego $A \subset A \cap A$ y por estas dos inclusiones tenemos que $A = A \cap A$. El resto de las pruebas de las proposiciones queda a cargo del estudiante UNA.

El siguiente resultado es importante y se aplica con frecuencia.

Teorema 5 (Leyes de De Morgan). Sean *A* y *B* subconjuntos de *T*. Entonces,

1. $(A \cup B)_T^c = A_T^c \cap B_T^c$ y
2. $(A \cap B)_T^c = A_T^c \cup B_T^c$.

 Aquí A_T^c indica al complemento del conjunto *A* en el conjunto *T*, esto es, representa al conjunto de todos los elementos que no están en *A* y están en *T*. Cuando

está claro cuál es el conjunto T se acostumbra simplificar la notación anterior y se escribe A^c. Eso es lo que haremos en la demostración. En todo caso, debe evitarse la *paradoja de Cantor* como ya sabe el estudiante UNA.

Demostración. Veamos ahora la prueba de (1). Sea $x \in (A \cup B)^c$, luego $x \notin A \cup B$ por definición de complemento de un conjunto, entonces $x \notin A$ y $x \notin B$ por definición de unión –sería un error afirmar que $x \notin A$ o $x \notin B$, luego $x \in A^c$ y $x \in B^c$ por definición de complemento. Entonces $x \in A^c \cap B^c$ (definición de intersección). De esto se deduce, por definición de subconjunto, que

$$(A \cup B)^c \subset A^c \cap B^c \qquad \text{(I)}$$

Falta probar que $(A \cup B)^c \supset A^c \cap B^c$. Sea $x \in A^c \cap B^c$, entonces $x \in A^c$ y $x \in B^c$ por definición de intersección de los conjuntos A^c y B^c. Por lo tanto $x \notin A$ y $x \notin B$ por la definición de complemento de un conjunto, de donde $x \notin A \cup B$. Entonces $x \in (A \cup B)^c$. Luego,

$$(A \cup B)^c \supset A^c \cap B^c \qquad \text{(II)}$$

De (I) y (II) se deduce que $(A \cup B)^c = A^c \cap B^c$. ■

 La segunda parte se deja como ejercicio al lector.

Proposición 6. Sea $A \subset T$, entonces:

1. $A \cap A_T^c = \varnothing$
2. $A \cup A_T^c = T$

3. $\left(A_T^c\right)_T^c = A$

Demostración. Se deja como actividad para el lector. Trate de hacerla antes de ver la solución que sigue a continuación.

1. Es claro que no podemos tener que exista un *x* que este en *A* y que no este en *A*, luego $A \cap A_T^c = \varnothing$
2. Como $A \subset T$ y $A^c \subset T \Rightarrow A \cup A^c \subset T$. Pero si yo tomo un *x* cualquiera de *T* es claro que *x* está en *A* o *x* no está en *A* luego $T \subset A \cup A^c$, de donde sigue la igualdad a demostrar. La parte 3. queda a cargo de nuestro estudiante.

1.4. Cardinalidad de un conjunto

Dados dos conjuntos, *A* y *B*, podemos compararlos en términos de la cantidad de elementos que poseen. Si *A* es un conjunto con una cantidad finita de elementos, entonces se dice que su cardinal es finito. Así, si $x_1, x_2, x_3, \ldots, x_n$ son todos los elementos de *A* se escribe que $card\left(A\right) = n$. Así, la comparación del número de elementos de dos conjuntos es sencilla cuando éstos son finitos. No obstante, si *A* y *B* son infinitos la comparación no es tan elemental. *Para saber si dos conjuntos tienen o no la misma cantidad de elementos es menester establecer una biyección entre los dos conjuntos, si tal biyección existe entonces los dos conjuntos tienen la misma cantidad de elementos.* Veamos un ejemplo: consideremos a los conjuntos $\mathbb{N}$ y $\mathbb{Z}$. Ambos son infinitos, pero aunque pueda contrariar nuestras concepciones previas, ¡$\mathbb{N}$ tiene exactamente la misma cantidad de elementos que $\mathbb{Z}$!

Cantor utilizó la idea de comparar conjuntos por medio de *funciones* definidas entre ellos, a saber $card(A) = card(B)$ si, y sólo si, existe una función $f : A \to B$ biyectiva. Si dos conjuntos tienen el mismo cardinal se dice que son *equipotentes*.

1. **($\mathbb{N}$ y $\mathbb{Z}$ tienen la misma cantidad de elementos).** Si hacemos corresponder al cero con el cero y a los naturales (no cero) con los enteros positivos (ver la lista adjunta)

$$\begin{array}{c} \vdots \\ -2 \\ -1 \\ 0 \to 0 \\ 1 \to 1 \\ 2 \to 2 \\ \vdots \end{array}$$

Entonces los enteros negativos no tendrán su "correspondiente" en $\mathbb{N}$. Así, ¡ésta no es una biyección entre $\mathbb{N}$ y $\mathbb{Z}$! Pero existen formas de establecer una correspondencia biyectiva entre $\mathbb{N}$ y $\mathbb{Z}$. ¡De hecho existen infinitas formas! Exponemos la que sigue.

$$
\begin{aligned}
0 &\rightarrow 0\\
1 &\rightarrow 1\\
2 &\rightarrow -1\\
3 &\rightarrow 2\\
4 &\rightarrow -2\\
5 &\rightarrow 3\\
6 &\rightarrow -3\\
7 &\rightarrow 4\\
8 &\rightarrow -4\\
&\vdots
\end{aligned}
$$

correspondencia que permite definir a *f* como: $f:\mathbb{N}\rightarrow\mathbb{Z}$ por la regla

$$
f(x)=\begin{cases}-\frac{x}{2} & si\ x\ es\ par\\ \frac{x+1}{2} & si\ x\ es\ impar\end{cases}
$$

Sugerimos al lector mostrar otra correspondencia biyectiva entre $\mathbb{N}$ y $\mathbb{Z}$. (En la semana 3 se estudiará detalle la idea de función).

2. ¡Los lectores advertirán que $\mathbb{N}$ también es equipotente, por ejemplo, al conjunto de los números pares, o bien, al conjunto de los múltiplos de 11! Así, es factible que dado un conjunto *A* contenido en *B*, con $A\neq B$ y aún así *A* y *B* tengan el mismo cardinal. El mundo de los conjuntos infinitos ofrece muchos retos al pensamiento. Fue Galileo Galilei quien señaló de manera explícita que se podía establecer una correspondencia biunívoca entre el conjunto de los números naturales $\mathbb{N}$ y el conjunto los números cuadrados $\{0,1,4,9,\cdots\}$ por medio de la función $f(n)=n^2$ que es con claridad una biyección. Esto le pareció sospechoso al genio de Pisa e indicó que tal paradoja se debía a trabajar con el infinito.

De la misma manera, puede verse que $\mathbb{N}$ y $\mathbb{Q}$ tienen la misma cantidad de elementos. En cambio, ¡de $\mathbb{R}$ puede afirmarse que tiene mayor cantidad de elementos que $\mathbb{N}$! Así, el infinito de $\mathbb{R}$ es más grande que el infinito de $\mathbb{N}$ –este es el famoso *problema del continuo* que ocupó de manera importante a Cantor; de hecho es el primero de los diez problemas expuestos por David Hilbert en 1900 (en su conferencia en el Segundo Congreso Internacional de Matemática en París, del 6 al 12 de agosto de 1900. Más adelante publicó una lista de veintitrés problemas que influyeron enormemente en las matemáticas del siglo XX). Lo anterior advierte sobre distintos tipos de infinitos.

En este último caso, decimos que $card(A) < card(B)$ si, y sólo si, $P(A) < P(B)$. Es decir, el cardinal de *A* es menor que el cardinal de *B* si, y sólo si, el conjunto de partes de *A* tiene menos elementos que el conjunto de partes de *B*.

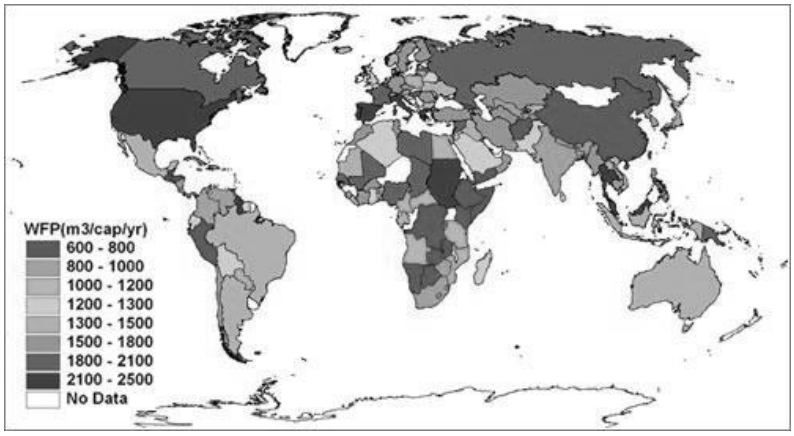
Así, el *problema del continuo* tiene que ver con la existencia o no de un conjunto *X* que verifique lo siguiente:

$$card(\mathbb{N}) < card(X) < card(\mathbb{R})$$

–¿existe algún conjunto *X* con un cardinal comprendido entre los cardinales de $\mathbb{N}$ y $\mathbb{R}$? Es fácil ver que el menor de los cardinales de los conjuntos infinitos es el cardinal de $\mathbb{N}$. Además, si un conjunto *A* es equipotente con $\mathbb{N}$ entonces se dice que *A* es numerable o enumerable. En términos "prácticos", ello significa que podemos contar sus elementos. Este conteo, en ciertos casos, implica un problema muy complejo (ver los problemas propuestos).

 En la nota al final de esta sección (El argumento de la "diagonal de Cantor") se expone la prueba de la no enumerabilidad del intervalo real $(0,1)$ y de $\mathbb{R}$.

1. ¿Qué conjuntos distingue el siguiente gráfico?



Mapa del consumo mundial de agua (cantidad de metros cúbicos por persona en un año) (período 1997-2001). Fuente: waterfootprint.org.

(a) ¿Qué significado tiene la unión de dos o más de estos conjuntos?

(b) ¿Cuál es la intersección de dos de estos conjuntos?

El consumo de agua por persona al año en cada país se ha asociado, erróneamente, a la cantidad de alimentos que se ingiere; sin embargo, ciertos patrones de consumo en países como EE.UU., España, Italia, etc. (innecesaria calefacción, enfriamiento del aire, iluminación, diseños no-ecológicos, muy escaso o nulo tratamiento de las aguas servidas, entre otros) muestran una relación directa con los altos volúmenes que reseña el gráfico.

2. Describa el conjunto que se ha destacado con sombreado.

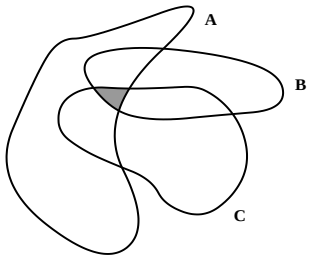


Gráfico de A, B y C

3. Calcule el índice de la cantidad de desechos sólidos por persona (y por entidad federal) para 2008 en Venezuela. ¿De qué manera puede definirse un conjunto que reúna estos índices y que se diferencien entre sí? ¿Sirve listarlos?
4. Si $A=\{a,b\}$, ¿cuáles son los elementos de *P*(*A*) y $P\left(P\left(A\right)\right)$? ¿Cuál es el cardinal de *A*, *P*(*A*), y de $P\left(P\left(A\right)\right)$?
5. Responda la cuestión anterior en el caso de $A=\varnothing$.
6. Si *A* es un conjunto con *n* elementos, ¿cuántos elementos tiene $P\left(A\right)$? Aporte una prueba de ello.
7. ¿Es posible escribir el intervalo (0,1) como una unión numerable de intervalos cerrados?.
8. Dados dos conjuntos *A* y *B* se define su diferencia como

$$A-B=\{x:x\in A\wedge x\notin B\}$$

De lo que se deriva inmediatamente que

$$A-B=A\cap B^c$$

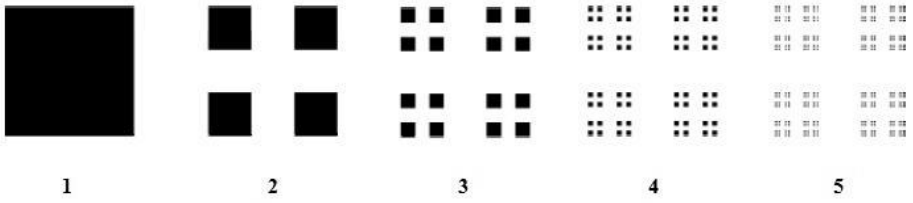
(Aquí sobreentendemos que *A* y *B* son parte de un conjunto *T* y que el complemento de éstos, de su diferencia, de su unión o de su intersección, por ejemplo, se determinan en *T*).

¿Es $\left(A-B\right)^c$ parte de A^c-B^c?

Y más allá, ¿Es $\left(A\cup B\right)^c$ parte de $A^c\cup B^c$?

9. ¿Es cierto que $\left(A-B\right)-C\subset A-\left(B-C\right)$?
10. Si para cualquier conjunto *C* se tiene que $A\cap C=B\cap C$ y $A\cup C=B\cup C$, ¿entonces $A=B$?
11. Compare las propiedades de las operaciones con conjuntos con las del álgebra de proposiciones. ¿Qué semejanzas encuentra? ¿Qué significa esto?

12. El siguiente conjunto es una generalización en el Plano del *conjunto de Cantor*. Se construye a partir de un cuadrado de lado *x* (etapa 1), luego dividimos a éste en nueve cuadrados de igual área y omitimos los que no tengan un vértice común con el cuadrado de la etapa 1 (esta es la etapa 2), y así hasta el infinito! El gráfico que sigue ilustra el *"cuadrado" de Cantor* hasta la etapa 5. Sugerimos al lector elaborar una tabla en la que se compile información sobre el número de cuadrados que se generan en cada etapa, de la suma del área de los cuadrados en cada etapa, así como del perímetro. ¿Existe alguna regla general que describa la etapa *n*? Si es así, cuál es. ¿Puede generalizar estas cuestiones para un cubo en la etapa 1?



"Cuadrado" de Cantor

13. Probar que el conjunto de los múltiplos de 11 es enumerable.
14. ¿Es enumerable un subconjunto infinito cualquiera de un conjunto enumerable?
15. Probar que $card(\mathbb{N}) = card(\mathbb{Q})$.
16. Probar que la unión de cualquier colección finita o enumerable de conjuntos enumerables es enumerable.
17. Probar que el producto de dos conjuntos finitos (enumerables) es un conjunto (finito) enumerable. ¿Qué ocurre en el caso del producto infinito?
18. Una sucesión de números naturales puede representarse por $(x_1, x_2, x_3, x_4, ...)$ con $x_i \in I$ e $I \subset \mathbb{N}$. Pruebe que
    (a) el conjunto de todas las sucesiones finitas de números naturales es enumerable.

(b) el conjunto de todas las sucesiones infinitas de números naturales no es enumerable.

1. Es claro que cada tono en el gráfico representa los habitantes del planeta o países que tienen un mismo nivel de consumo de agua.
   (a) La unión va a representar que consideramos los países que están entre dos rangos de consumo.
   (b) Se trata de una partición en países que tienen un determinado nivel de consumo de agua, luego los elementos son disjuntos y la intersección debiese ser el conjunto vacío.
2. Se trata de la intersección de los tres conjuntos *A,B* y *C* de la figura.
3. Se deja al lector.
4. Partes de *A* está formado por los conjuntos $\varnothing,\{a\},\{b\},\{a,b\}$, recuerde que el vacío es subconjunto de cualquier conjunto. Ahora, el conjunto de partes de *A* tiene la siguiente lista de elementos

   $$\varnothing,\{\varnothing\},\{\{a\}\},\{\{b\}\},\{\{a,b\}\},\{\{a\},\varnothing\},\{\{b\},\varnothing\},\{\{a,b\},\varnothing\}$$
   $$\{\{a\},\{b\}\},\{\{a\},\{a,b\}\},\{\{b\},\{a,b\}\},\{\varnothing,\{b,a\},\{a\}\},\{\varnothing,\{b\},\{a\}\}$$
   $$\{\varnothing,\{b\},\{a,b\}\},\{\{a\},\{b\},\{a,b\}\},$$
   $$\{\varnothing,\{a\},\{b\},\{a,b\}\}$$

   El cardinal de *A* es 2, el de *P*(*A*) es 4 y el de *P*(*P*(*A*)) es de 16, esto sugiere la fórmula $card(P(A)) = 2^{card(A)}$. Veremos en una próxima solución que es correcta.
5. Se deja al lector.
6. Aunque inducción matemática será tratada en detalle en el módulo II, el estudiante UNA debio estudiarlo en quinto año de bachillerato, ver por ejemplo el libro [Gi] en la bibliografía. En primer lugar, por los ejemplos tratados anteriormente pareciera que *P*(*A*) tiene 2^n elementos si *A* tiene *n* elementos. Es claro que la proposición es cierta para el conjunto vacío $\varnothing$ que tiene 0 ele-

mentos pero $P(\varnothing)$ tiene un elemento, precisamente $\{\varnothing\}$. Supongamos ahora que la proposición es cierta para un conjunto *A* de *k* elementos, esto es el cardinal de *P*(*A*) tiene 2^k, es lo que se llama la hipótesis inductiva. ¿Qué ocurre cuando le añadimos a *A* un nuevo elemento? Es claro que tenemos todos los mismos subconjuntos que aparecían en *A* más estos subconjuntos con el elemento añadido, es decir duplicamos la cantidad de subconjuntos, luego tendremos $2 \cdot 2^k = 2^{k+1}$ subconjuntos, luego el resultado es cierto por inducción matemática.

7. Sí lo es, aunque parece sorprendente. Considere

$$I_n = \left[\frac{1}{n}, \frac{n}{n+1}\right], n = 2,3,\cdots$$

por ejemplo, I_N $I_2 = \left[\frac{1}{2}, \frac{2}{3}\right], I_3 = \left[\frac{1}{3}, \frac{3}{4}\right], \cdots$. Es claro que

$$I_n = \left[\frac{1}{n}, \frac{n}{n+1}\right] \subset (0,1), n = 2,3,\cdots$$

Ya que $0 < \frac{1}{n} < \frac{n}{n+1} < 1$, para $n>1$, el estudiante UNA debe decir por qué, luego

$$\bigcup_{n=1}^{\infty} I_n \subset (0,1)$$

Pero, si tomo cualquier x que verifique $0<x<1$, podemos tomar un *N* muy grande tal que $\frac{1}{N} < x < \frac{N}{N+1}$, ya que $\lim_{n\to\infty} \frac{1}{n} = 0$ y $\lim_{n\to\infty} \frac{n}{n+1} = 1$. Luego, x está en I_N pero

$I_N \subset \bigcup_{n=1}^{\infty} I_n$ de donde el intervalo $(0,1)$ está incluído en $\bigcup_{n=1}^{\infty} I_n$ y luego $\bigcup_{n=1}^{\infty} I_n = (0,1)$.

8. Debemos responder a la pregunta: ¿es $(A-B)^c$ parte de $A^c - B^c$?. Sabemos que $(A-B)^c = (A \cap B^c)^c = A^c \cup B$. Por otro lado, $A^c - B^c = A^c \cap \left(B^c\right)^c = A^c \cap B$ y luego lo que se tiene es

$$A^c - B^c \subset (A-B)^c$$

La otra parte se deja al estudiante UNA.

9. Tenemos

$$A-\left(B-C\right) = (A \cap (B-C)^c) = (A \cap (B \cap C^c)^c) =$$
$$A \cap (B^c \cup C) = \left(A \cap B^c\right) \cup \left(A \cap C\right) =$$
$$\left(A-B\right) \cup \left(A \cap C\right)$$

Por otro lado,

$$A-(B-C) = (A \cap (B \cap C^c)^c) = (A \cap (B^c \cup C)) =$$
$$\left(A \cap B^c\right) \cup (A \cap C) = (A-B) \cup (A \cap C)$$

Luego los conjuntos son de hecho iguales.

10. Sabemos que $A \cap C = B \cap C$, luego si tomamos C=A y lo sustituímos arriba se tiene que

$$A \cap A = B \cap A$$
$$A = B \cap A \Rightarrow A \subset B$$

Similarmente, partiendo de que

$$A \cup C = B \cup C \Rightarrow$$
$$A \cup A = B \cup A \Rightarrow$$
$$A = B \cup A \Rightarrow B \subset A$$

De donde los conjuntos son iguales por la doble contención.

11. Revise la idea de álgebra de Boole y vea que relación tiene ésta con el álgebra de conjuntos y la lógica proposicional.
12. Tomemos la función

$$f:\mathbb{N}\to\{\text{múltiplos de 11}\}$$
$$f(n)=11n$$

El estudiante UNA debe verificar que *f* es sobreyectiva. Para la inyectividad se debe verificar que si

$$f(n)=11n=\ f(m)=11m\Rightarrow n=m$$

Pero si $11n=11m$ dividiendo ambos lados por 11 se tiene que $n=m$ como queríamos ver. Luego, *f* es biyectiva y los naturales tienen la misma cantidad de elementos que el conjunto de todos los múltiplos de 11.

13. ¿Es enumerable un subconjunto infinito cualquiera de un conjunto enumerable?

    Al ser el primer cardinal infinito el de los naturales el resultado es cierto, el estudiante Una debe reflexionar sobre lo que afirmamos.
14. Hay varias formas de demostrar este hecho, la demostración que damos es muy bonita y se debe a Kolmogorov. Es claro que la unión numerable de conjuntos finitos es numerable, ¿por qué? Tomemos ahora una fracción cualquiera irreducible $\frac{p}{q}$, q distinto de 0 y p,q sin factores primos comunes. Definimos la altura de $\frac{p}{q}$, denotada por $\left\|\frac{p}{q}\right\|$, como

$$\left\|\frac{p}{q}\right\|=|p|+|q|$$

Es claro que $\left\| \frac{p}{q} \right\|$ es siempre un número natural. Si damos un natural *n* definimos el conjunto

$$A_n = \left\{ \frac{p}{q} \in \mathbb{Q} \text{ tales que } \left\| \frac{p}{q} \right\| = n \right\} \varnothing$$

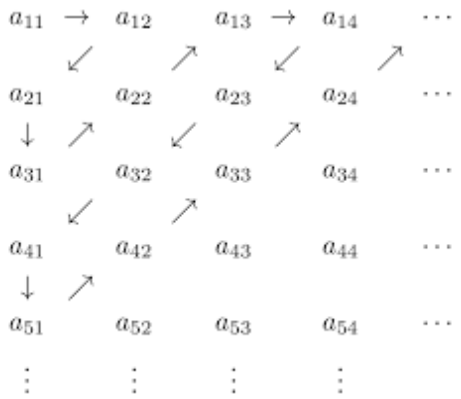
Vemos que $\left\| \frac{p}{q} \right\| = |p| + |q| = n$ implica que $-n \le p \le n, -n \le q \le n$ de donde A_n tiene a lo más n^2 elementos, pero $\mathbb{Q} = \bigcup_{n=1}^{\infty} A_n$ lo que demuestra el resultado ya que escribimos $\mathbb{Q}$ como una unión numerable de conjuntos finitos.

Otra solución: Trate de resolver primero el problema 17, y luego escriba los racionales de la siguiente manera $\mathbb{Q} = \bigcup_{n=1}^{\infty} A_n$ donde cada $A_n = \left\{ \frac{m}{n}, m \in \mathbb{Z} \right\}$, es decir son todas las fracciones que tienen denominador *n*. Claramente cada $A_n = \left\{ \frac{m}{n}, m \in \mathbb{Z} \right\}$ es numerable y luego $\mathbb{Q}$ se escribe como una unión numerable de conjuntos numerables.

15. Vamos a suponer que tenemos una cantidad numerable de conjuntos $A_n, n = 1, 2, \cdots$ y que cada $A_n, n = 1, 2, \cdots$ es numerable. Escribimos entonces

$$A_n = \{a_{n1}, a_{n2}, a_{n3}, \cdots\}$$

El siguiente dibujo demuestra la proposición pero dejamos al estudiante la tarea de traducir el mismo al lenguaje matemático



16. b) Puede aplicar una rgumento tipo diagonal y suponer que tiene una cantidad numerable de sucesiones de números naturales y construir una que no aparezca en la numeración, por favor piense en cómo hacer el resto del problema.

1.5. Modelando con los conjuntos

A – La longitud del conjunto de Cantor. Observemos que el segmento inicial tiene longitud 1. En el primer paso de la iteración para construir a *C* la longitud de C_1 es $\frac{1}{3}+\frac{1}{3}=\frac{2}{3}$ (apóyese en el gráfico expuesto al inicio de esta "semana"); en el segundo paso, C_2 tiene longitud $\frac{1}{9}+\frac{1}{9}+\frac{1}{9}+\frac{1}{9}=\frac{4}{9}$; en el tercer paso, C_3 tiene longitud $\frac{1}{27}+\frac{1}{27}+\frac{1}{27}+\frac{1}{27}+\frac{1}{27}+\frac{1}{27}+\frac{1}{27}+\frac{1}{27}=\frac{8}{27}$. C_4 tiene longitud $\frac{16}{81}$. (Fíjese que $\frac{2}{3}=\frac{2^1}{3^1}$, $\frac{4}{9}=\frac{2^2}{3^2}$, $\frac{8}{27}=\frac{2^3}{3^3}$, $\frac{16}{81}=\frac{2^4}{3^4}$ …). Podemos ver que C_n tiene longitud $\frac{2^n}{3^n}$ (para *n* iteraciones). Y $\frac{2^n}{3^n}$ tiende a 0 cuando *n* tiende al infinito. Entonces, la longitud de *C* es 0.

B – El Hotel Infinito (o de Hilbert) ∞**.** Supongamos que hubiera un número infinito de personas en el mundo. Y supongamos también que hay un hotel, en una ciudad, que contiene infinitas habitaciones. Estas habitaciones están enumeradas, correspondiéndole a cada una un número natural. Así, la primera lleva el número 1, la segunda el 2, la tercera el 3, etcétera. Es decir: en la puerta de cada habitación, hay una placa con un número que sirve de identificación.

Ahora, supongamos que todas las habitaciones están ocupadas y sólo por una persona. En un momento determinado, llega al hotel un señor con cara de muy cansado. Es tarde en la noche y todo lo que este hombre espera es terminar rápido con el papeleo para poder ir a descansar. Cuando el empleado de la recepción le dice que "lamentablemente no tenemos ninguna habitación disponible ya que todas las habitaciones están ocupadas", el recién llegado no lo puede creer. Y le pregunta:

–Pero, cómo... ¿no tienen ustedes infinitas habitaciones?
–Sí –responde el empleado del hotel.
–Entonces, ¿cómo me dice que no le quedan habitaciones disponibles?
–Y sí, señor. Están todas ocupadas.
–Vea. Lo que me está contestando no tiene sentido. Si usted no tiene la solución al problema, yo lo ayudo.

Y acá conviene que ustedes piensen la respuesta. ¿Puede ser correcta la respuesta del recepcionista, o sea que "no hay más lugar", si el hotel tiene infinitas habitaciones? ¿Se les ocurre alguna solución? Veamos:

–Fíjese –continuó el pasajero–. Llame al señor de la habitación que tiene el número 1 y dígale que pase a la que tiene el 2. A la persona que está en la habitación 2, que vaya a la del 3. A la del 3, que pase a la del 4. Y así, siguiendo de esta forma, toda persona seguirá teniendo una habitación que no compartirá con nadie (tal como era antes), pero con la diferencia de que ahora quedará una habitación libre: la número 1.
El recepcionista lo miró incrédulo, pero comprendió lo que le decía el pasajero. Y el problema se solucionó.
Ahora bien: algunos problemas más:

(a) Si en lugar de llegar un pasajero, llegan dos, ¿qué sucede? ¿Tiene solución el problema?
(b) ¿Y si en lugar de dos, llegan 1000?

(c) ¿Cómo se puede resolver el problema si llegan *n* pasajeros inesperadamente durante la noche (donde *n* es un número cualquiera). ¿Siempre tiene solución el problema independientemente del número de personas que aparezcan buscando una pieza para dormir? ¿Y si llegaran infinitas personas? ¿Qué pasaría en ese caso? –discuta estas preguntas con sus compañeros y asesor.

1.6. El argumento de la "diagonal de Cantor"

Uno de los resultados más importantes de Cantor es la prueba de que el conjunto de los números Reales tiene un cardinal mayor que el del conjunto de los números Naturales. Esto es, que aún teniendo $\mathbb{R}$ y $\mathbb{N}$ infinitos elementos, ¡ $\mathbb{R}$ tiene más elementos que $\mathbb{N}$! el infinito de $\mathbb{R}$ es distinto (diríamos que "superior") al infinito de $\mathbb{N}$. La prueba de Cantor emplea un *argumento diagonal* que el lector advertirá, veamos:

Consideremos el intervalo de números reales $(0,1)$. Si fuese posible corresponder a este intervalo con $\mathbb{N}$ de manera que (1) a cada número real de $(0,1)$ se asocie un único número natural, (2) que a números reales distintos, en este intervalo, se le asocian números naturales distintos, y (3) que cada número natural está asociado con un número real en $(0,1)$. Este tipo de correspondencia se denomina "uno a uno". Esto significaría que los reales en $(0,1)$ se pueden contar. Y si se pueden contar podemos listarlos como sigue:

$$x_1 = 0, a_{11}, a_{12}, ..., a_{1n}, ...$$
$$x_2 = 0, a_{21}, a_{22}, ..., a_{2n}, ...$$
$$\vdots$$
$$x_n = 0, a_{n1}, a_{n2}, ..., a_{nn}, ...$$
$$\vdots$$

Sin embargo, podemos probar que existe al menos un número real en $(0,1)$ que no está en la lista anterior.

Definamos un $y \in (0,1)$ de la siguiente manera:

$$y = 0, y_{11}, y_{22}, ..., y_{nn}, ...$$

con

$$y_{ii} \neq a_{ii}$$

Observemos que $y \neq x_1$ pues difieren al menos en el primer decimal ($y_{11} \neq a_{11}$), $y \neq x_2$ pues difieren al menos en el primer decimal ($y_{22} \neq a_{22}$) y así sucesivamente. Entonces *y* no es igual a ninguno de los reales que se han listado. Así, la hipótesis de que esta lista contenía todos los números reales comprendidos entre 0 y 1 es falsa.

Con esto podemos concluir que $(0,1)$ no puede corresponderse "uno a uno" con $\mathbb{N}$, y de esta manera tampoco $\mathbb{R}$ podría corresponderse "uno a uno" con $\mathbb{N}$.

Por el argumento diagonal, vemos que $\mathbb{R}$ tiene más elementos que $\mathbb{N}$.

El Teorema de Cantor: o sobre la cardinalidad de $P(A)$

Tiempo después Cantor probó un resultado mucho más general que el anterior, justo uno de los que comentamos en una de las secciones anteriores. Este resultado se conoce como "teorema de Cantor": para cualquier conjunto *A*, $P(A)$ tiene una cardinalidad mayor que *A*. Cantor lo probó de la manera que sigue.

La esencia de la prueba es mostrar que para cualquier conjunto *A* que se considere y para cualquier función $f : A \to P(A)$, existe un elemento de $P(A)$ que no es la imagen a través de *f* de ningún elemento de *A*.
Para ello sugerimos al lector considerar el conjunto

$M = \{a \in A : a \notin f(a)\}$.

¿Cómo puede proseguir la prueba?

El papel de los problemas en el pensamiento de Cantor

Para Cantor "In re mathematica ars proponendi pluris facienda est quam solventi" (en las Matemáticas, el arte de plantear problemas es más importante que su solución). A lo largo de su vida propuso muchas cuestiones abiertas en diversas áreas de las Matemáticas. Algunas de sus soluciones permitieron superar ideas que eran consideradas "definitivas". En ocasiones le fue negado publicar algunos de sus artículos o trabajos. Es curioso que en uno de ellos se colocó la nota "llega con cien años de anticipación". De hecho, sus ideas en la *Teoría de Conjuntos* eran nuevas y consideradas insólitas por algunos. Además de las paradojas que se encontraron en el seno de su teoría, Cantor se enfrentó al *problema del continuo* –el cual creyó estar cerca de su solución pero cuya demostración nunca pudo alcanzar. Lo anterior y el hecho de que sus detractores hicieron honda mella en su estabilidad psicológica –tal vez ya signada por ciertas condiciones genéticas. Una de las primeras aplicaciones de la teoría de Conjuntos de Cantor se hizo en la teoría de Funciones (con los trabajos de, por ejemplo, Mittag-Lefflert). Las Matemáticas también le deben a Cantor sus importantes contribuciones al Análisis (su estudio del *infinito*, la construcción de un número real, la introducción de muchos conceptos topológicos como la derivación de un conjunto, su clausura, denso, denso en sí, "perfecto", entre muchos otros). Hay varios teoremas importantes que Cantor expuso en su teoría y que fueron probados por otros matemáticos, tal es el caso de, por ejemplo, el

Teorema de equivalencia de Cantor-Schröder-Bernstein: Si existe una función inyectiva de *A* en *B* y una función inyectiva de *B* en *A*, entonces existe una biyección entre *A* y *B*.

¿Qué ejemplos puede dar?

Las paradojas que se avistaron en la teoría de Conjuntos de Cantor influenciaron en gran medida la discusión de los fundamentos de las matemáticas, y hasta cierto punto, su formalización; contrario a la idea platónica que tenía Cantor de las Matemáticas.

En el fondo, los problemas para Cantor importaron tanto en su formulación (en especial de aquellos que se correspondían con el desarrollo de las matemáticas) como en su solución, contrario a como había expresado.

1. Con base en los datos: 45 casos de dengue en la ciudad *A* para 1990, 52 en 1995 y 59 en 2000, un informe concluyó que en esa ciudad se ha incrementado el número de casos de dengue entre 1990 y 2000. ¿Es correcta esta conclusión?
2. Con los datos de unas encuestas de opinión sobre la preferencia de cierto candidato, efectuadas en 100 puntos de la ciudad *A*, se concluye que en el Estado (donde está la ciudad *A*) el nivel de aceptación de tal candidato es bajo. ¿Es correcta esta conclusión?
3. ¿Es $A \cap (T - A) = \varnothing$? De ser así, pruébelo; de lo contrario, muestre un contraejemplo.
4. Si $A \subset B$, ¿$A \cup T \subset B \cup T$?
5. Si $A \subset B$, ¿$A \cap T \subset B \cap T$?
6. Si $A \subset B$, ¿$T - A \subset T - B$?

7. Si $A \subset B$, ¿$T - B \subset T - A$?
8. Probar que $T - (A \cap B) = (T - A) \cup (T - B)$.
9. ¿Son equivalentes las proposiciones siguientes? ¿Algunas de ellas son equivalentes?

    a. $A - B = \varnothing$
    b. $A \cap B = A$
    c. $A \cup B = B$
    d. $A \subset B$

10. Si $P(A) = P(B)$ probar que $A = B$.
11. Probar la proposición 4 en sus partes 5 a 10.

1. En cualquier proceso de medición es muy importante diferenciar entre los datos relativos y los datos absolutos. Por ejemplo, si al medir una distancia obtengo un error de 11 Km puede parecer que ese es un error my grande, pero si me dicen que ese error se cometio al medir la distancia de la tierra al sol entonces es un error muy pequeño.

   Igualmente en el problema considerado no basta sólo examinar los casos de dengue registrados, se debiese medir el crecimiento de la población y hacer el cociente

$$\frac{\#CasosDengue}{Población}$$

2. Es claro que se está omitiendo información de lo que ocurre en el resto del estado, un candidato puede ser muy popular en las zonas urbanas pero no disponer de apoyo en el resto del estado.

3. Es cierto ya que $A \cap (T - A) = A \cap (T \cap A^c) \subset A \cap A^c = \varnothing$

4. Es cierto, veamos por qué

$$x \in A \cup T \Rightarrow x \in A \text{ o } x \in T \Rightarrow x \in B \text{ o } x \in T$$
$$\Rightarrow x \in B \cup T$$

5. Muy similar al 4. y se deja al estudiante UNA.

6. Falso, ver 7.

7. Es cierto, ya que

$$T - B = T \cap B^c \; T - B = T \cap B^c$$

Pero si $A \subset B \Rightarrow B^c \subset A^c$, luego $T \cap B^c \subset T \cap A^c$ de donde

$$T - B \subset T - A$$

8. Como

$$T - (A \cap B) = T \cap (A \cap B)^c =$$
$$T \cap (A^c \cup B^c) = (T \cap A^c) \cup (T \cap B^c) =$$
$$(T - A) \cup (T - B)$$

9.

$$A - B = A \cap B^c \subset B \cap B^c = \varnothing \Rightarrow$$
$$A \subset B$$

Y de esta inclusión se tiene que

$$A \subset B \Rightarrow A \subset A \cap B \text{ y como } A \cap B \subset A \Rightarrow$$
$$A \cap B = A$$

Similarmente se demuestra que también

$$A \cup B = B$$

Por otro lado, si $A \cup B = B$, entonces

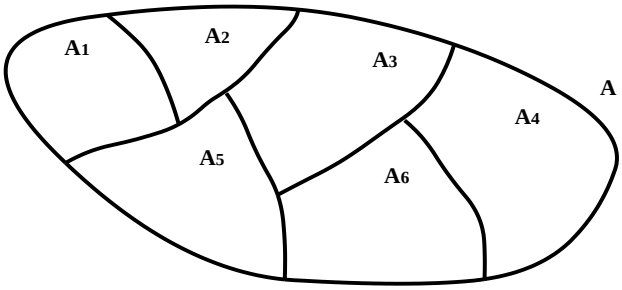
$$A - B = A \cap B^c \subset B \cap B^c = \varnothing$$

De donde las proposiciones son equivalentes.

10. Queda como ejercicio para el estudiante UNA.

UNIDAD 2

Relaciones



Una partición de A

Semana 2

Aplicar el concepto de relación en la resolución de problemas, en el modelado matemático y en la demostración de nuevos resultados.

Contenidos a tratar: Relaciones de equivalencia, conjunto cociente. Relaciones de orden, orden en un conjunto. Elementos distinguidos en un conjunto ordenado. Algunas aplicaciones en el modelado.

2.1 Introducción

Contar es una idea matemática propia a todas las culturas originarias alrededor del mundo, ello implica establecer una relación entre un conjunto de objetos, animales, personas o, incluso, fenómenos físicos (o astronómicos) y un subconjunto de los números naturales $\mathbb{N}$. El concepto de relación está imbricado históricamente con el desarrollo del concepto de número y con el de conjunto. Incluso, en la construcción formal de los números naturales $\mathbb{N}$ se introduce una relación denominada *"sucesor"* o *"siguiente"* que caracteriza este conjunto de acuerdo a Peano. También se utiliza

una relación de equivalencia definida en el *producto cartesiano* de $\mathbb{N}\times\mathbb{N}$ para construir a $\mathbb{Z}$ – esta idea se estudiará más adelante. La Geometría es también una fuente de relaciones de importancia, tal es el caso del *paralelismo* entre rectas, planos u otros espacios y la *congruencia* entre figuras o cuerpos. La *medida* es un ejemplo importante de relación tanto en el seno de las matemáticas como en el contexto real: desde cierta noción de medida se pueden comparar dos puntos cualquiera, o bien, dos objetos físicos o no (tal es el caso de los conjuntos, por ejemplo). En reportes tan comunes como las gráficas en el Plano o en el Espacio, los electrocardiogramas, imágenes "3d" del bebé en formación, exámenes sanguíneos, en la encriptación de datos por medio de códigos de barras, en las comunicaciones y tarjetas de débito o crédito, imágenes fotográficas y satelitales, tasas de impuestos, en la codificación de los semáforos en términos del flujo vehicular, la compatibilidad de los grupos sanguíneos en las parejas, en las redes de distribución de cierto alimento en la localidad o en el ámbito nacional, en el volumen de extracción de petróleo en función de las cuotas establecidas por la OPEP, la demanda por estaciones, el clima político internacional, etc., conexiones entre los centros de acopio de gas doméstico, rutas de transporte público... las relaciones son su concepto base. Esta mirada matemática del mundo permite soportar decisiones medulares para la vida, gubernamentales o no. Lo mismo sucede en las diversas áreas en que se ha configurado la matemática en los últimos siglos. De hecho, comprender la naturaleza de cierto objeto matemático (o no) pasa por estudiar las relaciones entre ellos.

1. **(el antígeno prostático).** La siguiente relación

$$\begin{aligned} 0 \text{ a } 2{,}5\ ng/ml &\leftrightarrow 40-49 \text{ años} \\ 0 \text{ a } 3{,}5\ ng/ml &\leftrightarrow 50-59 \text{ años} \\ 0 \text{ a } 4{,}5\ ng/ml &\leftrightarrow 60-69 \text{ años} \\ 0 \text{ a } 6{,}5\ ng/ml \text{ o más} &\leftrightarrow 70-79 \text{ años} \end{aligned}$$

muestra algunos rangos de *antígeno prostático* (PSA) en la sangre considerados "normales" (El PSA es una proteína que produce la próstata); no obstante, algunos estudios sostienen que no hay un rango considerado "normal" (pues hay hombres con un nivel bajo de PSA y, aún así, presentan complicaciones importantes en esta glándula). Los valores están expresados en nanogramos de PSA por cada mililitro de sangre (*ng*/*ml*). Como sabemos, 1 $ng = 10^{-9}\ g$. El nivel de PSA en el hombre es un indicador, aunque muy discutido, del cáncer de próstata (justo una de las afecciones más comunes del hombre en la República Bolivariana de Venezuela).

2. **(las reservas de gas).** En los yacimientos de petróleo se estima que por cada metro cúbico de crudo hay unos 83 m^3 de gas (ver www.pdvsa.com).

Reserva de gas natural por países (en billones de m^3)

Rusia	48,1	Irak	3,1
Irán	22,9	Turkemistán	2,9
Qatar	8,5	Malasia	2,3
Emiratos A. U.	5,8	Indonesia	2,0
Arabia Saudita	5,4	Canadá	1,9
EE UU	4,7	México	1,9
Venezuela	4,0	Holanda	1,8
Argelia	3,7		
Nigeria	3,2		

3. **(humedad del suelo).** La capacidad del suelo para retener agua (índice de retención de humedad) es una de las propiedades importantes a considerar en la evaluación de ciertos procesos agrícolas, e incluso, pecuarios. En algunas regiones del país, esta relación varía muchísimo durante el año. Por ejemplo, en Tejos (1984, UCV: Análisis del crecimiento, valor nutritivo, reservas y descomposición de cinco gramíneas de sabanas inundables) se mostró que en una región de nuestro país, sus valores en la sabana alta, bien drenada y de textura gruesa, osciló entre 3,6 y 21 %. Pero en el bajío y estero, de textura

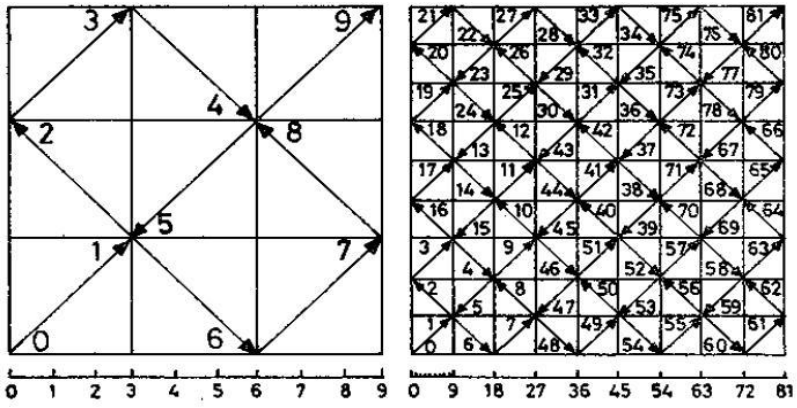
media y fina, este rango fue de 3,4 a 45 % y de 12,6 a 50 %, respectivamente.

4. **(transporte).** Ciertos problemas sobre flujo vehicular (mínimo y máximo), número de recorridos entre dos puntos en una red vial que conecta a varias ciudades, entre muchos otros en el campo de las comunicaciones y la informática pueden modelarse con apoyo en el concepto de *relación de orden.*
5. **(consumo de energía eléctrica en Latinoamérica).** Venezuela es el país en Latinoamérica con mayor consumo per cápita de energía eléctrica. En 2008 se alcanzaron 4.126 Kwh/habitante, en segundo lugar estuvo Chile con 3.505, Argentina 2.979, Uruguay 2.585, Brasil 2.447, Ecuador 1.222 y Colombia con 1207. En 2009 Venezuela sobrepasó los 4.370 Kwh/ habitante (Fuente: http://www.minci.gob.ve).

2.2 La idea de Relación. Relaciones de equivalencia y de orden

1. La *curva de Peano* es un buen ejemplo de una relación entre sus puntos y los puntos de un cuadrado.

Expondremos de seguida la construcción que da Shoenflies de la Curva de Peano – justo una de las que "llena" el Plano.



Construcción de Shoenflies de la curva de Peano

“Dado un segmento y un cuadrado, dividamos aquél en nueve partes iguales, y éste en nueve cuadrados también iguales, haciendo corresponder éstos a aquéllos en el orden indicado en la primera figura. Obtenemos así diez puntos del segmento (los de división), a los cuales asignamos sus correspondientes en el cuadrado, como indican los extremos de los trazos marcados en la figura. Subdividamos ahora cada segmento y cada cuadrado en nueve partes iguales, haciéndolas corresponder en el orden indicado por la segunda figura. Así tenemos 82 pares de puntos correspondientes. Siguiendo de este modo, obtenemos dos redes de puntos, cada vez más densas, en el segmento y en el cuadrado. Dado un punto cualquiera del segmento, caben dos posibilidades: o llega a obtenerse como punto de subdivisión, en cuyo caso ya le hemos asignado su correspondiente en el cuadrado, o aparece dicho punto como límite de una sucesión indefinida de segmentos, cada vez más pequeños, contenido cada uno en el anterior, a los cuales corresponden cuadrados también contenidos unos en otros, y que también tienden a cero; por consiguiente, en virtud del axioma de Dedekind, existe un punto único contenido a la vez en todos; y este punto lo asignamos a aquel primero como correspondiente. Recíprocamente, todo punto del cuadrado tiene al menos un correspondiente en el segmento”.

Ahora…

(a) A cada punto del segmento ¿cuántos puntos le corresponden en el cuadrado?

(b) Y, dado un punto del cuadrado, ¿cuántos puntos le corresponden en el segmento?

2. **(congruencia módulo 3).** Consideremos el conjunto de los números enteros $\mathbb{Z}$ y el número 3. Podemos establecer una “relación” en $\mathbb{Z}$ de la manera que sigue: diremos que dos enteros están “relacionados” si, y sólo si, la diferencia entre ellos es divisible por 3. Esta relación la estudiaremos en general en la Unidad del texto correspondiente a los enteros módulo *n.* Este el es caso de 1 y 4, pues 3 divide a $4-1$, o bien de 1 y 25, ya que 3 divide a $1-25$; pero 1 y 2, por ejemplo, no están relacionados ya que 3 no divide a $1-2$. De inmediato

observamos que dado un número entero cualquiera *x*, siempre existe algún entero relacionado con *x*, más aún, existen infinitos enteros relacionados con *x*. Formalmente escribimos que

$$a \equiv b \left(\textit{mód } 3\right) \Leftrightarrow 3 \mid a-b$$

Lo cual leemos "*a* está relacionado con *b* (en módulo 3) si, y sólo si, tres divide a $a-b$". Esta relación en particular recibe el nombre de *"congruencia módulo n"* (en nuestro caso, *n*=3. Pero la escogencia de *n* es arbitraria –siempre que $n \neq 0$). Observe que $1 \equiv 4,\ 4 \equiv 7,\ 7 \equiv 10,\ 10 \equiv 13$ …, $2 \equiv 5,\ 5 \equiv 8,\ 8 \equiv 11$ … y $0 \equiv 3,\ 3 \equiv 6,\ 6 \equiv 9,$ $9 \equiv 12,$ … Esta relación en particular cumple las siguientes propiedades: (i) como $3 \mid 0$, entonces $3 \mid a-a$. Así, $a \equiv a \left(\textit{mód } 3\right)$ [*a* es congruente consigo mismo en módulo 3]. (ii) Si $a \equiv b \left(\textit{mód } 3\right)$, entonces $3 \mid a-b$. Y escribiendo esto como $3 \mid a-b = (-1)(b-a)$, concluimos que $3 \mid b-a$, esto es, $b \equiv a \left(\textit{mód } 3\right)$ [si *a* es congruente con *b*, entonces *b* es congruente con *a* en módulo 3]. Otra manera de ver lo anterior es: si $a \equiv b \left(\textit{mód } 3\right)$ entonces $3 \mid a-b$, por tanto $\exists x \in \mathbb{Z} : 3x = a-b$. Y como $3x = a-b = (-1)(b-a) \Rightarrow 3(-x) = b-a$ entonces $3 \mid b-a$. Con lo que podemos decir que $b \equiv a \left(\textit{mód } 3\right)$. (iii) Ahora, si $a \equiv b \left(\textit{mód } 3\right)$ y $b \equiv c \left(\textit{mód } 3\right)$, entonces $3 \mid a-b$ y $3 \mid b-c$; con lo cual $\exists x, y \in \mathbb{Z} : 3x = a-b \wedge 3y = b-c$. De la primera expresión tenemos que $a-3x = b$ y sustituyendo en la segunda expresión obtenemos que $3y = (a-3x)-c \Rightarrow 3(y+x) = a-c$. Así, $3 \mid a-c$, en consecuencia $a \equiv c \left(\textit{mód } 3\right)$ [si *a* es congruente con *b* y *b* es congruente con *c*, entonces *a* es congruente con *c* módulo 3].

Para escribir en términos de conjunto la relación que acabamos de estudiar, necesitamos la noción de *producto cartesiano de conjuntos*. Dados dos conjuntos *X* y *Y*, el producto cartesiano $X \times Y$ está dado por la reunión de los objetos de la forma (x, y), donde $x \in X$ y $y \in Y$; tales objetos se denominan *pares ordenados* –los cuales en-

tenderemos intuitivamente (el lector puede investigar sobre la manera de definir un par ordenado con base en la idea de conjunto).

Ahora bien, podemos escribir que

$$R = \{(a,b) \in \mathbb{Z} \times \mathbb{Z} : 3 | a-b\}$$

R caracteriza la relación de congruencia dada anteriormente. Así,

Definición. Una relación *R* de un conjunto *X* en un conjunto *Y* (no necesariamente distintos) es un subconjunto del producto cartesiano $X \times Y$. Por otra parte, si

Si $aRa, \forall a \in X$, R se dice *reflexiva.*

Si $aRb \Rightarrow bRa$, *R* se dice *simétrica.*

Si $aRb \wedge bRc \Rightarrow aRç R$ se dice *transitiva*.

Las propiedades de la relación "congruencia módulo 3" en $\mathbb{Z}$ definida por $a \equiv b \,(mód\ 3) \Leftrightarrow 3 | a-b$ inducen una *partición* de $\mathbb{Z}$, es decir, podemos expresar a $\mathbb{Z}$ como la reunión de cierta cantidad de conjuntos disjuntos entre sí. Preguntémonos, por ejemplo, ¿qué enteros están relacionados con el 0?, ¿qué enteros están relacionados con el 1?, etc. Con esta información podemos definir los conjuntos $\bar{0}$, $\bar{1}$, y $\bar{2}$ (llamados clases de equivalencia):

$$\bar{0} = \{x \in \mathbb{Z} : x \equiv 0\} = \{..., -6, -3, 0, 3, 6, 9, 12, ...\}$$
$$\bar{1} = \{x \in \mathbb{Z} : x \equiv 1\} = \{..., -5, -2, 1, 4, 7, 10, 13, ...\}$$
$$\bar{2} = \{x \in \mathbb{Z} : x \equiv 2\} = \{..., -4, -1, 2, 5, 8, 11, 14, ...\}$$

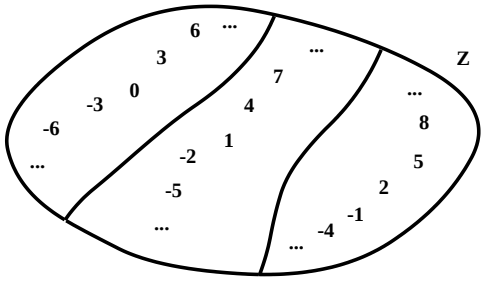
El lector advertirá que

$$\mathbb{Z} = \bigcup \bar{x} \quad \text{con } x = 0,1,2$$
$$\bigcap \bar{x} = \varnothing$$

Para una prueba de ello véanse las proposiciones 3 y 4.

Si nos preguntamos por la clase del 3 (lo que lleva a preguntarse: ¿qué enteros se relacionan con el 3?), vemos que son justo los múltiplos de 3, y ya los hemos listado en $\bar{0}$. Así, $\bar{0}=\bar{3}$. Con un razonamiento similar llegamos a que $\bar{1}=\bar{4}$, $\bar{2}=\bar{5}$ y así sucesivamente. Lo que significa que hemos expresado al conjunto de los números enteros como la reunión de tres conjuntos disjuntos, precisamente las clases de equivalencia que etiquetamos con $\bar{0}$, $\bar{1}$ y $\bar{2}$.

Gráficamente



Una partición de $\mathbb{Z}$ (asociada a la relación de congruencia en módulo 3)

Dado un conjunto *A* y una relación de equivalencia *R* definida en él, el conjunto que consta de todas las clases de equivalencia módulo *R* que podemos formar con los elementos de *A* se le denomina *conjunto cociente* y se denota como sigue

$$A/R=\left\{\bar{a}:a\in A\right\}$$

donde $\bar{a}$ consta de todos los elementos *x* de *A* tales que xRa.

En el caso del ejemplo anterior,

$$\mathbb{Z}/\left(\equiv m\acute{o}d\,3\right)=\left\{\bar{0},\bar{1},\bar{2}\right\}$$

Este conjunto cociente determina la partición de $\mathbb{Z}$ dada antes.

Finalizamos este ejemplo con una observación. Sabemos desde nuestra escuela Primaria que al dividir los enteros positivos *p* y *q* en $\mathbb{Z}$, con $q\neq 0$, es posible escribir la

relación $p = q \cdot c + r$, donde $0 \le r < q$. Este es el famoso *algoritmo de Euclides.* Por ejemplo, $5 = 3 \cdot 1 + 2$, esto es, al dividir 5 entre 3, el cociente es 1 y el resto es 2. Así, el 5 está en la clase $\bar{2}$. Ahora proponemos al lector efectuar la divisiones "-5 entre 3" y "-4 entre 3", es decir, en el caso en el que el dividendo es menor que 0. En una próxima semana (Módulo II) se expondrá una demostración del *Algoritmo de Euclides*.

Definición. Si una relación *R* de un conjunto *X* en un conjunto *Y* (no necesariamente distintos) verifica que, Si $aRb \wedge bRa \Rightarrow a = b$, *R* se dice *antisimétrica.*

 Si en $\mathbb{N}$ definimos la relación

a es menor o igual que *b* si, y sólo si, $\exists x \in \mathbb{N} : a + x = b$

entonces, de un modo similar a lo visto antes se comprueba que (i) $\le$ es reflexiva y (ii) $\le$ es transitiva. (iii) Además, si $a \le b \wedge b \le a$, tenemos que, $\exists x, y \in \mathbb{N} : a + x = b \wedge b + y = a$. De lo que se deduce que $b + (y + x) = b$, y necesariamente $x = y = 0$, pues la relación está definida en $\mathbb{N}$. Así, *a*=*b*. Esto es, tal relación es *antisimétrica.* En este caso, $R = \{(a,b) : a,b \in \mathbb{N} \wedge a \le b\}$.

2. Consideremos ahora el conjunto de los números naturales $\mathbb{N}$ y la relación "es menor que" definida como sigue: dados $a, b \in \mathbb{N}$, diremos que

a es menor que *b*, si y sólo si, $\exists x \in \mathbb{N} - \{0\} : a + x = b$

Como en el caso de la relación expuesta en el ejemplo anterior, exploremos las propiedades de "<". (i) Dado que $\nexists x \in \mathbb{N} - \{0\} : a + x = a$ entonces *a* no está relacionado consigo mismo; así, < no es reflexiva. (ii) Es inmediato que si *a*<*b* entonces $b \not< a$ (*b*

no es menor que *a*). Por lo anterior, < no es simétrica. (iii) En cambio, si $a<b$ y $b<c$, entonces $\exists x, y \in \mathbb{N}-\{0\} : a+x=b \wedge b+y=c$.

Con lo cual, $(a+x)+y=a+(x+y)=c$, donde $x+y \in N-\{0\}$. Así, $a<c$. En resumen, < en $\mathbb{N}$ no es reflexiva, no es simétrica y sí es transitiva. En este caso tenemos que

$$0<1<2<3<4<5<\cdots$$

Por tanto, si convenimos en que *aRb* indica que *"a está relacionado con b"* entonces

$$\begin{array}{cccc} 0R1 & 0R2 & 0R3 & \ldots \\ 1R2 & 1R3 & 1R4 & \ldots \\ 2R3 & 2R4 & 2R5 & \ldots \\ \vdots & \vdots & \vdots & \end{array}$$

Y $R=\{(a,b) : a,b \in \mathbb{N} \wedge a<b\}$.

3. **(significados de arroba).** Considerando los distintos significados de la "arroba" como una de las unidades de masa muy común durante el período de resistencia que inició con la invasión del imperio Español a nuestro continente, aunque hoy día sigue usándose en algunas regiones del país –aún ante la reglamentación y popularidad del *sistema métrico decimal*, en especial a la República Bolivariana de Venezuela, podríamos establecer un orden entre ellas. A saber,

	Entidad Federal	Equivalente del arroba en Kg	Uso (agricultura)
An	Anzoátegui	11,5	Granos
Ar	Aragua	11,5	Granos
C	Carabobo	11,5	Granos
L	Lara	11,5	Granos
M	Monagas	11,5	Granos
D	Distrito Capital	11,5	Tomate

S	Sucre	12,5	Café
	Yaracuy	27,8	Caña de azúcar

Distintos valores del "arroba" como unidad de masa en Venezuela. Fuente: Rodríguez, Leonardo (2000): Pesas y medidas antiguas en Venezuela. Nota: también se usa la arroba para expresar la masa en el ganado.

Aquí la relación está dada por el conjunto

$$R=\{(an,11.5),(ar,11.5),(c,11.5),(l,11.5),(m,11.5),(d,11.5),(s,12.5),(y,27.8)\}.$$

4. Sea $A=\{1,2,3,4\}$. $R=\{(1,1),(2,2),(3,3),(1,3)\}\subset A\times A$ define una relación en *A*, observemos que 1 *R* 1, 2 *R* 2, 3 *R* 3, pero $4 \not R 4$ (4 no está relacionado consigo mismo). Por tanto, *R no es reflexiva*. Es fácil ver que la relación *R* tampoco es simétrica ni transitiva. En éste y en los ejemplos anteriores podemos hacer un gráfico que muestre las asociaciones entre los elementos de *A* determinadas por la relación *R*.

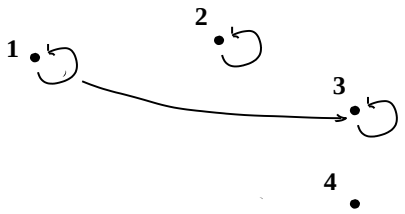


Gráfico de R

La siguiente definición es fundamental en matemáticas. Las relaciones de equivalencia y las de orden son las más importantes en nuestra ciencia. Permiten construir las importantes estructuras de espacio cociente (relaciones de equivalencia) y retículo (relaciones de orden). Ellas aparecerán con frecuencia en Unidades posteriores.

Definición. Las relaciones que cumplen las propiedades (1) reflexiva, (2) simétrica y (3) transitiva, se llaman de *equivalencia*.

Dejamos al lector la tarea de dar ejemplos de otras relaciones de equivalencia y de orden, así como de relaciones que no sean de equivalencia ni de orden.

Ahora bien, Sea $R: A \to B$ una relación dada.

Definición. La relación inversa R^{-1} se define como $R^{-1} = \{(b,a) \in B \times A : (a,b) \in R\}$.

En el caso del ejemplo anterior, tenemos que $R^{-1} = \{(1,1),(2,2),(3,3),(3,1)\}$.

Si $R: A \to B$ y $S: B \to C$ son dos relaciones, se define la composición de las relaciones R y S como el conjunto $S \circ R = \{(a,c) \in A \times C : (a,b) \in X \wedge (b,c) \in Y\}$. Con estas ideas podemos probar las propiedades que siguen

Propiedad 1. Si *R* es una relación de equivalencia de *A* en *A*, entonces R^{-1} también es de equivalencia.

Demostración. (i) Como *R* es de equivalencia, es en particular reflexiva. Así, aRa. De esto se deduce que $(a,a) \in R^{-1}$. Por ello, R^{-1} es reflexiva. (ii) Por ser *R* simétrica se cumple que $(a,b) \in R \Rightarrow (b,a) \in R$. Es decir, tanto (a,b) como (b,a) están en *R*. En consecuencia, (b,a) y (a,b) están en R^{-1}. Por lo que podemos afirmar que R^{-1} es simétrica. (iii) Si $(a,b) \in R^{-1}$ y $(b,c) \in R^{-1}$, entonces $(b,a),(c,b) \in R$, por definición de R^{-1}. Y como *R* es transitiva, se tiene que $(c,a) \in R$. Y por definición de R^{-1}, $(a,c) \in R^{-1}$. Concluimos entonces que R^{-1} es transitiva. Por i, ii y iii, R^{-1} es de equivalencia. Y la prueba está completa. ■

Propiedad 2. Sean *R* y *S* dos relaciones

1. $\left(R^{-1}\right)^{-1} = R$.
2. $(S \circ R)^{-1} = R^{-1} \circ S^{-1}$.

Prueba. Para probar la igualdad dada en (1) debemos ver que se verifica la doble inclusión entre $\left(R^{-1}\right)^{-1}$ y *R*, y esto se deduce de las equivalencias

$(a,b) \in R \Leftrightarrow (b,a) \in R^{-1} \Leftrightarrow (a,b) \in \left(R^{-1}\right)^{-1}$, por definición de *R*, de R^{-1} y de $\left(R^{-1}\right)^{-1}$.

Veamos ahora (2):

$(c,a) \in R^{-1} \circ S^{-1} \Leftrightarrow (c,b) \in S^{-1} \wedge (b,a) \in R^{-1} \Leftrightarrow (b,c) \in S \wedge (a,b) \in R \Leftrightarrow$
$(a,c) \in S \circ R \Leftrightarrow (c,a) \in R \circ S$ ¿Cuáles son los argumentos? Con esto se verifica la doble inclusión, y con ello la igualdad entre $(S \circ R)^{-1}$ y $R^{-1} \circ S^{-1}$. ■

Propiedad 3. Si *A* es un conjunto no vacío, *R* es una relación de equivalencia definida en *A* y $a \in A$, entonces $\bar{a} \neq \varnothing$. Por otra parte, aRb si y sólo si $\bar{a} = \bar{b}$.

El ejemplo que vimos sobre la congruencia módulo 3 en *Z* nos ilustra estos hechos. Observe que dado $x \in \mathbb{Z}$, entonces $x \in \bar{i}$, con $i = 1,2,3$; esto es, todo número entero pertenece a alguna clase. Además, si $i \neq j$, $\bar{i} \cap \bar{j} = \varnothing$; lo cual significa que las clases son disjuntas. Sigamos ahora su demostración para el caso general.

Demostración. Como *aRa*, por ser *R* reflexiva, entonces $a \in \bar{a}$. Así, $\bar{a} \neq \varnothing$. Ahora, como aRb, tenemos que $a \in \bar{b}$. Y se cumple que para todo *a** en $\bar{a}$, $a^* \in \bar{b}$, pues *R* es simétrica y transitiva. De ello se deriva que $\bar{a} \subset \bar{b}$ (i). De forma similar se prueba que $\bar{a} \supset \bar{b}$ (ii). De i y ii concluimos que $\bar{a} = \bar{b}$. Recíprocamente, si $\bar{a} = \bar{b}$ entonces $a \in \bar{b}$. Por tanto, *aRb*. Esto completa la prueba. ■

Con base en esto escribimos, refiriéndonos al ejemplo de la congruencia módulo 3, que $\cdots = \overline{-6} = \overline{-3} = \bar{0} = \bar{3} = \bar{6} = \bar{9} = \cdots$, $\cdots = \overline{-5} = \overline{-2} = \bar{1} = \bar{4} = \bar{7} = \cdots$, y $\cdots = \overline{-4} = \overline{-1} = \bar{2} = \bar{5} = \bar{8} = \cdots$.

Propiedad 4. Sean *A* y *R* como antes. Sean además, $\bar{a}$ y $\bar{b}$ dos clases de equivalencia en $\bar{a} \in A/R$. Entonces, se da sólo uno de los siguientes casos: $\bar{a} = \bar{b}$ ó $\bar{a} \cap \bar{b} = \varnothing$.

Demostración. (i) si suponemos que $\bar{a} = \bar{b}$ es claro que no se verifica que $\bar{a} \cap \bar{b} \neq \varnothing$. En este caso la prueba es inmediata. (ii) Ahora consideremos el caso en que $\bar{a} \neq \bar{b}$. Procedamos por reducción al absurdo, esto es, supongamos además que $\bar{a} \cap \bar{b} \neq \varnothing$. Así, las clases de equivalencia $\bar{a}$ y $\bar{b}$ comparten algún elemento en común. Sea *x* tal elemento. En consecuencia *xRa* y *xRb*. Y por la proposición 3, necesariamente debe cumplirse que $\bar{a} = \bar{b}$. ¡Pero esto último es absurdo! Éste proviene de suponer que $\bar{a} \cap \bar{b} \neq \varnothing$. En conclusión, si $\bar{a} \neq \bar{b}$ entonces $\bar{a} \cap \bar{b} = \varnothing$. Las partes i y ii nos muestran que los casos $\bar{a} = \bar{b}$ y $\bar{a} \cap \bar{b} = \varnothing$ no se dan al mismo tiempo. ■

Las propiedades 3 y 4 significan que toda relación de equivalencia definida en un conjunto no vacío *A*, induce una partición de éste en clases de equivalencia disjuntas. Y *A* se puede escribir como la unión de tales clases. Formalmente,

Definición. Una partición de un conjunto *A* es una colección $(A_i)_{i \in I}$ de subconjuntos de *A* tal que (i) $\bigcup_{i \in I} A_i = A$ y (ii) $A_i \cap A_j = \varnothing$ si $i \neq j$.

Luego, *una relación de equivalencia,* por nuestra proposición anterior, *induce una partición del conjunto en que se define*. La totalidad de los conjuntos involucrados en la partición se denomina el *espacio cociente.* Esta idea es de mucho valor en las matemáticas. Por ejemplo, la construcción que se hará del sistema de los números enteros $\mathbb{Z}$ tomará como base el conjunto cociente $\mathbb{N} \times \mathbb{N} / \sim$, para una relación de equivalencia $\sim$ que veremos más adelante (Módulo II). Una construcción similar amerita el sistema de los números racionales $\mathbb{Q}$. Y recíprocamente,

Propiedad 5. Una partición en *A* induce una relación de equivalencia en *A*.

Demostración. Consideremos una partición *P* en *A*. Así, $P = \left\{ \overline{x_i} : i \in I \right\}$ donde *I* es un conjunto de índices $I = \left\{ i : i = 1, 2, 3, ..., n \right\}$. Ahora definamos una relación *R* de manera que *aRb* si y sólo si $a, b \in \overline{x_i}$ para algún *i*. Observemos que (1) *R* es una relación en *A*

pues $R \subset A \times A$; fijémonos en que los pares $(a,b) \in A \times A$. Resta preguntarnos por las propiedades de *R*. (2) Si $a \in A = \cup \overline{x_i}$, entonces existe un entero positivo *i* de manera que $a \in \overline{x_i}$. Por tanto, $(a,a) \in R$. Esto es, *R* es reflexiva. Por otra parte, si $a,b \in \overline{x_i}$, para algún *i*, es claro que $b,a \in \overline{x_i}$, con lo cual si *aRb* entonces *bRa*. Así, *R* es simétrica. Finalmente, si *aRb* y *bRc*, se sigue que $\exists i, j \in I : a,b \in \overline{x_i} \wedge b,c \in \overline{x_j}$. Pero hemos probado que si dos clases no son disjuntas necesariamente son iguales (proposición 4); así $\overline{x_i} = \overline{x_j}$. En consecuencia *a, b* y *c* están en el mismo conjunto, y con ello es claro que *aRc*. ¡*R* es transitiva! Por todo lo visto en (2), *R* es de equivalencia. Y la prueba está completa. ■

Definición. Si una relación verifica las propiedades

Reflexiva
Antisimétrica
Transitiva, y
$\forall a,b \in A$ se verifica que *a* está relacionado con *b* ó *b* está relacionado con *a*

se dice de *orden total*. En cambio, si tal relación verifica las propiedades 1, 2 y 3, pero no necesariamente la 4, se le dice de *orden parcial*. Además, un conjunto dotado de una relación de orden, que suele denotarse con el símbolo $\leq$, se denomina conjunto ordenado (total o parcialmente, según sea el caso). En ocasiones particulares se usan otros símbolos para denotar una relación de orden.

Como advertirá, un orden parcial en un conjunto *A* no implica que todos los elementos de *A* sean comparables por medio de esa relación. Pongamos por caso la relación "*a* divide a *b*", que se denota con el símbolo $a|b$, en el conjunto de los números Enteros (recordemos que *a* divide a *b* si y sólo si $\exists x \in \mathbb{Z} : ax = b$, es decir, *a* es un factor de *b*). Como $a|b \wedge b|a \Rightarrow a = b$; y si $a|b \wedge b|c \Rightarrow a|c$ (el lector puede convencerse de todo esto), "*a* divide a *b*" es antisimétrica y transitiva (y de acuerdo con la propiedad

6 es también reflexiva). Así, "*a* divide a *b*" en $\mathbb{Z}$ es un *orden parcial*. Por tanto, podemos decir que $\mathbb{Z}$ está parcialmente ordenado por la relación $a|b$. Queremos enfatizar en que en un conjunto parcialmente ordenado no es necesario que todos sus elementos sean comparables por medio de tal relación. En nuestro ejemplo vemos que hay enteros que son comparables por medio de tal relación, como 7 y 49, 3 y 47811, 11 y 14641, etc., pero hay otros que no, como 9 y 10, 15 y 8, 9001 y 9973, 0 y 0, etc. El término parcial significa que pueden existir elementos en el conjunto que no sean comparables.

Por otra parte, la relación $\leq$ en $\mathbb{Z}$ hace que $\mathbb{Z}$ sea parcialmente ordenado, y como para cualesquiera enteros es posible decir que uno de ellos es menor o igual que el otro, esto es, todos los enteros son comparables, entonces $\leq$ es también un *orden total* en $\mathbb{Z}$. Y $\mathbb{Z}$ es totalmente ordenado por la relación $\leq$. Estos ejemplos también nos muestran que un conjunto ordenado totalmente lo es también parcialmente, pero el recíproco no es cierto. Como vimos $(\mathbb{Z}, |)$ es ordenado parcialmente y no totalmente. Este sería un contraejemplo de tal proposición.

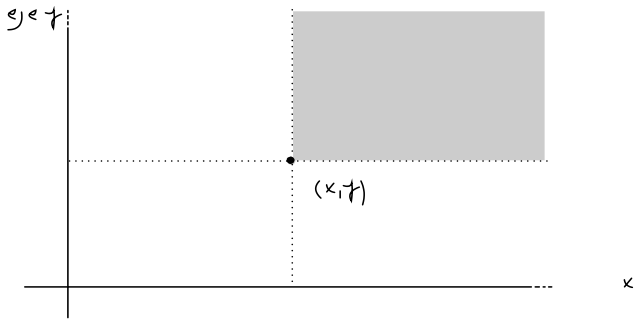
Para ilustrar de otra forma estas ideas, suponga que en una oficina de servicios de telefonía fija los usuarios hacen una única cola para cancelar su cuenta, allí podemos definir la relación "*a* está antes que *b* si *a* será atendido en la taquilla primero que *b*", con esto, todos los miembros distintos de la cola pueden compararse con excepción de un usuario consigo mismo (*a* no puede ser atendido antes de él mismo). En cambio, si en otra oficina, esta vez con dos taquillas de pago, los usuarios hicieran dos colas (una para cada taquilla), esta relación permite comparar a todos los miembros distintos de una misma cola, pero no a miembros de colas distintas. Observe que en este último caso, dados dos usuarios, uno en cada cola, no puede decirse a priori cuál de ellos será atendido primero en su taquilla, es muy probable que hayamos vivido esto en situaciones similares. La relación "*a* está antes que *b* si *a* será atendido en la taquilla primero que *b*", en ambos casos (con una y dos taquillas) no es de *orden parcial* ni de *orden total*.

1. La relación $\subset$ en $P(A)$ es un *orden parcial*. ¿Por qué no es un orden total? ¿Se cumple lo anterior en el caso $A=\varnothing$? ¿Qué otros ejemplos de relaciones de *orden parcial* y *orden total* puede dar?

2. Consideremos al conjunto de los pares de números reales y *R* una relación definida de la siguiente forma

$$(x,y)R(x^*,y^*) \Leftrightarrow x \le x^* \wedge y \le y^*$$

Dado el par (x,y) el gráfico que sigue ilustra los pares que están relacionados con éste



Puntos del Plano relacionados con (x,y) *por medio de R*

Ahora, ¿es *R* un *orden total*? Por ejemplo, ¿$(1,3)R\left(2,\sqrt{5}\right)$? Fijémonos en que $1 \le 2$, pero $3 \not\le \sqrt{5}$. Esto es, $(1,3)$ y $\left(2,\sqrt{5}\right)$ no son comparables por medio de tal relación. Así, no se verifica la propiedad 4 de la definición. De hecho, el lector advertirá que existen infinitos casos como este en el *Plano*. Es fácil ver que *R* es antisimétrica y transitiva (la propiedad 6 nos garantiza que *R* es también reflexiva), en efecto: si $(x,y)R(x^*,y^*) \wedge (x^*,y^*)R(x,y)$, entonces $x \le x^* \wedge y \le y^* \wedge x^* \le x \wedge y^* \le y$. En consecuencia, $x = x^* \wedge y = y^*$ ¿por qué? Dejamos al lector la prueba de la transitividad de *R*.

2.3 Elementos distinguidos en un conjunto ordenado

En un conjunto ordenado parcial o totalmente pueden existir ciertos elementos distinguidos. La definición que sigue los precisa. La identificación de estos elementos permite ampliar la descripción del conjunto ordenado *A*.

Definición. Si *A* es un conjunto ordenado por la relación $\leq$ y $X \subset A$. Se dice que:

1. $y \in A$ es una *cota superior* de *X* si para todo $x \in X$ se tiene que $x \leq y$
2. $y \in A$ es una *cota inferior* de *X* si para todo $x \in X$ se tiene que $y \leq x$. Si al menos una de tales cotas existe, se dice que *X* es un *conjunto acotado* (superior o inferiormente, según sea el caso).
3. Si *X* está acotado superior e inferiormente, se dice que *X* está *acotado*.

Si *X* está acotado (superior o inferiormente), entonces diremos que

4. *X* tiene *máximo* si existe una cota superior *y*, tal que $y \in X$
5. *X* tiene *mínimo* si existe una cota inferior *y*, tal que $y \in X$
6. *X* tiene *supremo* si $\exists s \in A$ que verifica las dos condiciones:
   s es una cota superior de *X*
   Si s^* es una cota superior de *X*, entonces $s \leq s^*$.
7. *X* tiene *ínfimo* si $\exists i \in A$ que verifica las dos condiciones:
   i es una cota inferior de *X*
   Si i^* es una cota inferior de *X*, entonces $i^* \leq i$.

   Al mínimo, máximo, ínfimo y supremo de un conjunto *X* se le denotan por *mín X*, *máx X*, *inf X* y *sup X* (respectivamente).

Una primera observación que haremos es la siguiente: si *X* está acotado inferiormente; sea *y* una cota inferior de *X*, entonces cualquier otro $y^* \leq y$ es también una cota

inferior de *X*. Una observación similar aplica para el caso de *X* acotado superiormente. Ahora, una forma de probar que un elemento *y* es una cota inferior de un conjunto *X* consiste en mostrar que ningún elemento $y^* \leq y$ está en *X*. También, las definiciones de mínimo y máximo se corresponden con las ideas de "menor" y "mayor" elemento del conjunto, respectivamente. Más aún, si tiene mínimo, éste es único. Si *m* y *m** son mínimos de *X*, entonces $m, m^* \in X$ y además, $m \leq m^*$ y $m^* \leq m$. Así, como $\leq$ es antisimétrica, *m=m**. Lo mismo sucede para el máximo de *X*.

La definición de ínfimo se asocia con la "mayor" de las cotas inferiores de *X*. Y el supremo con la "menor" de las cotas superiores de *X*.

Es inmediato que si un conjunto *X* tiene mínimo entonces tiene ínfimo, y además, *mín X = ínf X*. Veamos: si *X* tiene mínimo, entonces, *mín X* es una cota inferior de *X* (1). Con lo cual verifica que $mín\ X \leq x,\ \forall x \in X$. Y como $mín\ X \in X$, $x^* \leq mín\ X \leq x$ para cualquier otra cota inferior *x** (2). Por (1) y (2), *mín X* es ínfimo de *X*. Es decir, si el mínimo existe, el ínfimo también. Ahora, *¿mín X=inf X*?

$mínX \leq ínfX$, pues *mín X* es una cota inferior y el *ínf X* es el "mayor" de las cotas inferiores, además

$ínf\ X \leq mín\ X$, pues $mín\ X \in X$ y cualquier elemento de *X* es "mayor" que cualquiera de sus cotas inferiores.

Estas dos condiciones implican que *mín X=ínf X*. Con un razonamiento similar podemos probar que si *X* tiene máximo, entonces tiene supremo y *máx X=sup X*.

Un axioma importante, denominado *Axioma del Supremo* será expuesto en una semana posterior, justo cuando se construya el sistema de los números reales.

Propiedad 7. Sean *A* y *B* dos conjuntos de números reales. Consideremos a los conjuntos $A+B=\{x+y : x \in A \wedge y \in B\}$ y $A \cdot B=\{x \cdot y : x \in A \wedge y \in B\}$. Entonces,

a) $\sup(A+B)=\sup(A)+\sup(B)$

b) $\sup(A\cdot B)=\sup(A)\cdot\sup(B)$Con $\quad A,B\subset[0,\infty)$

Demostración. (1) Dado $j\in A+B$, $\exists x\in A,\exists y\in B: j=x+y$ (todo elemento de $A+B$ tiene la forma $x+y$). Como $x\le\sup A$ y $y\le\sup B$ entonces $x+y\le\sup A+\sup B$. Es decir, $\sup A+\sup B$ es una cota superior de $A+B$. Por tanto, por la definición de supremo, el supremo de $A+B$ debe verificar que $\sup(A+B)\le\sup A+\sup B$ (i).

Ahora veremos que $\sup A+\sup B\le\sup(A+B)$. En efecto, dados $x\in A, y\in B$, es claro que $x+y\le\sup(A+B)$, con lo cual $x\le\sup(A+B)-y$. Esto último equivale a decir que $\sup(A+B)-y$ es una cota superior de A para cualquier y en B. Entonces, $\sup A\le\sup(A+B)-y$. Además, $y\le\sup(A+B)-\sup A,\forall y\in B$ ¿por qué? Así, $\sup A+\sup B\le\sup(A+B)$ (ii). ■

(i) y (ii) implican la parte 1 de la propiedad. Dejamos 2 como un ejercicio para el lector.

1. En el conjunto $(-\infty,2]\subset\mathbb{R}$ no hay cotas inferiores ya que $\nexists y\in\mathbb{R}: y\le x$ con x en $(-\infty,2]$. Como no hay cotas inferiores entonces tampoco hay ínfimo ni mínimo (ambos, por definición, son cotas inferiores). Como $\forall x\in(-\infty,2]: x\le 2$, 2 es una cota superior de $(-\infty,2]$. Además, todo $y^*\in\mathbb{R}: 2\le y^*$, es también una cota superior. Es decir, todo elemento en $[2,+\infty)$ es cota superior de $(-\infty,2]$. Y como $(-\infty,2]\cap[2,+\infty)=\{2\}$, el 2 es máximo. Y *máx*$(-\infty,2]$=*sup*$(-\infty,2]$, por una propiedad probada.

2. $\mathbb{N}$ no es acotado superiormente, por tanto, no tiene supremo ni máximo. Su cota inferior (en $\mathbb{N}$) es el 0. Y como $0 \in \mathbb{N}$, 0 es mínimo y supremo.

a) ¿Cuál es el supremo y el ínfimo del conjunto siguiente?

$$S = \left\{ x \in \mathbb{R} : x = 2^{-p} + 3^{-q} - 5^{-r}, \textit{ donde } p,q,r \in \mathbb{Z}^{+} \right\}$$

b) ¿Es cierto que $\sup(A \cdot B) = \sup(A) \cdot \sup(B)$ para cualesquiera conjuntos de números reales *A* y *B*?

c) Sean $A, B \subset R$, supA=a y supB=b. Muestre que $\sup(A \cup B) = máx\{a,b\}$.

a) Sea $S = \{ y + z : y \in S^{*} \wedge z \in S^{**} \}$con

$S^{*} = \left\{ y \in \mathbb{R} : y = 2^{-p} + 3^{-q},\ p,q \in \mathbb{Z}^{+} \right\}$ y $S^{**} = \left\{ z \in \mathbb{R} : z = -5^{-r},\ r \in \mathbb{Z}^{+} \right\}$.

S* posee como supremo a $\frac{5}{6}$ ya que:

$2^{-1} > 2^{-2} > 2^{-3} > \cdots$ y $3^{-1} > 3^{-2} > 3^{-3} > \cdots$ esto es, $2^{-1} > 2^{-m}$ y $3^{-1} > 3^{-m}$, con $m \in Z^{+} - \{1\}$. Así, $2^{-1} > 2^{-p}$ y $3^{-1} > 3^{-q}$ (ambas sucesiones son decrecientes). Por tanto,

$2^{-1} + 3^{-1} = \frac{1}{2} + \frac{1}{3} = \frac{5}{6} \geq 2^{-p} + 3^{-q}$ (esta sucesión también es decreciente) y esto implica que $\frac{5}{6} \geq y, \forall y \in S^{*}$. Entonces, $\frac{5}{6}$ es cota superior de *S**.

Ahora, si $\frac{a}{b}$ es cota superior de *S** y $\frac{a}{b} < \frac{5}{6}$ se tiene que $\frac{a}{b} \geq 2^{-p} + 3^{-q} \Rightarrow \frac{a}{b} \geq \frac{5}{6}$ con *p*=*q*=1, pero $\frac{a}{b} < \frac{5}{6}$, he allí un absurdo. Entonces debe cumplirse que $\frac{a}{b} \geq \frac{5}{6}$. Luego, $\sup S^* = \frac{5}{6} = máx S^*$ ya que $\frac{5}{6} \in S^*$.

Y como *S*** posee como supremo al 0 ya que: $-5^{-r} = -\frac{1}{5^r} \in Q^- \Rightarrow 0 > -5^{-r} \Rightarrow$ 0 es cota superior de *S***. Ahora supongamos que $\exists a : a > -5^{-r}$ y *a*<0. Así, $a > -5^{-r} \Rightarrow a - a = 0 > -5^{-r} - a$. Lo cual es absurdo pues $-5^{-r} - a \in \mathbb{R}^+$. Entonces 0 es la menor de las cotas superiores de *S***. Con lo cual, 0=*supS***.

Y, apoyándonos en la propiedad antes probada, tenemos que $\sup S = \frac{5}{6} + 0 = \frac{5}{6}$.
Procedamos de forma similar para hallar el ínfimo de *S*.

El *ínfS**=0 ya que:

$2^{-p} + 3^{-q} = \frac{1}{2^p} + \frac{1}{3^q}$ donde $2^p, 3^q \in \mathbb{Z}^* \Rightarrow \frac{1}{2^p} + \frac{1}{3^q} \in \mathbb{Q}^+$. Entonces, $0 < 2^{-p} + 3^{-q}$; $p, q \in \mathbb{Z}^+$. En consecuencia, 0 es una cota inferior de *S**. Supongamos ahora que $\exists b \in \mathbb{R}^+ :$ *b* es cota inferior de *S**. En este caso, como la sucesión $2^{-p} + 3^{-q}$ es decreciente y 0 es una cota inferior de *S**, existen *p* y *q* en $\mathbb{Z}^+$ tales que $0 < 2^{-p} + 3^{-q} < b$, lo cual contradice en hecho de que *b* sea cota inferior de *S**. Así, podemos concluir que 0 es ínfimo de *S**.

Además, $ínf\ S^{**} = -\frac{1}{5}$ ya que:

$-\frac{1}{5} \leq -\frac{1}{5^r}, r \in \mathbb{Z}^+$ entonces $-\frac{1}{5}$ es una cota inferior de *S***. Observe que no existe otra cota inferior *a* de *S*** que verifique $a > -\frac{1}{5}$ (por lo visto antes).

Finalmente, $ínf\ S = ínf\ S^* + ínf\ S^{**} = 0 - \frac{1}{5} = -\frac{1}{5}$, de acuerdo con la propiedad 7.

(b) Tomemos $A=\{-1,0\}, B=\{-1,-2,-3,\cdots\}$ $A=\{-1,0\}, B=\{-1,-2,-3,\cdots\}$, el estudiante UNA debe indicar, completando los detalles, por qué esto es un contraejemplo de que

$$\sup(A\cdot B)=\sup(A)\cdot\sup(B)$$

Observe que en la propiedad 7 se hace la restricción $A,B\subset[0,1)$. Pero si ello no se cumple, un contraejemplo es: Sean $A=(-\infty,3)$ y $B=(-\infty,-5)$. Fíjese que *A* y *B* no son acotados inferiormente, sup*A*=3 y sup*B*=-5. Así, $A\cdot B=(-\infty,-\infty)=\mathbb{R}$; y no tiene supremo. Aunque basta con un contraejemplo, expongamos uno más a manera de ilustración:

Sean $A=(-2,-1)$ y $B=(0,1)$. En este caso, ambos conjuntos son acotados (superior e inferiormente). Entonces, sup*A*=-1, sup*B*=1, pero

$$\sup(A\cdot B)=(-2,0)=0\neq-1\cdot1=-1.$$

Un caso interesante en el que sí se cumple la propiedad sin que *A* y *B* sean parte de $\mathbb{R}^+$ es: $A=(-2,2)$ y $B=(-3,3)$. Aquí, sup*A*=2, sup*B*=3 y

$$\sup(A\cdot B)=(-6,6)=6=2\cdot3=\sup A\cdot\sup B.$$

Proponemos al lector encontrar otros casos similares.

(c) Supongamos, sin perder generalidad, que $a\geq b$. Entonces se verifica que $a\geq x,\forall x\in A$ y $b\geq y,\forall y\in B$. Y como $a\geq y$, *a* es cota superior de $A\cup B$ (1). Supongamos ahora que *a** es cota superior de $A\cup B$ y *c*<*a*. Lo anterior implica que $a^*\geq x\wedge a^*\geq y$. Pero como *a*=sup*A*, $\nexists m<a, m\in\mathbb{R}: m\geq x, x\in A$. He allí el absurdo. Por (1) y (2), $a=\sup(A\cup B)$. Así, podemos escribir

$$\sup(A\cup B)=a=máx\{a,b\}, \text{ pues } a\geq b.$$

Como problema propuesto al lector se encuentra una propiedad similar que vincula las ideas del ínfimo de la unión de dos conjuntos con el mínimo de sus ínfimos.

Veamos que si $a \equiv b(mód\ m)$ y , $c \equiv d(mód\ m)$ entonces

(i) $a+c \equiv b+d(mód\ m)$.

(ii) $ac \equiv bd(mód\ m)$.

Como $ac=(b+mx)(d+my)=bd+m(by+dx+mxy)$, donde $by+dx+mxy$ es un entero. Por tanto, $m \mid ac-bd$, lo que queríamos probar.

(iii) $-a \equiv -b(mód\ m)$.

Como $m \mid a-b$, $\exists x \in \mathbb{Z}: a-b=mx$. Ello implica que $a=b+mx$. Entonces, $(-1)a=(-1)(b+mx) \Leftrightarrow -a=-b+m(-x)$. Es decir, *–a* y *–b* son congruentes módulo *m*.

1. En efecto, como $m \mid a-b$ y $m \mid c-d$, $\exists x, y \in \mathbb{Z}: a-b=mx \wedge c-d=my$. Con esto podemos escribir que $a=b+mx \wedge c=d+my$.
2. *Así,* $a+c=b+d+(mx+my)=b+d+m(x+y)$, donde x+y está en $\mathbb{Z}$. Entonces, $m \mid (a+c)-(b+d)$. Es decir, $a+c \equiv b+d(mód\ m)$.
3. Como $ac=(b+mx)(d+my)=bd+m(by+dx+mxy)$, donde $by+dx+mxy$ es un entero. Por tanto, $m \mid ac-bd$, lo que queríamos probar.
4. Otra manera más elegante de hacer el problema es construir un **"puente"** de la siguiente manera, queremos ver que *m* divide a *ac-bd*, pero *ac-bd=ac-ad+ad-bd=a*(*c-d*)+*d*(*a-b*). Pero *m* divide a *c-d* y a *a-d*, de donde se tiene el resultado.

Criterios de simetría (en coordenadas polares). Dada una ecuación de *r* en términos de θ, que escribiremos $r = g(\theta)$, entonces

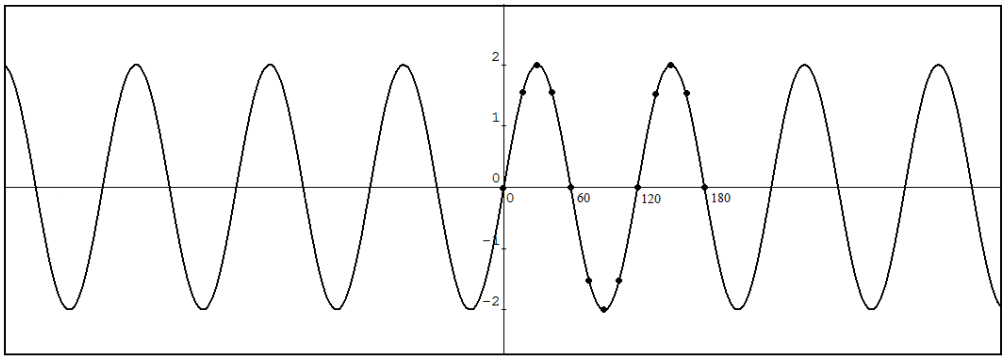
- La gráfica de *r* es simétrica con respecto al eje *x* si $r = g(\theta)$ y $r = g(-\theta)$ son ecuaciones equivalentes.
- La gráfica de r es simétrica con respecto al eje y si (i) $r = g(\theta)$ y $r = g(\pi - \theta)$ o (ii) $r = g(\theta)$ y $-r = g(-\theta)$ son ecuaciones equivalentes.
- La gráfica de r es simétrica con respecto al origen si (i) $r = g(\theta)$ y $-r = g(\theta)$ o (ii) $r = g(\theta)$ y $r = g(\pi + \theta)$ son ecuaciones equivalentes.

El problema que sigue ilustra una de estas ideas.

e. La rosa de tres pétalos. Tracemos la gráfica de $r = 2sen3\theta$. Veamos… Algunas soluciones de esta ecuación están en la tabla que sigue. Los valores de *r** son aproximados.

θ	0^0	15^0	30^0	45^0	60^0	75^0	90^0	120^0	135^0	150^0	180^0
*r**	0	1,41	2	1,41	0	-1,41	-2	0	1,41	2	0
r	0	$\sqrt{2}$	2	$\sqrt{2}$	0	$-\sqrt{2}$	-2	0	$\sqrt{2}$	2	0

Su gráfica, en un sistema rectangular es una *onda senoidal* con período $\frac{2\pi}{3}$.



Gráfica de $r = 2sen3\theta$ *(en el Plano Cartesiano)*

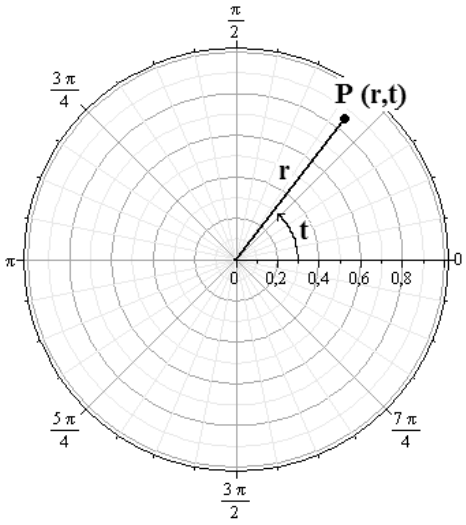
Ahora bien, una manera de aproximarse al gráfico de

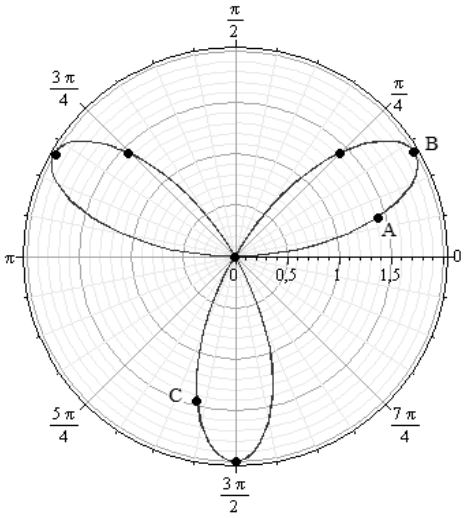
$$r = 2sen3\theta$$

en coordenadas polares es la que sigue. Recordemos que $P(r,\theta)$ representa al punto cuyo ángulo de inclinación con respecto al *eje polar* (justo el eje horizontal en el gráfico adjunto) es θ y su distancia hasta el *polo* (punto *O*) es *r*. Hemos representado los todos los puntos de la tabla. Observe que aquí los puntos $(0,0)$, $(0,60)$, $(0,120)$, etc. tienen la misma idea gráfica (contrario a lo que sucede en un sistema de coordenadas rectangulares). Aquí, por ejemplo, $A(\sqrt{2},15)$, $B(2,30)$, y $C(-\sqrt{2},75)$ (pues se conviene que –*r* se corresponde con medir $|r|$ unidades sobre el rayo de dirección opuesta).

También puede razonarse del modo que sigue. Si $0 \le \theta \le \frac{\pi}{6}$, entonces $0 \le sen3\theta \le 1$ y por tanto, $r = 2sen3\theta$ va de 0 a 2. Ahora, si $\frac{\pi}{6} \le \theta \le \frac{\pi}{3}$, tenemos que $0 \le sen3\theta \le 1$, con lo cual $r = 2sen3\theta$ va de 2 a 0. Esto es, la gráfica de $r = 2sen3\theta$ en el intervalo $0 \le \theta \le \frac{\pi}{3}$ es el lazo del primer cuadrante. Ahora, si $\frac{\pi}{3} \le \theta \le \frac{\pi}{2}$, *r* va de 0 a -2; gráficamente es la curva del tercer cuadrante. Y como $2sen3(\pi - \theta) = 2sen3\theta$, la curva es simétrica con respecto al eje *y*.

Como $-2 \le r = 2sen3\theta \le 2$, entonces, el conjunto solución de la ecuación dada está acotado (-2 y 2 son cotas inferior y superior, respectivamente). Y como -2 y 2 pertenecen al conjunto solución, -2 es mínimo y 2 es máximo.





Gráfica de $r = 2sen3\theta$ *(en coordenadas polares)*

1. Sea el conjunto $X = \{a, b\}$. ¿Cuántas relaciones binarias se pueden de finir en *X*? Exponga todas las relaciones de equivalencia y de orden que se pueden definir en *X*.

2. Exponga ejemplos, si ello es posible, de relaciones que

   (a) Sólo sean simétricas pero no transitivas.

   (b) Sea transitiva pero no simétrica ni reflexiva.

   (c) Sea antisimétrica y transitiva pero no reflexiva.

   (d) Simétricas y reflexivas pero no transitivas.

   (e) Simétricas y transitivas pero no reflexivas.

   (f) Antisimétricas, transitivas y reflexivas.

   En los casos en que sea imposible el ejemplo, si los hay, muestre por qué.

3. Sea $R : \mathbb{N} \to \mathbb{N}$ una relación definida por $R = \{(n, m) : n + 5m = 15; n, m \in \mathbb{N}\}$. (a) Escriba a *R* por extensión, (b) Determine R^{-1}.

4. Sea *R* una relación definida en el conjunto de los números reales definida por . $xRy \Leftrightarrow 0 < x - y < 2$ Construya una gráfica de *R* y de R^{-1}.

5. Sean el conjunto $A = \{i : 1 \leq i \leq 10, i \in \mathbb{N}\}$ y *R* la relación dada por *xRy* si y sólo si *x* es primo relativo con *y*.
   (a) Escriba a *R* por extensión.
   (b) Construya un gráfico coordenado de *R*.
   (c) ¿Qué propiedades tiene esta relación?

6. Considere las siguientes relaciones definidas en el conjunto de los números reales:
   (a) $R = \{(x, y) : x - y > 1\}$
   (b) $R = \{(x, y) : x^2 + y^2 \leq 25\}$
   (c) $R = \{(x, y) : x^2 - 4x + y^2 \leq 1\}$
   (d) $R = \{(x, y) : x^2 - y < 2\}$
   (e) $R = \{(x, y) : x - y^2 < 2\}$

   Construya sus gráficas en el plano cartesiano.

7. ¿Es la composición de relaciones conmutativa? De ser cierto, demuéstrelo. De lo contrario, muestre un contraejemplo.

8. ¿Es la composición de relaciones asociativa?

9. Considere a *S* una relación en el conjunto de los números reales definida por . $(a,b)R(c,d) \Leftrightarrow a \leq c \wedge b \leq d$ Pruebe que *R* es reflexiva, antisimétrica y transitiva.

10. Si *R* es una relación definida en un conjunto *A*
    (a) De manera que *R* es simétrica y transitiva, investigue si *R* es reflexiva.
    (b) De manera que *R* es antisimétrica, investigue si R^{-1} es antisimétrica.
    (c) ¿Es $R \cap R^{-1}$ de equivalencia?

(d) ¿Es $R \cap R^{-1}$ de orden?

11. Sea A un conjunto con $card(A) = n$. ¿Cuántas formas distintas hay de definir un orden en A?

12. Si A es un conjunto de siete elementos y definimos la relación R así: ^{xRy} si x tiene un poder de decisión en asamblea menor o igual al de y. Además si sabemos que en A hay dos elementos con igual poder de decisión y el resto tiene menor poder de decisión que éstos. Un gráfico de A es

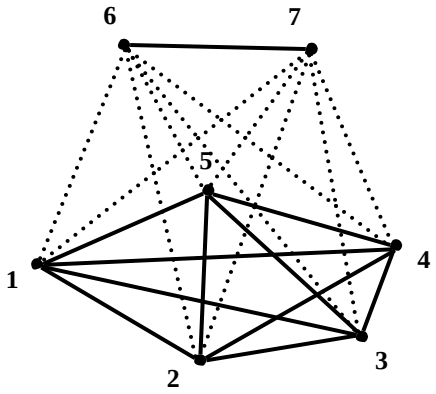


Gráfico de A

¿Qué propiedades tiene R? Si A es el conjunto de países de la ONU, con la misma relación de orden, su diagrama sería similar al anterior; 6 y 7 se comportarían como los cinco países miembros del consejo de seguridad. ¿Cómo debería ser el gráfico si todos los países de la ONU tuvieran el mismo poder de decisión, esto es, si su estructura fuese democrática?

13. Responda lo anterior en el caso

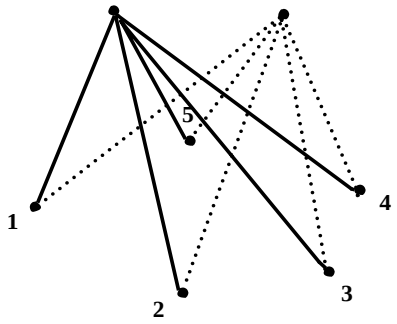


Gráfico de A

Aquí xRy si x tiene un poder de decisión en asamblea menor al de y.

14. Sean $A, B \subset \mathbb{R}$, $ínf A = a$ y $ínf B = b$. Muestre que $ínf\,(A \cup B) = mín\{a, b\}$

1. Tomemos el conjunto $X=\{a,b\}$ y formemos $X \times X = \{(a,a),(a,b),(b,a),(b,b)\}$ que tiene, como el estudiante UNA puede ver, 4 elementos. Cualquier relación binaria en X es un subconjunto de $X \times X = \{(a,a),(a,b),(b,a),(b,b)\}$ y sabemos, ver la primera unidad, que hay $2^4 = 16$ elementos en el conjunto de partes de $X \times X = \{(a,a),(a,b),(b,a),(b,b)\}$, luego tenemos precisamente 16 relaciones binarias. Para que una relación sea de equivalencia debe contener los elementos (a,a) y (b,b) ya que tiene que ser reflexiva, por otro lado si contiene al par (a,b) debe contener por simetría al par (b,a), eso permite afirmar que solamente hay dos relaciones de equivalencia en X que escribimos aquí

$$R_1 = \{(a,a),(b,b)\}$$

$$\cap$$

$$R_2 = \{(a,a),(b,b),(a,b),(b,a)\}$$

La relación R_1 puede ser interpretada como la relación de igualdad.

2.

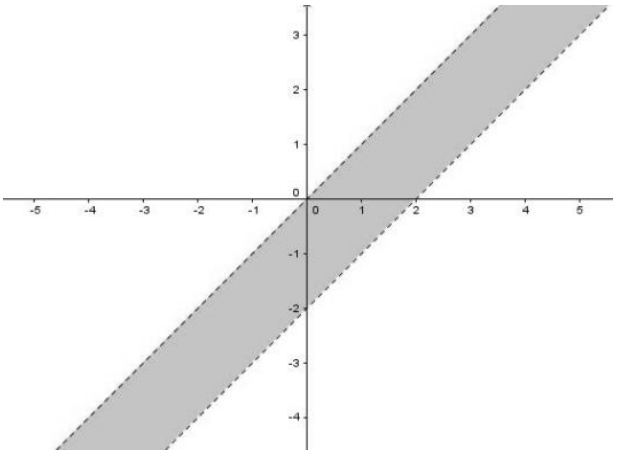
a) Una relación que es simétrica pero no transitiva es la relación $R=\{(a,b),(b,a)\}$ definida en el conjunto $A=\{a,b\}$. La relación no es transitiva ya que el par (a,a) no pertenece a R.

b) Sea $A=\{a,b,c\}$ y $R=\{(a,b),(b,c),(a,c)\}$, Claramente, R es transitiva pero no reflexiva ni simétrica.}

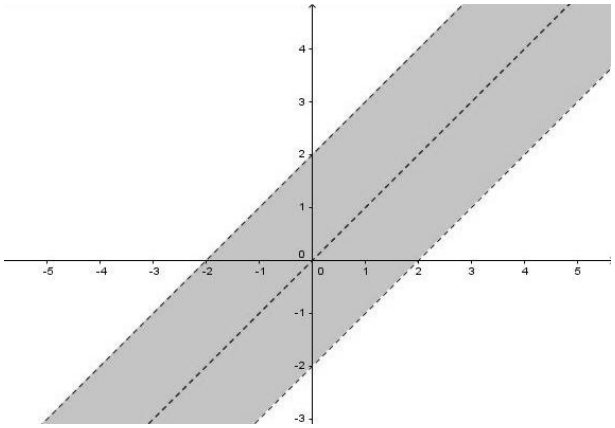
c) Sea $R=\{(a,b),(b,a),(a,a),(b,b)\}$ definida en $A=\{a,b,c\}$, explique en detalle porqué R constituye un ejemplo de lo que se requiere.

d) Consideremos $R=\{(a,b),(b,a),(a,a),(b,b),(b,c),(c,b),(c,c)\}$ definida en $A=\{a,b,c\}$.Vemos que R es simétrica y reflexiva pero no transitiva ya que el par (a,c) no está en R. ¿Es posible construir un ejemplo como el anterior si A sólo tiene dos elementos? El resto de las partes queda como ejercicio para el estudiante UNA.

3. La relación R está dada por todos los pares (x,y) que verifican las desigualdades $0<x-y<2$. Estas inecuaciones se resuelven de manera sencilla de forma gráfica de la siguiente manera, graficamos las rectas $0=x-y$ y $2=x-y$ y la región entre ellas es la solución de las inecuaciones



Para hallar la relación inversa reflejamos la zona sobre la recta $y=x$, con mayor precisión, tomamos una simetría de la zona respecto la recta $y=x$. Obtenemos,



Observe que una simetría respecto a la recta y=x lleva el punto (a,b) en el punto (b,a).

4. a) Sean el conjunto $A=\{i:1\le i\le 10, i\in\mathbb{N}\}$, podemos escribir A por extensión, $A=\{1,2,3,4,5,6,7,8,9,10\}$ y sea R la relación dada por xRy si y sólo si x es primo relativo con y, y $x<y$. Por ejemplo, todos los pares de la forma $(1,k)$, k desde 2 hasta 10 están en R. También los pares $(2,2j+1)$, con $j=1,2,3,4$ ¿porqué?. El estudiante UNA debe completar la lista de pares de la relación para poder escribir R por extensión.

   b) Queda como ejercicio para el estudiante UNA.

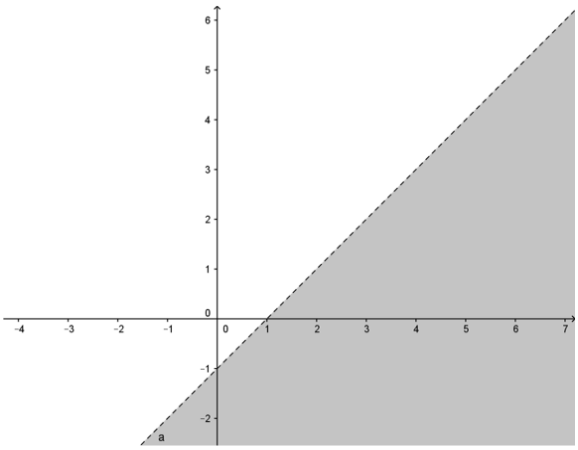
   c) Claramente R no es reflexiva ni simétrica. Tampoco es transitiva, ya que (2,3) y (3,4) están en R pero (2,4) no está.

5. Consideremos la relación $R=\{(x,y):x-y>1\}$

Para hallar los puntos del plano que cumplen la relación debemos resolver la inecuación $x-y>1$. Estas inecuaciones de dos variables se resuelven de la siguiente manera:

- Grafique Ud. la recta $x-y=1$, dicha recta divide al plano en dos semiplanos, uno de ellos va a ser la solución de la inecuación planteada.

- Tome un punto arbitrario en uno de los semiplanos, por ejemplo el (0,0) y vea si satisface o no la desigualdad, en nuestro caso 0-0>1, que es falsa, luego la solución es el semiplano que no contiene al origen de coordenadas. Veamos su gráfica hecha con Geogebra



6. Las funciones que conoce el estudiante UNA son un caso particular pero muy importante de relaciones. Tomemos las siguientes funciones $f(x)=x^2$ y $g(x)=\cos x$ definidas en el dominio de los números reales, veamos que $f\bullet g(x)=\left(\cos x\right)^2$, que son dos cosas completamente distintas, luego la composición de relaciones (o funciones) no es conmutativa $g\bullet f(x)=\cos(x^2)$

7. Es claro que no siempre una relación es asociativa, el estudiante UNA debe proporcionar un ejemplo.

8. Tenemos la relación

$$(a,b)R(c,d)\Leftrightarrow a\le c\wedge b\le d$$

Definida en puntos del plano, como

$$a\le a \text{ y } b\le b\Rightarrow (a,b)R(a,b)$$

Entonces la relación es reflexiva. Por otro lado si *a* es menor igual que *a'* y *a'* es menor o igual que *a* entonces *a=a'*, luego la relación es antisimétrica. Queda para el estudiante UNA verificar que la relación dada es simétrica.

9. a) Falso, el estudiante UNA debe dar un ejemplo.
   b) Cierto, de la prueba de este hecho.
   c) Falso, por ejemplo puede fallar la reflexividad, construya el contraejemplo.
   d) Falso, ¡proporcione un ejemplo!.

10. Hay $n!$ maneras. Para ver esto, vemos que hay n formas de tomar el menor elemento del conjunto, pero una vez fijado este hay n-1 maneras de tomar el elemento que sigue a este, y así sucesivamente. Luego hay un total de $n(n-1)(n-2)\cdots 3\cdot 2\cdot 1$ maneras, pero esto es precisamente $n!$.

11. Queda claro que el $\min\{a,b\}$ es una cota inferior de ya que a es una cota inferior de A y b es una cota inferior de B. Luego, por definición de ínfimo $\inf(A\cup B)\geq \min\{a,b\}$. Ahora bien, $\inf(A\cup B)$ es una cota inferir tanto de A como de B y por ende $\inf(A\cup B)$ debe ser menor que a y menor que b, luego $\inf(A\cup B)\leq \min\{a,b\}$ y luego se debe tener la igualdad como queríamos demostrar

2.6 Modelando con las relaciones

1. **ISBN.** El código ISBN (International Standard Book Number) para los libros hasta el 1-1-2007 tenía 10 dígitos. Los primeros nueve se asignaban atendiendo a categorías como la identificación general del grupo (país, área geográfica o lingüística), del editor, del título y un último dígito (de control) que se calculaba del modo que ilustraremos. Si el ISBN de un libro es, digamos

   99905-0-874-7

este último dígito es la solución de la congruencia

$$9\cdot 1+9\cdot 2+9\cdot 3+0\cdot 4+5\cdot 5+0\cdot 6+8\cdot 7+7\cdot 8+4\cdot 9\equiv a\ (\mathit{mód}\ 11)$$

Con esto tenemos

$$227 \equiv a \left(mód\ 11 \right)$$

es decir

$$11 \left| 227 - a \right.$$

Por tanto, $\exists y \in \mathbb{Z} :\ 11y = 227 - a$. Y como $0 \le a \le 10$ (pues esta relación induce una partición de $\mathbb{Z}$ en 11 clases de equivalencia), $0 \le 227 - 11y \le 10$. Así, para *y*=20 se verifica que $0 \le 227 - 11(20) \le 10$. Entonces, $a = 227 - 11(20) = 227 - 220 = 7$. Y 7 es el último dígito. Si la solución de esta ecuación inicial es *a*=10 se conviene en colocar la letra X como último dígito.

Luego del 1-1-2007 el código ISBN tiene 13 dígitos, se han incluido tres descriptores más, y el último dígito es de nuevo un número de control que se obtiene con la fórmula

$$a \equiv \sum_{i=1}^{6} \left(x_{2i-1} + 3x_{2i} \right) \left(mód\ 10 \right)$$

Tomemos por caso el código 978-99954-802-1-*a*. ¿Cuál es el número de control? Veamos…

$$\begin{aligned} \sum_{i=1}^{6} \left(x_{2i-1} + 3x_{2i} \right) &= \left(x_1 + 3x_2 \right) + \left(x_3 + 3x_4 \right) + \left(x_5 + 3x_6 \right) + \left(x_7 + 3x_8 \right) + \left(x_9 + 3x_{10} \right) + \left(x_{11} + 3x_{12} \right) \\ &= 9 + 3 \cdot 7 + 8 + 3 \cdot 9 + 9 + 3 \cdot 9 + 5 + 3 \cdot 4 + 8 + 3 \cdot 0 + 2 + 3 \cdot 1 \\ &= 131 \end{aligned}$$

con lo cual

$$a \equiv -131 \left(mód\ 10 \right)$$

es decir, $10 \left| a - \left(-131 \right) = a + 131 \right.$. Por tanto, $\exists y \in \mathbb{Z} :\ 10y = a + 131$. Pero como $0 \le 10y - 131 \le 9$, tomamos *y*=14. Así, $0 \le 10(14) - 131 \le 9$. Y $a = 140 - 131 = 9$.

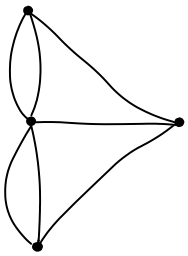
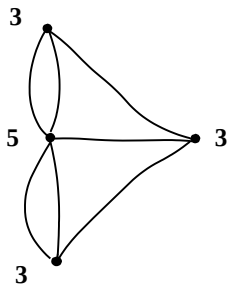
Siga este método para verificar el dígito de control en uno de sus libros.

2. **Fotografía.** Un ejemplo interesante del uso de las relaciones de equivalencia se encuentra en el procesamiento de imágenes fotográficas. Dada una fotografía, supongamos que en escala de grises, con una resolución de 1600x1200 píxeles (lo cual indica que la fotografía está dividida en una 1920000 píxeles o partes cuadradas –lo que frecuentemente se redondea diciendo que es de 2 mega píxeles), podemos definir una relación como la que sigue: "dos píxeles *a* y *b* están relacionados si son adyacentes y tienen el mismo nivel de gris". Es inmediato que tal relación es reflexiva, simétrica y transitiva, por tanto de equivalencia. Ciertos algoritmos, como los instalados en algunas cámaras para detectar sonrisas y accionar automáticamente la toma, pueden basarse en la detección de clases de equivalencia con color piel (en algún rango) y con una clase de equivalencia "en su interior" con color blanco (correspondiente a los dientes). La compresión de imágenes, cambios en su resolución, y algunos retoques (como la eliminación de algunas arrugas, "unificación" del color, etc.) también pueden basarse en la identificación de tales clases. Lo mismo sucede en un proceso tan común como el ajuste en la resolución de impresión de un documento cualquiera (incluyendo el texto) –allí estas clases juegan un papel importante.

La imagen ampliada corresponde a la pupila derecha. En ella pueden verse los píxeles y distinguirse algunas clases

3. **Los puentes de Königsberg.** Este problema histórico, que muestra los estrechos vínculos entre las matemáticas y la realidad, y al mismo tiempo su poder de generalización y abstracción, consiste en **encontrar un trayecto alrededor de siete puentes que cruce sólo una vez por cada uno de ellos** (hoy en día ya no existen todos estos, pues la ciudad fue parcialmente destruida durante de Segunda Guerra Mundial). Lo cual tiene que ver con introducir una relación de orden en el conjunto de los lugares a recorrer de esa manera tan peculiar. Euler publicó en 1736 una solución al caso general, problema que contribuyó de manera importante al nacimiento de la Topología. Euler consideró los cuatro lugares que se deseaba comunicar por medio del trayecto y los puentes entre ellos; a los primero los representó con puntos y a los segundos, con curvas. En el gráfico que sigue se muestra un mapa antiguo de la ciudad, una idea del problema, un diagrama, y el *orden* de cada uno de los vértices (también llamado *grado*). Este orden indica el número de puentes (o conexiones) entre los lugares.

   Euler dio una respuesta sencilla. El problema se asocia con la idea de dibujar un trayecto con lápiz sin levantar el lápiz del papel ni pasar por una conexión más de una vez. Al hacer el dibujo, en el caso de los vértices intermedios entraremos por una conexión y saldremos por otra (para así no recorrer la misma conexión dos veces). Entonces, el número de conexiones que convergen en cada vértice debe ser par, exceptuando posiblemente a los vértices inicial y final del dibujo. Esto significa que para que el problema tenga solución es necesario que el diagrama tenga a lo sumo dos vértices de orden impar. Pero en el problema de los puentes de Königsberg sus cuatro vértices tienen orden impar, lo que lo implica que no tenga solución (ver el diagrama que sigue).

			
mapa antiguo	*idea del problema*	*diagrama*	*orden vértices*

Además,

1. Un diagrama se puede recorrer sin pasar dos veces por una misma conexión si no tiene vértices de orden impar. En este caso se puede dibujar comenzando desde cualquiera de sus vértices (gráficos de Euler).
2. Si el diagrama tiene exactamente dos vértices de orden impar, entonces se puede dibujar (comenzando en uno de ellos).
3. Si un diagrama tiene cuatro o más vértices de orden impar, no se puede dibujar.

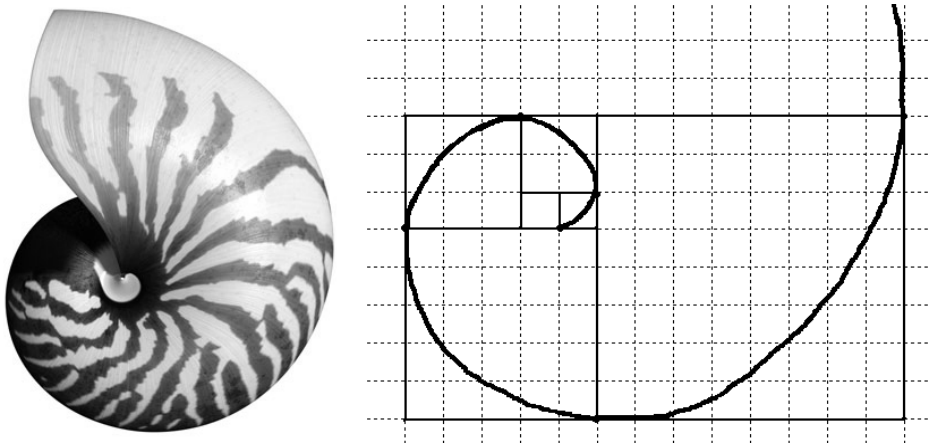
4. **El Nautilus.** La naturaleza nos ofrece múltiples relaciones matemáticas sorprendentes. Por ejemplo, si dividimos un segmento en dos partes de medidas *a* y *b*, de manera que se verifique que la razón entre la medida total *a*+*b* y *a* (la medida del segmento mayor) sea igual que la razón entre las partes:

$$\frac{a+b}{a}=\frac{a}{b}$$

Es decir, *a* está relacionado con *b*, si y sólo si, $\frac{a+b}{a}=\frac{a}{b}$. Ese número se conoce como el *número de oro*, y se conviene en denotarlo con la letra griega φ (se lee *Phi*).

$$\varphi \approx 1,6180339$$

Ahora, podemos construir una serie de rectángulos que en cada paso de la iteración que haremos se aproximará más a φ. Veamos… (i) comenzamos representando un cuadrado con lado de medida 1, (ii) sobre uno de sus lados representamos otro cuadrado, (iii) sobre el segmento de medida 2 disponemos otro cuadrado, (iv) sobre el segmento de medida 3 disponemos otro cuadrado, y así sucesivamente. Observe que se van obteniendo cuadrados cuyos lados miden 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, … ¡Justo la famosísima *sucesión de Fibonacci*! Finalmente, trazamos la espiral que toca los vértices que se indican en la figura adjunta. Esta espiral, denominada *espiral de Fibonacci*, se similar a la espiral de las conchas de Nautilus (un tipo de caracol). Entre sus propiedades se encuentran que su forma y proporciones no se alteran aún cuando aumente de tamaño.



Nautilus y espiral de Fibonacci

Ahora al dividir términos consecutivos de la sucesión de Fibonacci obtenemos

$$\frac{1}{1} = 1$$
$$\frac{2}{1} = 2$$
$$\frac{3}{2} = 1,5$$
$$\frac{5}{3} \approx 1,66$$
$$\frac{8}{5} = 1,6$$
$$\frac{13}{8} = 1,625$$
$$\frac{21}{13} \approx 1,615384$$

$$\tfrac{34}{21} \approx 1,619047$$
$$\tfrac{55}{34} \approx 1,617647$$
$$\ldots$$

Fijémonos en que estos cocientes se aproximan a φ por defecto y por exceso, alternadamente. Puede comprobarse que el valor exacto del número de oro es

$$\varphi = \frac{1+\sqrt{5}}{2}$$

Supongamos que $a+b=1$, entonces $\frac{1}{a} = \frac{a}{1-a}$. Así, $1-a = a^2 \Rightarrow a^2 + a - 1 = 0$, cuya solución positiva es $a = \frac{-1+\sqrt{5}}{2}$. Ahora veamos la relación entre la medida de los dos segmentos:

$$\frac{a}{1-a} = \frac{\frac{-1+\sqrt{5}}{2}}{\frac{3-\sqrt{5}}{2}} = \frac{1+\sqrt{5}}{2} \approx 1,61803$$ ¡Justo el número de oro!

Algunas notas

Buen orden

Ernst Zermelo(1871-1953), matemático alemán, probó en 1908 que **en cualquier conjunto no vacío se puede definir una relación de manera que ésta sea un buen orden**. Enunciado que es conocido como el *Principio del Buen Orden*. El mismo Zermelo probó que tal principio es equivalente al denominado *Axioma de Elección*. Dicho axioma es necesario para poder definir con propiedad el concepto de cardinal, sin embargo eso esca al alcance de nuestro texto. Contribuyó en la axiomatización de la Teoría de Conjuntos, construyendo la axiomática más usada para la misma.

La experimentación y la inferencia

Gauss realizó muchos cálculos que empleó como base para formular conjeturas y pruebas en la Teoría de Números, Probabilidades, Geometría, Astronomía... Justo una muestra de la importancia de la experimentación en la construcción de ideas matemáticas. Por ejemplo, ¡elaboró tablas con los números primos comprendidos entre 1 y 3000000! Hoy en día, **la experimentación (con o sin el uso de computadoras) y las conjeturas siguen siendo parte medular de la actividad matemática**.

1. Dé otros ejemplos de relaciones de orden y de equivalencia y compruebe sus propiedades.
2. Consideremos el conjunto $\mathbb{N}^*$ de los números naturales sin el 0. Definimos en $\mathbb{N}^*$ la relación siguiente: *a* está relacionado con *b* al verificarse $\frac{a}{b+2}=\frac{b}{a+2}$, ¿qué propiedades tiene esta relación?
3. Ordene por medio de la relación de inclusión el conjunto de las partes de $A=\{a,b,c\}$. Haga un diagrama de esta relación.
4. Consideremos los datos

América Latina	22%
Asia del Sur	21%
Pakistán	29%
India	19%
Asia del Este + Pacífico	13%

Irlanda	979%
España	169%
Portugal	233%
Grecia	168%
Alemania	148%
Estados Unidos	100%
Gran Bretaña	400%

Deuda total externa (suma de las deudas pública y privada) en % del PIB en 2009 *(Fuente: Toussaint, Crisis global y alternativas desde la perspectiva del sur, 2011, p. 41).*

Clasifique esta relación.

5. ¿Puede una relación ser no reflexiva y simétrica?
6. ¿Hay algún caso de una relación tanto de equivalencia como de orden?
7. Pruebe que la *congruencia módulo n* es una relación de equivalencia –ver el problema 2.4 (d).
8. Exponga la partición de $\mathbb{Z}$ por medio de la relación de congruencia módulo 6.
9. Pruebe la parte dos de la propiedad 7.
10. Pruebe que una relación dada en *A* es simétrica si y sólo si es igual a su inversa.
11. Encuentre el supremo, ínfimo, máximo y mínimo (si existen) de los conjuntos siguientes:

    $\mathbb{Q}$.

    $(a,b]$ donde *a* y *b* son números reales y $a<b$.

$A = \left\{ (-1)^n : n \in \mathbb{Z}^+ \right\}$.

$B = \left\{ \frac{1}{n} : n \in \mathbb{Z}^+ \right\}$.

$A + B$.

12. Construya un gráfico en $\mathbb{R}^2$ de una relación simétrica.

13. Hay un insecto en cada uno de los vértices de un triángulo equilátero. Etiquetemos los insectos con las letras *A, B* y *C*. Los insectos comienzan a moverse al mismo tiempo y con velocidad constante con el siguiente criterio: *A* va hacia *B, B* va hacia *C* y *C* va hacia *A*. Construya un gráfico que ilustre la trayectoria de los tres insectos.

14. Construya el gráfico de $r = \theta$ (en coordenadas polares). ¿Alcanza *r* mínimo o máximo? Si es así, expóngalos.

15. Repita la actividad anterior pero considerando las relaciones

$r = 1 + \cos\theta$ (cardioide)
$r = e^{2\theta}$ (espiral logarítmica)
$r = a\theta,\ r \geq 0$ (espiral de Arquímedes)
$r^2 = a^2 \cos 2\theta$ (lemniscata de Bernoulli)

1. Los números naturales tienen un orden $\lhd\ \lhd$ muy importante que pasamos a describir.

$$1 \lhd 2 \lhd 4 \lhd 6 \cdots \lhd 3 \lhd 9 \lhd 15 \lhd \cdots 5 \lhd 25 \cdots$$

Es decir, ordenamos los pares primero y luego le siguen los múltiplos de 3 que no son pares y a estos siguen los múltiplos de 5 que no son ni pares ni múltiplos de 3, etc, etc. Es claro, que esto es una relación de orden ya que los primos están bien ordenados.

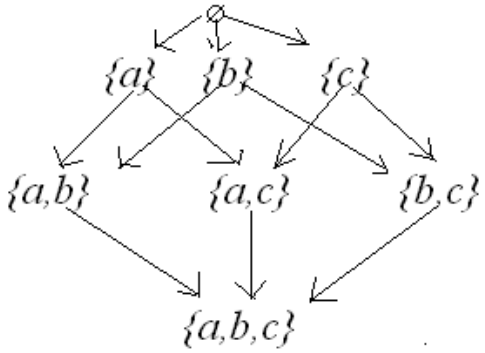
Consideremos ahora en el plano cartesiano el conjunto *L* de todas las rectas. Para dos rectas T,W en *L* decimos que T *R* W si y sólo si T es paralela a W o que T y W tienen la misma dirección(se considera que una recta es paralela a si misma). Esta relación *R* es reflexiva, dejamos al estudiante UNA completar los detalles. Piense en otras relaciones de orden y de equivalencia, discuta las misma con su asesor y compañeros.

2. Tomemos la relación

$$\frac{a}{b+2}=\frac{b}{a+2}$$

definida en los naturales, esta relación es claramente simétrica ya que si el par (a,b) pertenece a la misma entonces el par (b,a) se encuentra en la misma. Veamos que también es reflexiva, si $a=b$ entonces $\frac{a}{b+2}=\frac{b}{a+2}$ como el estudiante UNA debe ver. Dejamos al estudiante UNA verificar si la relación es o no transitiva.

3. Las flechas indican inclusión



4. Lo dejamos al estudiante UNA.
5. La respuesta es sí, considere el conjunto $\{a,b\}$ y la relación $R=\{(a,b),(b,a)\}$, dicha relación es simétrica pero no reflexiva.
6. Lo dejamos al estudiante UNA.

7. Lo dejamos al estudiante UNA.

8. Las clases son

$$\overline{0} = \{\cdots, -12, -6, 0, 6, 12, \cdots\}$$
$$\overline{1} = \{\cdots, -11, -5, 1, 7, 13, \cdots\}$$
$$\overline{2} = \{\cdots, -10, -4, 2, 8, 14, \cdots\}$$
$$\overline{3} = \{\cdots, -9, -3, 3, 9, 15, \cdots\}$$
$$\overline{4} = \{\cdots, -8, -2, 4, 10, 16, \cdots\}$$
$$\overline{5} = \{\cdots, -7, -1, 5, 11, 17, \cdots\}$$

9. Una relación R es simétrica si y sólo si (a,b) está en R entonces (b, a) está en R pero si (a,b) está en R si y sólo si (b, a) está en R^{-1}, luego las dos condiciones son equivalentes, $R = R^{-1}$equivale a que R es simétrica.

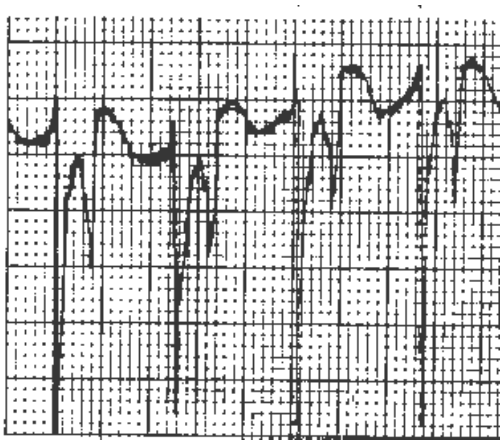
10. Encuentre el supremo, ínfimo, máximo y mínimo (si existen) de los conjuntos siguientes:

- $\mathbb{Q}$; no es acotado ni superiormente ni inferiormente luego no tiene ni máximo ni mínimo, ni supremo ni ínfimo.
- $(a,b]$ donde a y b son números reales y $a<b$; Tiene máximo igual a b que también es el supremo, no tiene mínimo ¿porqué? Su ínfimo es a.
- $A = \left\{(-1)^n : n \in \mathbb{Z}^+\right\}$ Máximo =1, mínimo=-1.
- $B = \left\{\frac{1}{n} : n \in \mathbb{Z}^+\right\}$. Tiene ínfimo pero no mínimo, ¿cuál es el ínfimo?. El máximo es 1.
- $A+B$ se deja al estudiante UNA.

11. Cualquier gráfica o región del plano que sea simétrica respecto a la recta $y=x$ sirve. Construya varios ejemplos.

12. Lo dejamos al estudiante UNA.

UNIDAD 3
Funciones



Una sección de un electrocardiograma

Semana 3

Aplicar el concepto de función en la resolución de problemas, en el modelado matemático y en la demostración de nuevos resultados.

Contenidos a tratar: Funciones. Sobreyectividad e inyectividad, biyectividad. Igualdad y composición o producto de funciones. Propiedades básicas. Gráficas. Aplicaciones.

3.1 Introducción

1. **(el Carbono 14).** Un problema central en la arqueología, biología y geología, así como en muchas otras ciencias, es la datación (ubicación de una fecha o período al que corresponde una muestra dada). Uno de los métodos, aunque

controversial por las premisas en que se apoya, está basado en el Carbono 14 (C^{14}). Éste es un elemento muy común en la atmósfera, en la tierra, el agua y en los seres vivos; es un isótopo radiactivo, de carácter inestable (se descompone a Nitrógeno-14), lo cual implica que *su proporción en una muestra cualquiera varíe al trascurrir el tiempo.* Se estima que el C^{14} tiene una *vida media* de 5730 años (la cual es una de las *premisas* base de este método. Otra de las premisas consiste en suponer que la proporción de C^{12} y C^{14} en la atmósfera ha sido constante hasta la fecha actual). Es decir, la mitad de una muestra de C^{14} tarda 5730 en descomponerse. (La mitad de la mitad que quedó tarda otros 5730 años, y así sucesivamente).

Vida media (en años) del C^{14}

Pongamos por caso una muestra (digamos de un hueso) en la que hay un 72% de C^{14}. La regla

$$t = 5730 \cdot \frac{\ln p}{\ln 2}$$

con p la proporción de C^{14} en la muestra dada, nos da un aproximado de la "edad" de la muestra. A saber,

$$t = 5730 \cdot \frac{\ln 0,72}{\ln 2} \approx 2715,6 \text{ años.}$$

Así, en los casos donde este método es el recomendado, el problema se reduce a calcular la proporción de C^{14} en la muestra. La regla dada es un ejemplo de función en la que *p* toma valores entre 0 y 1, sin incluir los extremos (por qué).

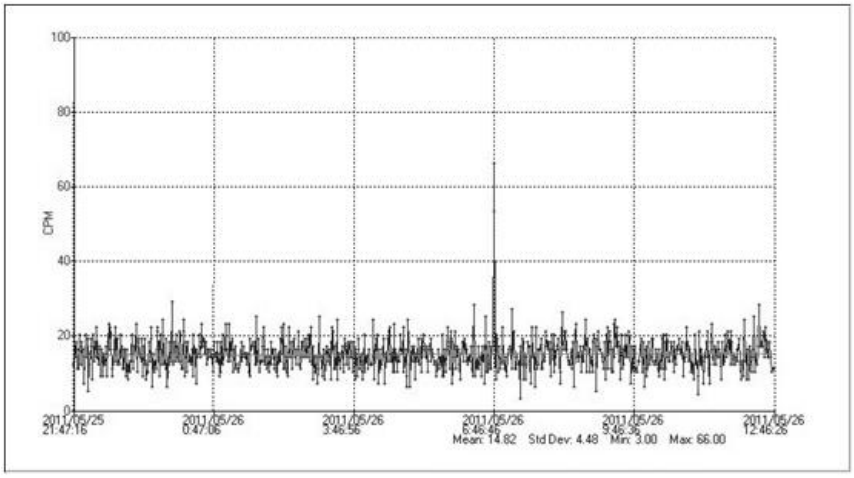
2. **(radiación – desastre nuclear en Japón).** El gráfico que sigue muestra la radiación en Hino (Tokio, Japón) entre el 25-5-2011 y el 26-5-2011. El máximo que alcanza la curva (66 CPM) es entre 4 y 5 veces la radiación media en este punto para meses anteriores al Terremoto de marzo de 2011. Un CPM es un conteo de sonido por minuto medido con un *contador Geiger* (detector de partículas de alta energía y de radiaciones ionizantes: como las generadas por la desintegración radiactiva, la radiación cósmica, las que se dan en un generador de partículas o en un generador de rayos X, con las ondas de radio, entre muchas otras). Además la *relación*:

   100 CPM = 1 uSV (un micro *Sievert* por hora)

   permite expresar estos valores en el sistema internacional de medidas.

La curva dada representa la medida de la radiación en CPM en términos del tiempo. Así, suele decirse (en este caso) que la medida de la radiación está en función del tiempo.

El estudio de funciones como esta da información importante sobre temas que van más allá de las matemáticas (alcanzando lo social y ético).



Radiación (medida en CPM) en Hino (Tokio, Japón) para el 25/26-5-2011

3. **(las cuotas balón)** Ciertos tipos de créditos, ya ilegales en nuestro país, incluían entre las cláusulas, aparte del pago de cierta cantidad por cierto número de cuotas a un interés dado, una cuota última (también denominada "especial"); en ésta se reunía parte del capital no pagado y los intereses dejados de pagar en correspondencia con las variaciones de la tasa de interés durante la vida del crédito. Lo cual se traducía en montos totales que fácilmente duplicaban la suma del préstamo. En este tipo de decisiones las matemáticas tienen un rol destacado.
4. **(distancia entre dos puntos en el Plano).** Como sabemos, si $A=(a_1,b_1)$ y $B=(a_2,b_2)$ representan a dos puntos del Plano, la distancia entre ellos está dada por la regla (la cual asocia a un par de puntos del Plano un número real no negativo):

$$d(A,B)=\sqrt{(b_1-a_1)^2+(b_2-a_2)^2}\,.$$

donde $d: R\times R\to \mathbb{R}^+\cup\{0\}$.

3.2 La noción de Función

Definición. Consideremos a A y B conjuntos no vacíos. Una *función o aplicación* de un conjunto A en un conjunto B es un subconjunto f de $A\times B$ de manera que para cada $a\in A$ existe un único $b\in B$, tal que $(a,b)\in A\times B$.

Los conjuntos A y B se denominan, respectivamente, *conjuntos de partida* (dominio) y *conjunto de llegada* (codominio), y decimos que f va de A en B. Observe que así, *una función es en sí misma una relación.* Y basados en la discusión de la semana anterior, no toda relación es una función -¿qué ejemplos puede dar el lector?

La anterior es la definición formal de función, sin embargo, es muy usual describir una función *f*, indicando sus conjuntos de partida y llegada, así como una regla que haga corresponder a cada elemento de A un único elemento de B.

$$f : A \to B$$
$$x \in A \to f(x) \in B$$

Si $(a,b)\in A\times B$ decimos que *b* es *imagen* de *a*. De forma equivalente, si seguimos la segunda caracterización que comentamos, escribimos que $f(a)=b$, lo cual se lee "*f* de *a* es igual a *b*"; representando con ello que *b* es imagen de *a*. Al conjunto $f(A)=\{f(x): x\in A\}\subset B$ se le llama *imagen directa de A por f (o a través de f).*

Una observación más. Sería un error pensar que la propiedad 2 que probamos en la semana previa se cumple también en el caso de las funciones. De hecho, dada una función *f* no siempre existe su inversa; más aún, dadas dos funciones *f* y *g* no siempre existe su composición. Las dos últimas definiciones que siguen precisan estas ideas.

La primera se refiere a dos tipos especiales de función, las cuales revisten importancia en todas las matemáticas.

Definición. Una función *f* de *A* en *B* es *sobreyectiva* si $\forall b \in B, \exists a \in A: \ f(a) = b$. Esto es, todo elemento de *B* es imagen de algún elemento de *A*. Por otra parte, *f* es *inyectiva* si dados $a, a^* \in A$, con $a \neq a^*$, entonces $f(a) \neq f(a^*)$. Es decir, a elementos del dominio distintos le corresponden imágenes distintas.

1. Consideremos la función *f* de los números reales en los números reales definida por medio de $f(x) = x^3$. Veamos que *f* es sobreyectiva, sea $y \in \mathbb{R}$ queremos encontrar un *x* en los reales tal que $f(x) = x^3 = y \Rightarrow x = \sqrt[3]{y}$ y recordamos que siempre podemos extraer la raíz cúbica ne un real cualquiera. Esto demuestra que *f* es sobreyectiva.
2. Consideremos el conjunto $A=\{1,2,3\}$ y definimos $f: A \to A$ por medio de dar las imágenes de los elementos de *A*, en este caso *f* queda determinada por medio de $f(1) = 2, f(2) = 1, f(3) = 3$. El estudiante UNA debe indicar si *f* es inyectiva y sobreyectiva. La función dada es un ejemplo de lo que se denomina una permutación de los elementos 1,2 y 3, volveremos a ella en la Unidad de Grupos.
3. Cada venezolano mayor de 12 años debe tener un número de cedula identidad. Defina una función indicando su dominio y codominio que modele esta situación. Diga si la función es o no inyectiva.

La siguiente definición es muy importante en matemáticas. *Una función que es, simultáneamente, inyectiva y sobreyectiva se denomina biyectiva.*

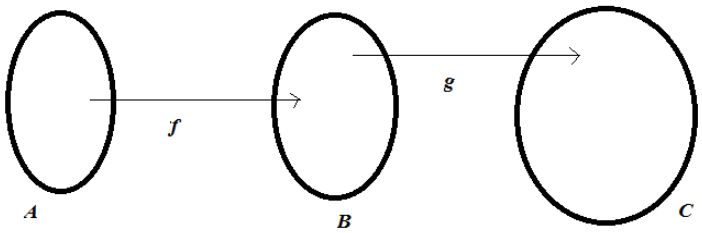
Nuevamente debemos acotar, como ya debe ser claro para el lector, que una función no tiene por qué ser inyectiva o sobreyectiva.

 En este punto pedimos al lector que aporte ejemplos de funciones no inyectivas y no sobreyectivas.

Definición. Dos funciones f y g definidas de A en B son iguales si $f(a) \neq g(a), \forall a \in A$.

Definición. Dadas dos funciones *f* y *g*, tales que $f : A \to B$ y $g : B \to C$. Entonces la composición o producto de f y g es la función $g \cdot f : A \to C$ dada por $g \cdot f(a) = g(f(a))$.

 Aquí el orden de composición es importante. La imagen de *a* por medio de $g \cdot f$ se obtiene calculando primero la imagen de *a* por medio de *f* y luego la imagen de esta última a través de *g*. Tampoco tiene sentido hacer la composición en el otro orden ya que es importante que el codominio de *f* coincide con el dominio de *g*. Esta será nuestra convención; en otros textos siguen un orden contrario. El lector debe estar atento a tales convenciones.



Composición de funciones

Considere las funciones *f,g* de $\mathbb{R}$ en $\mathbb{R}$ definidas por $f(x)=\cos x$ y $g(x)=x^2$, tenemos que $f\cdot g(x)=\cos x^2$ pero $g\cdot f(x)=\left(\cos x\right)^2$ que son completamente distintos. Observe que en este caso se pueden realizar ambas composiciones.

Definición. Si $f:A\to B$ es una función y $M\subset B$. Entonces la *imagen recíproca* de de *M* por *f* (o a través de *f*) es el conjunto $f^{-1}(M)=\{a:a\in A,\ f(a)\in B\}$. Se suele denotar con este mismo símbolo, f^{-1}, a la *función inversa* de *f*. Esto es, si $f:A\to B$ es inyectiva, se define la función inversa de *f*, $f^{-1}:f(A)\to A$, de manera que

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

Es decir, f^{-1} asocia cada elemento de $f(A)$ con un único elemento de *A*. Así, usaremos el mismo símbolo para la *imagen recíproca de un conjunto* y para la *función inversa de una función inyectiva*.

Los lectores deben estar atentos a sus distintos significados entre la función inversa y la imagen inversa de un conjunto, son completamente distintos. El siguiente ejemplo aclara la situación.

1. Consideremos la función *g* definida por medio de $g:\mathbb{R}\to\mathbb{R}, g(x)=x^2$. El estudiante UNA debe explicar porqué la función *g* no es inyectiva y luego no

tiene función inversa. Sin embargo, para cualquier subconjunto *A* de los números reales se puede calcular $g^{-1}(A)$.

2. En bachillerato trabajamos con dos funciones importantes: $\ln x, e^x$ la función logaritmo y la función exponencial, desde un punto de vista matemático se debe aclarar cual es el dominio y codominio de cada una de ellas ya que definir una función no es dar una fórmula. Luego, $\ln x : \mathbb{R}_*^+ \to \mathbb{R}$ y $e^x : \mathbb{R} \to \mathbb{R}_*^+$. Observe que la composición es posible en cualquier orden y que se obtiene la importante relación $e^{\ln x} = \ln(e^x) = x$. Es decir las funciones son inversas la una de la otra.

1. Sabemos que dadas $f : A \to B$ y $g : B \to C$ entonces la composición o producto de *f* y *g* es la función $g \cdot f : A \to C$ dada por $g \cdot f(a) = g(f(a))$. Demuestre que si *f,g* son sobreyectivas entonces también lo es $g \cdot f : A \to C$.
2. Sabemos que dadas $f : A \to B$ y $g : B \to C$ entonces la composición o producto de *f* y *g* es la función $g \cdot f : A \to C$ dada por $g \cdot f(a) = g(f(a))$. Demuestre que si *f,g* son inyectivas entonces también lo es $g \cdot f : A \to C$.
3. Combine las actividades anteriores para obtener el importante resultado que usaremos en la Unidad de grupos:

Dadas $f : A \to B$ y $g : B \to C$ entonces la composición o producto de *f* y *g* es la función $g \cdot f : A \to C$ dada por $g \cdot f(a) = g(f(a))$. Demuestre que si *f,g* son sbiyectivas entonces también lo es $g \cdot f : A \to C$.

1. Tomemos un *c* en el conjunto *C*, como *g* es sobreyectiva existe un *b* en el conjunto *B* tal que *g*(*b*)=*c*. Por otro lado, *f* es sobreyectiva luego existe un *a* en el conjunto *A* tal que *f*(*a*)=*b*, de donde *c*=*g*(*b*)=*g*(*f*(*a*)), lo que implica la sobreyectividad de $g \cdot f : A \to C$.
2. Supongamos que tomamos *a,a'* elementos distintos de *A*, entonces *f*(*a*) es distinto de *f*(*a'*) por ser *f* inyectiva. Luego, *g*(*f*(*a*)) es distinto de *g*(*f*(*a'*)) por ser *g* inyectiva y esto implica la inyectividad de la función compuesta.
3. Se deja al lector, debe combinar lo hecho en **1.** y **2.**

(función parte entera). Sabemos que dado un número real *x*, existen enteros *n* y *n*+1 tales que $n \le x \le n+1$. Definamos entonces $f : \mathbb{R} \to \mathbb{R}$ con la regla $f(x) = n$ si $n \le x < n+1$. Explique si la función es inyectiva. ¿Cuál es la gráfica de *f*? Observe que, por ejemplo, si *x*=1,618, entonces $1 \le x < 2$, así $f(x) = 1$. Más aún, si $1 \le x < 2$, $f(x) = 1$. En este intervalo, *f* es constante y su representación es un segmento. Por tanto,

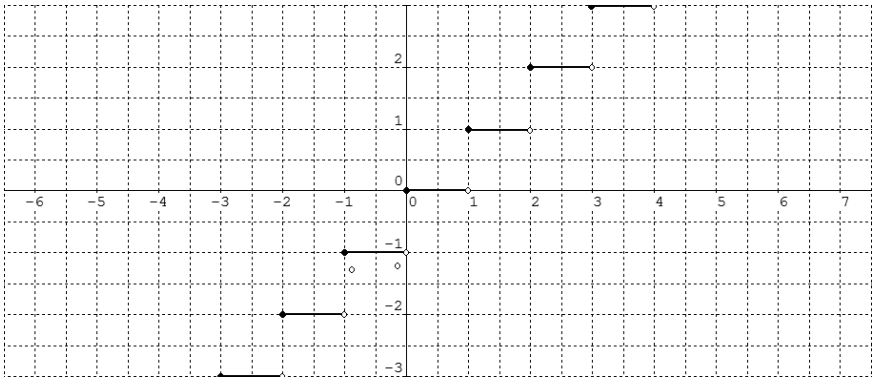
$$f[-1, 0) = -1$$

$$f[0, 1) = 0$$

$$f[1, 2) = 2$$

…

Con esto podemos construir el gráfico que sigue.



Parte entera de x

Las dos propiedades que siguen tienen que ver con el hecho de que las funciones conserva la relación de inclusión y la operación de unión de conjuntos, así como con la relación entre $f(X \cap Y)$ y $f(X) \cap f(Y)$.

Propiedad 1. Sea *f* una función con $f : A \to B$, y sean $X, Y \subset A$. Entonces se verifica que

$$\text{(a)} \quad X \subset Y \Rightarrow f(X) \subset f(Y)$$

$$\text{(b)} \quad f(X \cup Y) = f(X) \cup f(Y)$$

Demostración. (a) Para probar que $f(X) \subset f(Y)$ debemos ver que todo elemento de $f(X)$ es también un elemento de $f(Y)$. Supongamos entonces que $n \in f(X)$. Lo anterior implica, por la definición de imagen directa de *f*, que $\exists m \in X : f(m) = n$. Y como $X \subset Y$ (por hipótesis), *m* también está en *Y*. En consecuencia, y nuevamente con base en la definición de imagen directa de *f*, $f(m) = n \in f(Y)$. La igualdad dada en (b) se sigue de la doble inclusión entre los conjuntos $f(X \cup Y)$ y $f(X) \cup f(Y)$. Veamos: $n \in f(X \cup Y) \Leftrightarrow \exists m \in X \cup Y : f(m) = n \Leftrightarrow \exists m \in X \vee m \in Y : f(m) = n \Leftrightarrow$ $n \in f(X) \vee n \in f(Y) \Leftrightarrow n \in f(X) \cup f(Y)$. Aquí nos hemos apoyado en la definición de imagen directa de *f*, la definición de unión de conjuntos, de nuevo la defini-

ción de imagen directa y la definición de unión de conjuntos. Esto completa la prueba. ■

Propiedad 2. Sea *f* una función con $f : A \to B$, y sean $X, Y \subset A$. Entonces se cumple que $f(X \cap Y) \subset f(X) \cap f(Y)$.

Demostración. Si $n \in f(X \cap Y)$ entonces, por la definición de imagen directa, $\exists m \in X \cap Y : f(m) = n$. Por la definición de intersección de conjuntos, *m* está tanto en *X* como en *Y*. Así, $f(m) = n \in f(X) \wedge n \in f(Y)$. En consecuencia, $n \in f(X) \cap f(Y)$. ■ Es necesario comentar que la inclusión contraria no siempre se cumple. Observe que si $X = \{-1, 0, 1\}$, $Y = \{0, 1, 2, 3, 4\}$ y definimos $f : \mathbb{Z} \to \mathbb{Z}$ por $f(a) = -a^3$; entonces, $f(X) = \{-1, 0, 1\}$ y $f(Y) = \{0, -1, -8, -27, -64\}$. Sin embargo, $f(X) \cap f(Y) = \{0, -1\} \not\subset \{0, 1\} = f(X \cap Y)$. Aunque resulta interesante estudiar algunos ejemplos en los que se verifica la inclusión contraria, actividad que proponemos a los lectores. No obstante, lo correcto es decir que en general no se cumple la inclusión contraria.

Ahora bien, si *f* es inyectiva entonces se cumple que $f(X \cap Y) = f(X) \cap f(Y)$. Y recíprocamente, si $f(X \cap Y) = f(X) \cap f(Y)$ para cualesquiera subconjuntos *X* y *Y* de *A* entonces *f* tiene que ser inyectiva. Veamos:

Propiedad 3. *f* es inyectiva si y solo si $f(X \cap Y) = f(X) \cap f(Y)$, para cualesquiera subconjuntos *X* y *Y* de *A*.

Demostración. $(\Rightarrow)$ Probemos en primer lugar la implicación directa, esto es, si *f* es inyectiva entonces $f(X \cap Y) = f(X) \cap f(Y)$. (i) Ya sabemos que

$f(X \cap Y) \subset f(X) \cap f(Y)$, por la propiedad 2; así que resta probar la inclusión contraria. Para ello supongamos que $n \in f(X) \cap f(Y)$, en ese caso $\exists m \in X : f(m) = n \wedge \exists m^* \in Y : f(m^*) = n$. Pero como *f* es inyectiva debe suceder que $m = m^*$. Por tanto, *m* tiene que estar en la intersección de *X* y *Y*. Con esto, y la definición de imagen directa, podemos escribir que $n \in f(X \cap Y)$. (ii) Hemos visto que $f(X) \cap f(Y) \subset f(X \cap Y)$. Por i y ii, tenemos que $f(X \cap Y) = f(X) \cap f(Y)$. Probemos ahora el recíproco $(\Leftarrow)$. Para ello probaremos el contrarrecíproco, considerando que tienen el mismo valor de verdad. Es decir, suponiendo que *f* no es inyectiva veremos que $f(X) \cap f(Y) \neq f(X \cap Y)$. En efecto, sea $n \in f(X) \cap f(Y)$, entonces $n \in f(X) \wedge n \in f(Y)$. Y por la definición de imagen directa $\exists m \in X : f(m) = n \wedge \exists m^* \in Y : f(m^*) = n$. Pero como *f* no es inyectiva (por hipótesis), lo anterior no implica que *m* sea igual a *m**. Supongamos entonces que $m \neq m^*$. Ahora podemos preguntarnos

$$¿\{m' : f(m') = n\} \subset X \cap Y\,?$$

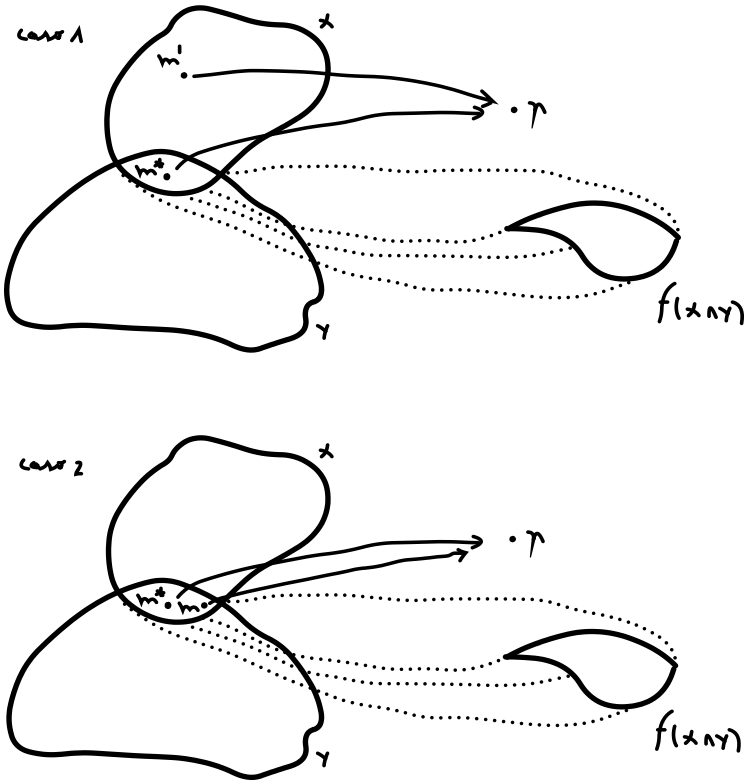
Veamos… para ello consideremos dos casos:

Caso 1: $\exists m' \notin X \cap Y$. Si esto se cumple, tenemos que $f(m') \notin f(X \cap Y)$.

Caso 2: $\forall m', m' \in X \cap Y$. En este caso, escojamos convenientemente los conjuntos unitarios $\{m\}$ y $\{m^*\}$. Con lo cual, $n = f(m) = f(m^*) \in f(\{m\}) \cap f(\{m^*\})$, pero $n \notin f(\{m\} \cap \{m^*\})$, ya que $\{m\} \cap \{m^*\} = \varnothing$.

En ambos casos, hemos visto que, si f no es inyectiva, existen elementos en $f(X)\cap f(Y)$ que no están en $f(X\cap Y)$. Justo lo que queríamos probar. ■

Observe que la elección de los conjuntos $\{m\}$ y $\{m^*\}$ para el análisis último de la prueba se basa en que la proposición aplica para cualesquiera conjuntos *X* y *Y* de *A*. Vale la pena hacer un gráfico de estos casos.



Casos 1 y 2

Además, note que probamos $(\Leftarrow)$ por medio del contrarrecíproco. ¿De qué otra manera se puede probar $(\Leftarrow)$?

Propiedad 4. $f(X)-f(Y)\subset f(X-Y)$. Con f una función, $f:A\to B$, y $X,Y\subset A$.

Demostración. Si $n \in f(X) - f(Y)$ entonces, por diferencia de conjuntos, $n \in f(X) \wedge n \notin f(Y)$. Esto es, $\exists m \in X : f(m) = n$. Pero un *m* con tal propiedad no existe en *Y*. Ello implica que $m \in X - Y$, por la definición de imagen directa. Así, $f(m) = n \in f(X - Y)$. Las implicaciones anteriores se verifican para todo *n* en $f(X) - f(Y)$. Por tanto, $f(X) - f(Y) \subset f(X - Y)$. ■

Las propiedades 1(b) y 2, podemos generalizarlas para el caso de la unión e intersección de una familia de subconjuntos de un conjunto.

Propiedad 5. Consideremos a una familia de subconjuntos A_i, donde *i* está en un conjunto de índices *I*, de un conjunto *A* y a una función $f : A \to B$. Entonces se verifican las dos propiedades siguientes:

$$\text{(a)} \qquad f\left(\bigcup_{i \in I} A_i\right) = \bigcup_{i \in I} f(A_i).$$

$$\text{(b)} \qquad f\left(\bigcap_{i \in I} A_i\right) \subset \bigcap_{i \in I} f(A_i).$$

Demostración. (b) Si $n \in f\left(\bigcap_{i \in I} A_i\right)$ entonces $\exists m \in \bigcap_{i \in I} A_i : f(m) = n$, por la definición de imagen directa. En consecuencia, $m \in A_i, \forall i \in I$. Por tanto, $f(m) = n \in \bigcap_{i \in I} f(A_i)$. ■ La prueba de la parte (a) de deja como ejercicio.

Propiedad 6. Si B_i es una familia de subconjuntos de un conjunto *B* y *f* una función $f : A \to B$. Entonces se cumple que:

(a) $f^{-1}\left(\bigcup_{i\in I} B_i\right)=\bigcup_{i\in I} f^{-1}(B_i)$.

(b) $f^{-1}\left(\bigcap_{i\in I} B_i\right)=\bigcap_{i\in I} f^{-1}(B_i)$.

Demostración. Parte (a): $m\in f^{-1}\left(\bigcup_{i\in I} B_i\right)\Leftrightarrow \exists m\in A: f(m)\in\bigcup_{i\in I} B_i$ $\Leftrightarrow \exists i\in I: f(m)\in B_i \Leftrightarrow m\in f^{-1}(B_i) \Leftrightarrow m\in\bigcap_{i\in I} f^{-1}(B_i)$. Aquí nos apoyamos en la definición de imagen recíproca, definición de la unión de una familia de subconjuntos, definición de imagen recíproca de *f*, y por la definición de unión de conjuntos. ■

Dejamos la parte (b) a los lectores.

Antes de probar la siguiente propiedad de las funciones, las cuales vinculan los conceptos de imagen directa e imagen recíproca, así como una caracterización de las funciones inyectivas con base en estos conceptos, exploremos un par de ejemplos. Pongamos por caso un conjunto $A=\{x_1, x_2\}$ y $B=\{y_1\}$. Y sea $f: A\to B$ definida por $f(x)=y_1, \forall x\in A$. Así, si consideramos $X=\{x_1\}\subset A$, entonces

$$f(X)=\{y_1\}$$

y

$$f^{-1}(f(X))=f^{-1}(\{y_1\})=\{x_1, x_2\}\neq X$$

Y esto sucede justo porque *f* no es inyectiva.

Ello también puede verse en el caso $f:\mathbb{R}\to\mathbb{R}$ definida por $f(x)=x^2$. Considerando, por ejemplo, $X=[0,1]$. Observe que $f(X)=[0,1]$ y $f^{-1}(f(X))=[-1,1]\neq X$.

Note además que si $X = \mathbb{R}$, entonces $f^{-1}\left(f\left(X\right)\right) = \mathbb{R} = X$. Compare estas ideas con las propiedades que siguen.

Propiedad 7. Nuevamente, consideremos a f una función con $f : A \to B$, y sea $X \subset A$. Entonces:

(a) Si X=A se tiene que $f^{-1}\left(f\left(X\right)\right) = X$. Además,

(b) Si $X \subset A$ con $X \neq A$ se tiene que $X \subset f^{-1}\left(f\left(X\right)\right)$.

Demostración. (a) Como $f\left(X\right) = \left(A\right) = \left\{f\left(x\right) : x \in A\right\}$, tenemos que $f^{-1}\left(f\left(X\right)\right) = f^{-1}\left(f\left(A\right)\right) = \left\{x \in A : f\left(x\right) \in f\left(A\right)\right\} = A = X$. Exponga el lector los argumentos. (b) Consideremos x en X. Así, $f\left(x\right) \in f\left(A\right)$ por la definición de imagen directa y esto sucede si, y solo si, $x \in f^{-1}\left(f\left(A\right)\right)$, por la definición de imagen recíproca. ■

Proposición 8. Sea la función f con $f : A \to B$, y sea $X \subset A$. $f^{-1}\left(f\left(X\right)\right) = X$, para todo subconjunto X de A, si y solo si, f es inyectiva.

Demostración. $\left(\Rightarrow\right)$ Sea $\left\{y\right\} \subset f\left(X\right) \subset B$.

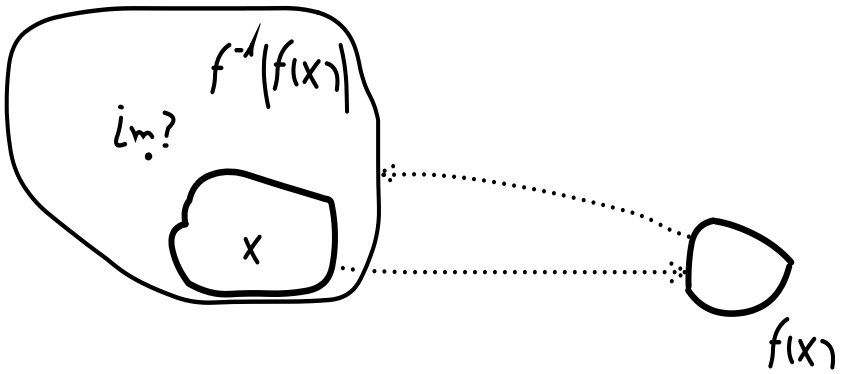
La clave está en responder cuántos elementos tiene $f^{-1}\left(\left\{y\right\}\right)$. Sabemos que $\exists x \in X : f\left(x\right) = y$, por la definición de imagen recíproca de f. Así,

$$f^{-1}\left(f\left(\left\{x\right\}\right)\right) = \left\{x\right\}$$

Por la hipótesis. Observe que esto sucede para todo elemento de A.

Entonces, f es inyectiva.

$(\Leftarrow)$ Supongamos ahora que *f* es inyectiva. Sea $X \subset A$. Consideremos dos casos. Caso 1: si $X = A$, por la propiedad 7(a), $f^{-1}\left(f\left(X\right)\right) = X$. Caso 2: si $X \neq A$, la propiedad 7(b) nos garantiza que $X \subset f^{-1}\left(f\left(X\right)\right)$.



¿Existe un m en A tal que esté en el conjunto $f^{-1}\left(f\left(X\right)\right) - X$ *?*

Ahora, ¿ $\exists m \in A : m \in f^{-1}\left(f\left(X\right)\right) - X$?

Si esto es así, se debería cumplir que $f\left(m\right) \in f\left(X\right)$, lo cual es absurdo ¡pues $m \notin X$ y *f* es inyectiva! Entonces, $f^{-1}\left(f\left(X\right)\right) = X, \forall X \subset A, X \neq A$. Esto completa la prueba. ■

Por otra parte, sea $f : \mathbb{R} \to \mathbb{R}$ definida por $f\left(x\right) = 2^x$. Tomemos $Y = \left[-1, 1\right]$. En este caso,

$$f^{-1}\left(Y\right) = \left\{x \in \mathbb{R} : f\left(x\right) \in Y\right\}$$

$$= \left\{x \in \mathbb{R} : -1 \leq 2^x \leq 1\right\}$$

$$= \left(-\infty, 0\right]$$

Así,

$$f\left(f^{-1}\left(Y\right)\right) = f\left(-\infty, 0\right] = \left(0, 1\right] \subset \left[-1, 1\right] = Y$$

Esto es, aquí $f\left(f^{-1}(Y)\right)\subset Y$. La propiedad que sigue tiene que ver con esta idea.

Proposición 9. Sea la función f con $f:A\to B$, y sea $Y\subset B$. Entonces se verifica que $f\left(f^{-1}(Y)\right)\subset Y$.

Demostración. Si $n\in f\left(f^{-1}(Y)\right)$, esto implica que $\exists m\in f^{-1}(Y): f(m)=n$ (por la definición de imagen recíproca); por tanto, $n\in Y$ (por la definición de imagen directa). ■

Proposición 10. Sea la f con $f:A\to B$, y sea $Y\subset B$. Entonces se verifica que $f\left(f^{-1}(Y)\right)=Y$ si y solo si, f es sobreyectiva.

Demostración. Por lo visto antes (propiedad 9), solo resta probar que $Y\subset f\left(f^{-1}(Y)\right)$. En efecto, Si $n\in Y$, como f es sobreyectiva, $\exists m\in f^{-1}(Y): f(m)=n$, por la definición de imagen recíproca. Así, $n\in f\left(f^{-1}(Y)\right)$. Esto completa la prueba. ■

1. ¿Qué distingue a las relaciones de las funciones?
2. Considere las siguientes relaciones definidas en el conjunto de los números Reales:

   (a) $R=\{(x,y): x-y>1\}$.

   (b) $R=\{(x,y): x^2-y<2\}$.

   (c) $R=\{(x,y): x-y^2=1\}$.

   ¿Cuáles de ellas corresponden a funciones?

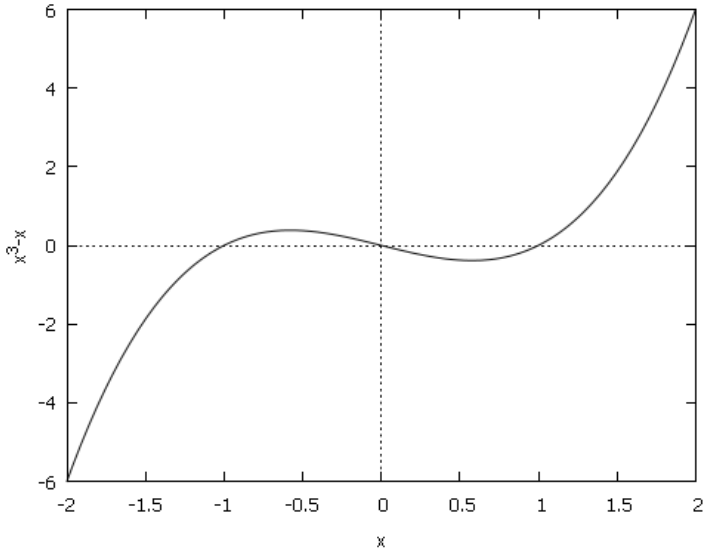
3. Exponga ejemplos de funciones (a) no inyectivas, (b) no sobreyectivas, (c) no inyectivas y no sobreyectivas, (d) sobreyectivas pero no inyectivas, (e) inyectivas pero no sobreyectivas.
4. Exponer un contraejemplo que muestre la falsedad del recíproco de $X \subset Y \Rightarrow f(X) \subset f(Y)$. Con f una función, $f : A \to B$, y $X, Y \subset A$.
5. Muestre la falsedad del recíproco de la propiedad 2.
6. Una manera de mostrar que $\mathbb{N} \times \mathbb{N}$ es enumerable es a través de la función $g : \mathbb{N} \to \mathbb{N} \times \mathbb{N}$ definida recursivamente así:

$$g(x) = \begin{cases} (0,0) \; si \; n = 0 \\ (i+1, \; j-1) \; si \; g(n-1) = (i, \; j) \; con \; j > 0 \\ (0, i+1) \; si \; g(n-1) = (i, 0) \end{cases}$$

   Preguntamos entonces, ¿cuál es la imagen de 7? ¿Es *g* sobreyectiva? ¿Es inyectiva?
7. ¿Son equipotentes los pares de conjuntos que siguen? (En ese caso debe encontrar funciones biyectivas entre los conjuntos *A* y *B* dados).
   (a) $A = \mathbb{N}$ y $B = \{n \in \mathbb{N} : n \geq 2\}$
   (b) $A = \{n^2 : n \in \mathbb{N}\}$ y $B = \mathbb{N}$
   (c) $A = \{x \in \mathbb{R} : 0 < x < 1\}$ y $B = \{x \in \mathbb{R} : 5 < x < 7\}$
   (d) $A = \{X : X \subset \{a,b,c\}\}$ y $B = \{0,1\} \times \{0,1\} \times \{0,1\}$
   (e) $A = \{f : \{0,1\} \to \{a,b,c\}, \; f \; \textit{función}\}$ y $B = \{a,b,c\} \times \{a,b,c\}$
8. Si f es una función de *A* en *A* tal que su inversa existe. Pruebe que $f^{-1} \cdot f = f \cdot f^{-1} = I$, donde *I* es la *función identidad* , *I*(*x*)=*x*

1. En una función si el par (a,b) pertenece a la misma y c es distinto de b entonces es imposible tener que el par (a,c) pertenezca a la función, eso no ocurre para relaciones arbitrarias, como el estudiante UNA puede leer en el texto, una función es una clase particular de relación.
2. Ninguna es una función como el estudiante UNA debe verificar cuidadosamente.
3. Vamos a realizar este ejercicio de manera cuidadosa, de forma que el estudiante vea lo importante de escoger el dominio de una fución, así como el conjunto de llegada.
   a) Tomemos $f:\mathbb{R}\to\mathbb{R}, f(x)=x^4-1$. Vemos que $f(1)=f(-1)=0$, luego la función f no es inyectiva. Sin embargo, $g:\mathbb{R}^+\to\mathbb{R}, g(x)=x^4-1$

      $g:\mathbb{R}^+\to\mathbb{R}, g(x)=x^4-1$ si lo es. Queda para el estudiante UNA construir otros ejemplos, justificando sus afirmaciones.
   b) La función anterior $f:\mathbb{R}\to\mathbb{R}, f(x)=x^4-1$ no es sobreyectiva ya que por ejemplo nunca toma el valor -2. Para ver esto observe que $f(x)=x^4-1\geq -1$. De nuevo, el conjunto de llegada puede ser modificado para que esta función sea sobreyectiva, dejamos al estudiante que reflexione como hacerlo.
   c) Use a) y b) para construir ejemplos.
   d) Consideremos la función $h(x)=x^3-x$ definida sobre todos los reales y con conjunto de llegada todo los reales. Veamos su gráfica



El estudiante debe recordar de su curso de Matemática I que

$$\lim_{x\to\pm\infty} h(x) = \pm\infty$$

Lo que implica la sobreyectividad pero $h(0)=h(-1)=h(1)=0$ de donde la función no es inyectiva.

e) Queda para el estudiante UNA.

4. Tomemos por ejemplo $A=B=\{a,b\}$ y $f(a)=f(b)=a$, complete los detalles para ver que esto sirve como contraejemplo de la propiedad mencionada.
5. Se deja al estudiante UNA.
6. Se deja al estudiante UNA.
7. Se deja al estudiante UNA.
   a) Tomemos la función que a cada natural n le asigna $n+2$, esto es una biyección entre el conjunto de los naturales y $B=\{n\in\mathbb{N}: n\geq 2\}$
   b) Este ejemplo es importante desde el punto de vista histórico ya que Galileo indicó que era peligroso el uso del infinito en Matemáticas debido a que hay tantos números naturales como cuadrados $1,4,9,\cdots$ a pesar que claramente los cuadrados son un subconjunto propio de los naturales. Sea

$$A = \left\{ n^2 : n \in \mathbb{N} \right\}$$

Consideramos ahora la función *f* que asigna a cada natural *n* el elemento

$$f(n) = n^2 \in A$$

Es claro que *f* es una biyección (diga porqué) y que por ende hay tantos elementos en *A* como números naturales.

c) Tome la función

$$f(x) = \frac{6}{5}x + 1$$

Y verifique que es una byección entre el intervalo (0,1) y el i.ntervalo (5,7)

d) Queda a cargo del estudiante UNA, como ayuda le indicamos que la respuesta es afirmativa.

e) Queda a cargo del estudiante UNA, consulte con su asesor si no puede resolver el problema.

8. Tenemos que por definición

$$f^{-1}(b) = a \Leftrightarrow f(a) = b,$$

Luego,

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

De donde se tiene el resultado.

3.4 Funciones estrictamente crecientes y decrecientes, crecientes y decrecientes; pares e impares

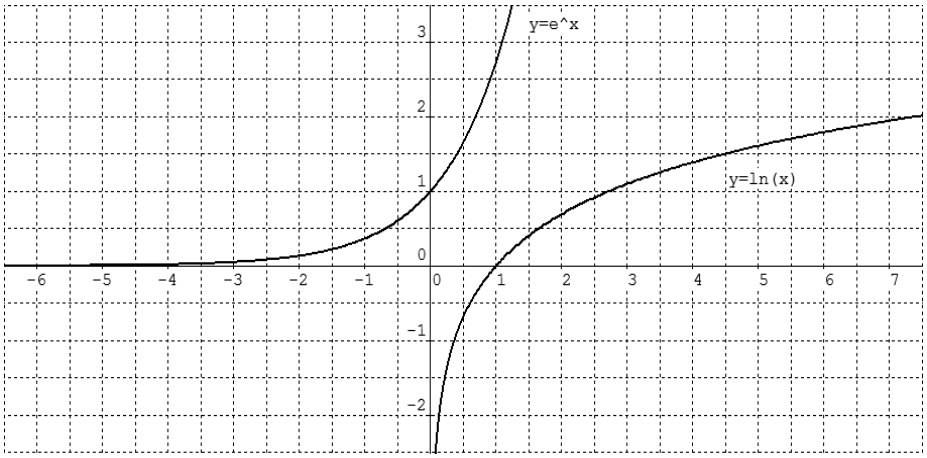
Definición. Sean *M* y *N* dos conjuntos ordenados por las relaciones r_1 y r_2, respectivamente. Decimos que la función $f : M \to N$ es

– **estrictamente creciente** si ar_1b y $a \neq b$ implica que $f(a) r_2 f(b)$ y $f(a) \neq f(b)$

- **estrictamente decreciente** si $ar_1 b$ y $a \neq b$ implica que $f(b) r_2 f(a)$ y $f(a) \neq f(b)$
- **creciente** si $ar_1 b$ implica que $f(a) r_2 f(b)$
- **decreciente** si $br_1 a$ implica que $f(a) r_2 f(b)$
- **monótona** si *f* es creciente o bien *f* es decreciente.

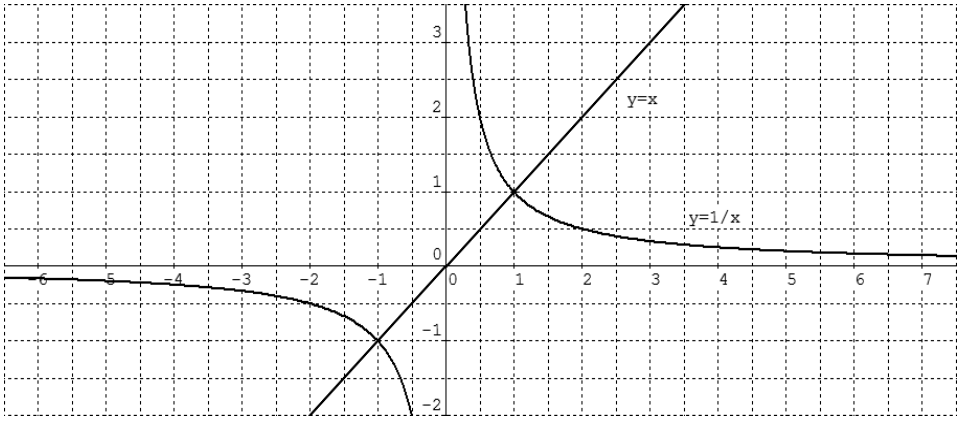
Por otra parte, si *f* es una función definida en los reales y conjunto de llegada los reales entonces *f* es par si $f(a) = f(-a)$.Y, *f* es impar si $f(-a) = -f(a)$, $\forall a \in A$.

1. La función $f : \mathbb{R} \to \mathbb{R}^+$ definida por $f(x) = e^x$, donde *e* es el *número de Euler* ($e \approx 2{,}7182818$), es estrictamente creciente en todo su dominio, ya que si $a<b$ entonces $f(a)<f(b)$. Además, su inversa, la función $f^{-1} : \mathbb{R}^+ \to \mathbb{R}$ definida por $f^{-1}(x) = \ln x$, también lo es.



Curvas correspondientes a $y = e^x$ *y* $y = \ln x$

2. La función $f:\mathbb{R}^*\to\mathbb{R}$ definida por $f(x)=\dfrac{1}{x}$, es impar, ya que $f(-x)=\dfrac{1}{-x}=-\dfrac{1}{x}=-f(x),\ \forall x\in\mathbb{R}^*$. También es estrictamente decreciente como debe verificar el estudiante UNA. La función identidad también es impar pero es estrictamente creciente.



Función identidad y $\dfrac{1}{x}$

3. Como $sen(-x)=-sen\,x$ y $\tan(-x)=-\tan x$, para todo x en sus dominios, entonces son impares. Y, por tanto, sus gráficas son simétricas con respecto al origen. Por otra parte, como

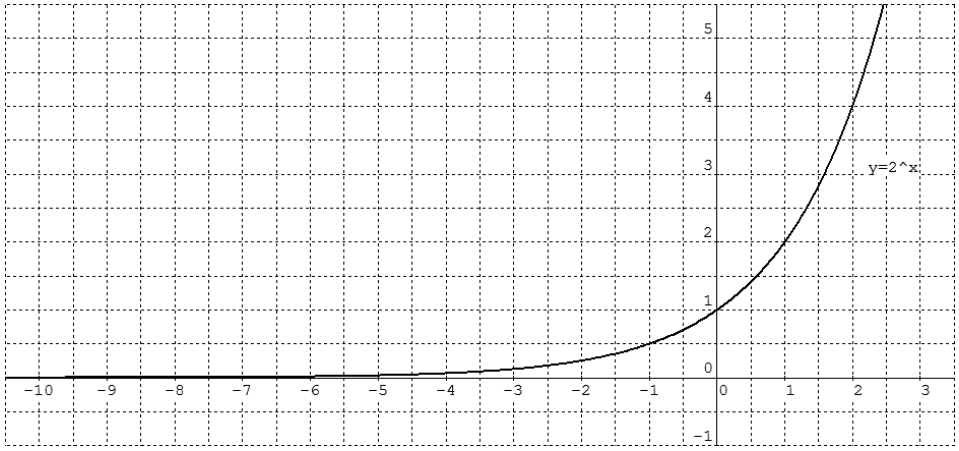
$$|x|=\begin{cases}x & si\ x\geq 0\\ -x & si\ x<0\end{cases}$$

entonces $|x|=|-x|$, para todo x en el dominio, con lo cual $|x|$ es par y su gráfica es simétrica con respecto al eje y.

4. Estudie si la función coseno es par o impar, recuerde que $\cos(-x)=\cos x$.

3.5 Construyendo gráficas

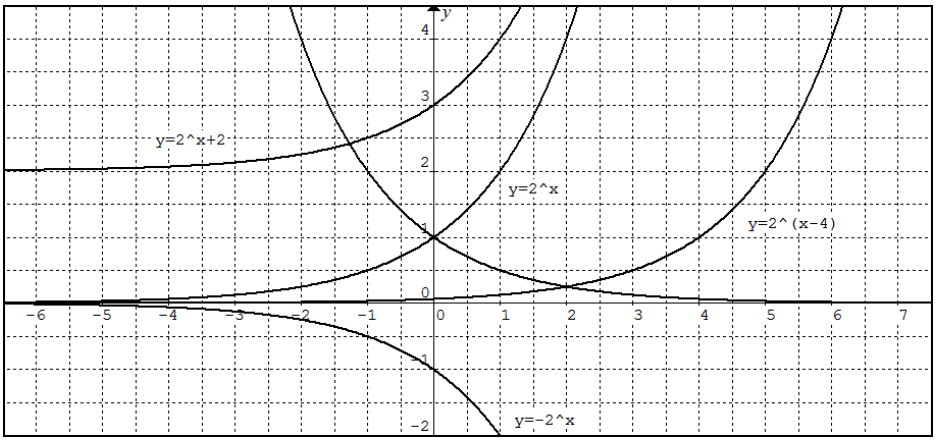
Tomemos por caso la función $f:\mathbb{R}\to\mathbb{R}$ dada por la regla $f(x)=2^x$. Observemos que si *x*=0, $f(x)=2^0=1$; así que la curva toca al eje y en el punto $(0,1)$. Si $x>0$, $2^x>0$. Y si $x_1<x_2$, entonces $2^{x_1}<2^{x_2}$, con lo que *f* es creciente. Pero si $x<0$ también se cumple que $2^x>0$ y se acerca a cero para valores grandes de $|x|$. Entonces su gráfica tiene la forma que sigue.



Gráfica de la función $f(x)=2^x$

Además, como $2^x\neq 2^{-x}$ y $2^{-x}\neq -2^x$, entonces *f* no es ni par ni impar.

Pero, ¿cómo se afecta la curva de $y=f(x)$ al multiplicar esta expresión por -1, al multiplicar por -1 el argumento, al sumar $-b$ al argumento, o al sumar *a* a la expresión? Es decir, dada $y=f(x)$, ¿cómo son las gráficas de $y=-f(x)$, $y=f(-x)$, $y=f(x-b)$, y $y=f(x)+a$? Para ilustrar esto, consideremos la función del caso anterior (ver el gráfico que sigue).



Sobre la construcción de gráficas

En general se cumple que dada $y = f(x)$

$y = -f(x)$ es simétrica con $y = f(x)$ respecto al eje *x*

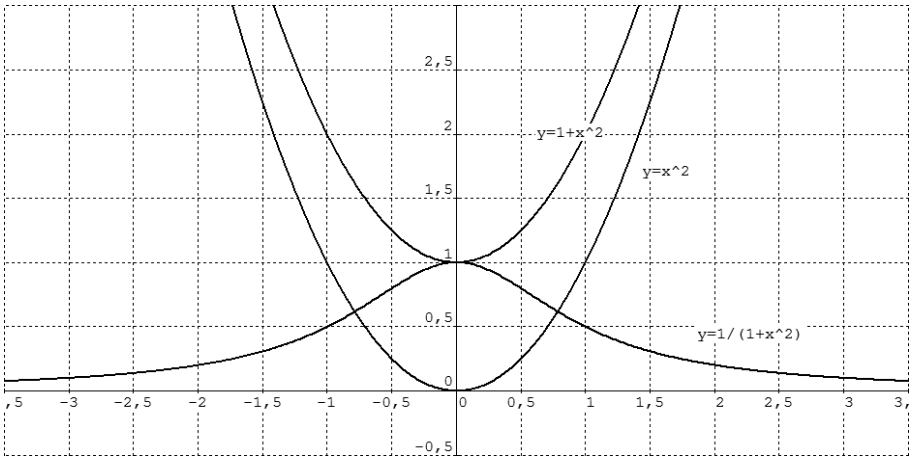
$y = f(-x)$ es simétrica con $y = f(x)$ respecto al eje *y*

$y = f(x-b)$ es la gráfica de $y = f(x)$ pero desplazada en el eje *x* con magnitud *b*

$y = f(x)+a$ es la gráfica de $y = f(x)$ pero desplazada en el eje *y* con magnitud *a*

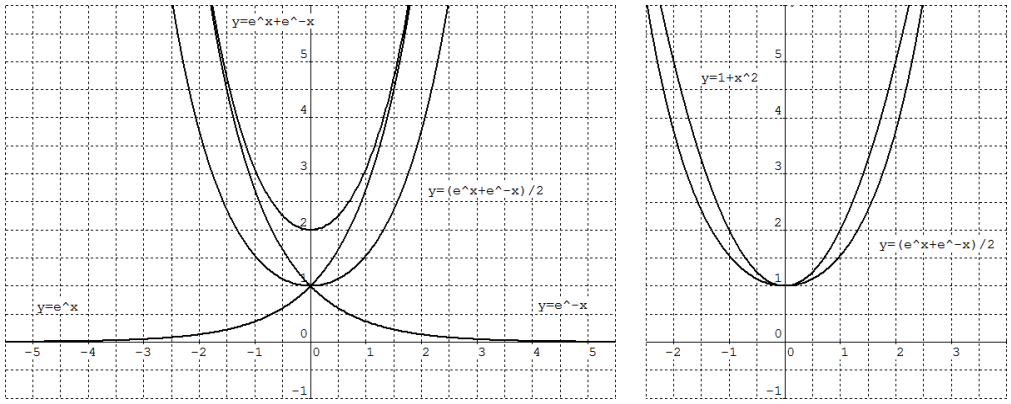
Construyamos ahora la gráfica de $f : \mathbb{R} \to \mathbb{R}$ dada por la regla $f(x) = \dfrac{1}{1+x^2}$ (*curva de Agnesi*). Para ello podemos representar la curva $y = x^2$, y a partir de ésta, la de $y = 1+x^2$ (la cual está desplazada en el eje *y* con magnitud 1 –con respecto a la curva $y = x^2$). La curva $y = \dfrac{1}{1+x^2}$ toca al eje *y* en el punto $(0,1)$. Observe que para $a, b \in \mathbb{R}^+$, con $a < b$, se tiene que $1+a^2 < 1+b^2$. Y por tanto $\dfrac{1}{1+a^2} > \dfrac{1}{1+b^2}$. *f* es decreciente en el intervalo $[0, \infty)$. ¿Y en el intervalo $(-\infty, 0]$? Además,

$\frac{1}{1+x^2} > 0, \forall x \in \mathbb{R}$, así que la curva nunca toca el eje *x* (la recta *y*=0 es una asíntota horizontal de la curva).

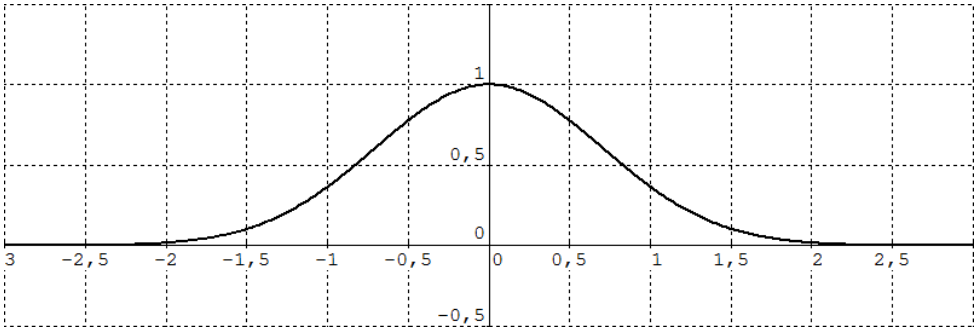


Construcción de $y = \frac{1}{1+x^2}$ *(Curva de Agnesi)*

Consideremos ahora la función $f : \mathbb{R} \to \mathbb{R}$ dada por $f(x) = \cosh x = \frac{e^x + e^{-x}}{2}$. Aquí, $\cosh x$ es el *coseno hiperbólico* de *x*. Con base en las gráficas de $y = e^x$ y $y = e^{-x}$ podemos construir la de $y = \frac{e^x + e^{-x}}{2}$. Observe que $y = e^{-x}$ es una curva simétrica a $y = e^x$ con respecto al eje de las ordenadas (ver el gráfico). Si (x_1, y_1) es un punto de $y = e^x$ y (x_1, y_2) es un punto de $y = e^{-x}$, entonces $(x_1, y_1 + y_2)$ es un punto de $y = e^x + e^{-x}$. La curva $y = \frac{e^x + e^{-x}}{2}$ se conoce como *catenaria*. En realidad no es una parábola. Y se corresponde con la forma que describe una cadena o cable suspendido por sus extremos, tal es el caso del tendido eléctrico o de las guayas de un teleférico. El gráfico que sigue ilustra la diferencia entre la catenaria y la parábola. En este caso ambas tocan el eje *y* en $(0,1)$. 1 es el punto mínimo de $f(\mathbb{R})$.



Construcción de la catenaria (izquierda) y su diferencia con la parábola (derecha)



Curva de Gauss

La *curva de Gauss o campana de Gauss* tiene por ecuación $y = e^{-x^2}$. Esta curva corta al eje de las ordenadas en el punto $(0,1)$, pues $e^{-0^2} = 1$. Además, si $x \to \infty$, $x^2 \to \infty$ y $e^{x^2} \to \infty$. Por tanto, $e^{-x^2} = \dfrac{1}{e^{x^2}} \to 0$. De forma similar, si $x \to -\infty$, $e^{-x^2} \to 0$. Los puntos $\left(\frac{1}{\sqrt{2}}, e^{-\left(\frac{1}{\sqrt{2}}\right)^2}\right)$ y $\left(-\frac{1}{\sqrt{2}}, e^{\left(\frac{1}{\sqrt{2}}\right)^2}\right)$ sirven de guías para el trazo de la gráfica. Esta función es fundamental en la estadística y en las probabilidades.

3.6 Modelando con las funciones

A – ¿Qué tan grandes pueden ser las "lagunas" en la sucesión de números primos? Los números primos constan solo de dos divisores albergan desde matemáticas

muy sencillas hasta las complejidades y retos de la construcción de nuevas ideas. ¿Se distribuyen azarosamente o caóticamente entre los naturales, o bien, existe un patrón (función) que genere esta sucesión infinita? Justo este problema ha ocupado a grandes matemáticos a lo largo de la historia.

2 3 5 7 11 13 17 19 23 29 31 37 41 43 47 53 59 61 67 71 73 79 83 89 97 …

En lo que sigue nos ocuparemos del siguiente problema: ¿Qué tan grandes pueden ser las *lagunas* en la sucesión de números primos? Veamos…

Hagamos una lista de (2, 3, 4, 5 y 6) números compuestos consecutivos.

8, 9

14, 15, 16

122, 123, 124, 125

264, 265, 266, 267, 268

492, 493, 494, 495, 496, 497

…

Parecería extraño que existiendo infinitos números primos, encontremos lagunas cada vez más grandes. Un ejemplo de una laguna de 237 números compuestos consecutivos está entre los primos 9551 y 9787.

Una inferencia entonces es que existen lagunas tan grandes como queramos. ¿Cómo nos convencemos de ello? Supongamos que queremos mostrar un procedimiento para encontrar una laguna de tamaño 7. Consideremos los números

8!+2

8!+3

8!+4

8!+5

$8!+6$

$8!+7$

$8!+8$

Observe que ninguno de ellos es primo, pues $a \mid 8!+a$ con $2 \le a \le 8$. Fíjese que a es un factor de 8! Así,

40322, 40323, 40324, 40325, 40326, 40327, 40328

El lector advertirá que pudimos dar un ejemplo más sencillo, observando una tabla de números primos; tal es el caso de 402, 403, 404, 405, 406, 407, 408. Pero nuestra intención es obtener una respuesta general. En efecto, consideremos los números

$$(n+1)!+2$$

$$(n+1)!+3$$

$$\vdots$$

$$(n+1)!+(n+1)$$

Y observe que 2 es factor del primero, 3 lo es del segundo, …, y n+1 lo es del último. ¡Por esta razón, ninguno de ellos es primo! Por tanto, tenemos

$(n+1)!+(n+1)-\big((n+1)!+2\big)+1=n$ números compuestos consecutivos.

Y esto vale $\forall n \in \mathbb{N}^*$.

Ahora, es fácil encontrar lagunas de tamaño un millón (en las que todos son compuestos consecutivos), o de tamaño mil millones… Aún así, como sabemos, después ellas siempre habrá números primos (por lo probado por Euclides).

B – ¿Cuántos primos hay en el intervalo $[1, n]$? Para hacer una inferencia debemos exponer varios casos y observar en ellos algún posible patrón. Para ello, llamemos a $p(n)$ el número de primos menores o iguales a *n*. Por ejemplo: $p(1)=0$, $p(2)=1$, $p(3)=2$, $p(4)=2$, $p(5)=3$, $p(6)=3$, $p(7)=4$, $p(8)=4$, $p(9)=4$, $p(10)=4\ldots$ Y observando una lista de números primos, sabemos que $p(100)=25$, $p(1000)=168$, $p(10000)=1229\ldots$ Organicemos algunos de estos datos. Para los $n>9$, consideraremos solo los *n* que son potencias de 10 (hasta *n* igual a mil millones –aunque podríamos ampliar esta tabla tanto como queramos). Además, incluiremos columnas para los cocientes $\frac{p(n)}{n}$ y $\frac{n}{p(n)}$. La primera de ellas nos informa sobre la proporción de números primos en el intervalo $[1, n]$. Una proporción de 0,168 nos indica que hay 16,8% de primos en el intervalo dado, en este caso $[1,1000]$. La segunda es el inverso de esta proporción. Los datos a partir de la tercera columna son aproximados y se obtuvieron con apoyo en un programa de cálculo de dominio libre.

N	$p(n)$	$\frac{p(n)}{n}$	$\frac{n}{p(n)}$
1	0	0	-
2	1	0,5	2
3	2	0,666666667	1,5
4	2	0,5	2
5	3	0,6	1,666666667
6	3	0,5	2
7	4	0,571428571	1,75
8	4	0,5	2
9	4	0,444444444	2,25
10	4	0,4	2,5
100	25	0,25	4
1000	168	0,168	5,952380952

10000	1229	0,1229	8,136696501
100000	9592	0,09592	10,42535446
1000000	78498	0,078498	12,73917807
10000000	664579	0,0664579	15,04712006
100000000	5761455	0,05761455	17,35672673
1000000000	50847534	0,050847534	19,66663713

…

Más allá del hecho de la disminución de la cantidad de primos a medida que *n* crece, lo cual se infiere inmediatamente al observar la tabla, nos interesa encontrar una regla general que nos informe de la cantidad de primos en el intervalo $[1, n]$. Veamos un gráfico de $p(n)$ en función de *n* (para *n*=1000, 10000, 100000).

Gráfica de la proporción de primos para n=1000, 10000 y 100000

En la tabla que sigue hemos agregado una columna para las diferencias

$$\frac{n_{i+1}}{p(n_{i+1})} - \frac{n_i}{p(n_i)}.$$

Si *n*=2 entonces $e^{\frac{2}{p(2)}} = e^{\frac{2}{1}} = e^2 \approx 7,389056099$. Aquí vemos que a partir de *n*=10, cuando *n* toma potencias de 10 (los no sombreados en la tabla), $\frac{n}{p(n)}$ crece muy lentamente; en cambio, las potencias de *e* crecen aproximadamente en un factor de

10. Por ejemplo: $e^{2,5} \approx 12,18249396$, $e^{4} \approx 54,59815003$, $e^{5,952380952} \approx 384,6681259$, etc. ¡El número *e* aparece en muchos y diversos fenómenos dentro y fuera de las matemáticas! Justo estas ideas permiten identificar un patrón.

N	$\frac{n}{p(n)}$	$\frac{n_{i+1}}{p(n_{i+1})} - \frac{n_i}{p(n_i)}$	$e^{\frac{n}{p(n)}}$
1	-	-	-
2	2	-	7,389056099
3	1,5	-0,5	4,48168907
4	2	0,5	7,389056099
5	1,666666667	-0,333333333	5,294490052
6	2	0,333333333	7,389056099
7	1,75	-0,25	5,754602676
8	2	0,25	7,389056099
9	2,25	0,25	9,487735836
10	2,5	0,25	12,18249396
100	4	1,5	54,59815003
1.000	5,952380952	1,952380952	384,6681259
10.000	8,136696501	2,184315549	3417,609131
100.000	10,42535446	2,288657959	33703,41545
1.000.000	12,73917807	2,31382361	340843,283
10.000.000	15,04712006	2,30794199	3426740,446
100.000.000	17,35672673	2,30960667	34508862,39
1.000.000.000	19,66663713	2,3099104	347625785,5

…

Entonces, al aumentar *n* en un factor de 10, $e^{\frac{n}{p(n)}}$ también aumenta (aproximadamente) en un factor de 10. Llamemos $\frac{n}{p(n)} = t(n)$. Es decir, para *n*>10,

$$e^{t(10n)} \approx 10e^{t(n)} \quad (1)$$

Por otra parte, como $e^{\ln(n)} = n$ (¿por qué?) y $e^{\ln(10n)} = 10n$ (¿por qué?), tenemos que

$$e^{\ln(10n)} = 10e^{\ln(n)} \qquad (2)$$

Y observamos que (1) y (2) tienen aproximadamente el mismo comportamiento. Con lo cual podemos escribir, para *n* grande, que

$$t(n) \approx \ln(n)$$

Esta relación es muy importante. A partir de ésta concluimos que $t(n) = \dfrac{n}{p(n)} \approx \ln(n)$. Y así,

$$\frac{p(n)}{n} \approx \frac{1}{\ln(n)}$$

Y ésta es la inferencia: **la proporción de números primos en el intervalo** $[1, n]$ **es aproximadamente el inverso del logaritmo neperiano de *n***. Por ejemplo,

$$\frac{p(1000000)}{1000000} = 0,078498 \approx \frac{1}{\ln(1000000)}.$$

Nota: para una demostración de este importante teorema, llamado *Teorema de los números Primos*, consultar el libro de T. Apostol *Teoría Analítica de Números.* También pueden leerse los apuntes de Gauss al respecto, un siglo antes de que se diera la prueba.

3.7 Algunas notas

La Teoría de Números

Algunos de los problemas abiertos en esta interesante y compleja rama de las Matemáticas son: (a) ¿hay primos en el intervalo $\left(n^2,(n+1)^2\right), \forall n \in \mathbb{N}^*$? Lo cual conduciría a un resultado similar al *Teorema de Bertrand*, el cual garantiza que para cualquier entero positivo existe un número primo *p* tal que $n < p \leq 2n$. Esto, es, podemos encontrar al menos un primo en intervalos del tipo $(n, 2n]$, tesis que agrega más "misterios" a la luz del resultado sobre el tamaño de las *lagunas* en la sucesión de primos. (b) ¿Hay infinitos primos de la forma n^2+1? Como por ejemplo: 17, 101 y 160001; en efecto: $17=4^2+1$, $101=10^2+1$ y $160001=400^2+1$. (c) ¿Hay infinitas parejas de primos gemelos? Esto es, de primos cuya diferencia sea 2, tal es el caso de

3 y 5, 11 y 13, 17 y 19, 29 y 31, 41 y 43, ¿etcétera?

Aunque ya se sabe que la serie formada por sus inversos converge, y se conoce una cota superior para su suma. Y, (d) ¿Hay infinitos primos en la sucesión de Fibonacci? Tal es el caso de

2, 3, 5, 13, 89, 233, 1597, 28657 y 514229, entre otros.

Por otra parte, ¿existen infinitos tripletes de números primos? (Tres números primos forman un triplete si tienen la forma *p*+2, *p*+3 y *p*+4, respectivamente. Tal es el caso de 3, 5 y 7).

El número *e*

El número *e* es tan importante como π. Fue propuesto por John Napier (Neper), no obstante, fue Euler quien descubrió propiedades importantes vinculadas con este

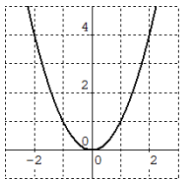
número; razón por la que se le conoce como *número de Euler*. Por ejemplo, los modelos matemáticos de crecimiento de muchas poblaciones, animales o vegetales, se basan en el número *e*, y como vimos, en la datación de un fósil, en el cálculo del interés compuesto...

$$e \approx 2.71828182845904523536028747135 27\ldots$$

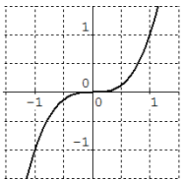
Valor que está dado por la ecuación de Bernoulli: $e = \lim_{n\to\infty}\left(1+\frac{1}{n}\right)^n$. Bien por medio de fracciones continuas de Euler: $e = 2 + \cfrac{2}{2 + \cfrac{3}{3 + \cfrac{4}{4 + \cfrac{5}{5 + \cfrac{6}{6+\cdots}}}}}$; o con los factoriales de Euler: $e = \sum_{n=0}^{\infty} \frac{1}{n!}$.

Algunas parábolas

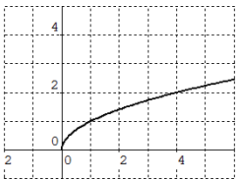
Como sabemos $y = x^2$ es una parábola (con $x \in \mathbb{R}$), pero no es el único tipo… también lo son $y = x^3$, $y = \sqrt{x}$, $y = \sqrt[3]{x}$, y $y = x^{\frac{2}{3}}$. Veamos…



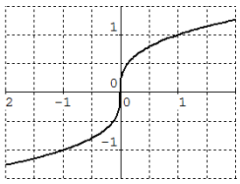
$y = x^2$



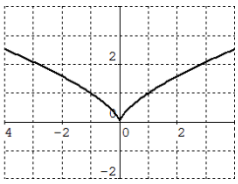
$y = x^3$



$y = \sqrt{x}$



$y = \sqrt[3]{x}$

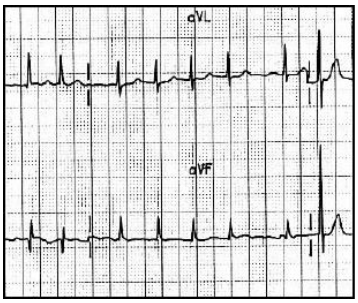


$y = x^{\frac{2}{3}}$

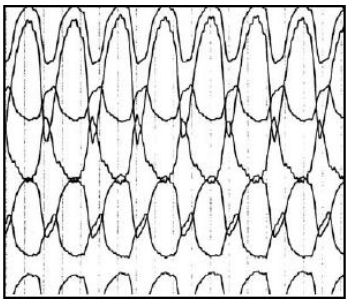
El electrocardiograma

El registro de la actividad eléctrica del corazón en función del tiempo, a través de un electrocardiograma, aporta información importante sobre diversas afecciones y/o lesiones cardíacas, las cuales pueden reconocerse por el comportamiento de la curva (y su comparación con las que corresponden a estudios clínicos de referencia). En con-

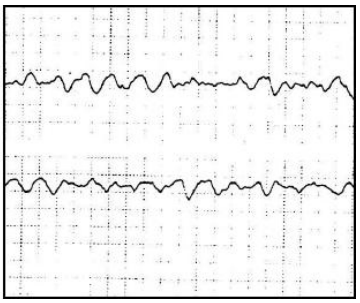
diciones normales, pero también en el caso de ciertas cardiopatías, esta función es periódica; es decir, existe un intervalo para el cual la curva repite el patrón indefinidamente.



fibrilación auricular



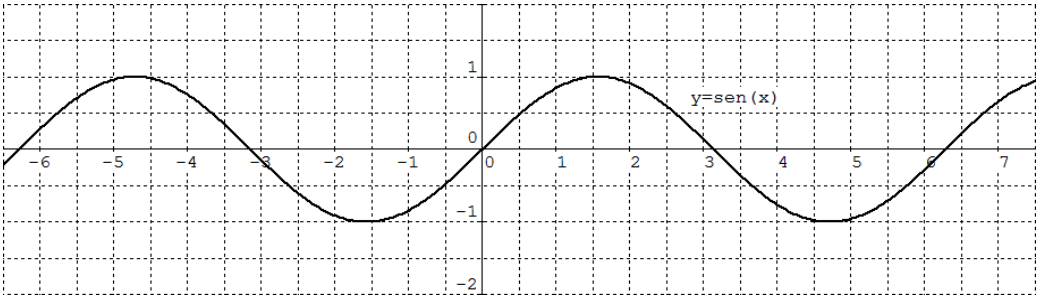
taquicardia ventricular



fibrilación ventricular

1. ¿Es la distancia de puntos en $\mathbb{R}^3$, definida de forma canónica, una función? Argumente su respuesta.
2. Muestre funciones biyectivas entre los siguientes conjuntos
   a) $A=\{X:\ X\subset U\}$ y $B=\{f: U\to\{0,1\}\,|\,f\ es\ función\}$ donde $U=\{a,b,c\}$
   b) $A=\{x\in\mathbb{R}:\ 0<x<1\}$ y $B=\{x\in\mathbb{R}:\ 0<x<1\}\times\{x\in\mathbb{R}:\ 0<x<1\}$
3. Demostrar que si *A* es finito y *B* es subconjunto de *A* entonces *B* es finito.
4. Pruebe que los siguientes conjuntos no son enumerables:
   - El conjunto de los números reales comprendidos entre 0 y 1
   - El conjunto de todas las funciones de $\mathbb{N}$ en $\{0,1\}$
   - Todas las funciones de $\mathbb{N}$ en $\{0,1,...,m-1\}$
   - Los subconjuntos de $\mathbb{N}$.
5. ¿Son equipotentes los conjuntos $B=\{x\in R:\ 0\le x<1\}$ y $A=\{x\in\mathbb{R}:\ 5<x\le 7\}$.

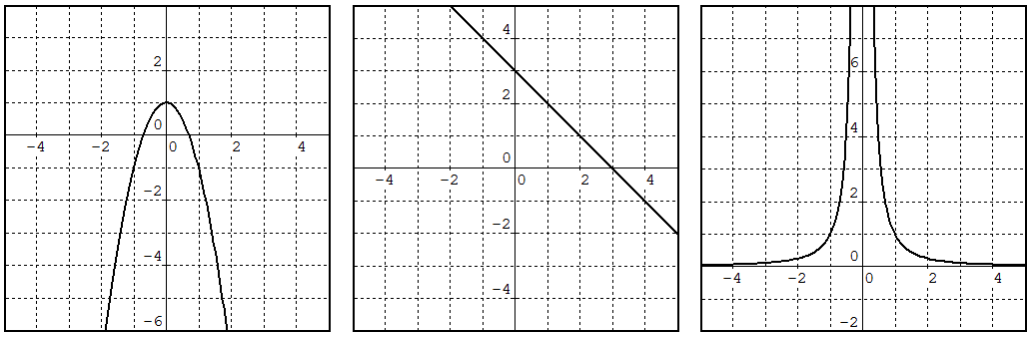
6. Muestre ejemplos de funciones estrictamente crecientes y decrecientes, no-crecientes y no-decrecientes. La imagen directa de su dominio, ¿tiene máximo? ¿y mínimo?
7. ¿Es creciente, decreciente, no-creciente, o no-decreciente la función $g:\mathbb{R}\to[-1,1]$ definida por $g(x)=sen\,x$? ¿Tiene máximo? ¿Y mínimo?



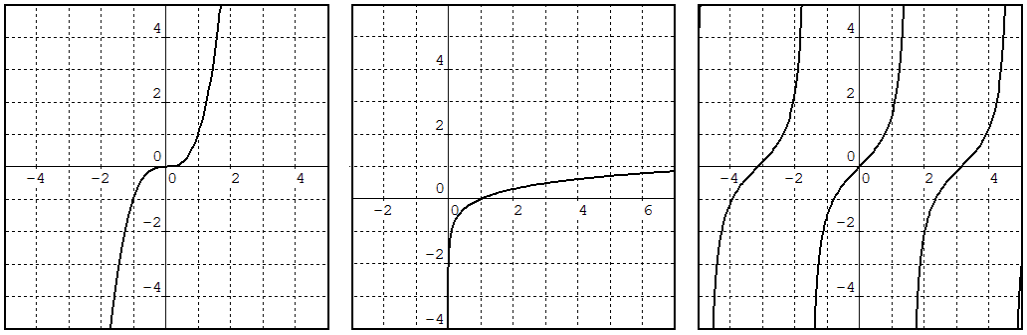
Función seno de x

8. ¿Son las funciones $f:\mathbb{R}\to\mathbb{R}^+$ definida por $f(x)=e^x$, y $f^{-1}:\mathbb{R}^+\to\mathbb{R}$ definida por $f^{-1}(x)=\ln x$, pares? ¿son impares? Argumente su respuesta.
9. Haga lo mismo para las funciones reales $g:\mathbb{R}\to\mathbb{R}$
   - $g(x)=-\sqrt{2}$
   - $g(x)=3x^5-5x^3$
   - $g(x)=|x|-1$

   Además, dé una idea gráfica de cada una.
10. ¿Cuáles de las siguientes curvas se asocian a funciones pares (impares o ninguna de éstas)?



(a) (b) (c)



(d) (e) (f)

11. ¿Cuál es la regla y cuáles son los conjuntos de definición que se corresponden con cada una las gráficas del problema anterior? ¿Son crecientes, decrecientes, no-crecientes, o no-decrecientes? ¿Tienen máximo(s)? ¿Y mínimo(s)?
12. Dé un contraejemplo de $f(X)-f(Y)\supset f(X-Y)$, con f una función, $f:A\to B$, y $X,Y\subset A$. (falsedad del recíproco de la propiedad 4).
13. Probar la propiedad 5(a).
14. Probar la propiedad 6(b).
15. Al colgar un cable entre dos postes, su forma se relaciona con el número *e*. De hecho, se aproxima a la gráfica de $y=\dfrac{e^{x}+e^{-x}}{2}$. Sin apoyo en algún software, idee un método para construir esta gráfica.
16. Haga lo mismo en el caso de la función $y=\dfrac{sen\ x}{x}$.

1. Es una función definida desde $\mathbb{R}^3 \times \mathbb{R}^3$ a los reales positivos.
2. Sugerencia: El problema no es complicado si se entiende la idea del mismo: dar un subconjunto *A* de *U* es lo mismo que dar una función de *U* en {0,1}, la función toma el valor 1 en *a* si y sólo si *a* está en *A*(verdad) y toma el valor 0 en caso contrario. Por ejemplo si $A=\{a,b\}$ entonces $f(a)=f(b)=1$ pero $f(c)=0$. Intente ahora resiolver el ejercicio.
3. Si *B* es infinito podemos encontrar una sucesión de elementos en *B* $x_1, x_2, \cdots$ que son distintos dos a dos. La construcción de tal sucesión e ssencilla, si *B* es infinito debe tener algún elemento, digamos x_1. Saquemos este elemento x_1 de *B* y obtenemos un conjunto que tiene elementos, de lo contrario *B* fuese un conjunto unitario, llamemos x_2 x_2 a ese elemento, y continuamos este proceso. Pero dicha sucesión de infintos elementos está contenida también en *A*, luego *A* es un conjunto infinito, una contradicción.
4. Voy a explicar solamente que no es numerable el conjunto de todas las funciones de $\mathbb{N}$ en $\{0,1\}$.

   Usaremos un argumento diagonal, supongamos lo contrario, que podemos enumerar todas las funciones como

   $$f_1, f_2, f_3, \cdots$$

   Definimos una nueva función *g* por medio de la regla

   $$g(0) \neq f_1(0)$$
   $$g(1) \neq f_2(1)$$
   $$\vdots$$

Claramente *g* se puede construir, la pregunta es ¿dónde esta *g* en la sucesión

$$f_1, f_2, f_3, \cdots$$

Si fuese el término

$$f_k$$

Entonces

$$g = f_k \text{ y}$$
$$g(k-1) = f_k(k-1)$$

Pero, por construcción

$$g(k-1) \neq f_k(k-1)$$

Lo cual es absurdo.

UNIDAD 3

Funciones

Un aspecto de la contaminación del aire. Fuente: Correo del Orinoco.

 **Semana 4**

 Aplicar el concepto de función en la resolución de problemas, en el modelado matemático y en la demostración de nuevos resultados.

Contenidos a tratar: Modelación con funciones.

4.1 Introducción

Ciertas funciones pueden sustentar la comprensión de fenómenos importantes que afectan a la localidad o región, e incluso, en ámbitos más amplios, así como la toma de decisiones y la acción al respecto; y naturalmente los que tienen que ver con otras áreas del conocimiento. En esta semana encontraremos funciones, siempre que sea posible, que se ajustan a un conjunto de datos tomados de la realidad.

4.2 Tomando datos

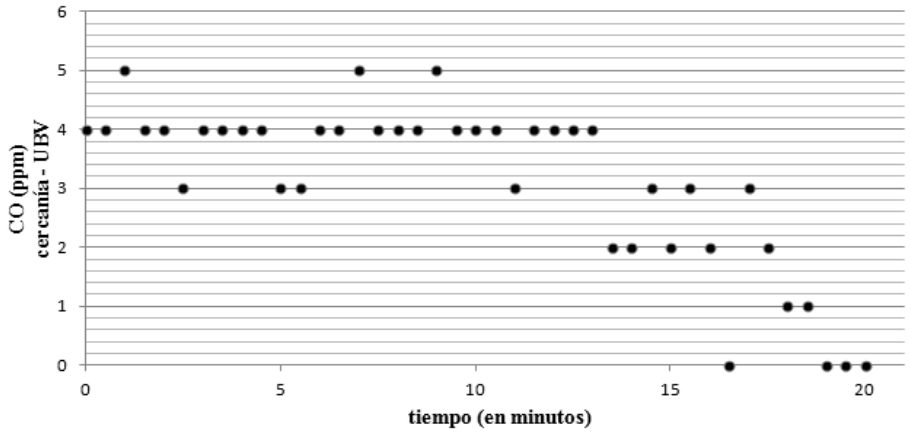
A – Concentración de monóxido de Carbono (CO) en el aire. Los datos que siguen se tomaron con un medidor digital de CO en partes por millón (ppm) (sensor que da valores enteros entre 0 y 1000.) en dos puntos cercanos a la UBV de Los Chaguaramos, Caracas el 12 de diciembre de 2011: (1) en la acera lateral a su entrada principal y (2) en el nivel 2 del estacionamiento colindante. El sensor se dispuso lejos de las fuentes fijas de emisión y copiamos valores cada 30 segundos por un espacio de 20 minutos. Adicionalmente, se calculó la proporción de vehículos por minuto que fluyeron por cada uno de los puntos de obtención de datos. Nota: Los estudios especializados obtienen también datos de temperatura ambiente, humedad, presión, pluviometría, velocidad del viento y radiación solar, durante períodos que pueden alcanzar todo el verano o el invierno, con tiempos de muestreo recomendados de unas 8 horas. En la tabla: T: Tiempo (en minutos); B: niveles de concentración de CO en el aire (acera que comunica la UBV con el CC Los Chaguaramos, a 6 *m* del paso vehicular); y C: niveles de concentración de CO en el aire (estacionamiento colindante con la UBV, nivel E2). En la tabla la concentración 0 no indica necesariamente la ausencia de CO en el aire, pues aquí interviene la fidelidad del instrumento empleado.

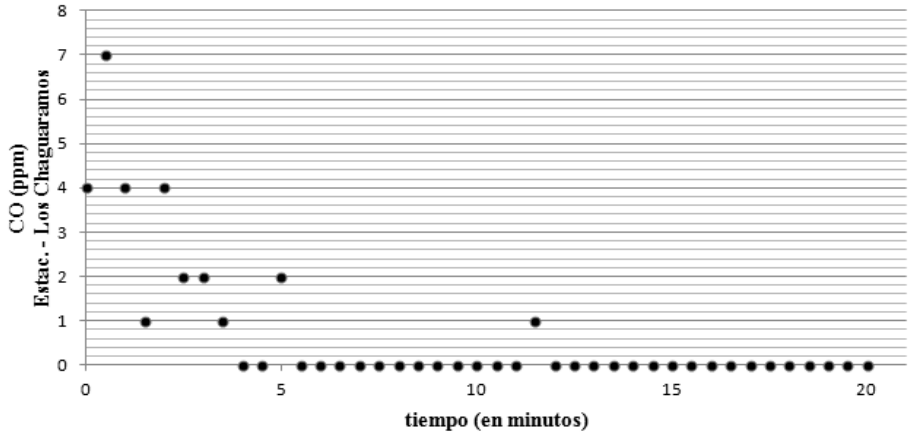
T	B	C	T	B	C
0	4	4	10	4	0
0,5	4	7	10,5	4	0
1	5	4	11	3	0
1,5	4	1	11,5	4	1
2	4	4	12	4	0
2,5	3	2	12,5	4	0
3	4	2	13	4	0
3,5	4	1	13,5	2	0
4	4	0	14	2	0
4,5	4	0	14,5	3	0
5	3	2	15	2	0
5,5	3	0	15,5	3	0
6	4	0	16	2	0

6,5	4	0	16,5	0	0
7	5	0	17	3	0
7,5	4	0	17,5	2	0
8	4	0	18	1	0
8,5	4	0	18,5	1	0
9	5	0	19	0	0
9,5	4	0	19,5	0	0
			20	0	0

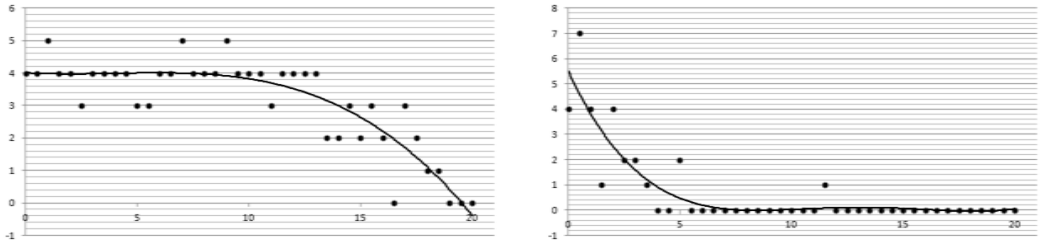
Con estos datos construimos los gráficos siguientes. En ellos observamos que el mínimo fue 0 y el máximo 12 y 7, respectivamente. Es importante destacar que en el primer caso el flujo fue de 29 vehículos/min, en cambio, en el segundo caso (nivel E2 del estacionamiento), este flujo fue de 2 vehículos/min.

Ahora bien, **¿qué curva o función describe el comportamiento de estos datos?** De hecho, es un problema matemático importante. Si hubiese una alta dispersión de los datos, lo que puede apreciarse luego de construir el gráfico correspondiente, no tendría sentido encontrar tal curva o función, pues no sería un buen modelo para proyectar el comportamiento del fenómeno o problema en un intervalo mayor que el dado por los datos.



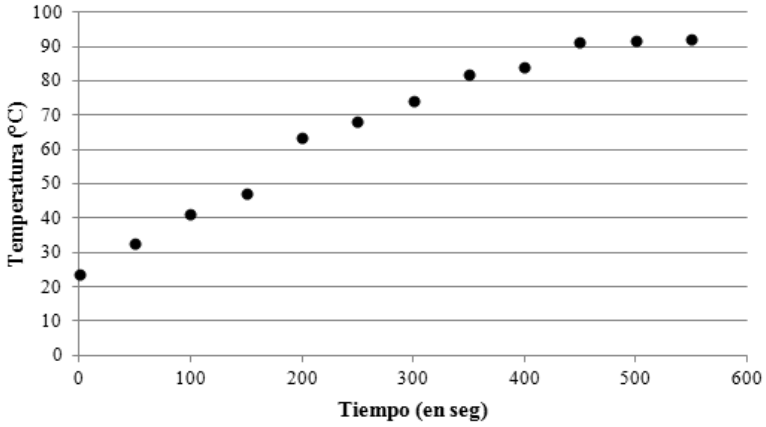


Con este primer ejemplo, sólo mostraremos gráficamente dos de los polinomios que se aproximan a tales comportamientos:



Ya en el que sigue, estudiaremos cómo obtener tales ajustes.

B – Ebullición del agua. En la experiencia que sigue, hemos tomado datos sobre la temperatura de cierta cantidad de agua con algunas sales minerales al exponerla a una fuente de calor aproximadamente constante. Empleamos un medidor de temperatura infrarrojo (sin contacto) y tomamos medidas cada 50 segundos (ver la tabla que sigue).



x_i	y_i
T	°C
0	23,7
50	32,7
100	41,2
150	47,4
200	63,3
250	68,1
300	74
350	82
400	83,9
450	91,2
500	91,6
550	92,1

Con base en gráfico de dispersión correspondiente, **interesa encontrar una curva que se ajuste (aproxime) a este comportamiento de los datos**, esto es, encontraremos una expresión del tipo

$$y = a + bx + cx^2$$

Para ello procederemos como sigue.

(1) Si los puntos estuvieran en una misma parábola (lo que experimentalmente es muy poco probable, entonces se cumpliría que:

$$\begin{aligned} y_1 &= a + bx_1 + cx_1^{\,2} \\ y_2 &= a + bx_2 + cx_2^{\,2} \\ &\vdots \\ y_{12} &= a + bx_{12} + cx_{12}^{\,2} \end{aligned}$$

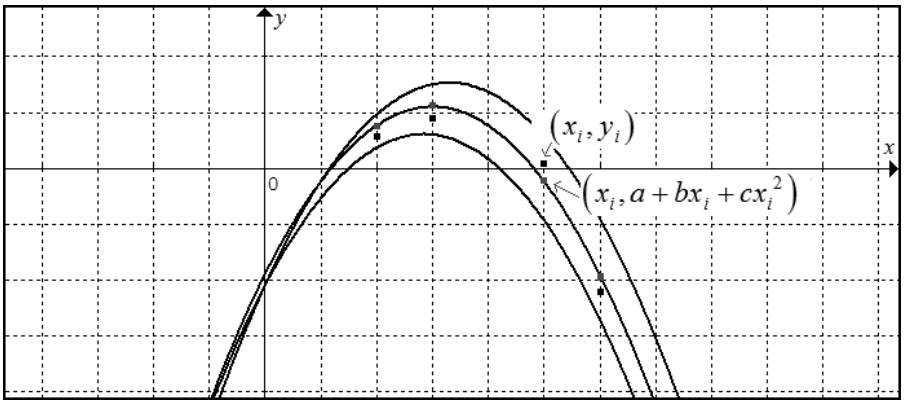
$$\text{Y con } y=\begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_{12} \end{bmatrix},\ A=\begin{bmatrix} 1 & x_1 & x_1^{\,2} \\ 1 & x_2 & x_2^{\,2} \\ \vdots & \vdots & \vdots \\ 1 & x_{12} & x_{12}^{\,2} \end{bmatrix}\ y\ \ w=\begin{bmatrix} a \\ b \\ c \end{bmatrix}$$

Este sistema se puede escribirse en forma matricial así

$$\begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_{12} \end{bmatrix}=\begin{bmatrix} 1 & x_1 & x_1^{\,2} \\ 1 & x_2 & x_2^{\,2} \\ \vdots & \vdots & \vdots \\ 1 & x_{12} & x_{12}^{\,2} \end{bmatrix}\begin{bmatrix} a \\ b \\ c \end{bmatrix}$$

En tal caso $y - Aw = 0$. Así, este sistema tendría solución.

(2) Pero en una *dispersión*, los puntos (x_i, y_i) no están todos en una misma parábola. Además, es posible que existan varias e incluso infinitas parábolas que se aproximen al comportamiento de los datos que tenemos (ver el gráfico que sigue). En el gráfico, (x_i, y_i) representa uno de los datos obtenidos (son los puntos de la dispersión). Y $\left(x_i, a + bx_i + cx_i^{\,2}\right)$ representa al punto, con la misma abscisa que (x_i, y_i), correspondiente a una de las parábolas que se aproximan a la dispersión. Entonces resulta relevante la pregunta ¿cómo escoger la parábola que mejor se ajuste a estos puntos? ¿Cuál es el criterio para su selección?



Recordemos que la distancia en $\mathbb{R}^2$ entre dos puntos (p_1, q_1) y (p_2, q_2) es $d = \sqrt{(p_1 - p_2)^2 + (q_1 - q_2)^2}$. Observemos que

$$d_{(x_1, y_1)\left(x_1, a+bx_1+cx_1^2\right)} = \sqrt{(x_1 - x_1)^2 + \left(y_1 - \left(a + bx_1 + cx_1^2\right)\right)^2}$$

$$= \sqrt{0 + \left(y_1 - \left(a + bx_1 + cx_1^2\right)\right)^2}$$

$$= y_1 - \left(a + bx_1 + cx_1^2\right)$$

Por tanto, resulta lógico suponer que el mejor ajuste (o aproximación) se obtiene cuando la suma de las distancias entre (x_i, y_i) y $\left(x_i, a + bx_i + cx_i^2\right)$ es mínima. Lo que equivale a encontrar la parábola que verifique que la suma

$$\left[y_1 - \left(a + bx_1 + cx_1^2\right)\right]^2 + \left[y_2 - \left(a + bx_2 + cx_2^2\right)\right]^2 + \cdots + \left[y_{12} - \left(a + bx_{12} + cx_{12}^2\right)\right]^2$$

sea mínima.

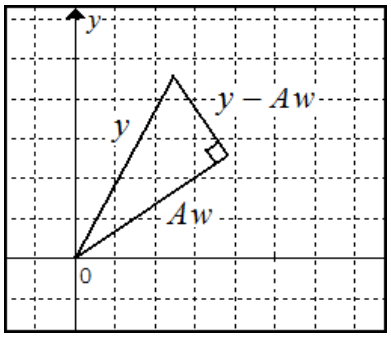
Los valores *a*, *b* y *c* que hacen mínima esta suma, harán que $y = a + bx + cx^2$ sea el ajuste (por medio de una parábola) a los puntos $(x_1, y_1), (x_2, y_2), \ldots, (x_{12}, y_{12})$.

Una observación: el lector advertirá que los cuadrados en $\left[y_i - \left(a + bx_i + cx_i^2\right)\right]^2$ hacen que cada sumando sea positivo, lo cual nos permite analizar la suma total.
Ahora bien, ¿cómo encontrar tales valores de *a*, *b* y *c*? Como $y - Aw = 0$, el problema que tenemos es el mismo que el de encontrar un vector $w = \begin{bmatrix} a \\ b \\ c \end{bmatrix}$ que haga mínima la norma $\|y - Aw\|$. ¿Qué relación hay entre $y - Aw$ y Aw? Para visualizar esto, supongamos que *n*=2. En $\mathbb{R}^2$, Aw representa un vector (en una recta que pasa por el

origen). Igual pasa con *y*. ¡Ya con el gráfico es fácil ver que $\|y - Aw\|$ es mínima cuando $y - Aw$ y Aw son ortogonales!

Es decir,

$$0 = Aw \cdot (y - Aw)$$



(Si son ortogonales su producto escalar es cero). Esta ecuación nos permitirá encontrar a *w*:

$$\begin{aligned} 0 &= (Aw)^T \cdot (y - Aw) \\ &= w^T A^T (y - Aw) \\ &= w^T (A^T y - A^T Aw) \end{aligned}$$

¿Qué argumentos usamos? Ahora como $c \neq 0$ (pues la ecuación $y = a + bx + cx^2$ es de grado 2), entonces ni *w* ni su traspuesta, w^T, son cero –fíjese que al menos $c \neq 0$. En consecuencia,

$$A^T y - A^T Aw = 0$$

Con lo cual

$$\begin{aligned} -A^T Aw &= -A^T y \\ A^T Aw &= A^T y \end{aligned}$$

Y finalmente, $w = (A^T A)^{-1} A^T y$ siempre que $A^T A$ tenga inversa.

Con la relación anterior estamos en condiciones de encontrar *w* en nuestro caso. Así,

$$y = \begin{bmatrix} 23,7 \\ 32,7 \\ 41,2 \\ 47,4 \\ 63,3 \\ 68,1 \\ 74 \\ 82 \\ 83,9 \\ 91,2 \\ 91,6 \\ 92,1 \end{bmatrix}, \quad A = \begin{bmatrix} 1 & 0 & 0^2 \\ 1 & 50 & 50^2 \\ 1 & 100 & 100^2 \\ 1 & 150 & 150^2 \\ 1 & 200 & 200^2 \\ 1 & 250 & 250^2 \\ 1 & 300 & 300^2 \\ 1 & 350 & 350^2 \\ 1 & 400 & 400^2 \\ 1 & 450 & 450^2 \\ 1 & 500 & 500^2 \\ 1 & 550 & 550^2 \end{bmatrix}, \quad w = \begin{bmatrix} a \\ b \\ c \end{bmatrix}$$

Por tanto (aquí nos apoyamos en un *paquete libre* –disponibles en la *red*)

$$w = \left(\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 50 & 100 & 150 & 200 & 250 & 300 & 350 & 400 & 450 & 500 & 550 \\ 0^2 & 50^2 & 100^2 & 150^2 & 200^2 & 250^2 & 300^2 & 350^2 & 400^2 & 450^2 & 500^2 & 550^2 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0^2 \\ 1 & 50 & 50^2 \\ 1 & 100 & 100^2 \\ 1 & 150 & 150^2 \\ 1 & 200 & 200^2 \\ 1 & 250 & 250^2 \\ 1 & 300 & 300^2 \\ 1 & 350 & 350^2 \\ 1 & 400 & 400^2 \\ 1 & 450 & 450^2 \\ 1 & 500 & 500^2 \\ 1 & 550 & 550^2 \end{bmatrix} \right)^{-1} A^T y$$

$$= \begin{bmatrix} 12 & 3300 & 1040000 \\ 3300 & 1265000 & 432000000 \\ 1040000 & 432000000 & 187962500000 \end{bmatrix}^{-1} A^T y$$

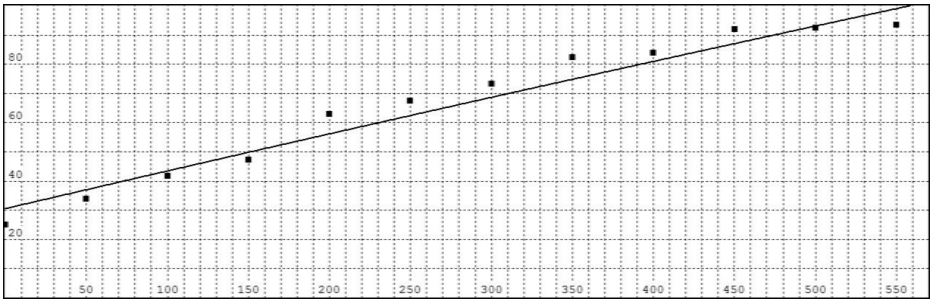
$$= \begin{bmatrix} \frac{818377}{2622322} & -\frac{136797}{131116100} & \frac{22}{32779025} \\ -\frac{136797}{131116100} & \frac{23479}{3277902500} & -\frac{219}{20486890625} \\ \frac{22}{32779025} & -\frac{219}{20486890625} & \frac{429}{16389512500000} \end{bmatrix} A^T y$$

$$= \begin{bmatrix} \frac{818377}{2622322} & \frac{342990}{1311161} & \frac{562383}{2622322} & \frac{223793}{1311161} & \frac{341589}{2622322} & \frac{122196}{1311161} & \frac{155995}{2622322} & \frac{38199}{1311161} & \frac{5601}{2622322} & -\frac{1226}{57007} & -\frac{505593}{2622322} & -\frac{76995}{1311161} \\ -\frac{136797}{131116100} & -\frac{93343}{131116100} & -\frac{56897}{131116100} & -\frac{27459}{131116100} & -\frac{5029}{131116100} & \frac{10393}{131116100} & \frac{18807}{131116100} & \frac{20213}{131116100} & \frac{14611}{131116100} & \frac{87}{5700700} & \frac{297743}{131116100} & -\frac{44243}{131116100} \\ \frac{22}{32779025} & \frac{53}{262232200} & -\frac{223}{1638951250} & -\frac{2251}{6555805000} & -\frac{344}{819475625} & -\frac{479}{1311161000} & -\frac{59}{327790250} & \frac{893}{6555805000} & \frac{478}{819475625} & \frac{331}{285035000} & -\frac{527}{131116100} & \frac{3553}{1311161000} \end{bmatrix} y$$

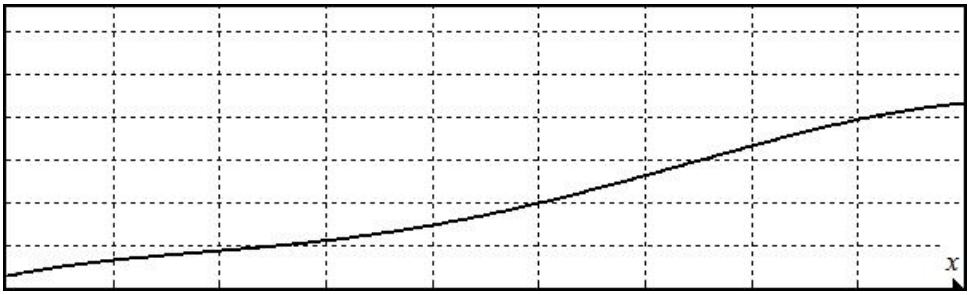
$$= \begin{bmatrix} 30,5320055660593966 \\ 0,134330238620581271 \\ -0,0000143017829236836877 \end{bmatrix}$$

$$\begin{bmatrix} 30{,}532 \\ 0{,}13433 \\ -0{,}00001 \end{bmatrix}$$

Observe que no hemos escrito la igualdad con respecto a la última matriz, pues allí sólo tomamos cinco decimales.



Gráfica de $y = 30{,}532 + 0{,}13433x - 0{,}00001x^2$



Modelo teórico para la temperatura de una solución de agua y sales

Algunos comentarios de cierre: (a) Con un mayor número de datos y acortando el intervalo de obtención de medidas para la temperatura del agua con sales, puede apreciarse un comportamiento como el que sigue –donde el proceso de disolución de las sales ralentiza la evolución de la temperatura. (b) Por otra parte, el método que se ha mostrado aquí se denomina **estimación por mínimos cuadrados**. (c) Dado un conjunto de datos de los cuales observamos que se pueden ajustar con una curva del tipo $y = a + bx + cx^2$, ¿cómo saber si se encuentran en una misma parábola? Tal como dijimos en (1), simplemente comprobamos si el sistema

$$\begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_{12} \end{bmatrix} = \begin{bmatrix} 1 & x_1 & x_1^{\,2} \\ 1 & x_2 & x_2^{\,2} \\ \vdots & \vdots & \vdots \\ 1 & x_{12} & x_{12}^{\,2} \end{bmatrix} \begin{bmatrix} a \\ b \\ c \end{bmatrix}$$

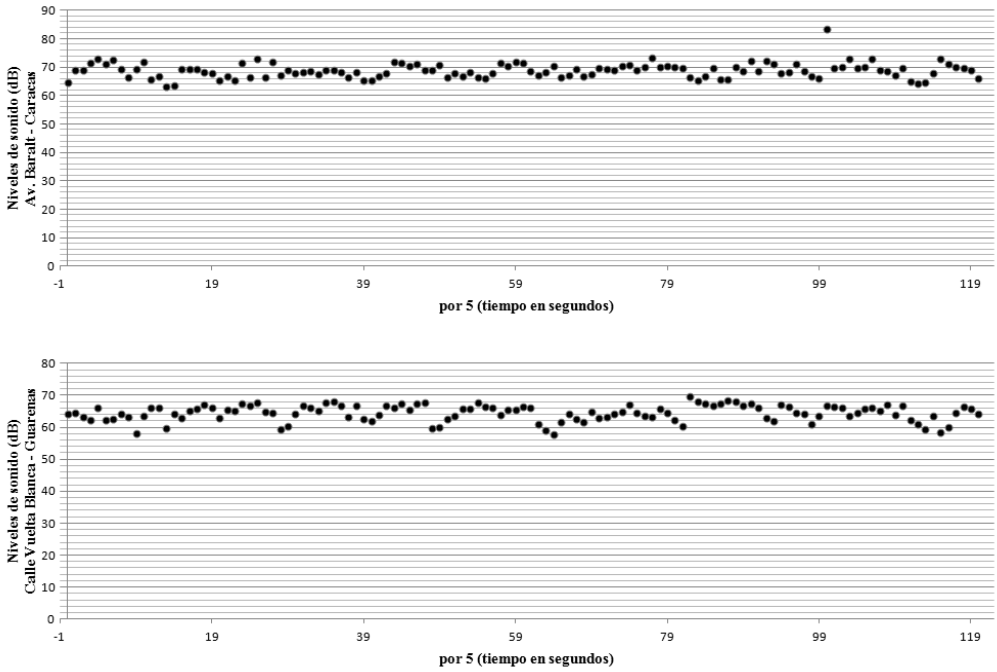
tiene solución. Si la tiene, significa que hay sólo una parábola que pasa por tales puntos (siempre que tengamos al menos tres puntos y el eje de la parábola sea paralelo al eje *y*). Si no la tiene, entonces debemos encontrar un ajuste, tal como hicimos en (2). (d) una función ajuste representa una aproximación a la dispersión de datos en el dominio $[x_1, x_n]$, donde x_1 y x_n son la menor y la mayor coordenada *x* de los datos. Fuera de este intervalo la función puede no comportarse como en los modelos teóricos conocidos del problema o fenómeno estudiado.

C – Niveles de sonido ambiente. La tabla adjunta muestra los datos sobre la intensidad de sonido (en decibeles –dB) en dos puntos: uno de ellos ubicado en una zona residencial/comercial (Avenida Baralt, Caracas) y el otro está en una zona residencial (Calle Vuelta Blanca, Guarenas). El instrumento utilizado tiene un rango de 30-130 dB con un margen de fidelidad de $\pm 1{,}5$ dB. Las tomas se hicieron cada cinco segundos. En el primer caso se llevó a cabo desde las 10:12 a.m. y en el segundo desde las 4:30 p.m. Al mismo tiempo se calculó la densidad vehicular (52 vehículos/min y 2 vehículos/min, respectivamente). En la tabla, al multiplicar cada valor de la columna 1 por 5, tendremos el tiempo en segundos; las columnas 2 y 3 corresponden con los datos para el primer y segundo punto de muestreo.

0	64,6	64,2	41	66,9	64	82	66,4	69,6
1	68,8	64,4	42	67,7	66,8	83	65,2	68,1
2	69,1	63,1	43	71,9	66,2	84	66,7	67,4
3	71,5	62,2	44	71,4	67,4	85	69,6	66,8
4	73	66,1	45	70,4	65,6	86	65,7	67,3
5	71,2	62,2	46	71,1	67,5	87	65,7	68,3
6	72,6	62,7	47	69	67,7	88	70,2	68

7	69,4	64,1	48	68,8	59,8	89	68,6	66,7
8	66,3	63,1	49	70,6	59,9	90	72,3	67,3
9	69,2	58	50	66,5	62,6	91	68,5	66,2
10	72	63,4	51	67,8	63,6	92	72,2	63
11	65,8	66,2	52	66,7	65,9	93	71	62,1
12	66,9	66	53	68,1	65,7	94	67,8	67,1
13	63,2	59,8	54	66,5	67,6	95	68,1	66,3
14	63,6	64,1	55	66	66,4	96	71,3	64,6
15	69,4	62,8	56	67,9	66,1	97	68,5	64,2
16	69,5	65,3	57	71,4	63,8	98	66,7	60,9
17	69,3	65,7	58	70,5	65,5	99	66,2	63,6
18	68,1	67	59	71,7	65,6	100	83,6	66,7
19	68	66,2	60	71,5	66,3	101	69,8	66,5
20	65,5	63	61	68,7	66,1	102	70,2	66,2
21	66,9	65,5	62	67,2	60,9	103	72,8	63,5
22	65,5	65,3	63	68,2	59,1	104	69,8	64,6
23	71,5	67,4	64	70,4	57,8	105	69,9	65,7
24	66,6	66,7	65	66,5	61,6	106	73	66
25	73,1	67,6	66	67,2	64,3	107	68,9	65,3
26	66,5	64,9	67	69,5	62,6	108	68,6	67,1
27	72	64,6	68	66,7	61,5	109	67,3	63,9
28	67	59,3	69	67,5	64,8	110	69,8	66,8
29	68,8	60,2	70	69,6	62,8	111	65	62,3
30	67,9	64,1	71	69,4	63,1	112	64,2	61,1
31	68,3	66,8	72	69,1	64,1	113	64,8	59,3
32	68,7	66	73	70,3	64,7	114	68	63,7
33	67,6	65,3	74	70,9	67	115	72,8	58,4
34	68,8	67,8	75	68,9	64,4	116	71,3	59,9
35	69	68,1	76	70,1	63,4	117	70,1	64,4
36	68,4	66,6	77	73,4	63,2	118	69,6	66,3
37	66,5	63,1	78	70,2	65,8	119	69,1	65,7
38	68,2	66,6	79	70,4	64,4	120	66,2	64,3
39	65,3	62,7	80	70	62,2	82	66,4	69,6
40	65,4	61,8	81	69,7	60,4	83	65,2	68,1

Sus gráficas de dispersión son:



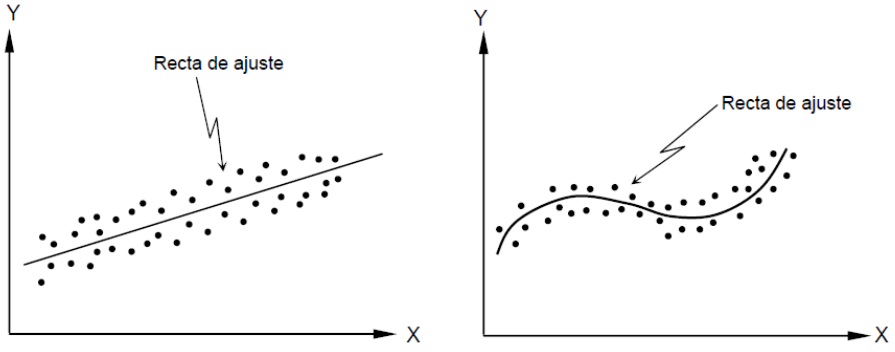
Aquí, **en vez de encontrar un ajuste (debido a la alta dispersión, interesa más bien acotar las mediciones obtenidas; esto es, exponer el o los intervalos del eje *y* en los que se encuentren imágenes de tal relación** (valores mínimos y máximos). En nuestro caso, son $[63.2, 83.6]$ y $[57.8, 69.6]$, respectivamente. Un comentario: En vez de $[63.2, 83.6]$, se pudo tomar (considerando que el máximo 83.6 quizás sea un caso aislado –atípico), el intervalo $[63.2, 73.4]$. Ya con esto hay elementos para comparar el nivel de ruido en estos dos puntos geográficos, en especial si se consideran proporciones como la densidad de tránsito vehicular, las horas en que se tomaron las mediciones, etc.

1. Suponga al ver el gráfico de dispersión de *n* mediciones de cierto fenómeno o problema, éstos tienen un comportamiento aproximadamente lineal. ¿Cómo encontrar la recta que dé el mejor ajuste a tal dispersión?

2. Exponga los argumentos empleados para las deducciones en el ejemplo B.
3. En los casos siguientes (siempre referidos a Venezuela), busque datos en el intervalo que considere, construya el gráfico de dispersión y encuentre el mejor ajuste (si tiene sentido hacerlo):
   (a) Población
   (b) Pobreza extrema en nuestro país
   (c) Casos de dengue en la localidad
   (d) Producto interno bruto
   (e) Número de miembros de una especie en peligro de extinción
   (f) Densidad vehicular a lo largo de un día en un punto de la ciudad
   (g) Otro que considere relevante para su localidad.
   (h) Nivel de la marea, de un río o lago.

1. Si se trata del modelo lineal, entonces la gráfica es una recta que se llamará

Recta de ajuste o **Recta de regresión**. En todo caso, los puntos registrados en el diagrama de dispersión sugieren el tipo de función de regresión que se debe utilizar.



- Desde luego que, encontrar la expresión de esta función, no siempre es sencillo, por lo que, se propone como una buena alternativa el modelo de la ecuación lineal:

$$y=a+bx$$

Ahora:

¿Cuáles son los parámetros **a** y **b** que determinan una función lineal?

¿Cómo encontrar las rectas de ajuste para un problema en particular?

¿Qué criterio se debe utilizar para asegurar la recta de mejor ajuste?

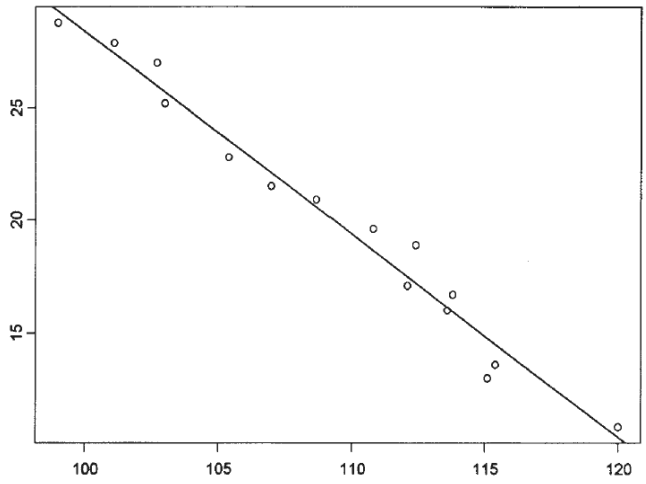
Para hallar la **Recta de regresión**, se usará el **Método de Mínimos Cuadrados**, en los cálculos, se utilizarán los valores cuadráticos x^2, y^2 , xy, así como también las sumatorias correspondientes Σx_i , Σy_i , $\Sigma x_i{}^2$, $\Sigma y_i{}^2$, $\Sigma x_i y_i$, así que:

$$y = \frac{\sum y}{n} - \left(\left(\frac{n\sum xy - (\sum x)(\sum y)}{n\sum x^2 - (\sum x)^2}\right)\left(\frac{\sum x}{n}\right)\right) + \left(\frac{n\sum xy - (\sum x)(\sum y)}{n\sum x^2 - (\sum x)^2}\right)x$$

- Para un ensayo científico realizado en comunidades endémicas por paludismo, se empleó un análisis de mínimos cuadrados para estudiar cómo los efectos secundarios ***y*** (en términos de porcentaje) están asociados al ***x*** consumo de Cloroquina en los pacientes. Se presentaron los siguientes datos:

Obs	*x*	*y*	x^2	*xy*	y^2
1	99.0	28.8	9 801.00	2851.20	829.44
2	101.1	27.9	10 221.21	2820.69	778.41
3	102.7	27.0	10 547.29	2772.90	729.00
4	103.0	25.2	10 609.00	2595.60	635.04
5	105.4	22.8	11 109.16	2403.12	519.84
6	107.0	21.5	11 449.00	2300.50	462.25
7	108.7	20.9	11 815.69	2271.83	436.81
8	110.8	19.6	12 276.64	2171.68	384.16
9	112.1	17.1	12 566.41	1916.91	292.41
10	112.4	18.9	12 633.76	2124.36	357.21
11	113.6	16.0	12 904.96	1817.60	256.00
12	113.8	16.7	12 950.44	1900.46	278.89
13	115.1	13.0	13 248.01	1496.30	169.00
14	115.4	13.6	13 317.16	1569.44	184.96
15	120.0	10.8	14 400.00	1296.00	116.64
Suma	1640.1	299.8	179 849.73	32 308.59	6430.06

Con ***b*****=** - 0.905 (justifique los cálculos) se estima que los efectos secundarios asociados con el consumo de Cloroquina es de - 0.905% (reducción de 0.905%). La ecuación de la línea de regresión estimada (línea de mínimos cuadrados) es entonces ***y*** =118.91 - 0.905***x***.



Para determinar cómo afecta la difusión de una onda ultrasónica en la resistencia de un producto para la construcción de viviendas, se consideraron los datos adjuntos sobre resistencia a la fractura (*x*, como porcentaje de resistencia a la tensión última) y atenuación (*y*, en neper/cm, onda de esfuerzo):

x	12	30	36	40	45	57	62	67	71	78	93	94	100	105
y	3.3	3.2	3.4	3.0	2.8	2.9	2.7	2.6	2.5	2.6	2.2	2.0	2.3	2.1

Según un modelo de regresión lineal simple, determine onda de esfuerzo para una resistencia del 50% del producto.

Aquí

$n = 14;\ \sum x_i = 890$; $\sum x_i^2 = 67182$; $\sum y_i = 37.6$; $\sum y_i^2 = 103.54$; $\sum x_i y_i = 2234.30$.

Se deja al estudiante el cálculo de:

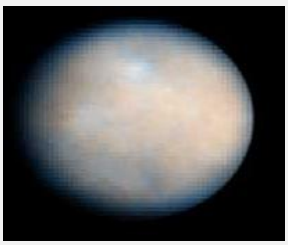
$$y = \frac{\sum y}{n} - \left(\left(\frac{n\sum xy - (\sum x)(\sum y)}{n\sum x^2 - (\sum x)^2}\right)\left(\frac{\sum x}{n}\right)\right) + \left(\frac{n\sum xy - (\sum x)(\sum y)}{n\sum x^2 - (\sum x)^2}\right)x$$

2. Queda a cargo del estudiante UNA.

3. La recolección y busqueda de los datos es labor de nuestro estudiante.

4.4 Algunas notas

El método de los mínimos cuadrados



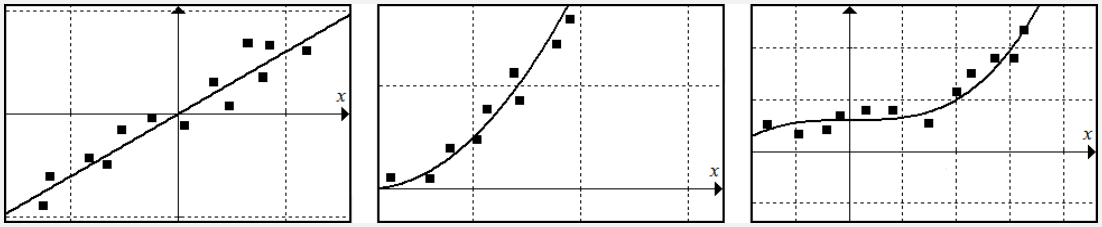
Luego de descubrirse el planeta enano *Ceres* (en 1801) y de compilarse datos sobre su órbita por un período de alrededor de 40 días, fue un problema muy difícil prede cir su trayectoria.

El método que permitió tal descripción fue el de los mínimos cuadrados, ideado por el destacado matemático Carl Friedrich Gauss cuando apenas tenía 18 años, aunque lo publicó algunos años después en *Theoria Motus Corporum Coelestium in sctionibus conicis solem ambientium.*

Legendre llegó al mismo método de manera independiente.

Curvas de ajuste

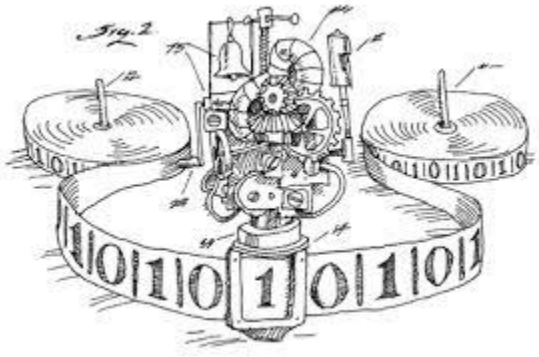
Los siguen se corresponden con ejemplos de ajuste lineal, cuadrático y cúbico para las dispersiones dadas.



1. Responda la cuestión 1 (de 4.3) en el caso que el comportamiento similar al de un polinomio de grado 3.
2. En el caso siguiente, busque datos en el intervalo que considere, construya el gráfico de dispersión y encuentre el mejor ajuste, si tiene sentido hacerlo:
   (a) Nacimientos vivos en madres menores de edad (en Venezuela).

UNIDAD 4

El número natural



Semana 6

Hablamos de puntos, rectas y planos pero pudimos hablar en su lugar de mesas, sillas y jarras de cerveza

David Hilbert

Aplicar el concepto de número natural y entero y sus propiedades en el modelado matemático y en la demostración de nuevos resultados

Contenidos a tratar: El número natural, el principio de inducción.

5.1 Introducción: Los axiomas y los objetos matemáticos

En los *Elementos* de Euclides encontramos la idea de nociones primitivas en matemática. "Punto es lo que no tiene partes" escribió el sabio de Alejandría. Esta definición es vaga y apela a lo sensorial. Por otro lado, nadie nos explica qué es una parte. Hilbert toma una posición diferente e importante respecto a definir los objetos matemáticos de una teoría. Para él *los axiomas caracterizan el comportamiento de los objetos matemáticos y por ende los definen.* Sucede lo mismo que en el ajedrez, un alfil

se mueve en diagonal y permanece en las casillas de un cierto color. Eso determina lo que llamamos alfil. No importa el nombre o la figura que usemos, el alfil queda determinado por la forma en como se mueve. En su famosa obra *Grundlagen der Geometrie*[1], Hilbert da una serie de axiomas que capturan las relaciones entre los objetos que llamamos punto, recta y plano. Pero no hace ninguna definición similar a la de Euclides de lo que es una recta o un punto. Euclides dijo: una recta es la curva que yace uniformemente respecto a los puntos que están en ella. Hilbert prefiere decir: dos puntos determinan unívocamente una recta. Es una manera de caracterizar los objetos matemáticos que no se basa en alusiones vagas o pictóricas.

La escogencia de los axiomas de una teoría matemática es importante. Nuestra analogía entre matemática y juego termina cuando pensamos en la relevancia y aplicaciones de la mayor parte de las matemáticas que conocemos. En el libro de Marshall Hall sobre la *Teoría de Grupos*, todo se construye a partir de tres axiomas. Ellos definen lo que llamamos un *grupo abstracto.* Dicho concepto tiene muchas aplicaciones e importancia, desde un punto de vista puramente matemático, y todo lo que conocemos de los grupos deriva de tres suposiciones o axiomas fundamentales. La labor de escoger los axiomas no proviene de una revelación o inspiración de algún matemático, es, usualmente, la labor de muchos hombres y pasa por un proceso de evolución y decantación histórica. De Euclides pasamos a Pfaff y de éste a la axiomática de Hilbert en su famosa obra *Grundlagen der Geometrie*. En el camino se descubre que ciertos axiomas propuestos por otros matemáticos son redundantes y se vela porque la teoría sea consistente, aunque probar esto último es muy difícil.

David Hilbert

[1] Disponible en books.google.co.ve en español con el título *Fundamentos de Geometría*

Las tres condiciones que Hilbert imponía a una axiomática son:

- **Independencia de los axiomas**: un axioma no debe ser consecuencia de los otros axiomas
- **Consistencia**: ninguna contradicción se puede derivar de nuestros axiomas
- **Completez**: todas las verdades matemáticas son consecuencia de los axiomas

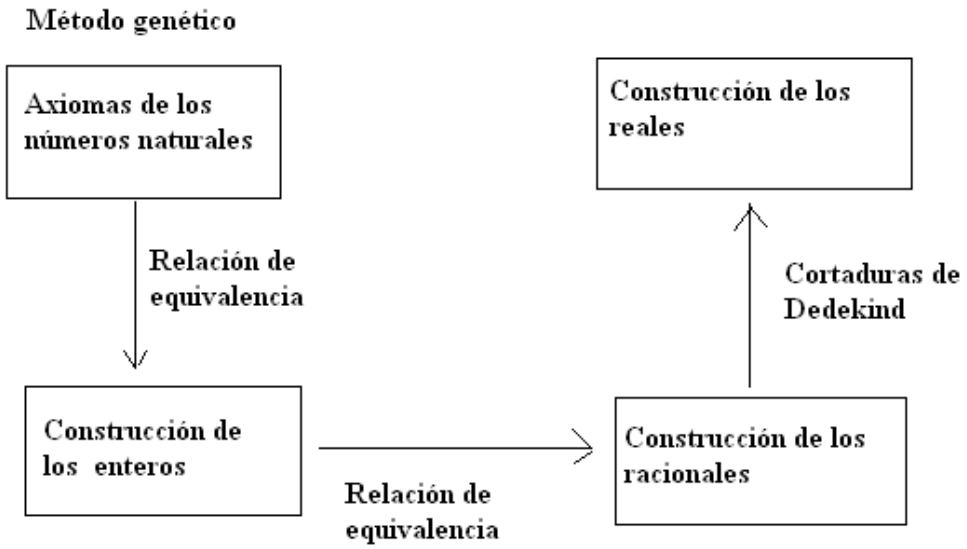
Las condiciones de Hilbert son imposibles de verificar en las axiomáticas suficientemente ricas para incluir a los números naturales, sin embargo el pensamiento hilbertiano condicionó la forma de estudio de las matemáticas durante todo el siglo XX.

5.2 Los axiomas de Peano y su significado

5.2.1 Introducción

Nosotros vamos a seguir el enfoque axiomático para introducir el concepto de número natural. De alguna manera Peano pensó que los axiomas que enunció en 1889 capturaban la esencia de lo que era un número natural y que determinaban de manera unívoca dicho conjunto. Similares axiomas habían sido dados por Dedekind un año antes.

Después, introduciremos los sistemas numéricos de los enteros y los números racionales de manera constructiva, edificando sobre el concepto de número natural y siguiendo la frase de Kronecker: Dios creó el número natural, lo demás es creación del hombre. Eso nos llevara a una construcción del grupo de los enteros y al cuerpo de los números racionales. Sin embargo, volveremos al final al enfoque axiomático para introducir el sistema de números reales como fue hecho por Hilbert alrededor de 1900. Pudimos continuar la construcción de los números reales $\mathbb{R}$ mediante el expediente de las cortaduras de Dedekind siguiendo lo que se conoce como el *método genético.*



Sin embargo, pensamos que el estudiante debe adquirir habilidades y destrezas en el manejo tanto del método axiomático como del método constructivo. Además, el estudiante de Matemática encontrará en el curso Historia de la Matemática (cod. 760), en su Guía Instruccional, una completa discusión de las cortaduras de Dedekind que complementan nuestra discusión del método genético de construcción de los números reales.

5.2.2 Axiomas de Peano sobre los números naturales

El conjunto de todos los números naturales lo denotaremos por $\mathbb{N}$. Cada axioma irá seguido por un comentario nuestro que pretende aclarar la idea que motiva el mismo.

El primer axioma de Peano es importante:

Axioma 1: 0 es un número natural.

Con ese axioma garantizamos que los números naturales es un conjunto no vacío, ya que al menos contiene al 0. Este axioma lo podemos escribir así $0 \in \mathbb{N}$.

Axioma 2: Todo número natural *k* tiene un sucesor que llamamos *s*(*k*).

El axioma es claro: 1 es *s*(0), 2 es *s*(1) y así sucesivamente. La operación de sucesor permite definir operaciones más complicadas como la suma o dar una noción de orden a los números naturales. Esto lo explicaremos luego. Es importante que la operación de sucesor esté definida unívocamente y esto lo garantiza nuestro axioma siguiente.

Axioma 3: Si el sucesor de *n* es igual al sucesor de *m* entonces *n*=*m*.

Precisamente, esto es lo que permite construir a partir de la operación de sucesor operaciones más complejas en los naturales. Este axioma establece que la función sucesor es inyectiva.

Axioma 4: 0 no es el sucesor de natural alguno.

Esto captura la idea de que 0 es el "primer natural" y que todos los demás siguen al cero por aplicación sucesiva de la operación de sucesor.

Axioma 5 (Principio de inducción completa): Sea *A* un subconjunto de los números naturales tal que:

1. **el 0 está en *A*.**
2. **Si *n* está en *A* entonces *s*(*n*) está en *A*. Entonces *A* es el conjunto de los números naturales $\mathbb{N}$.**

El último axioma es muy importante. Es en realidad el axioma que le da riqueza matemática a los números naturales. Constituye un recurso valioso para la demostración de proposiciones, la definición de objetos matemáticos y operaciones. Es conocido como el Principio de Inducción Matemática.

Giuseppe Peano (1858 – 1932) Matemático, filósofo y profesor italiano. Hombre de una personalidad polifacética, ideó un lenguaje con el que pretendía lograr la comunicación entre todos los hombres. Impulsó el uso de la lógica y simbología matemática. Construyó sistemas de axiomas para los espacios vectoriales, la geometría euclidea y el más famoso, el de los números naturales. Su uso del formalismo llevó a una revuelta estudiantil que causó su expulsión de la Academia Militar para pasar a la Universidad de Turín. Es importante su teorema de existencia de soluciones a ecuaciones diferenciales y su construcción de una curva que llena un cuadrado

Peano pensaba que estos axiomas resumen la esencia de los números naturales y que los caracterizan. Nosotros vamos a suponer que los números naturales quedan determinados por los postulados de Peano y que existe un conjunto denotado por $\mathbb{N}$ que satisface los axiomas propuestos.

5.3 El principio de inducción matemática

Vamos a dar ejemplos de cómo demostrar una proposición por medio del principio de inducción matemática. También daremos ejemplos de la construcción de operaciones y definiciones por medio de relaciones recursivas. En todo esto, la inducción matemática es muy útil.

Siempre que una proposición enuncie que determinada propiedad es válida para todo número natural *n*, *el primer enfoque* que debemos adoptar para demostrar la misma es usar el principio de inducción matemática. Como decía el Profesor Charles Saltzer de Ohio State University: “just one word: induction”(Una sola palabra: inducción).

Siguiendo el libro de Sominski, *Método de Inducción Matemática* vamos a considerar diferentes apartes con ejemplos del uso de tan poderosa herramienta.

Demostración de proposiciones aritméticas

Proposición. Todo número de la forma n^2+n es par donde n es un número natural cualquiera.

Demostración. La proposición es cierta para $n=0$ ya que 0 es un número par.

Supongamos que la proposición es cierta para $n=k$, esto es k^2+k es par. *Esta asunción se conoce como hipótesis inductiva.*

Veamos que ocurre para $n=k+1$, como $(k+1)^2+k+1=k^2+k+2k+2$ y esto es un número par por ser la suma de tres números pares. El resultado sigue para cualquier natural n.

Proposición. Para cualquier natural n se tiene que $1+3+\cdots+2n+1=(n+1)^2$.

Antes de establecer el resultado formalmente hagamos algunos experimentos que exploren si el resultado anterior es plausible.[2]

La siguiente tabla recoge lo que obtenemos para diversos valores de n.

Valor de n	Cálculo de $1+3+\cdots+2n+1$	Cálculo de $(n+1)^2$	¿Obtenemos la igualdad?
1	1+3=4	$(1+1)^2=4$	Si
2	1+3+5=9	$(2+1)^2=9$	Si
3	1+3+5+7=16	$(3+1)^2=16$	Si

¡El resultado se verifica para todos los valores de n usados!

[2] Los libros de Polya "Como plantear y resolver problemas" y "Matemáticas y razonamiento plausible" tratan del rol del experimento en el descubrimiento de verdades matemáticas.

Como actividad le propongo al estudiante UNA que haga una tabla como la anterior para nuevos valores de *n*.

Terminemos la demostración de la igualdad anterior usando inducción matemática, ya sabemos que la proposición es cierta para los primeros valores de *n* como está reflejado en la tabla. Supongamos que la proposición es cierta para *n*=*k*, tenemos

$$1+3+\cdots+2k+1=(k+1)^2 \Rightarrow$$
$$1+3+\cdots+2k+1+(2k+3)=(k+1)^2+(2k+3)$$
$$\mathbb{N}$$

Pero, $(k+1)^2+(2k+3)=k^2+4k+4=(k+2)^2$ de donde el resultado es válido para *k*+1.

Los experimentos en Matemática

El estudiante puede hacer experimentos que comprueben una fórmula matemática. Sin embargo, aunque hayamos verificado una conjetura muchas veces esto **no sustituye a una demostración matemática.** Quizás el resultado sea cierto muchas veces pero si falla una vez es, matemáticamente, falso. Fermat pensó que los números de la forma $2^{2^n}+1$ eran siempre primos. Por ejemplo, si *n*=1 obtenemos el número 5 que es primo. Para *n*=2 obtenemos 17, que es un número primo. Hagamos una tabla de los primeros casos.

Valor de *n*	Valor de $2^{2^n}+1$	¿Es primo el resultado?
3	257	Si
4	65537	Si

Sin embargo, Fermat no pudo demostrar su afirmación. Años después Euler calculó que $2^{2^5}+1=2^{32}+1=4294967297$ y este número es divisible por 641. Luego, Fermat había realizado una conjetura errónea y por ello no la pudo demostrar. Resumiendo nuestras ideas:

1. Experimente libremente con los objetos matemáticos y las relaciones entre ellos.
2. Formule conjeturas basadas en sus experimentos.
3. Demuestre las mismas usando inducción matemática u otras técnicas.

Luego, la proposición es cierta para $k+1$ y por inducción matemática es cierta para todo *n.*

Tomemos la sucesión $4^n - 1$ donde *n* es un número natural arbitrario. Hagamos una tabla de los valores de $4^n - 1$ para distintos valores de *n.*

n	$4^n - 1$
1	3
2	15
3	63
4	255
5	1023

¿Qué propiedades tienen los números calculados? Trate de listar algunas de esas propiedades. Reflexione su respuesta y no vuelva al texto hasta formular algunas conjeturas sobre los números de la forma $4^n - 1$.

¿Vio Ud. alguna cosa? Seguro que sí. Déjeme mostrarle mis observaciones.

Conjetura 1: Al parecer una característica común de *los números de la forma* $4^n - 1$, *con n natural, es que son impares*. ¿Puede Ud. demostrarlo?. Recuerde que la conjetura se debe demostrar matemáticamente, no basta que sea cierta para los primeros 5 números naturales, ni para los siguientes cien, etc. Por supuesto, que se verifique muchas veces la hace más plausible pero no constituye una demostración. De hecho la demostración que $4^n - 1$ es siempre impar es muy sencilla. En primer lugar 4^n es un número par. ¿Por qué? Y si a un número par le restamos 1, obtenemos un número

impar, fin de la demostración. Invitamos al estudiante UNA a pensar en una prueba alterna de este resultado por inducción matemática. Sugerencia: Use la identidad $4^{n+1}-1=4\left(4^{n}-1\right)+4-1$.

Conjetura 2: Esta conjetura es más sutil que la anterior. Factoricemos los números de la forma $4^{n}-1$ que tenemos en la tabla en sus factores primos. Pongamos nuestros resultados en una nueva tabla.

n	$4^{n}-1$	Factorización
1	3	3
2	15	(3).(5)
3	63	(3).(3).(7)
4	255	(3).(5).(17)
5	1023	(3)(11)(31)

Al parecer, ¡Cualquier número de la forma $4^{n}-1$ es divisible por 3! Esto es una hermosa conjetura. El estudiante puede hacer unos cálculos más que refuercen esta hipótesis. Ahora intentamos demostrar la misma, e insisto *debemos hacer una demostración,* por inducción matemática.

Demostración. El resultado es cierto para n=0 ya que 3 divide a $4^{0}-1=0$. La hipótesis inductiva es que 3 divide a $4^{k}-1$ para un natural k. Tratamos de ver que el resultado es cierto para k+1, esto es que 3 divide a $4^{k+1}-1$. Pero, $4^{k+1}-1=4(4^{k}-1)+3$ y esto es divisible por 3 ya que es la suma de dos números divisibles por 3. El resultado está demostrado.

Ejercicio: ¿Se atreve el estudiante a formular alguna conjetura más derivada de la tabla que contiene la factorización de $4^{n}-1$?.

Demostración de desigualdades por inducción matemática

Es propio del Cálculo y el Análisis Matemático establecer desigualdades entre expresiones matemáticas. Es lo que los matemáticos llaman acotar. Muchas veces la inducción acude en nuestra ayuda para demostrar la desigualdad propuesta. Estudiemos la relación entre las sucesiones n y 2^n. Hagamos una tabla para distintos valores de n.

n	2^n	Comparación
1	2	1<2
2	4	2<4
3	8	3<8
4	16	4<16

Al parecer siempre 2^n es mayor que n, esa es nuestra conjetura que pasamos a demostrar por medio de inducción matemática. El estudiante UNA que recuerde su curso de Matemática I (177), Módulo IV, observará que estamos comparando una sucesión de crecimiento lineal vs. una sucesión de crecimiento exponencial y no se debería sorprender de nuestra conjetura. *El estudiante debe saber que el crecimiento exponencial supera siempre al crecimiento polinomial.* Demostremos a continuación nuestra conjetura.

Thomas Robert Malthus (1766-1834)

Pocos trabajos han tenido una influencia sobre diversas áreas como *Un ensayo sobre el principio de la población* de Malthus. Charles Darwin halló en el la razón de la evolución de las especies. Malthus plantea que el crecimiento de la población sigue un modelo exponencial, mientras que el crecimiento de los recursos es de carácter lineal. Inevitablemente este conflicto, según Malthus, va a llevar al hambre y a conflictos entre los pobladores de la tierra. Aquí ve Darwin lo que motiva la supervivencia del

mejor adaptado, flexibilizando la idea de Malthus para adaptarla a diferentes situaciones y especies.

 Demostrar que $n \leq 2^n$ para cualquier natural *n.*

Demostración: La proposición es válida *n*=0 ya que $0 \leq 1$. Supongamos la proposición cierta para *n*=*k*, esto es $k \leq 2^k$. Luego $k \leq 2^k \Rightarrow k+1 \leq 2k \leq 2^{k+1}$ para *k* mayor o igual que 1, de donde se concluye el resultado para todo natural *n*.

 Demostrar que $(1+\alpha)^n \geq 1+n\alpha, \alpha > 0$ y $n \geq 1$

Demostración: Para *n*=1 el resultado es cierto ya que $1+\alpha = 1+\alpha$.

Supongamos el resultado cierto para *n*=*k*, esto es $(1+\alpha)^k \geq 1+k\alpha, \alpha > 0$. Tenemos que demostrarlo para *n*=*k*+1. Como $(1+\alpha)^{k+1} = (1+\alpha)(1+\alpha)^k \geq (1+\alpha)(1+n\alpha)$ pero $(1+\alpha)(1+n\alpha) = 1+(n+1)\alpha + n\alpha^2 > 1+(n+1)\alpha$ y el resultado sigue.

Demostración de identidades trigonométricas

Distintas fórmulas trigonométricas pueden ser demostradas por medio de inducción matemática. Empezamos con la importantísima fórmula de DeMoivre.

 (Fórmula de DeMoivre)

Demostrar que $(\cos x + isenx)^n = \cos nx + isennx$ para cualquier natural $n \geq 1$, aquí $i^2 = -1$

Demostración: La fórmula es cierta para *n*=1.

Supongamos que la fórmula es cierta para *k*, esto es $(\cos x + isenx)^k = \cos kx + isenkx$. Probaremos la identidad para *k*+1. Tenemos que $(\cos x + isenx)^{k+1} = (\cos x + isenx)(\cos x + isenx)^k$. Pero, aplicando la hipótesis inductiva vemos que $(\cos x + isenx)(\cos x + isenx)^k = (\cos x + isenx)(\cos kx + isenkx)$.

Por tanto,

$$cos\, x \cos kx + i\left(cos\, xsenkx + cos\, kxsenx\right) - senxsenkx$$

$$cos\left(k+1\right)x + isen\left(k+1\right)x$$

De donde el resultado es cierto para todo *n* mayor que 1.

Resumimos en el siguiente cuadro la demostración por medio de inducción matemática

La demostración por inducción

Queremos demostrar la afirmación P(n) es cierta para cualquier numero natural n.

Es decir, queremos ver que $A=\{n \text{ tales que } P(n) \text{ es cierta}\} = \mathbb{N}$

Lo que hacemos es demostrar que el conjunto *A* satisface el axioma 5 dado anteriormente. Es decir, demostramos por un cálculo directo que 0 está en *A* (esto es la parte fácil de las demostraciones por inducción) y luego demostramos que si un entero cualquiera *k* está en *A* su sucesor *k*+1 también está en *A* (parte difícil de la inducción, conocida como paso inductivo). La inducción matemática es una herramienta fundamental para la demostración, fue empleada inicialmente por Maurolico. Posteriormente, Pascal y Fermat la convirtieron en una importante técnica matemática y fue generalizada por Zorn para abarcar conjuntos que no fueran numerables.

Maurolico, el creador de la inducción matemática

Una pelea entre amigos

Se cuenta que el matemático Pi Calleja le gustaba pensar que el principio de inducción matemática era análogo al juego de poner una pila de fichas de dominó una tras otra, de tal forma que si la primera cae, caen todas las demás, sucesivamente. La primera ficha que cae representa el 0 y que la ficha n tumbe a la ficha $n+1$ es el paso inductivo. Mientras escribía la obra de *Análisis Matemático* con Trejo y Rey Pastor, Pi Calleja pensó en usar esta analogía en el libro, causando la molestia de Rey Pastor, quien amenazó con retirarse del trabajo. Finalmente, Rey Pastor aceptó la didáctica idea de su colega.

Definiciones por recurrencia o recursivas

El principio de inducción matemática se usa para hacer *definiciones por recurrencia o recursivas.* Veamos unos ejemplos de lo que queremos decir.

Vamos a definir la *potencia* a^k, k natural, de un número real $a>0$.

En primer lugar, definimos $a^0 = 1$ y suponemos que la operación de potencia a^k está definida para cualquier natural menor o igual que k. Definimos entonces $a^{k+1} = a^k a$. Observe que, de esta manera, ha quedado determinada el valor de a^k para cualquier natural k.

Números de Fibonacci.

La histórica e importante sucesión de Fibonacci se define por medio de la recurrencia

$$F_0 = 1, F_1 = 1$$
$$F_{n+1} = F_n + F_{n-1}$$

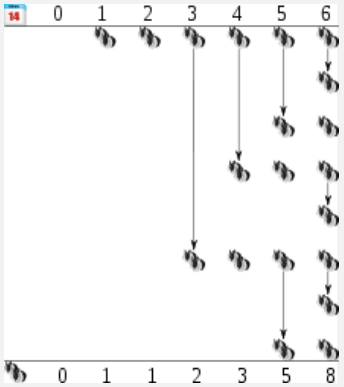
Observe que cada número es generado por los dos que le anteceden y por eso necesitamos dar los dos primeros números de Fibonacci para calcular los restantes. El principio de inducción garantiza que la sucesión está bien definida para cualquier natural *n*. ¿Por qué?

Luego los primeros números de Fibonacci son

1, 1, 2, 3, 5, 8, 13, 21, 34,…

Los conejos de Fibonacci

Fibonacci introdujo su sucesión para estudiar el crecimiento de una población de conejos que empieza con una pareja y con la condición de que la pareja tiene una pareja de crías el segundo mes. Luego el primer mes tenemos una sola pareja. En el segundo mes dos parejas, una de las cuales va tener una pareja el cuarto mes. En el tercer mes, la pareja inicial tiene otra pareja de crías, y así sucesivamente.



En el gráfico Ud. puede ver el crecimiento de la población de conejos. Un matemático experto en los números de Fibonacci odiaba esta historia y decía que solo le interesaban los conejos acompañados de arroz blanco y una buena botella de vino tinto.

Gráfico tomado de http://es.wikipedia.org/wiki/Sucesi%C3%B3n_de_Fibonacci

(Una propiedad de la sucesión de Fibonacci)

Si continuamos la sucesión de Fibonacci podemos observar lo siguiente

$$F_5 = 5, F_{10} = 55, F_{15} = 610$$

El estudiante atento puede observar que 5 divide tanto a $F_5 = 5, F_{10} = 55, F_{15} = 610$ y adelantar la hipótesis

$$5 \text{ divide a } F_{5k}$$

Pero, como ya sabemos, a diferencia de lo que ocurre en algunas ciencias experimentales tal hipótesis *debe ser demostrada.* Sin embargo, consideramos muy importante este trabajo de manipulación experimental de los objetos matemáticos, sin el cual no hubiéramos enunciado la ley que tratamos de probar.

Como es una proposición que involucra a los números naturales el método que usaremos es inducción matemática. La proposición es válida para n=5 ya que 5 divide a 5.

Supondremos que la proposición es válida para F_{5k} y trataremos de demostrarla para $F_{5(k+1)}$. Pero, observamos que

$$F_{5(k+1)} = F_{5k+5} = F_{5k+4} + F_{5k+3} = 2F_{5k+3} + F_{5k+2} = 2(F_{5k+2} + F_{5k+1}) + F_{5k+1} + F_{5k}$$

Luego,

$$2(F_{5k+2} + F_{5k+1}) + F_{5k+1} + F_{5k} = 2(F_{5k} + 2F_{5k+1}) + F_{5k+1} + F_{5k} = 5F_{5k+1} + 3F_{5k}.$$

Observe que 5 divide a $5F_{5k+1} + 3F_{5k}$ ya que en primer lugar 5 divide a $5F_{5k+1}$ y en segundo lugar 5 divide a $3F_{5k}$ por hipótesis inductiva. Luego 5 divide a $F_{5(k+1)}$ y la

proposición es cierta para cualquier número natural *n.* Esto concluye la demostración del resultado.

Muchas veces es útil la siguiente forma del principio de inducción cuya demostración omitimos.

Teorema 1. *Supongamos que una proposición P(n) es cierta* $n=0$ *y que si es cierta* $0,1,\ldots k$ *esto implica que es cierta para* $k+1$ *entonces P(n) es cierta para cualquier natural n.*

La última proposición es importante porque nos dice que todos los números naturales se obtienen a partir del 0, mediante aplicación sucesiva de la función sucesor.

Teorema 2. *El conjunto A que se obtiene de tomar el 0,* $s(0)$, $s(s(0)),\ldots$ *es* $\mathbb{N}$

Demostración. 0 está en *A*, por otro lado supongamos que k está en *A*, luego $k=s(s(\ldots s(0)))$ de donde $s(k)=s(s(\ldots s(0)))$ y luego está en *A*. Por el principio de inducción $A=\mathbb{N}$.

5.4 Orden, principio de inducción y principio del menor elemento

Una relación de orden puede establecerse en los números naturales $\mathbb{N}$. Decimos que

$$n<m \text{ si y sólo si } m=s(s\ldots(n))$$

es decir, si *m* se obtiene a partir de *n* mediante una aplicación sucesiva finita de la función sucesor. Este orden es total, ya que empezando con el 0 y aplicando sucesivamente la función sucesor obtenemos todos los números naturales como establecimos en el último teorema de la sección anterior. Así, si *n* se obtiene primero que *m* aplicando la función sucesor escribimos $n<m$.

1. Demostrar que < es de hecho una relación de orden.

Sugerencia: Recuerde que una relación es de orden si y sólo si satisface la propiedad transitiva.

Luego, podemos escribir

$$0<1<2<3<4<5\ldots.<n<n+1<\ldots$$

Escribiremos $n \leq m$ para indicar que $n < m$ o que $n=m$.

El orden en los números naturales tiene varias propiedades importantes. Consideremos un conjunto cualquiera A de números naturales. Un elemento a en A se denomina el menor elemento de A si y sólo si $a \leq n$ para cualquier n que pertenezca a A. El siguiente resultado es fundamental.

Teorema 3. *Todo conjunto A no vacío de números naturales tiene un menor elemento*.

Demostración: Supongamos lo contrario: hay un conjunto A *no vacío* de números naturales que no tiene un menor elemento. Entonces el 0 no está en A, ya que de lo contrario sería el menor elemento de A. Supongamos ahora que 0, 1, $\cdots$, k no están en A, esto implica que $k+1$ tampoco está en A de o contrario $k+1$ sería el menor elemento de A. Luego el complemento de A es todo $\mathbb{N}$ y A debe ser vacío. Una contradicción que termina la demostración.

Fermat y el descenso infinito

Los primeros usos del principio de inducción en teoría de números fueron realizados por Pierre de Fermat.

Fermat

Nació en 1601 en Beaumont-de-Lomagne, fue abogado de profesión, aunque se le recordará como el más notable matemático amateur de la historia. Estudiaba matemáticas en su tiempo libre, en particular la obra de Diofanto en teoría de números. En uno de los volúmenes de la obra de Diofanto escribió:

La ecuación $x^n + y^n = z^n$ *no tiene soluciones si n>3, he encontrado una maravillosa demostración de este resultado pero no cabe en el margen del libro*. El estudiante debe saber que ese enunciado corresponde al último teorema de Fermat, el más famoso problema matemático de la historia y que fue resuelto por Andrew Wiles hacia finales del siglo XX.

Muere en Castres, Tam en 1665.

Este matemático gascón realizó entre otras cosas:

1. Creó con Pascal la teoría de Probabilidades
2. Fue creador, junto a Descartes, de la Geometría Analítica
3. Es, sin duda, pionero del desarrollo del Cálculo
4. Encontró originales métodos en teoría de números y nuevos resultados.

El descenso infinito era una técnica usada por Fermat para probar una propiedad de los números naturales. Se basaba en observar que si la propiedad fallaba para un natural k entonces era posible construir un natural $m<k$ para el cual la propiedad fallaba también. Esto obviamente contradice el principio del menor elemento y por ende las demostraciones por descenso infinito son solamente una variación del principio de inducción matemática. Sin duda, Fermat fue el más grande matemático amateur de la historia.

Por otro lado, el principio del menor elemento implica el de inducción matemática. Es decir, si hubiésemos asumido los primeros cuatro axiomas de Peano y el principio del menor elemento, el principio de inducción matemática hubiera sido un teorema en esta axiomática. Veamos por qué. Sea *A* un subconjunto de los números naturales tal que **el 0 *está en A. Además, si n está en A entonces s(n) está en A*.** Queremos demostrar que *A es el conjunto de todos los naturales.* Supongamos que no lo sea, entonces el complemento de *A* es no vacío y debe tener un menor elemento n_0, siendo este elemento distinto del 0. Podemos afirmar entonces que $n_0 = s(k)$ para algún *k.* Pero, esto implica que $k < n_0$ y al ser n_0 el menor elemento del complemento de *A* debemos tener que *k* está en *A,* luego $s(k)$ debe estar en *A* y $n_0 = s(k)$ está también en el complemento de *A,* una contradicción.

Así, desde un punto de vista lógico el principio de inducción es equivalente a la afirmación que todo conjunto no vacío de números naturales tiene un menor elemento.
En matemática cuando un orden verifica el principio del menor elemento decimos que es un *buen orden.*

En resumen:

Propiedades del orden en los números naturales
• El orden en los números naturales es total, es decir dados dos naturales *n,m* entonces $n=m$ o $n<m$ o $m<n$ • El orden en los naturales es un buen orden: todo conjunto A no vacío de números naturales tiene un menor elemento.

5.5 La operación de suma y producto de números naturales

Es importante recordar que no nos interesa únicamente el conjunto de los números naturales, sino también las operaciones de adición y multiplicación definidas en él, operaciones que constituyen la base de la teoría de números o la aritmética superior.

5.5.1 Adición o suma de números naturales

Fijemos $a \in \mathbb{N}$, queremos definir $a+b$ donde b es un natural arbitrario. Vamos a hacer la definición por recurrencia de manera muy sencilla. Definimos

1. $a+0=a,\ a+1=s(a)|$

2. Si hemos definido la suma $a+b$ hasta $b \leq k$ entonces

$$a+s(k)=s(a+k)$$

1. Demuestre que la suma $a+b$ ha sido definida para números naturales arbitrarios a,b.
2. Demuestre que 2+2=4.

1. Por inducción matemática la suma ha sido definida para cualquier b y a era completamente arbitrario en nuestra construcción, de donde se tiene el resultado.

2. 2+0 es 2, por definición de la suma, pero 2+1=s(2)=3 y 2+s(1)=s(3)=4, ahora ya puede contar a sus amigos que Ud. sabe demostrar que 2 y 2 son 4.

Vamos a demostrar, como ilustración del uso de nuestras definiciones y del principio de inducción que la suma de números naturales es conmutativa. Empezamos con un lema.

Lema 4. $s(a)+b=s(a+b)$ para naturales a,b cualesquiera

Demostración: Fijemos a y consideremos el conjunto $B=\{b \text{ tales que } s(a)+b=s(a+b)\}$. Obviamente $0 \in B$ ya que $s(a)+0=s(a+0)=s(a)$. Supongamos ahora que k está en B, es decir $s(a)+k=s(a+k)$. Queremos demostrar que $s(k)$ está en B. Esto equivale a demostrar que

$s(a)+s(k)=s(a+s(k))$. Pero $s(a)+s(k)=s(s(a)+k)$ por definición de la suma. Por otro lado, $s(s(a)+k)=s(s(a+k))$ por hipótesis inductiva y de nuevo, aplicando la definición de suma, obtenemos

$s(s(a+k))=s(a+s(k))$ de donde, aplicando el principio de inducción matemática, el resultado sigue para todo natural *b.*

Lema 5. $a+1=1+a$ para cualquier natural *a*

Demostración: Sea *A* el conjunto de los naturales *a* que verifican $a+1=1+a$. Tenemos de manera inmediata que 0 está en *A.* Supongamos ahora que *k* está en *A*, esto es

$$k+1=1+k$$

Entonces $s(k)+1=s(k+1)=s(1+k)=1+s(k)$. El estudiante UNA debe indicar qué hemos usado en cada una de las igualdades anteriores. Aplicando el principio de inducción completa obtenemos el resultado para cualquier *a* natural.

Finalmente,

Teorema 6. Se tiene que $a+b=b+a$ para naturales *a,b* cualesquiera

Demostración: Sea *A* el conjunto de todos los naturales *a* que verifican $a+b=b+a$ para cualquier *b* natural. Tenemos de inmediato que 0 y 1 están en *A.* ¿Por qué? Supongamos ahora que el natural *k* está en *A* . Esto es, $k+b=b+k$ para cualquier *b* natural. Queremos ver que $s(k)+b=b+s(k)$ para cualquier *b* natural. Como $s(k)+b=s(k+b)=s(b+k)=b+s(k)$ el resultado sigue por aplicación del principio de inducción.

 Demostrar que la suma de números naturales es asociativa.

Por último demostramos la ley de cancelación para la suma de números naturales, debo señalar que esta ley es muy importante para la construcción de los números enteros que haremos la próxima semana.

Teorema 7 (Ley de cancelación de la suma de números naturales)

Si los números naturales *a,b verifican* $a+c=b+c$ para un cierto natural c entonces $a=b$

Demostración: Definamos el conjunto $C=\{c \text{ tales que } a+c=b+c \Rightarrow a=b\}$. La idea es demostrar que *C* es todo el conjunto de números naturales. Vemos que $1 \in C$ ya que si $a+1=b+1 \Rightarrow s(a)=s(b) \Rightarrow a=b$. Supongamos ahora que *k* está en *C*, es decir si $a+k=b+k \Rightarrow a=b$. Queremos ver que $s(k)$ está en *C.*

Si suponemos que $a+s(k)=b+s(k) \Rightarrow s(a+k)=s(b+k) \Rightarrow a+k=b+k \Rightarrow a=b$.

Luego *C* es el conjunto de los números naturales.

El estudiante UNA debe verificar y justificar cuidadosamente las implicaciones finales de la demostración.

Producto de números naturales

Vamos a definir el producto de números naturales de manera recursiva y apoyándonos en la suma antes definida.

Tomemos un $a \in \mathbb{N}$, definimos *a*0=0 y $a1=a$. Si suponemos que el producto ab está definido hasta $b \leq k$ ponemos $as(k)=ak+a$. Queda el producto ab definido para cualesquiera naturales *a,b.*

La demostración de las propiedades del producto sigue lo que hicimos con la suma y van a ser propuestas como un proyecto con sugerencias importantes para demostrar las mismas. De cualquier manera las recapitulamos a continuación

Teorema 8

1. El producto de números naturales es conmutativo, esto es $ab = ba$ para naturales cualesquiera *a,b*
2. El producto de números naturales es asociativo, esto es $a(bc) = (ab)c$ para naturales cualesquiera *a,b*
3. El producto es distributivo respecto a la suma, es decir $a(b+c) = ab + ac$ para naturales cualesquiera *a,b,c*

1. Demostrar el teorema anterior.

Sugerencias:

- Observe bien lo que hicimos en el caso de la suma
- Defina los conjuntos análogos a lo que hicimos para la demostración de estas propiedades en la adición
- Aplique inducción matemática

1. Es un ejercicio importante y Ud. debe hacer el mismo.

Es importante notar que una ley de cancelación se verifica para el producto bajo ciertas restricciones.

Teorema 9. *Si* $ac = bc$ *para un natural* c *distinto de* 0 *entonces* $a=b$

Demostración: Sea $C = \{c \text{ tales que } ac = bc \Rightarrow a = b\}$, C contiene al 1 ya que $a1 = b1 \Rightarrow a = b$ por la definición de la multiplicación. Supongamos ahora que *k* está en *C,* esto significa si $ak = bk$ entonces $a=b$. ¿Qué pasa con $s(k)$? Tenemos que $as(k) = bs(k) \Rightarrow ak + a = bk + b$. Pero como $ak=bk$ y para la suma vale una ley de cancelación entonces $a=b$. Luego *C* es el conjunto de los naturales sin el 0.

5.6 Modelando con los números naturales

Sistemas dinámicos discretos

Consideremos un sistema *S* que evoluciona con el tiempo *t* de acuerdo a la ecuación S_t. Aquí *S* puede representar una diversidad de sistemas: un conjunto de partículas de un gas, el valor de una acción de la bolsa, el nivel del colesterol en la sangre de una persona, entre otras cosas. He aquí una de las virtudes de la matemática, su lenguaje unifica una serie de situaciones presentándolos bajo la misma estructura abstracta.

A continuación damos dos hipótesis que condicionan nuestro estudio del sistema *S*. Vamos a suponer que el tiempo *t* se puede medir de manera discreta, es decir los valores de *t* son 0, 1, 2, 3,…, La unidad de tiempo empleada va depender, sin duda, del problema planteado. Estos sistemas se denominan *sistemas dinámicos discretos.* La otra suposición que haremos es que el estado de *S* en el tiempo $n+1$ queda determinado por lo que ocurrió en el tiempo *n*, es decir, existe una función f

$$S_{n+1} = f(S_n)$$

Es decir, el sistema evoluciona de manera recursiva de acuerdo a una ley *determinista* donde un estado determina completamente el que le sigue, y a su vez queda determinado por el que lo antecedió. Observe que la ecuación $S_{n+1} = f(S_n)$ puede ser interpretada como una fórmula de recurrencia y que solo basta conocer S_0 para determinar los demás estados del sistema

$$S_0 \overset{f}{\rightarrow} S_1 \overset{f}{\rightarrow} \cdots$$

Los estados $S_0, S_1, S_2 \cdots$ se conocen como la órbita generada por S_0.

1. Ecuación logística

El estado del sistema está representado por un punto en el intervalo [0,1]. Sea λ un parámetro positivo y menor o igual que 4 y la ecuación definida por recurrencia

$$a_n = \lambda a_{n-1}(1-a_{n-1})$$
$$a_0 \in [0,1]$$

Es decir, tomamos un dato inicial a_0 y lo hacemos evolucionar de acuerdo a la ley anterior.

Lema. El máximo de la parábola $y = \lambda x(1-x)$ se alcanza en $x=\frac{1}{2}$ y vale $\frac{\lambda}{4}$

Demostración: Se deja al lector.

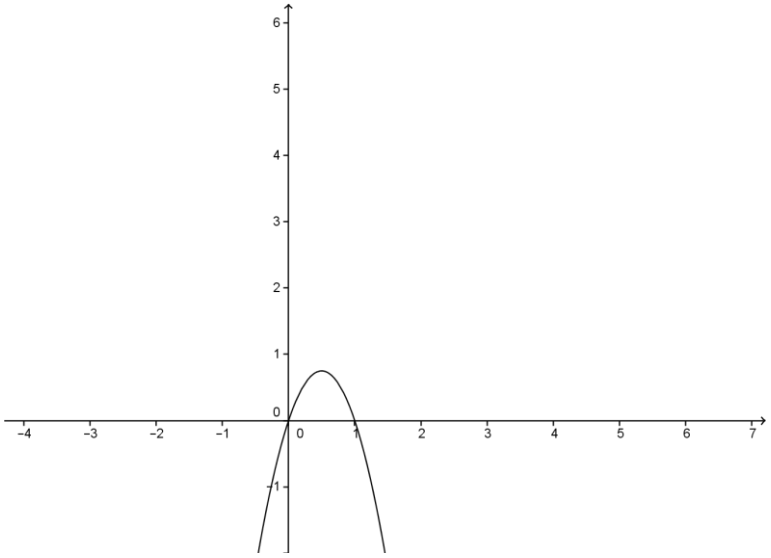


Gráfico de la parábola logística con parámetro 3

Teorema. Para cualquier n $a_n = \lambda a_{n-1}(1-a_{n-1})$, $a_0 \in [0,1]$ está en el intervalo [0,1]

Demostración: Lo demostraremos por inducción matemática. La afirmación es cierta para n=0 ya que $a_0 \in [0,1]$. Supongamos la afirmación cierta para n=k, esto es

$a_k = \lambda a_{k-1}(1-a_{k-1}) \in [0,1]$. Como $a_{k+1} = \lambda a_k(1-a_k)$, aplicando el lema anterior, obtenemos que $0 \le a_{k+1} = \lambda a_k(1-a_k) \le \frac{\lambda}{4} \le 1$ y esto concluye la demostración.

Es muy importante en un sistema dinámico determinar los llamados puntos fijos. Un punto a es un punto fijo de un sistema dinámico discreto $a_n = f(a_{n-1})$ si y sólo si

$$a = f(a)$$

Si un punto fijo a se alcanza en algún natural *n*, la orbita se trivializa a partir del mismo ya que

$$a_{n+1} = f(a_n) = f(a) = a$$
$$a_{n+2} = f(a_{n+1}) = f(a) = a$$
$$\vdots$$

El sistema no escapa al estado representado por *a*. Luego, encontrar los puntos fijos de un sistema es importante.

Los puntos fijos de la ecuación logística son las soluciones de la ecuación $a = \lambda a(1-a)$. Un cálculo sencillo muestra que son, precisamente, $a = 0, a = 1 - \frac{1}{\lambda}$.

El comportamiento de la sucesión logística depende completamente del parámetro λ que escojamos. Por ejemplo, si tomamos $\lambda = 2$ y un dato inicial $a_0 \in [0,1]$, se puede mostrar que $a_n = \lambda a_{n-1}(1-a_{n-1})$ se aproxima a uno de los puntos fijos.

a_n	n
0,4	0
0,48	1
0,4992	2
0,49999872	3
0,5	4
0,5	5

En la tabla anterior, tomamos $a_0 = 0,4$. Por otro lado, el comportamiento del sistema para $\lambda = 4$ y $a_0 = 0,9$ (este valor no es importante) es mucho más rico y extraño.

a_n	n
0,9	0
0,36	1
0,9216	2
0,28901376	3
0,82193923	4
0,58542054	5
0,97081333	6

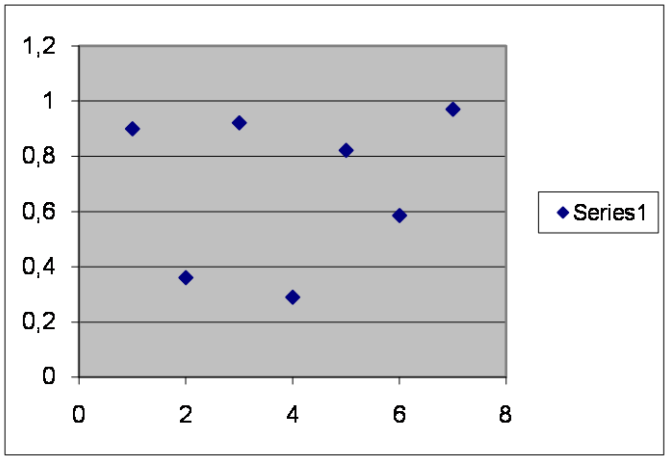


Gráfico de los puntos de la sucesión

La razón de este comportamiento cae en lo que se conoce como Teoría del Caos, una activa e interesante rama de las matemáticas.

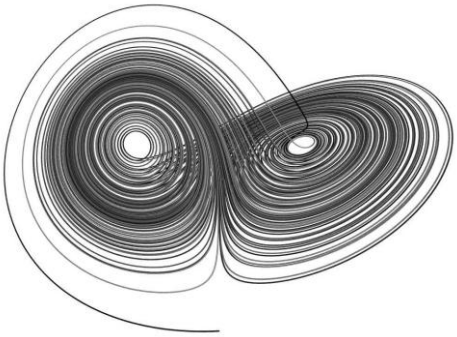


Gráfico del atractor extraño de Lorenz

Atractor de Lorenz: El físico Edward Lorenz estudiando las ecuaciones para el clima observó que las mismas tenían un comportamiento caótico: pequeños cambios de los datos iniciales se traducen en soluciones completamente distintas. Lorenz dijo: el aleteo de una mariposa en Pekín puede producir un tifón en pocos días a miles de kilómetros de distancia.(efecto mariposa)

Recomendamos al estudiante UNA interesado en la Teoría del Caos, leer el libro de James Gleick, *Caos, la creación de una nueva ciencia.*

1. Demuestre, usando inducción matemática, que el número de subconjuntos de un conjunto A de n elementos es 2^n.
2. Consideremos la sucesión de Fibonacci definida por medio de

$$F_0 = 1$$
$$F_1 = 1, F_{n+1} = F_n + F_{n-1}$$

Demuestre que la misma se puede escribir de manera matricial como

$$\begin{pmatrix} F_{n+1} \\ F_n \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} F_{n-1} \\ F_n \end{pmatrix}$$

Con las condiciones iniciales $F_0 = 1, F_1 = 1$.

3. Consideremos la sucesión de Fibonacci, con datos iniciales $F_0 = 0, F_1 = 1$ definida anteriormente. Demuestre usando inducción matemática que

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

4. Sea k un número que está entre 0 y 1. Definimos mediante la recurrencia

$$a_n = k a_{n-1}$$
$$a_0 \in \mathbb{R}, n = 0, 1, 2, \cdots,$$

la sucesión a_n.

1. Demuestre que la sucesión a_n equivale a la progresión geométrica de razón k

$$a_n = k^n a_0$$

2. Experimente con distintos valores de k y de a_0 para ver el comportamiento de la sucesión cuando n se hace grande.. ¿Qué ocurre con k=0? ,¿qué ocurre

con k=1?. Tome k=0,5 y haga una tabla de datos con distintos valores de a_0. Resuma sus observaciones.

5. Recordamos de quinto año de bachillerato que $n! = n(n-1)(n-2)\cdots 3.2.1$, con la convención que 0!=1. Si m,n son naturales, $m \geq n$, definimos el número combinatorio $\binom{m}{n}$, como

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

Demuestre usando inducción completa que $\binom{m}{n} + \binom{m}{n+1} = \binom{m+1}{n+1}$.

6. Demuestre por inducción completa que $1+2+3+\cdots+n = \frac{n(n+1)}{2}$.
7. Demuestre por inducción completa que $1+a+a^2+\cdots+a^n = \frac{1-a^{n+1}}{1-a}$ con a número real distinto de 1.
8. Demuestre que entre dos naturales consecutivos no puede haber otra natural.
9. Tomemos el polinomio de segundo grado x^2+x+41 y evalué con la ayuda de un CAS el mismo en 1,2,3,…40. Determine con el CAS si estos valores son números primos. ¿Puede formular el estudiante UNA alguna hipótesis?.
10. El polinomio de segundo grado x^2+x+41 no puede dar números primos para cualquier x número natural.
11. Demuestre que ningún polinomio con coeficientes enteros $p(x)$ con puede dar siempre números primos.
12. Demuestre que para cualquier numero natural n se tiene

$$1+2^3+3^3+\cdots+n^3 = (1+2+3+\cdots+n)^2$$

13. ¿Como demostramos que el polinomio $p(x) = x^2+x+1$ no puede dar siempre números primos?
14. Demuestre que para cualquier n natural se tiene que $1+3^2+5^2+\ldots+(2n-1)^2=n(2n-1)(2n+1)/3$.

15. Demuestra que para cualquier n natural $1\cdot 2\cdot 3+2\cdot 3\cdot 4+\cdots+n(n+1)(n+2)=\dfrac{n(n+1)(n+2)(n+3)}{4}$

1. La proposición es cierta para $n=0$ ya que el único subconjunto del conjunto vacío es el mismo conjunto vacío. Supongamos que la proposición es cierta para cualquier conjunto finito A de k elementos, es decir hay 2^k subconjuntos de A. Añadimos un elemento a al conjunto considerado y buscamos sus subconjuntos. Es claro que cualquiera de estos subconjuntos contiene o no a a. Hay 2^k que no lo contienen y 2^k que si lo contienes, es decir $2^k+2^k=22^k=2^{k+1}$ subconjuntos que era lo que teníamos que demostrar.

2. Efectuemos $\begin{pmatrix} F_{n+1} \\ F_n \end{pmatrix}=\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} F_{n-1} \\ F_n \end{pmatrix}=\begin{pmatrix} F_n+F_{n-1} \\ F_n \end{pmatrix}\Rightarrow F_{n+1}=F_n+F_{n-1}$.

3. Este problema da una fórmula importante para la sucesión de Fibonacci que no es recursiva sino explícita. El estudiante UNA debe verificar que la fórmula es válida para los casos 0 y 1. Suponga ahora que la fórmula es válida para k y $k+1$, esto es

$$F_k=\frac{\left(\frac{1+\sqrt{5}}{2}\right)^k-\left(\frac{1-\sqrt{5}}{2}\right)^k}{\sqrt{5}}+F_{k+1}=\frac{\left(\frac{1+\sqrt{5}}{2}\right)^{k+1}-\left(\frac{1-\sqrt{5}}{2}\right)^{k+1}}{\sqrt{5}}.$$ Luego,

$$F_k+F_{k+1}=\frac{\left(\frac{1+\sqrt{5}}{2}\right)^k-\left(\frac{1-\sqrt{5}}{2}\right)^k}{\sqrt{5}}+\frac{\left(\frac{1+\sqrt{5}}{2}\right)^{k+1}-\left(\frac{1-\sqrt{5}}{2}\right)^{k+1}}{\sqrt{5}}=$$

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

Con esta escritura solamente queda racionalizar y un poco mas de algebra que dejamos al estudiante UNA para que complete los detalles.

4. a) La sucesión está dada por medio de $\begin{matrix} a_n = ka_{n-1} \\ a_0 \in \mathbb{R}, n = 0,1,2,\cdots, \end{matrix}$ con *k* entre 0,1. Es claro que $a_1 = ka_0$ luego la fórmula es válida para *n*=1. Supongamos que sea válida para el natural *m*, es decir $a_m = k^m a_0$. Tenemos, por definición de la recurrencia, que $a_{m+1} = ka_m = k\left(k^m a_0\right) = k^{m+1} a_0$ y luego la fórmula es válida para *m*+1, por inducción se sigue su validez para todo *n* natural. La parte b) se la dejamos al estudiante UNA que debe organizar su exploración.
5. Es un ejercicio para el estudiante UNA.
6. La fórmula propuesta vale para *n*=1 ya que 1=1. Supongamos que sea valida para *k*, esto es $1+2+3+\cdots+k = \frac{k(k+1)}{2}$. Entonces $1+2+\cdots+k+k+1 = \frac{k(k+1)}{2}+k+1$ ya que sumamos *k*+1 a ambos lados de la primera igualdad. Pero $\frac{k(k+1)}{2}+k+1 = (k+1)\left(\frac{k}{2}+1\right) = \frac{(k+1)(k+2)}{2}$ de donde la expresión es válida para *k*+1 y por inducción a todo natural *n.* La fórmula antes considerada fue descubierta, en un caso particular, por Gauss cuando era un niño de 8 años, los invito a ver el libro *Matemáticas y Matemáticos, cuentas y cuentos* de uno de los autores para que lean la hermosa historia de ese descubrimiento.
7. Es claro que la expresión considerada tiene sentido únicamente para valores de *a* distintos de 1. En el caso *n*=1 se tiene claramente la igualdad y el estudiante UNA debe decir la razón. Supongamos que la expresión es cierta para *n=k,* esto es $1+a+a^2+\cdots+a^k = \frac{1-a^{k+1}}{1-a}$. Sumemos a^{k+1} a ambos lados de la igualdad anterior, se obtiene $1+a+a^2+\cdots+a^k+a^{k+1} = \frac{1-a^{k+1}}{1-a}+a^{k+1}$, pero $\frac{1-a^{k+1}}{1-a}+a^{k+1} = \frac{1-a^{k+1}+a^{k+1}-a^{k+2}}{1-a} = \frac{1-a^{k+2}}{1-a}$ de donde la expresión es válida para *k*+1 y el resultado sigue por inducción matemática para todo valor de *n.*
8. Razone por el absurdo y suponga que tal número existe. Recordamos que $a<b$ si *b* se obtiene de *a* mediante la aplicación sucesiva de la función sucesor. Indique que contradicción encuentra.

9. Recomendamos al estudiante usar Maxima que tiene programada la función primep ( ) que devuelve el valor True si el número es primo y False si el número es compuesto, un enlace para descargar el software y un manual del mismo van estar disponibles en el Moodle de la asignatura. El estudiante puede hacer un pequeño programa para esta actividad. Lo primero es definir la función x^2+x+41 y luego aplicarle la función primep ( ) para distintos valores.

```
(%i1) primep(12);
(%o1) false
(%i2) primep(17);
(%o2) true
```

(Busque en el plan de Curso información de cómo usar el Moodle del cursoÁlgebra I)

10. Es claro que x^2+x+41 para *x* igual a 41 ya no es un número primo.
11. Cualquier polinomio con coeficientes enteros se escribe como $p(x)=a_0+a_1x+\cdots+a_{n-1}x^{n-1}+a_nx^n, a_i\in\mathbb{Z}, i=0,1,\cdots,n.$ Si el término independiente no es 1, basta tomar $x=na_0$ ya que para algún natural *n* $p(x)=p(na_0)+a_0+a_1na_0+\cdots+a_{n-1}(na_0)^{n-1}+a_n(na_0)^n$ va a ser un múltiplo del término independiente. Invitamos al estudiante UNA a que de los detalles que permiten garantizar esta afirmación. El caso problemático es cuando el término independiente es 1.
12. Sin duda esta fórmula es muy hermosa, es cierta para $n=1$ ya que $1^3=1^2$. Supongamos que sea cierta para el natural *k*, esto es

$$1+2^3+3^3+\cdots+k^3=(1+2+3+\cdots+k)^2\Rightarrow$$

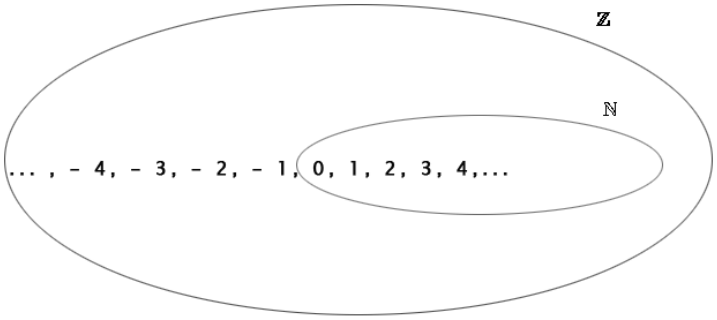
$$(1+2+3+\cdots+k+(k+1))^2=$$

$$(1+2+3+\cdots+k)^2+2(k+1)\left(\frac{k(k+1)}{2}\right)+(k+1)^2=$$

$$1+2^3+3^3+\cdots+k^3+(k+1)^3$$

UNIDAD 4

El número entero



Semana 7

"Dios creó el número natural, todo lo demás es creación del hombre" L. Kronecker(1823-1891)

Aplicar el concepto de número natural y entero y sus propiedades en el modelado matemático y en la demostración de nuevos resultados.

Contenidos a tratar: Construcción de los números enteros, divisibilidad, teorema fundamental de la aritmética.

Los Principios de Conservación en Física

El gran físico británico Michael Faraday demostró mediante brillantes experimentos que la carga eléctrica se conserva.

Michael Faraday (1791-1867). De origen muy humilde, solo pudo estudiar de manera autodidacta desempeñándose como bedel en el laboratorio de Davy. Su enorme originalidad y empeño lo llevo a sobrepasar a la mayor parte de los físicos de su época. Su trabajo sirvió de base experimental a Maxwell para enunciar sus leyes del electromagnetismo.

Por ejemplo, al frotar un material como el ámbar contra una piel de cuero, observamos que el ámbar se carga eléctricamente. Faraday disponía de ambos materiales, el ámbar y la piel en un globo metálico y medía la carga neta dentro del mismo con un galvanómetro. Observaba que la carga era nula. Es decir, la carga que ganaba el ámbar se debía a una pérdida de carga en la piel de cuero. Algún tiempo después, los físicos demostraron (Milikan) que la carga viene dada en unidades discretas, siendo la unidad básica la carga del electrón que identificaremos con -1. Por otro lado, la carga de un protón se identifica con +1. Un sistema como el átomo, tiene carga nula ya que tiene exactamente la misma cantidad de protones que de electrones. Si partimos de un sistema con carga nula y llamamos esta carga $q(t)$ en el tiempo t esta se va a conservar,

$$q(t) = 0$$

para cualquier instante t. Si algún componente del sistema adquiere una carga m positiva, el resto del sistema debe tener una carga $-m$ debido a que la carga total debe ser 0. Los números enteros son un *lenguaje adecuado* para la descripción de esta ley de conservación.

6.1 Introducción

La construcción que vamos a realizar es típica en matemáticas, de aquí su importancia. Se basa en introducir una relación de equivalencia en un conjunto y esperar que las clases de equivalencia resultantes gocen de determinada característica. Por eso empezaremos nuestra discusión repasando los conceptos de relación de equivalencia y producto cartesiano de conjuntos. Estos conceptos fueron estudiados en las unidades 1 y

La relación de equivalencia que vamos a definir trata de capturar la noción de *diferencia entre un par de números naturales.* Por supuesto, dicha noción es clara si tomamos la diferencia entre a y b con $a>b$. La construcción que realizamos permite clarificar qué entendemos por la diferencia entre a y b con $a<b$. *Esto permite construir el conjunto de los números enteros.* También, demostraremos que de manera canónica el conjunto de los números naturales *vive* dentro del conjunto de los números enteros, correspondiendo a lo que llamamos enteros positivos.

Posteriormente, revisaremos las nociones de divisibilidad en los enteros y el concepto de número primo. El algoritmo de Euclides y la criba de Eratóstenes son explicadas en detalle. Ideas como máximo común divisor y mínimo común múltiplo y sus relaciones mutuas son establecidas. Por último, demostramos el teorema fundamental de la aritmética, anticipándonos a desarrollos más avanzados de la Teoría de Anillos.

6.2 Ingredientes matemáticos de la construcción de los enteros

6.2.1 Relaciones de equivalencia

Como ya el lector conoce (vea la Unidad 2), las relaciones de equivalencia sirven para construir nuevos conjuntos conocidos como *clases de equivalencia*. Estos objetos poseen la propiedad que todos sus elementos son similares. Las clases de equivalencia son el elemento crucial para la construcción de los sistemas numéricos que vamos a emprender.

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$$

Cada paso de la construcción se logra mediante la introducción de una relación de equivalencia adecuada. Recordamos al lector que: *Una relación R es de equivalencia en un conjunto A si y sólo si*

1. *a R a para cualquier a en A (propiedad reflexiva),*
2. *a R b implica que b R a, y*

3. *Si a R b y b R c entonces a R c*

Ejemplos notables de relaciones de equivalencia fueron dados en la unidad 2 correspondiente a Relaciones. Recomendamos al estudiante volver sobre ellos en este momento.

Una clase de equivalencia agrupa a todos los elementos que están relacionados por una relación de equivalencia. Las clases de equivalencia son disjuntas entre sí y constituyen una partición del conjunto *A.* Esto es:

- Si dos clases A, B son distintas entonces $A \cap B = \varnothing$, y
- $\bigcup_{\alpha} \mathrm{A}_{\alpha} = A$

Debemos hacer notar que las propiedades anteriores caracterizan a las relaciones de equivalencia y que no ocurren para relaciones arbitrarias cualesquiera.
Vamos a recordar brevemente el otro ingrediente importante en la construcción de los sistemas numéricos.

6.2.2 Producto Cartesiano

Sean A,B dos conjuntos cualesquiera. El producto cartesiano de A y B es

$$A \times B = \{\text{todos los pares } (x, y) \text{ donde } x \in A, y \in B\}$$

Esto ya fue visto por el estudiante UNA en el Módulo I así que lo recordamos rápidamente. El producto cartesiano de conjuntos es una operación no conmutativa como debería verificar el lector mediante un ejemplo.

6.3 La idea detrás de la construcción

Consideremos los números naturales 0, 1, 2, 3, ⋯. Sabemos que este importante sistema tiene limitaciones para resolver ecuaciones del tipo $x + 2 = 1$. Durante mucho tiempo los matemáticos pensaron que tal ecuación era imposible de resolver. La idea

fue aceptar la aparición de números negativos que resolvían este problema. ¿Cómo se pueden poner los números negativos en un contexto matemático sólido? Vamos a responder a esto ahora de manera un poco informal y más adelante en el texto con la formalidad requerida para el futuro matemático o educador en matemática.

Observe los pares (3,0),(4,1),(5,2),(6,3),… Note que la diferencia entre la primera y la segunda entrada siempre es 3. Lo mismo ocurre con (24,21) y muchos otros. Podríamos pensar que si agrupamos a todos esos pares en un solo conjunto (clase de equivalencia) obtenemos una representación del 3. ¿Puede Ud. representar con la misma idea al número 2?. Note que los pares considerados pertenecen al producto cartesiano $\mathbb{N}\times\mathbb{N}$. Ahora bien, consideremos los pares (0,3),(1,4),(2,5)… note que la diferencia entre la segunda entrada del par y la primera es 3. Lo contrario que con nuestra primera agrupación. Aquí está la gran idea:¡ los pares (0,3),(1,4),(2,5)… representan al número negativo -3! ¿Puede Ud. Representar con la misma idea al número -2?. Así la idea para construir los números enteros consta de dos pasos:

1. Construir el producto cartesiano $\mathbb{N}\times\mathbb{N}$.
2. Introducir una relación de equivalencia en el que capture lo que significa ser un entero positivo y un entero negativo.

No se preocupe si estas ideas le parecen un poco difusas, por ahora lo son. Cuando el lector estudie la construcción de los enteros y racionales entre otros sistemas numéricos las verá en completo detalle y entenderá que la misma idea se repite una y otra vez.

6.2 La construcción de $\mathbb{Z}$

Definimos en el conjunto $\mathbb{N}\times\mathbb{N}$ la relación siguiente

$$(a,b)R(c,d) \Leftrightarrow a+d=b+c$$

Proposición 1. $(a,b)R(c,d) \Leftrightarrow a+d=b+c$ *es una relación de equivalencia.*

Demostración. Veamos que la relación es reflexiva. Tomemos un par ordenado (a,b), queremos ver que $(a,b)R(a,b)$, esto equivale a demostrar que $a+b=a+b$, lo cual es cierto. La relación es simétrica, ya que si

$$(a,b)R(c,d) \Rightarrow a+d=b+c \Rightarrow c+b=d+a \Rightarrow (c,d)R(a,b)$$

Por último, verificamos la propiedad transitiva. Supongamos que $(a,b)R(c,d)$ y $(c,d)R(m,n)$. Esto implica que $a+d=b+c$ y $c+n=d+m$, de donde $a+d+n=b+c+n \Rightarrow a+d+n=b+d+m$. Aplicando la ley de cancelación de los números naturales, la última igualdad implica que

$$a+n=b+m \Rightarrow (a,b)R(m,n)$$

Lo que concluye la demostración.

Cualquier relación de equivalencia particiona el conjunto $\mathbb{N}\times\mathbb{N}$ en clases de equivalencia, denotaremos como es usual estas clases por $[(a,b)]$.

Definición. El conjunto $\mathbb{Z}$ es el conjunto cociente $\mathbb{N}\times\mathbb{N}/R$

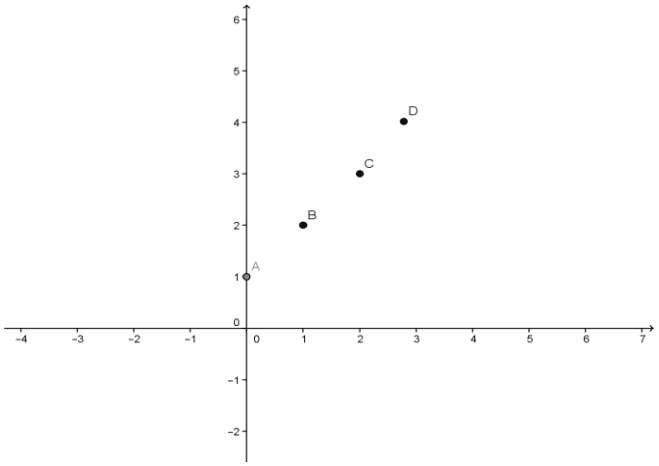
Vamos a calcular explícitamente una de esas clases y analizar su significado.

Un ejemplo de una clase de equivalencia

Los pares $\{(1,0),(2,1),(3,2),\cdots\}$ constituyen una clase de equivalencia, ya que cualquier elemento de este conjunto se escribe como $(n+1,n)$ donde *n* es un natural arbitrario y luego

$$(n+1,n)R(m+1,m)$$

ya que $n+1+m=m+1+n$. Esta clase representa al natural 1.



Clase de equivalencia que representa al natural 1

El lector ya debe intuir qué clase representa al entero -1, pero dejamos esto como un ejercicio.

Algo que es muy importante es observar que todos los números naturales son parte del conjunto cociente $\mathbb{N}\times\mathbb{N}/R$ como lo expresa el siguiente teorema.

Teorema 2. *La aplicación*

$$F:\mathbb{N}\to{}^{\mathbb{N}\times\mathbb{N}}\!/_{R}$$

dada por la regla

$$F(n)=\left[(n,0)\right]$$

Es inyectiva.

Demostración. Supongamos que $F(n)=F(m)$ para números naturales n,m. Entonces $F(n)=\left[(n,0)\right]=\left[(m,0)\right]=F(m)$, luego $\left[(n,0)\right]=\left[(m,0)\right]\Rightarrow(n,0)R(m,0)\Rightarrow n=m$ De donde la aplicación es inyectiva.

Así, podemos identificar de manera unívoca cada natural *n* con la clase $\left[(n,0)\right]$.

 Los matemáticos dicen que los naturales pueden ser "sumergidos" en el conjunto $\mathbb{Z}$ de mediante el homomorfismo que a cada natural *n* le asocia la clase $[(n,0)]$. El concepto de homomorfismo lo estudiaremos en el módulo 3

6.3 Operaciones en $\mathbb{Z}$

Adición o suma de enteros

Tenemos que definir una operación de suma en el conjunto cociente $\mathbb{N}\times\mathbb{N}/R$ y que esté basada en la suma que definimos para los números naturales.

Lo hacemos de manera natural.

Dadas dos clases de equivalencia $[(a,b)]$ y $[(c,d)]$ definimos

$$[(a,b)]+[(c,d)]=[(a+c,b+d)]$$

El estudiante debe observar algo muy importante. *La anterior definición es correcta sí y sólo sí la suma definida no depende de los representantes que tomemos de las clases* $[(a,b)]$ y $[(c,d)]$. Es decir, debemos demostrar que si
$(a,b)R(m,n)$ y $(c,d)R(p,q)$ entonces

$$[(a+c,b+d)]=[(m+p,n+q)]$$

De lo contrario la operación no tendría sentido matemático, ya que variando los representantes de la clase, se obtendrían resultados distintos.

Teorema 3. *Si* $(a,b)R(m,n)$ y $(c,d)R(p,q)$ *entonces*

$$[(a+c,b+d)]=[(m+p,n+q)]$$

Demostración. Sabemos que $(a,b)R(m,n)$ y $(c,d)R(p,q)$ y esto implica que $a+n=b+m$ y $c+q=d+p$. Luego $a+n+c+q=b+m+d+p$ y , aplicando la propiedad asociativa de la adición, esto implica que $(a+c)+(n+q)=(b+d)+(p+m)$: Luego

$$[(a+c,b+d)]=[(m+p,n+q)].$$

Hemos terminado la demostración.

 Los matemáticos usualmente se refieren a los resultados similares al anterior como *verificación que la ley de composición interna está bien definida.* El estudiante encontrará la definición de ley de composición en la Unidad 7.

La suma definida en los enteros verifica la *propiedad conmutativa*, en efecto

$$[(a,b)]+[(c,d)]=[(a+c,b+d)]$$

pero $[(c,d)]+[(a,b)]=[(c+a,d+b)]$ y usando la conmutatividad de la suma de los números naturales vemos que

$$[(a,b)]+[(c,d)]=[(a+c,b+d)]=[(c+a,d+b)] \ =[(c,d)]+[(a,b)]$$

 Verifique que la suma en los enteros cumple la propiedad asociativa.

Un hecho importante es que existe un elemento neutro para la suma de números enteros.

Teorema 4. *La clase de equivalencia* $[(a,a)]$ *donde a es un natural arbitrario verifica que*

$$[(a,a)]+[(c,d)]=[(c,d)]$$

Demostración. Basta ver que $[(a+c,a+d)]=[(c,d)]$. Pero esto sigue de manera inmediata de que $a+c+d=a+d+c$, lo que concluye la demostración. □

El gran propósito de los números enteros es poder resolver las ecuaciones del tipo $x+b=a$ donde *a,b* son números naturales *arbitrarios.* Muchas de estas ecuaciones no admiten solución en los números naturales. Por ejemplo, si *b>a* la ecuación no tiene solución en los naturales. Como sabemos, la introducción de los números enteros resuelve este problema.

Teorema 5. *Dado cualquier número entero* $[(a,b)]$ *con a,b naturales cualesquiera, existe un entero* $[(c,d)]$ *que verifica* $[(a,b)]+[(c,d)]=[(0,0)]$. *Es decir, todo entero tiene un inverso para la operación de la suma.*

Demostración. La idea es muy sencilla. Tomemos la clase $[(b,a)]$ y verifiquemos que $[(a,b)]+[(b,a)]=[(0,0)]$. En efecto, $[(a,b)]+[(b,a)]=[(a+b,b+a)]=[(0,0)]$. Esto concluye la de mostración. □

Observación: *Al invertir los elementos del par* (a,b) *hemos generado la clase que corresponde a la idea de inverso aditivo de* $[(a,b)]$. *Por ejemplo, el inverso aditivo de 2 es la clase* $[(0,2)]$. *Esta es la idea central de la construcción que hemos hecho*.

Hemos demostrado que los números enteros con la operación de suma antes definida constituyen un grupo abeliano. El concepto de grupo lo verá el estudiante en detalle en el módulo III de este curso.

Producto en los enteros $\mathbb{Z}$

Si la clase $[(a,b)]$ representa al entero $a-b$ y observando que $(a-b)(c-d)=ac+bd-(ad+bc)$ resulta natural definir

$$[(a,b)]\,[(c,d)]=[(ac+bd,ad+bc)]$$

Como hemos hecho anteriormente, debemos demostrar que la operación producto está bien definida en el conjunto cociente.

Teorema 6. *Si* $(a,b)R(m,n)$ y $(c,d)R(p,q)$ *entonces*

$$\left[(ac+bd,ad+bc)\right]=\left[(mp+nq,mq+np)\right]$$

Demostración. Es un ejercicio para el estudiante UNA ya que es muy similar a lo hecho para la suma.

Una cosa que siempre nos preguntan nuestros estudiante es por qué se verifica la regla "*menos por menos da más*". Hay muchas respuestas a esta pregunta, pero sería justo que obtengamos esta propiedad a partir de nuestra construcción. Observe que $\left[(0,1)\right]\left[(0,1)\right]=\left[(0\cdot 0+1\cdot 1,0\cdot 1+1\cdot 0)\right]=\left[(1,0)\right]$, es decir ¡(-1)(-1)=1!. La famosa regla de los signos ha sido demostrada dentro de nuestra construcción.

1. Demuestre de manera análoga que "menos por más es igual a menos"
2. Demuestre que la multiplicación de enteros es conmutativa.
3. Demuestre que $\left[(1,0)\right]\left[(a,b)\right]=\left[(a,b)\right]$ para cualquier clase $\left[(a,b)\right]$. Este problema demuestra que 1 es el elemento neutro para la multiplicación de enteros.

1. Multipliquemos (-1)(1), esto es $\left[(0,1)\right]\left[(1,0)\right]=\left[(0+0,0+1)\right]=\left[(0,1)\right]$.
2. Por definición, $\left[(a,b)\right]\left[(c,d)\right]=\left[(ac+bd,ad+bc)\right]$, luego $\left[(c,d)\right]\left[(a,b)\right]\left[(ca+db,da+cb)\right]$, pero al ser conmutativa la suma y producto de naturales se verifica el resultado.
3. Se deja al estudiante UNA que solamente debe aplicar la definición de la multiplicación.

Teorema 7. (Propiedad distributiva de la multiplicación respecto a la suma)

$[(a,b)]([(c,d)]+[(e,f)])=[(a,b)][(c,d)]+[(a,b)][(e,f)]$ *para cualesquiera clases* $[(a,b)],[(c,d)]$ y $[(e,f)]$.

Demostración. Como

$[(a,b)]([(c,d)]+[(e,f)])=$

$[(a,b)][(c+e,d+f)]=[(a(c+e)+b(d+f),a(d+f)+b(c+e)]=$

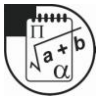
$[(ac+ae+bd+bf,ad+af+bc+be)]=[(ac+bd,ad+bc)]+[(ae+bf,af+be)]=$

$[(a,b)][(c,d)]+[(a,b)][(e,f)]$ □

Hemos demostrado que los números enteros con al operación de suma antes definida constituyen un anillo conmutativo. El concepto de anillo lo verá el estudiante en detalle en el módulo III de este curso.

Demuestre que $[(a,a)][(c,d)]=[(a,a)]$ para cualquier clase $[(c,d)]$. Este problema demuestra que 0xa=0 para cualquier entero a.

Por definición de producto, $[(a,a)][(c,d)]=[(ac+ad,ad+ac)]=[(a,a)]$.



Hemos demostrado que los números enteros son un anillo con unidad siendo la unidad la clase del par (1,0)

A partir de este momento, nuestro lector puede relajarse y considerar a los enteros como el conjunto $\mathbb{Z}=\{\cdots,-3,-2,-1,0,1,2,3,\cdots\}$ pero debe estar consciente de que existe una

manera rigurosa para construir tan importante conjunto. A los números naturales 0,1,2,… los denominaremos muchas veces como enteros positivos. Los números -1,-2,-3,… serán denominados como enteros negativos. El siguiente resultado demuestra que una clase muy grande de ecuaciones de primer grado siempre tiene solución única en $\mathbb{Z} = \{\cdots, -3, -2, -1, 0, 1, 2, 3, \cdots\}$

Teorema 8. La ecuación

$$x + a = b$$

donde *a* y *b* son enteros arbitrarios, siempre es soluble de manera única en el anillo de los enteros.

Demostración. Para resolver la ecuación sumamos a ambos lados el opuesto de *a,* esto es *–a*. Obtenemos, $x + a + (-a) = b + (-a) \Rightarrow x + 0 = b + (-a)$. Luego,

$$\overline{0}.$$

Hemos encontrado la solución de la ecuación, su unicidad se deduce del procedimiento empleado para hallarla.

Observación: Recomendamos a cada profesor de matemáticas que al resolver cualquier ecuación lo haga de manera sistemática y lógica. Eso de pasar de un lado para el otro, es propio del fútbol y no de la matemática.

Nuestra siguiente sección es muy importante.

6.5 Divisibilidad en los enteros

Un concepto importante en matemática es el de divisor. El concepto es muy antiguo ya que sin duda el hombre entendía claramente lo que era dividir un número entero en partes iguales. Los primeros resultados del tema aparecen ya en la obra de Euclides *Los Elementos (Stokheia).*

Definición. Sean a, b enteros cualesquiera con $b \neq 0$. Decimos que *b* divide a *a* si y sólo si existe un entero c tal que

$$a = bc$$

En este caso decimos que *b* es un divisor de *a* o que *a* es divisible por *b.*

Notación: Escribimos $a \mid b$ sí y sólo sí *a* divide a *b.*

1. -2 divide a 6 ya que 6=(-2)(-3)
2. Si *b* divide a *a* entonces *–b* también divide a *a.*
   En efecto, como $a = bc$ entonces $a = (-b)(-c)$ y esto implica, por la definición anterior que *–b* divide a *a*
3. 1 divide a cualquier entero *a.*
   En efecto, como $a = 1.a$ el resultado sigue de inmediato. Combinando este resultado con el ejemplo anterior, vemos que -1 divide a cualquier entero *a.*
4. Cada uno de los números 2,-3 y 5 tiene cuatro y solamente cuatro divisores.
   En efecto, por comprobación directa vemos que los divisores de 2 son ± 1, y ± 2.

Invitamos al estudiante UNA a que liste los divisores de -3 y 5 para comprobar la afirmación.

El siguiente resultado es muy útil en la teoría de números.

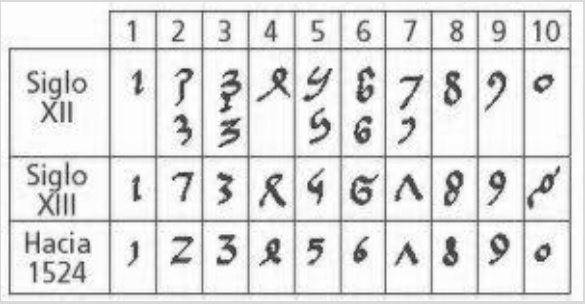
Teorema 9. *Sean a,b,c enteros con a distinto de 0. Si a divide a b y a divide a c entonces a divide a b+c.*

Demostración. Sabemos que *b=ak* para un cierto entero *k* y *c=aj* para un cierto entero *k* por la definición de divisibilidad. Pero, *b+c= ak+ aj=a*(*k+j*), luego *a* divide a *b+c.* □


(**Criterio de divisibilidad por 3 y 9)**

Escribamos el número *a* en base 10, tenemos $a = a_0 + a_1 10 + a_2 10^2 + \cdots + a_n 10^n$. Esto se puede escribir como $a = a_0 + a_1(9+1) + a_2(9+1)^2 + \cdots + a_n(9+1)^n$. Usando la fórmula del binomio de Newton para expandir $(9+1)^j$, obtenemos $a = 9N + (a_0 + a_1 + \cdots + a_n)$. De donde *a* es divisible por 3 o 9 si y sólo si la suma de sus dígitos es divisible por 3 o 9 ya que tanto 3 como 9 dividen a 9*N*.

Base 10 y los hindúe



Los hindúes introdujeron un sistema en base 10 posicional y con el número 0. Esto significó un avance extraordinario en la matemática ya que el sistema de numeración romano era engorroso para representar los números y efectuar con ellos operaciones aritméticas. El sistema posicional permitía con sólo 10 símbolos representar un número cualquiera. Este sistema fue expuesto por Fibonacci en su importante obra Liber Abaci en 1202.

Escriba y demuestre un criterio de divisibilidad por 5.

El número escrito en base 10, debe terminar en 5 o en 0. Para ver esto escriba el número como un polinomio en potencias de 10, por ejemplo 104 es 10^2+4 y es claro que 5 va a dividir a cada potencia de 10 que aparezca en la suma. Ud. debe completar los detalles.

Demostrar que es imposible que un cuadrado se pueda escribir como la suma de dos cuadrados impares

Solución. Vamos a aplicar reducción al absurdo. Supongamos que

$$x^2 + y^2 = z^2$$

Con *x,e impares*, luego $x = 2j+1, y = 2m+1$ con *j,m* enteros. Como z^2 es la suma de dos impares, entonces z debe ser par. ¿Porqué?. Luego $z = 2r$. Así,

$x^2 + y^2 = z^2 \Rightarrow (2j+1)^2 + (2m+1)^2 = (2r)^2$. Luego

$4j^2 + 4j + 1 + 4m^2 + 4m + 1 = 4r^2$ y esto implica que 4 debe dividir a 2, lo cual es un absurdo.

Las ternas pitagóricas.

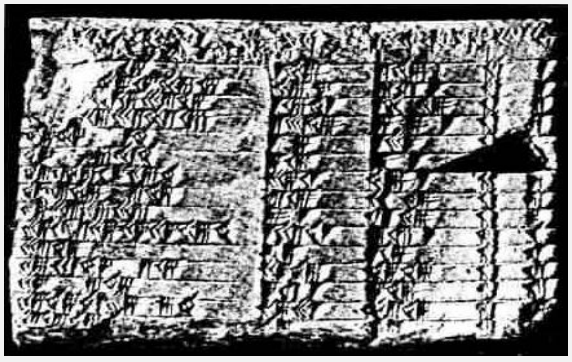
Un trío de números como 3,4, y 5 satisface

$$3^2+4^2=5^2.$$

Es decir, podemos construir un triángulo rectángulo que tenga como catetos lados que midan 3 y 4 y cuya hipotenusa mida 5. En honor a Pitágoras tales ternas se denominan Pitagóricas. Que existen infinitas ternas Pitagóricas se deduce de la identidad algebraica

$$(n^2-1)^2 + (2n)^2 = (n^2+1)^2, n \in \mathbb{N}$$

Tablas de ternas pitagóricas nos vienen desde Babilonia quienes las escribieron hacia 1800 a.C.



Tableta Plimpton 322 con ternas pitagóricas

Los egipcios también las conocían y usaban con fines prácticos ya que les permitían construir triángulos rectángulos mediante cuerdas con nudos. Todo esto ocurrió mucho antes que Pitágoras hubiese nacido.

Teorema 10. *Si* $a \mid b$ y $b \mid c \Rightarrow a \mid c$

Demostración. Es un ejercicio para el estudiante UNA.

1. Introducimos una relación *R* en los enteros definida por medio de *a R b* sí y sólo sí $a \mid b$. Demuestre que *R* es una relación de orden.

El siguiente concepto es fundamental para el desarrollo de la aritmética, es el concepto de número *primo*. Sabemos desde la escuela primaria que los números primos son los bloques fundamentales que permiten descomponer cualquier número. Por ejemplo, 122=2.61 siendo 2 y 61 números primos, es decir números "atómicos", números que no podemos descomponer más.

Definición. *Decimos que un número entero a es primo si tiene exactamente cuatro divisores.*

1. 7 es primo ya que los divisores de 7 son 1,-1,7 y -7.
2. 1 no es primo ya que admite solo dos divisores :1 y -1.

El siguiente teorema aparece en los *Elementos* de Euclides y es uno de los resultados más bonitos de esa obra. Probemos antes un lema muy sencillo

Lema 11. *Si a es distinto de* 1 *y* -1 *y a no es primo, entonces a debe admitir un divisor primo.*

Demostración. Sea *p* el menor entero positivo, distinto de 1 que divide a *a.* Si *p* tiene divisores distintos de 1,-1, *p* y *–p* entonces podemos encontrar un *q* entero positivo, distinto de 1 que divide *p.* Luego $1<q<p$. Como *q* divide *p* y *p* divide a *a* entonces *q* divide a *a.* Esto contradice la elección de *p.* □

El siguiente resultado y su demostración es una joya matemática, además de ser fundamental en aritmética y álgebra.

Teorema 12. (Infinitud de los números primos de Euclides)

Existen infinitos números primos positivos.

Demostración. Razonamos por reducción al absurdo. Si suponemos lo contrario, podemos listar todos los números primos naturales $\{q_1, q_2, \cdots, q_n\}$. Formemos el número

$$\prod_{i=1}^{n} q_i + 1 = q_1 \cdot q_2 \cdots q_n + 1.$$

Obviamente este número es mayor que cualquiera de los números de la lista $\{q_1, q_2, \cdots, q_n\}$. Luego no es primo y por el lema anterior, debe admitir un divisor primo q_j. Pero con seguridad q_j divide a $\prod_{i=1}^{n} q_i$ y luego q_j divide a 1. Una contradicción que viene de suponer que hay finitos números primos. □

6.5.1 Algoritmo de Euclides y Máximo común divisor

Sean *p, q* naturales cualesquiera con *q* distinto de 0. Vamos a demostrar que

$$p = q.c + r \text{ con } 0 \le r < q.$$

Aún más, la escogencia de *r* y *c* es única. Este resultado conocido por Euclides y por nuestros estudiantes de primaria constituye la base teórica de lo que llamamos división inexacta.

Tomemos 16 y 7. Vemos que 16=2.7+2, aquí *r*=2 y *c*=2.

Vamos a demostrar que de ser posible la escritura $p = q.c + r$ con $0 \le r < q$ está escritura es única.

Teorema 13. *Si* $p = q.c + r$ *con* $0 \le r < q$ *y* $p = q.c' + r'$ *con* $0 \le r' < q$ *entonces* $r = r', c = c'$.

Demostración. Como $p = q.c + r$ y $p = q.c' + r'$ restando ambas igualdades, obtenemos que 0= $q(c - c')' + r - r'$ de donde $q \mid r - r'$. Pero como $0 \le r < q$ y $0 \le r' < q$ entonces $r = r'$. Así, $q(c - c')' = 0 \Rightarrow c = c'$. □

Ahora finalizaremos nuestra demostración del algoritmo de Euclides.

Demostración del algoritmo de Euclides. Supongamos que tenemos *p,q* naturales con *p>q*. Sabemos que existe un natural *n* tal que $nq \ge p$. Tomemos el menor natural $c+1$ con esta propiedad, esto es $(c+1)q > p$. En el caso que fuera $cq = p$ estaríamos listos. Por otro lado si $cq > p$ entonces $c\ q < p \Rightarrow\ p = cq + r$ donde $0 \le r = p - cq$.

Pero $(c+1)q > p \Rightarrow cq + q > p \Rightarrow q > p - cq$ y de aquí se obtiene que $0 \le r < q$ y esto es lo que queríamos demostrar. □

Euclides tenía en mente usar su algoritmo para demostrar la existencia del máximo común divisor, sigamos sus pasos.

Dados dos enteros positivos *n,m* vamos a demostrar que existe un entero que divide a los dos enteros *n,m* y es el mayor entero con esta propiedad. Tal número *se denomina el máximo común divisor de n y m.*

Teorema 14. *Dados dos enteros positivos n,m existe un entero positivo que divide a los dos enteros n,m y es el mayor entero con esta propiedad.*

Demostración. Consideremos el conjunto $A = \{kn + jm > 0 \text{ con } k, j \in \mathbb{Z}\}$. Ese conjunto es no vacío y por ende tiene un menor elemento, que denominaremos *M.* Por definición de *M* podemos encontrar enteros k_0, j_0 tales que

$$M = k_0 n + j_0 m$$

Observe que cualquier divisor de *n* y *m* divide necesariamente a *M.* Pero, de hecho, *M* divide a *n* y *m.* En efecto, si ponemos

$n = Mc + r \Rightarrow n = (k_0 n + j_0 m) + r \Rightarrow n(1 - k_0) - j_0 m = r \in A$, así si $0 < r < M$

tendríamos una contradicción con la definición de *M* . Luego *M* divide a *n* y *m* y es el mayor entero con esta propiedad. □

Observación: La demostración anterior prueba que el máximo común divisor *M* de dos números *a, b* siempre se escribe como

$$M = ka + bj$$

Para ciertos enteros *k, j*. Esta propiedad es muy útil y la usaremos posteriormente.

El algoritmo de Euclides permite encontrar el máximo común divisor (M.C.D.) de dos números enteros positivos de manera muy ingeniosa. Al parecer este resultado fue el que motivó a Euclides a demostrar su algoritmo de la división.

Tome los números 40 y 16. Entonces $40=16\cdot 2+8$, ahora divida 16 por 8, $16=8\cdot 2+0$, como el residuo es 0, entonces 8 es el M.C.D. de 16 y 40. ¿Por qué funciona esto? Observe que el último residuo no nulo divide tanto a 40 como a 16, ¿porqué? Por otro lado, si *k* divide tanto a 40 como a 16 entonces *k* divide a 8. El estudiante UNA debe explicar claramente por qué.

1. Halle, usando el algoritmo de Euclides, el M.C.D. de 36 y 370. Al terminar, repita el cálculo tomando los factores primos que dividen tanto a 36 como a 370 con su menor exponente y calcule el M.C.D. como lo hacía en bachillerato.

2. Demuestre que si $2^n - 1$ es primo entonces *n* debe ser primo, aquí por supuesto *n* es un número natural.

1. Lo dejamos al estudiante UNA ya que es un cálculo elemental.
2. Supongamos que *n* se puede factorizar como $n = ab, a \neq 1$ y $b \neq 1$, recordamos de bachillerato que $x^{ab} - 1 = \left(x^a - 1\right)\left(1 + x^a + x^{2a} + \overset{\text{b-1 veces}}{\ldots} + x^{(b-1)a}\right)$. Ahora aplique la identidad anterior tomando *x* igual a 2 y se obtiene el resultado.

El siguiente teorema es básico.

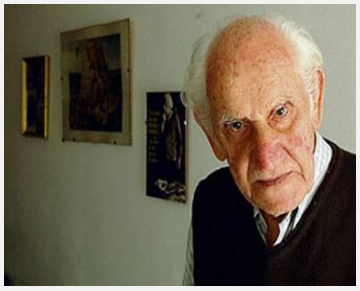
Teorema. *Si p es primo y p divide a ab entonces p divide a a o p divide a b.*

Demostración. Si *p* no divide a *a* entonces el MCD de *p* y *a* es 1, es decir $1 = ak + jp$ para ciertos enteros *j,k.* Luego $b = akb + pjb$ de donde *p* divide a *b*, ¿por qué?, como deseábamos demostrar. □

Nuestra próxima sección demuestra un resultado importante y que se generaliza a estructuras matemáticas más complejas que el anillo de los enteros.

6.6 El Teorema Fundamental de la Aritmética

El profesor Mischa Cotlar decía que los números primos eran los bloques que servían para construir los demás números, la idea es sencilla y la conocemos desde la primaria.



Mischa Cotlar (1912-2007) matemático argentino de origen ruso, desarrollo un importante trabajo en análisis funcional donde destaca su resultado fundamental: el Lema de Cotlar. Escribió sobre nuestro tema un excelente libro, con Cora Ratto de Sadovsky, Introducción al Álgebra (Eudeba, 1966).

Si tomamos el número 120, este se escribe como $5\cdot 24$ y el factor 5 es atómico: no admite otra descomposición. Pero 24 ¡si!, así $120=5\cdot 3\cdot 8=5\cdot 3\cdot 2\cdot 2\cdot 2$ y ya no podemos dividir ningún factor más porque todos son números primos. Este hecho constituye la base del siguiente importante teorema.

Teorema 15. (Fundamental de la Aritmética)

Todo número n natural se escribe de manera única, salvo en el orden de la descomposición, como un producto de números primos. Esto es,

$$n=\prod_{j=1}^{r} p_j$$

donde cada p_j es primo y en cualquier descomposición de n de este tipo deben aparecer los mismos primos p_j.

Demostración. La prueba es por inducción. Supongamos que hemos probado el enunciado hasta el entero $k>2$. Si $k+1$ es primo, no hay nada que probar. Si $k+1$ no es primo entonces debe existir un primo j que divide a $k+1$, esto es

$$k+1=jm$$

Pero $m<k$ y por hipótesis inductiva m admite una descomposición única de la forma $m=\prod_{j=1}^{r} p_j$. Luego,

$$k+1=j\prod_{j=1}^{r} p_j$$

De donde concluimos que $k+1$ admite una representación como producto de primos y solo faltaría ver que la descomposición es única. Supongamos que $k+1=\prod_{j=1}^{s} q_j$. Como j divide a $\prod_{j=1}^{s} q_j$ entonces, por el teorema anterior, j debe aparecer en la lista de los q_j. El estudiante UNA debe decir porqué. Luego $\prod_{j=1}^{s} q_j = j\prod_{j=1}^{s-1} q_j$ y luego $\prod_{j=1}^{s-1} q_j = m$. Pero m

admitía una representación única, así los q_j son los mismos p_j y esto termina la demostración. □

1. Demuestre que dado un número natural *n* que no es divisible por ningún número primo menor o igual que $\sqrt{n}$ entonces es *n* primo.
2. Construya un programa para computadora que verifique si un número es primo o no.
3. Demuestre que el número $2^n - 1$, con *n* número natural , es primo sólo sí *n* es impar o 2.
4. Considere la progresión aritmética 11+6*n*, $n = 0,1,2,\cdots$. Vemos que los primeros términos son 11, 17, 23 y 29 que son todos números primos. Demuestre que es imposible que la progresión 11+6*n* de solo valores primos.
5. Probar que cualquier primo es de la forma 4*m*+1 o 4*m*+3 para cierto entero *m.*

1. Supongamos lo contrario (reducción al absurdo) y que *n* no sea primo. Por inducción matemática existe un primo *p* que es el más pequeño que divide a *n.* Luego, $p > \sqrt{n}$. Como *n* no es primo entonces *n* es distinto de *p* y debe admitir otro divisor primo, digamos p_1 donde p_1 es mayor o igual a *p y luego* $p_1 > \sqrt{n}$. Pero pp_1 debe dividir a *n* y además $pp_1 > \sqrt{n}\ \sqrt{n} = n$ lo que es absurdo.
2. Sugerencia: Use el resultado anterior y la criba de Eratóstenes para su pequeño programa.
3. Si *n* es par mayor que 2 entonces *n* se escribe como 2*k* y *k*>1, *k* natural, luego $2^n - 1 = 2^{2k} - 1 = \left(2^k - 1\right)\left(2^k + 1\right)$, y esto nos dice que $2^n - 1$ es compuesto.
4. Tome 11+6*n* y considere valores de *n* que son múltiplos de 11, en este caso 11+6*n* es un número compuesto.
5. Si aplicamos el algoritmo de Euclides vemos que cualquier número natural es de la forma *4m, 4m*+1, *4m*+2 *o* de la 4*m*+3. Es claro que los números de la forma

4m y *4m*+2 son compuestos, así que los primos deben estar contenidos en los números de la forma 4*m*+1 o 4*m*+3.

1. Consideremos el polinomio $f(n)=n^2+n+17$ donde la variable n es un número natural. Estudie si *f*(0),*f*(1*),…*, *f*(16) son números primos. ¿Puede ser *f*(*n*) primo para todo natural *n*?.
2. Demuestre que para cualquier *n* natural es posible encontrar *n* naturales consecutivos ninguno de los cuales es un número primo.
3. Demuestre que hay infinitos primos de la forma 4*n*+3 donde *n* es un número natural.
4. Use la criba de Eratóstenes mejorada para hallar todos los primos del 1 al 400.
5. Sean *a,b* y m números naturales. Demuestre que si *a,b* son primos entre si y *a*/*bm* entonces *a/m*.
6. Halle, mediante el algoritmo de Euclides, el M.C.D. entre 1122 y 216.
7. ¿Es cierto que si *a /bc* entonces *a/b* o *a/c*?
8. Encuentre los posibles valores de *n*, con *n*<30, natural para poder escribir cualquier primo mayor que 30 como 30*m*+*n* donde *m* es un número entero.
9. Demuestre que si a^2+b^2 es divisible por 3 entonces tanto *a* como *b* son divisibles por 3, donde *a,b* son números naturales
10. ¿Es posible encontrar enteros no nulos *n,m* tales que $n^2=12m^2$?.

1. Es claro que si *n* es múltiplo de 17 entonces *f*(*n*) no es primo. Sin embargo, si el estudiante realizó la comprobación sugerida observó que todos los primeros casos son primos.
2. Tome *n*! y observe que *n*!+2 es compuesto, lo mismo que *n*!+3, y así sucesivamente, esto es *n*!+*k* es compuesto si *k*<*n*. El problema implica que, en la sucesión de los números naturales, hay lagunas tan grandes como usted quiera donde no hay primo alguno.

3. Un bonito problema con cierto grado de dificultad. Todas las variables n,m,k entre otras que usemos representan números naturales. Ya sabemos que cualquier primo impar debe ser de la forma $4n+1$ o de la forma $4n+3$. Luego, al menos una de estas sucesiones $4n+1$ o $4n+3$ debe contener infinitos primos. Observamos que cualquier número natural de la forma $4j+3$ compuesto debe admitir un divisor primo de la forma $4n+3$, esto es debido a que el producto de naturales de la forma $4n+1$ es un número de la misma forma, es decir $\prod_{i=1}^{n}(4k_i+1)=4m+1$. El estudiante UNA debe decir por qué. Ahora imitamos a Euclides, razonemos por reducción al absurdo suponiendo que hay una cantidad finita de primos de la forma $4n+3$ y que estos son $3<7<\cdots<4n+3<\cdots<4N+3$. Formemos el producto de todos ellos $\prod_{i=1}^{r}(4k_i+3)$, este número es impar, compuesto y debe ser de la forma $4T+1$ o de la forma $4G+3$. Supongamos la primera posibilidad, esto es $\prod_{i=1}^{r}(4k_i+3)=4T+1$. Sumemos 2 a ambos lados de la igualdad anterior y obtenemos $\prod_{i=1}^{r}(4k_i+3)+2=4T+3$, es claro que $4T+3$ es mayor que cualquiera de los primos $3<7<\cdots<4n+3<\cdots<4N+3$ y por ende es compuesto ya que $4N+3$ era el mayor primo de esta forma. Por nuestra observación hecha anteriormente, $4T+3$ debe admitir un divisor primo de la lista $3<7<\cdots<4n+3<\cdots<4N+3$ digamos $4w+3$. Pero esto implica que $4w+3$ debe dividir a 2 lo que es absurdo. En el caso que el producto $\prod_{i=1}^{r}(4k_i+3)+2=4T+3$ procedemos de manera similar, sumando 4 a ambos lados, para obtener una contradicción, esto lo dejamos para el estudiante UNA.
4. Debe ser realizado por el estudiante UNA.
5. Si a,b son primos entre sí entonces existen enteros x,y tales que $ax+by=1$. Luego, multiplicando por m la igualdad anterior se tiene que $max+mby=m$. Observe que max y mby son múltiplos de a, luego m lo es también como queríamos demostrar.
6. Realice las divisiones sucesivas y encuentre el último resto no nulo tal como fue indicado en el texto.

7. Eso es falso, ya que 6 divide a 2.3 pero 6 no divide ni a 2 ni a 3.
8. El número *n* debe ser coprimo con 30, luego *n* debe ser alguno de los siguientes naturales 1,7,11,13,17,19,23 y 29.
9. Un resultado muy hermoso el de este problema. Es claro que si *a* es múltiplo de 3 entonces *b* también lo es. Así, si vamos a trabajar por reducción al absurdo, podemos suponer sin perder generalidad alguna que ni *a* ni *b* son múltiplos de 3. Luego, $a=3n+1$ o $a=3n+3$ y $b=3k+1$ o $b=3k+2$. Debemos examinar entonces 4 posibilidades.

Caso 1

$a=3n+1,\ \ b=3k+1$, luego $(3n+1)^2+(3k+1)^2=9n^2+6n+1+9k^2+6k+1=3j$ y esto implica que 3 divide a 2, lo cual es absurdo. Los otros casos son similares y se los dejamos al estudiante UNA.

10. Esto es imposible ya que $12=2^2 3$.

UNIDAD 5

Los enteros módulo *n*

Semana 8

Aplicar el concepto de número entero módulo n y sus propiedades en la resolución de problemas, en el modelado matemático y en la demostración de nuevos resultados

Contenidos a tratar: El concepto de números congruentes módulo *n* y su aritmética.

7.1 Introducción: ¿Cómo contamos las horas?

Si le preguntamos a un niño de nueve años qué hora es al transcurrir 4 horas después de las 9 am, responderá, en poco tiempo, la 1pm. Esto nos lleva a considerar la extraña expresión

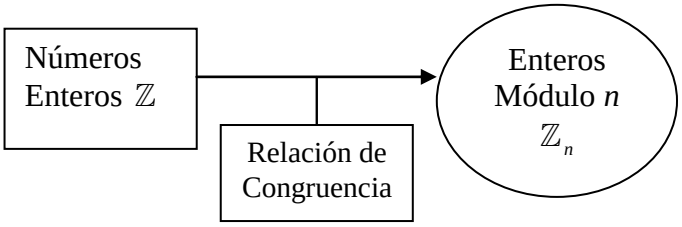
$$9+4=1$$

Alguien puede objetar la expresión anterior diciendo que el ciudadano común usa un sistema horario basado en la costumbre y señalar que, por ejemplo, el ejército es mucho más cuidadoso y habla de la hora 13 en el caso que hemos señalado. Sin embargo, si a un oficial del ejercito le preguntamos qué hora tenemos 3 horas después de la hora 23, dirá que son las 2. Luego

$$23+3=2$$

Para entender esta clase de suma observamos que al sumar horas totalizamos el resultado y luego debemos dividir por 12 y el resto es el resultado de la suma. Por ejemplo, $5+11=16$ pero 16 entre doce da como resto 4 ya que $16=1\cdot 12+4$. En el caso de los militares el procedimiento es el mismo pero debemos dividir por 24.

Esto nos lleva a considerar un nuevo tipo de número que llamamos *los enteros módulo n.* Desde un punto de vista matemático los enteros módulo *n* se construyen a partir de $\mathbb{Z}$ mediante la *relación de equivalencia de congruencia módulo n.*



Dicha relación fue estudiada sistemáticamente por Gauss en su importante obra *Disquisitiones Arithmeticae*[1] que muchos historiadores consideran *el primer texto de matemáticas modernas.*

Vamos en primer lugar a definir el concepto de congruencia módulo *n* y estudiar sus propiedades básicas. Luego, definimos el conjunto $\mathbb{Z}_n$ de los enteros módulo *n* como un conjunto cociente (de clases de equivalencia) a partir de la relación de equivalencia de congruencia. Al igual que hicimos con los enteros, construimos un par de operaciones aritméticas en $\mathbb{Z}_n$ la adición y el producto. Dichas operaciones están estrechamente vinculadas con las operaciones de suma y producto en $\mathbb{Z}$ como pronto veremos. En $\mathbb{Z}_n$

[1] Disponible en español en http://cimm.ucr.ac.cr/da/

con la operación del producto aparece un fenómeno extraño: *los divisores de* 0, su estudio se realiza al final de la semana y esto nos lleva al concepto de cuerpos finitos.

7.2 Congruencias

De acuerdo a Gauss

$$a \equiv b \bmod n \text{ si y sólo si } n \text{ divide } a-b,$$

donde n, a y b son enteros y $n \neq 0$. Leemos $a \equiv b \bmod n$ como a es congruente con b módulo n. Veamos algunos ejemplos.

1. $24 \equiv 3 \bmod 3$ ya que 3 divide a 24-3.
2. $(n+1)^2 \equiv n+1 \bmod 2$ ya que 2 divide a $n(n+1)$.
3. $a \equiv 0 \bmod n$ si y sólo si n divide a, es decir la noción de congruencia es más general que el concepto de divisibilidad.
4. Consideremos la ecuación $x \equiv -1 \bmod 5$. Cualquier solución x debe verificar que $5 / x+1 \Leftrightarrow x+1=5k \Rightarrow x=5k-1, k$ entero arbitrario. Observe que hay infinitas soluciones en $\mathbb{Z}$ de esta ecuación. Por ejemplo, 4,9,14, $\cdots$, son soluciones de la ecuación $x \equiv -1 \bmod 5$.
5. La ecuación $4x \equiv 1 \bmod 2$ no se puede resolver ya que $4x-1$ es siempre impar.

Carl F. Gauss

Matemático, físico y astrónomo alemán nacido en Brunswick en 1777. De origen muy humilde, dio muestras de precocidad matemática lo que llevo al Duque de Brunswick a ayudar con el pago de su educación. Siendo muy joven demostró que un polígono regular de 17 lados es constructible con regla y compás. En ese tiempo no estaba seguro si estudiaría matemática o filología en la Universidad, este descubrimiento lo llevó a escoger la matemática. Diseñó un procedimiento para determinar la órbita de un planeta a partir de una serie de mediciones hechas en la tierra. Su obra fundamental es *Disquisitione Arithmeticae*, conocida como *Disquisiciones*, donde introduce el concepto de congruencia y da las primeras pruebas de la Ley de Reciprocidad Cuadrática. Es el primero también en demostrar el Teorema Fundamental del Álgebra y en enunciar el método de los mínimos cuadrados. Su trabajo es también notable en las bases teóricas del electromagnetismo con el enunciado del Teorema de Gauss. Debemos mencionar que Gauss entendió la idea de Geometría No Euclidea antes que Bolyai y Lobachetvsky pero no quiso publicar nada en este tema para "no levantar la gritería de los beocios"[2]. Para algunos Gauss es el más grande matemático que ha existido.

Lo siguiente es muy fácil de verificar.

Proposición 1. Una congruencia no se deja de verificar si sumamos a ambos lados de la misma el mismo entero, esto es, si $a \equiv b \bmod n \Rightarrow a + c \equiv b + c \bmod n$.

Demostración. Ejercicio.

[2] Los beocios son estúpidos o tontos.

1. Como $17 \equiv 5 \bmod 3$ entonces, sumando 5 a ambos lados de la congruencia obtenemos $22 \equiv 10 \bmod 3$.
2. Hallar todos los enteros que satisfacen la ecuación $x+5 \equiv 7 \bmod 5$.

Restamos 5 a ambos lados y obtenemos $x \equiv 2 \bmod 5$, luego x-2=5k o x=5k+2 donde k es un entero arbitrario.

Nuestro siguiente resultado es importante para el resto de nuestra discusión.

Teorema 2. Sean a,b,c y n enteros cualesquiera

1. $a \equiv a \bmod n$
2. Si $a \equiv b \bmod n \Rightarrow b \equiv a \bmod n$
3. Si $a \equiv b \bmod n$ y $b \equiv c \bmod n \Rightarrow a \equiv c \bmod n$

Demostración.

1. es cierto ya que 0 es divisible por cualquier entero no nulo. Por otro lado, para probar 2., observamos que si $n/(a-b) \Rightarrow a-b=nk$ con $k \in Z \Rightarrow b-a=n(-k)$ de donde $b \equiv a \bmod n$.

Como,

$a \equiv b \bmod n$ y $b \equiv c \bmod n \Rightarrow a-b=nk$ y $b-c=nj$ para ciertos enteros k, j.

Sumando estas dos igualdades vemos que $a-c=n(j+k) \Rightarrow a \equiv c \bmod n$. □

Lo más importante de la sencilla proposición anterior es que demuestra que *la relación de ser congruente módulo n es una relación de equivalencia en los enteros*. Es decir, si fijamos un natural $n \neq 0$ y definimos una relación R en los enteros por medio de $aRb \Leftrightarrow a \equiv b \bmod n$ esta relación es de equivalencia. Esto es muy importante. Las clases de equivalencia resultantes serán denominadas enteros módulo n. Veamos en un ejemplo cuáles son las clases de equivalencia que obtenemos por medio de una relación de este tipo. Pero antes un resultado que nos ayudará a determinar las mismas.

Teorema 3. $a \equiv b \bmod n$ si y sólo si el resto al dividir a y b por n es el mismo.

Demostración. Supongamos que el resto al dividir a y b por n es el mismo entero r. Esto es $a = nk + r, b = nj + r$ con $0 \le r < n$. Luego, restando las igualdades anteriores, vemos que $a - b = n(j - k) \Rightarrow a \equiv b \bmod n$. Hemos probado que la condición es necesaria. Por otro lado, como $a = nk + r_1, b = nj + r_2$ con $0 \le r_1, r_2 < n$ entonces $a - b = n(k - j) + r_1 - r_2$.

Como $n | a - b$ entonces $n | r_1 - r_2$ y de aquí se deriva que $r_1 - r_2 = 0$ ya que $|r_1 - r_2| < n$, luego los restos son iguales.

1. Tomemos la relación módulo 3, es decir aRb si y sólo si $a \equiv b \bmod 3$. ¿Cuáles son las clases de equivalencia?. El teorema anterior nos da la clave. Al dividir un entero cualquiera por 3 obtenemos sólo tres posibles restos de la división: 0,1 y 2. Es decir que un entero cualquiera k sólo puede admitir tres posibles tipos de escritura

$$k = 3j$$
$$k = 3j + 1$$
$$k = 3j + 2$$

Ya sabemos que dos enteros están en la misma clase de equivalencia si tienen el mismo resto al dividirlos por 3, y como solo hay tres residuos posibles, estos son 0, 1 y 2, luego las clases de equivalencia son

$$\{0, \pm 3, \pm 6, \pm 9, \cdots\} \text{ clase del resto 0}$$
$$\{\pm 1, \pm 4, \pm 7, \cdots\} \text{ clase del resto 1}$$
$$\{\pm 2, \pm 5, \pm 8, \cdots\} \text{ clase del resto 2}$$

2. Las clases de equivalencia módulo 2 son aún más sencillas y consisten en los números pares y en los impares ya que la diferencia entre dos pares o impares es siempre par, luego las clases de equivalencia son

$$\{0, \pm 2, \pm 4, \cdots\}$$
$$\{\pm 1, \pm 3, \cdots\}$$

Las clases de equivalencia se denotan por medio de una barra, así $\overline{0}$ denota la clase del 0.

3. Si tomamos las clases de equivalencia módulo 12 obtenemos precisamente 12 clases correspondientes a los 12 posibles restos que obtenemos al dividir un número por 12. Por ejemplo, la clase del 5 está formada por los enteros de la forma $12k+5, k$ entero arbitrario.

Como ya dijimos esta clase la denotamos por $\overline{5}$. Observe que las clases de equivalencia módulo 12 corresponden a la forma que contamos las horas del día.

4. Demuestre que un número impar y que no es divisible por 3 es de la forma 6n+1 o de la forma 6n+5.

En efecto, al dividir por 6 obtenemos 6 posibles restos: 0,1,2,3,4 y 5. Es decir que cualquier entero es de una y de solo una de las siguientes formas
$6n, 6n+1, 6n+2, 6n+3, 6n+4$ o $6n$+5

Pero $6n, 6n+2$ y $6n+4$ son números pares (¿por qué?) y los descartamos por nuestra hipótesis que nuestro entero es impar. Por otro lado, $6n+3$ es múltiplo de 3 ya que $6n+3=3(2n+1)$. Luego, sólo quedan dos posibilidades o es de la forma $6n$+1 o de la forma $6n$+5.

Antes de proseguir damos un lema basado en el muy conocido Teorema de Ruffini que el estudiante recuerda de su quinto año de bachillerato (ver libro Matemática para el buen vivir, Quinto año, colección Bicentenario).

Lema 4. *Sea* $p(x)=a_0+a_1x+\cdots+a_{n-1}x^{n-1}+a_nx^n$ *un polinomio con coeficientes reales, entonces* $x-a$ *divide a* $p(x)-p(a)$.

Demostración. Basta ver que el residuo de la división, por el Teorema de Ruffini, es $p(a)-p(a)=0$, luego la división es exacta.

Teorema 5. *Sea* $p(x)=a_0+a_1x+\cdots+a_{n-1}x^{n-1}+a_nx^n$ *un polinomio con coeficientes enteros y supongamos que* $a\equiv b \bmod k$. *Entonces* $p(a)\equiv p(b) \bmod k$.

Demostración. Vemos, por el lema anterior, que $a-b$ divide a $p(a)-p(b)$. Pero por hipótesis k divide a $a-b$ y por transitividad de la relación de divisibilidad se deriva que k divide a $p(a)-p(b)$. □

Tomemos el polinomio $p(x)=x^2+1$ y la congruencia $11\equiv 4 \bmod 7$. Aplicando el polinomio a la misma se obtiene $11^2+1\equiv 4^2+1 \bmod 7 \Rightarrow 122\equiv 17 \bmod 7$.

7.3 El conjunto numérico de los enteros módulo *n*

Fijemos un número natural $n\neq 0$. Si dividimos un numero entero cualquiera por *n* podemos obtener solo *n* restos o residuos: 0,1,2,…,*n*-1. Esto lo conocemos desde la semana 9 donde demostramos el algoritmo de Euclides. Cada uno de estos residuos genera una clase de equivalencia: $\overline{0},\overline{1},\overline{2},\cdots,\overline{n-1},$. Por otro lado, como dos enteros están relacionados si y sólo si tienen el mismo resto al dividirlos por n entonces *estas son todas las clases de equivalencia.*

Definición (Enteros módulo *n*)

Los enteros módulo *n*denotado por $\mathbb{Z}_n$ son las clases de equivalencia o conjunto cociente definidas por medio de la relación de equivalencia $a\equiv b \bmod n$. Mas precisamente: son las clases *n* clases $\overline{0},\overline{1},\overline{2},\cdots,\overline{n-1}$ de los posibles restos que se obtienen al dividir un número por *n*.

Hemos dado varios ejemplos de la construcción en la sección anterior, pero debido a la importancia del concepto daremos un ejemplo más.

1. Tomemos los enteros módulo 5, $\mathbb{Z}_5$, este conjunto consiste en 5 clases, ya que los restos posibles, al dividir por 5, son 0,1,2,3,y 4.

Las clases de equivalencia son

$$\overline{0} = \{\cdots, -10, -5, 0, 5, 10, 15, \cdots\}$$
$$\overline{1} = \{\cdots, -9, -4, 1, 6, 11, \cdots\}$$
$$\overline{2} = \{\cdots, -8, -3, 2, 7, 12, \cdots\}$$
$$\overline{3} = \{\cdots, -7, -2, 3, 8, 13, \cdots\}$$
$$\overline{4} = \{\cdots, -6, -1, 4, 9, 14, \cdots\}$$

1. Considere el conjunto de los enteros módulo siete, $\mathbb{Z}_7$. ¿Cuántas clases de equivalencia tiene el conjunto $\mathbb{Z}_7$? Indique de manera comprensiva y explícita cada una de las clases de equivalencia.

7.4 Operaciones en $\mathbb{Z}_n$

Sabemos por nuestra discusión anterior que la relación de congruencia módulo *n* divide a los enteros en, precisamente, *n* clases de equivalencia. Cada clase de equivalencia tiene un representante distinguido: el resto de dividir un entero cualquiera por *n*. Una pregunta natural es ¿podemos definir operaciones algebraicas en estas clases de equivalencia? Vamos a considerar un ejemplo.

1. Tomemos la relación de equivalencia derivada de considerar que a está relacionado con b sí y sólo sí $a \equiv b \bmod 3$. Obtenemos tres clases de equivalencia como sabemos, la clase del 0, la del 1 y la del 2. ¿Cómo sumamos estas clases? Una respuesta posible es sumando en $\mathbb{Z}$ sus representantes y luego tomamos la clase de equivalencia del resultado. Por ejemplo, $\overline{2}+\overline{2}=\overline{4}=\overline{1}$. Procediendo así, obtenemos la tabla siguiente:

Suma en $\mathbb{Z}_3$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{1}$

La única objeción y es una objeción importante es que debemos demostrar que la adición o suma, definida de esta manera, *no depende del representante que tomemos de la clase*. El estudiante ya vio esta situación en la semana anterior.

 Los matemáticos usualmente dicen que debemos demostrar *que la ley de composición interna está bien definida.* El estudiante encontrará la definición de ley de composición en el Módulo III.

Es decir, 1+1 debe ser lo mismo que 1+4 módulo 3, ya que 1 y 4 están en la misma clase. Pero, 1+4=5=2 en la aritmética módulo 3. Esto ocurre en general ya que el siguiente teorema es cierto.

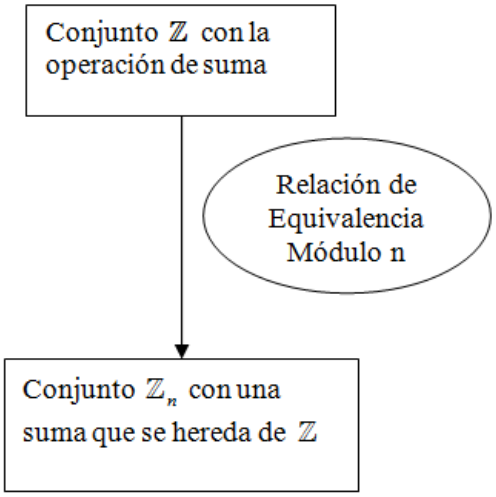
Teorema 6. Si $a \equiv b \bmod n$ y $j \equiv k \bmod n$ entonces $a + j \equiv b + k \bmod n$.

Demostración. Como $a \equiv b \bmod n$ y $j \equiv k \bmod n$ esto implica que $n/a-b$ y $n/j-k \Rightarrow n/a+j-(b+k) \Rightarrow a+j \equiv b+k \bmod n$. Lo que demuestra el resultado.

Lo más importante del resultado anterior es que indica que la operación de adición o suma está bien definida en las clases de equivalencia módulo *n* y verifica:

$$\bar{a} + \bar{b} = \overline{a+b}$$

Es decir, *para hallar la suma de dos clases de equivalencia sumamos dos de sus representantes y tomamos la clase de la suma.* El lector atento observará que es exactamente el mismo procedimiento que usamos para definir la suma en los enteros $\mathbb{Z}$.



Vamos a resumir en esta sección las propiedades más relevantes de la suma en $\mathbb{Z}_n$.

Teorema 7.

1. *La suma es conmutativa en* $\mathbb{Z}_n$*, es decir* $\bar{a}+\bar{b}=\bar{b}+\bar{a}$.
2. *Hay un elemento neutro para la suma en* $\mathbb{Z}_n$*, más precisamente* $\bar{a}+\bar{0}=\bar{0}+\bar{a}$ *para cualquier entero* $\bar{a}$ *módulo n*
3. *Todo entero* $\bar{a}$ *módulo n tiene un inverso aditivo, es decir existe un entero* $-\bar{a}$ *tal que* $\bar{a}+(-\bar{a})=\bar{0}$
4. *La suma en* $\mathbb{Z}_n$ *es asociativa, esto es* $\bar{a}+\left(\bar{b}+\bar{c}\right)=\left(\bar{a}+\bar{b}\right)+\bar{c}$ *para enteros cualesquiera.*

Demostración.

1. Ya que en $\mathbb{Z}$, $a+b=b+a$ entonces, tomando clases de equivalencia a ambos lados de la igualdad, obtenemos el resultado.
2. Se obtiene de nuevo del hecho que 0 es el elemento neutro de la suma en $\mathbb{Z}$.

3. Tomemos una clase cualquiera $\overline{a}$, podemos suponer, sin pérdida de generalidad, que $0 \le a < n$. Consideremos ahora $0 \le n - a$ entonces $\overline{a} + \overline{n-a} = \overline{0}$.

4. Se deriva del hecho que la suma es asociativa en $\mathbb{Z}$.

Hemos demostrado que los números enteros módulo *n* con la operación de suma antes definida constituyen un grupo abeliano. El concepto de grupo lo verá el estudiante en detalle en el módulo III de este curso.

Construya la tabla de la suma para $\mathbb{Z}_5$.

+	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$						
$\overline{1}$						
$\overline{2}$						
$\overline{3}$						
$\overline{4}$						
$\overline{5}$						

¿Qué pasa con el producto?. El estudiante UNA que ha seguido cuidadosamente nuestra discusión observará que debemos demostrar un teorema análogo al anterior para probar que un producto puede ser definido en $\mathbb{Z}_n$ *de manera natural* . Más precisamente, debemos demostrar el siguiente resultado.

Teorema 8. Si $a \equiv b \bmod n$ y $j \equiv k \bmod n$ entonces $aj \equiv bk \bmod n$.

Demostración. Queremos ver que $n/aj-bk$. Pero $aj-bk=aj-jb+jb-bk=j(a-b)+b(j-k)$. Como, por hipótesis, $n/a-b$ y $n/j-k$ entonces $n/j(a-b)+b(j-k)$ y esto concluye la demostración. □

La idea de la demostración anterior de sumar y restar la misma cantidad para *construir un puente* entre aj y bk. Esta idea es típica en matemáticas y aparece tanto en pruebas de análisis como de álgebra. Le pedimos al estudiante que repase la misma.

Luego, podemos multiplicar las clases de equivalencia por medio del expediente de multiplicar sus representantes. Si llamamos las clases de equivalencia módulo *n*, $\mathbb{Z}_n$, por medio de $\overline{0},\overline{1},\cdots,\overline{n-1}$ entonces definimos el producto de $\overline{a}$ y $\overline{b}$

$$\overline{a}\overline{b}=\overline{ab}$$

El siguiente teorema resume las propiedades del producto o multiplicación en $\mathbb{Z}_n$. La demostración del mismo es un ejercicio que dejamos al estudiante UNA.

Hagamos la tabla del producto para los enteros módulo 3, $\mathbb{Z}_3$. Esta es:

•	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{1}$

Observe que la tabla es *simétrica respecto a su diagonal*, esto indica que la *ley es conmutativa.*

Teorema 9. Consideremos el conjunto $\mathbb{Z}_n$ con la operación de producto antes definida. Entonces

1. *El producto es conmutativo, esto es* $\bar{a}\bar{b} = \bar{b}\bar{a}$ *para clases arbitrarias* $\bar{a}, \bar{b} \in \mathbb{Z}_n$
2. *El producto es asociativo* $\left(\bar{a}\bar{b}\right)\bar{c} = \bar{a}(\bar{b}\bar{c})$ *para clases arbitrarias* $\bar{a}, \bar{b}$ y $\bar{c} \in \mathbb{Z}_n$
3. $\bar{1}\bar{a} = \bar{a}$ para cualquier clase arbitraria $\bar{a} \in \mathbb{Z}_n$
4. $\bar{0}\bar{a} = \bar{0}$ para cualquier clase arbitraria $\bar{a} \in \mathbb{Z}_n$
5. $\bar{a}\left(\bar{b} + \bar{c}\right) = \bar{a}\bar{b} + \overline{ac}$ *para clases arbitrarias* $\bar{a}, \bar{b}$ y $\bar{c} \in \mathbb{Z}_n$ (ley distributiva del producto respecto a la suma)

Hemos demostrado que los números enteros módulo *n* con las operaciones de suma y producto antes definidas constituyen un anillo conmutativo con identidad. El concepto de anillo lo verá el estudiante en detalle en el módulo III de este curso.

1. Construir la tabla de la multiplicación para los enteros módulo 6.
2. Encuentre el inverso aditivo de la clase de 4 en el conjunto $\mathbb{Z}_9$.
3. ¿Tiene la clase de 3 un inverso multiplicativo en $\mathbb{Z}_9$? Razone su respuesta.

Solución: No lo tiene. Observe que la clase de 3 es un divisor de cero en $\mathbb{Z}_9$.

4. Escriba la tabla de la adición y la multiplicación de $\mathbb{Z}_{11}$.
5. Escriba la tabla de la multiplicación de $\mathbb{Z}_8$ ¿Cuánto es el producto de la clase del 2 y la clase del 4 en $\mathbb{Z}_8$?
6. Si es posible resuelva la ecuación 2x=1 mod 7 en $\mathbb{Z}_7$.
7. Resuelva, si es posible, 3x=5 mod 6 en $\mathbb{Z}_7$.

1. Solamente vea la tabla siguiente después de hacer un esfuerzo en conseguirla.

•	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{n}$ $\mathbb{Z}_6$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{0}$	$\overline{2}$	$\overline{4}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{2}$	$\overline{0}$	$\overline{4}$	$\overline{2}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{4}$	$\overline{2}$	$\overline{2}$	$\overline{1}$

2. Observamos que 4+5=9 y tomando clases a ambos lados, se tiene que la clase del 5 es el inverso aditivo de la clase del 9.
3. No lo tiene y veamos por qué, razonaremos por reducción al absurdo. Supongamos que existe una clase $\overline{n}$ tal que $\overline{3}\ \overline{n} = \overline{1}$ en $\mathbb{Z}_9$. Multipliquemos por la clase del $\overline{3}$ a ambos lados de la igualdad anterior y obtenemos $\overline{3}\,\overline{3}\ \overline{n} = \overline{1}\ \overline{3} = \overline{3}$ pero $\overline{3}\,\overline{3} = \overline{0}$ de donde $\overline{0} = \overline{3}$ un absurdo que se obtiene de suponer que existía un inverso multiplicativo. Hemos explotado un hecho curioso de $\mathbb{Z}_9$: la existencia de divisores de 0, eso lo estudiaremos en detalle pronto.
4. Es un ejercicio para nuestros estudiantes.
5. Usted debe realizar la tabla y observar que el producto da la clase del 0.
6. Multiplicamos por 4 ambos lados de la igualdad y obtenemos que x=4 mod 7 luego x=7j+4.
7. No tiene soluciones, veamos por qué. Si 6 divide a 3x-5 es claro que 3 divide también a 3x-5. Pero 3 divide a 3x y luego debe dividir a -5, lo cual es imposible.

7.5 Divisores de 0

Observe la tabla de la multiplicación de $\mathbb{Z}_6$ construida por Ud. como solución del ejercicio 1 en la sección anterior. En ella ocurre un fenómeno extraño: $\overline{2}\,\overline{3} = \overline{0}$, esta observación es importante ya que algo similar *no ocurre con los números enteros*: en los enteros si $ab=0$ entonces $a=0$ o $b=0$.

Definición. Consideremos el conjunto $\mathbb{Z}_n$ para un cierto número natural *n* fijo. Decimos que $\bar{a} \neq \bar{0}$ es un divisor de 0 si existe un $\bar{b} \neq \bar{0}$ no nulo tal que $\bar{a}\bar{b} = \bar{0}$.

 Los matemáticos dicen que $\mathbb{Z}$, lo mismo que $\mathbb{Q}$, es *un dominio de integridad* ya que en ambos conjuntos si *xy*=0 entonces *x*=0 o *y*=0. En un dominio de integridad vale la ley de cancelación: si *xy=xz* y *x* no es 0 entonces *y=z.* Observe que tal ley no aplica en $\mathbb{Z}_6$. **Consecuencia: Ud. puede cancelar términos no nulos en una igualdad entre productos sí y sólo sí Ud. está trabajando en un dominio de integridad.**

Una pregunta natural es: ¿cuándo $\mathbb{Z}_n$ es un dominio de integridad? o ¿en qué $\mathbb{Z}_n$ encontramos el fenómeno de los divisores de 0? Invitamos al lector a hacer los ejercicios siguientes.

1. Construya la tabla de multiplicación de $\mathbb{Z}_2$, $\mathbb{Z}_3$, $\mathbb{Z}_5$ y $\mathbb{Z}_7$. ¿Aparecen divisores de 0 en estas tablas?, ¿qué tienen en común 2,3,5 y 7?
2. Construya la tabla de multiplicación para $\mathbb{Z}_4$ y $\mathbb{Z}_{10}$. ¿Aparecen divisores en de 0 estas tablas?, ¿qué tienen en común 4 y 10?
3. Escriba su hipótesis sobre la existencia de divisores ceros en $\mathbb{Z}_n$.

El estudiante habrá establecido, a partir de los experimentos anteriores, que el fenómeno de la aparición de divisores de cero está asociado al hecho de que *n* sea o no primo. Vamos a demostrar esto en una serie de importantes resultados.

Teorema 10. *Si n no es primo entonces* $\mathbb{Z}_n$ *admite divisores de 0.*

Demostración. Recordamos que en $\mathbb{Z}_n$ la clase de 0 es igual a la clase de *n*. Si *n=ab* con *a,b* distintos de 1 y de *n,* esto es 1<*a*<*n*,1<*b*<*n*. Entonces tomando clases a ambos lados de la igualdad *n=ab* obtenemos,

$$n = ab \Rightarrow \bar{n} = \bar{a}\bar{b} \text{ pero } \bar{0} = \bar{n}$$

de donde tanto $\bar{a}$ como $\bar{b}$ son divisores de 0.

Teorema 11. *Si p es primo todo elemento* $\bar{a}$ *no nulo de* $\mathbb{Z}_p$ *tiene inverso multiplicativo, es decir, si* $\bar{a}$ *no es* $\bar{0}$ *entonces existe un* $\bar{b}$ *tal que* $\bar{a}\bar{b} = \bar{1}$.

Demostración. Como *a* no es múltiplo de *p* entonces *p* y *a* son primos entre si, es decir que el M.C.D. de *a* y *p* es 1. Luego, existen enteros *k,m* tales que

$$1=ak+mp$$

Tomando clases de equivalencia a ambos lados obtenemos

$$1=ak+mp \Rightarrow \bar{1}=\bar{a}\bar{k}+\bar{m}\bar{p}$$

pero $\bar{p} = \bar{0}$, luego $\bar{1}=\bar{a}\bar{k}+\bar{m}\bar{p}=\bar{1}=\bar{a}\bar{k}$ y por ende la clase de $\bar{a}$ tiene inverso multiplicativo.

Claramente este inverso multiplicativo de $\bar{a}$ es único ya que si $\bar{a}\bar{b} = \bar{1}$ y $\bar{a}\bar{c} = \bar{1}$ entonces $\bar{b}\bar{a}\bar{c} = \bar{b}$ pero también $\bar{b}\bar{a}\bar{c} = \bar{c}$, luego $\bar{b} = \bar{c}$. El estudiante UNA debe explicar el por qué de las últimas igualdades.

Teorema 12. *Si p es primo entonces* $\mathbb{Z}_p$ *no puede tener divisores de 0.*

Demostración. Supongamos que $\bar{a}\bar{b} = \bar{0}$ y que $\bar{a} \neq \bar{0}$, entonces, por el teorema anterior, $\bar{a}$ tiene un inverso multiplicativo que llamamos $\bar{c}$, luego $\bar{c}\bar{a}\bar{b} = \bar{1}\bar{b} = \bar{b} = 0$, de donde $\bar{b}$ debe ser nulo y no podemos tener divisores de 0.

El conjunto $\mathbb{Z}_p$ con *p* primo con la operación de suma y producto antes definida constituye un cuerpo. Es además un cuerpo finito. La noción de cuerpo será estudiada en el módulo III.

7.6 Dos bonitos resultados sobre congruencias

Vamos a enunciar y demostrar dos resultados básicos de la teoría de los enteros módulo *n,* el primero es el **teorema de Wilson** y el segundo es el pequeño **Teorema de Fermat**.

Observemos la siguiente tabla

Primo p	$(p-1)!+1$	Anote su observación
2	2	
3	3	
5	25	
7	721	

El estudiante UNA puede repetir el experimento con algunos primos *p* mayores que 7, ¿qué observó? Una observación que se puede inferir de la tabla es la siguiente: 2 divide a 2, 3 divide a 3, claramente 5 divide a 25 y como 721=700+21 entonces 7 divide a 721 también. Podemos formular la siguiente hipótesis: *si p es primo entonces p divide a (p-1)!+1*. Como (4-1)!+1=7 y 4 no divide a 7 no se puede omitir del resultado que *p* sea un número primo. Estamos listos para enunciar y demostrar el siguiente resultado.

Teorema 13. (Wilson) Si p es un número primo cualquiera entonces $(p-1)! \equiv -1 \bmod p$.

Demostración. Sabemos que en $\mathbb{Z}_p$ cada elemento no nulo tiene un *único* inverso

$$\left\{\overline{1},\overline{2},\overline{3},\cdots,\overline{p-2},\overline{p-1}\right\}$$

$$(p-1)^2 = p^2 - 2p + 1 \Rightarrow (p-1)^2 \equiv 1 \bmod p$$

multiplicativo. Tomemos el conjunto $\prod_{i=2}^{p-2} i \equiv 1 \bmod p$ de

$$2 \cdot 3 \cdot 4 \cdot \cdots \cdot (p-2) \equiv 1 \bmod p$$

$$a^{p-1} \equiv 1 \bmod p$$

$$|k - j| < p$$

todas las clases

de $\mathbb{Z}_p$ que no son la clase del 0. Observe que el inverso de la clase del 1, $\overline{1}$ es la misma clase del 1. Además,

$$(p-1)^2 = p^2 - 2p + 1 \Rightarrow (p-1)^2 \equiv 1 \bmod p$$

Luego, el inverso multiplicativo de la clase p-1 es la misma clase de p-1. Luego, los inversos multiplicativos de los elementos del conjunto $\left\{\overline{2},\overline{3},\cdots,\overline{p-2}\right\}$ están en el propio conjunto. De donde

$$\prod_{i=2}^{p-2} i \equiv 1 \bmod p$$

Así, $2 \cdot 3 \cdot 4 \cdot \cdots \cdot (p-2) \equiv 1 \bmod p$ y si multiplicamos por p-1 la congruencia anterior se obtiene $(p-1)! \equiv p-1 \bmod p$ pero es claro que $-1 \equiv p-1 \bmod p$ de donde, por transitividad de las congruencias tenemos $(p-1)! \equiv -1 \bmod p$ que es lo que queríamos demostrar.

Un bello resultado el teorema de Wilson que fue enunciado, según Waring, por John Wilson y demostrado por Lagrange en 1771.

El otro resultado es una perla que le debemos al gran Fermat y se conoce como el pequeño Teorema de Fermat.

Teorema 14. (pequeño Teorema de Fermat)

Sea *p* un número primo y *a* un número natural que verifica $1 \le a \le p-1$ entonces

$$a^{p-1} \equiv 1 \bmod p$$

Demostración. Consideremos la sucesión finita $a, 2a, 3a, \cdots, (p-1)a$, afirmamos que es imposible que dos elementos de la misma sean congruentes módulo *p*. De lo contrario ocurriría que *p* divide a (*ka*-*ja*)=*a*(*k*-*j*). Pero al ser *p* primo entonces *p* divide a *a* o a (*k*-*j*) lo cual es imposible por la condición $1 \le a \le p-1$ y $|k-j| < p$. Luego, si tomamos clases de equivalencia módulo *p* entonces $\left\{\overline{a}, \overline{2a}, \overline{3a}, \cdots, \overline{(p-1)a}\right\} = \left\{\overline{1}, \overline{2}, \overline{3}, \cdots, \overline{p}\right\}$. Luego,

$$a(2a)(3a)\cdots(p-1)a \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \bmod p$$

de donde $a^{p-1}(p-1)! \equiv (p-1)! \bmod p \Rightarrow a^{p-1} \equiv 1 \bmod p$ que es lo que queríamos demostrar.

Quizás al estudiante UNA le parezca que los últimos resultados son bastante teóricos y abstractos, la realidad es una muy distinta.

Modelando con los enteros módulo *n*

Aplicaciones del pequeño Teorema de Fermat y del Teorema de Wilson junto con otros resultados de la teoría de números son los que nos permiten realizar compras en Internet o usar nuestro banco en línea de manera segura. El protocolo de seguridad usado en la Web usa propiedades de los números primos para encriptar nuestro password o el número de nuestra tarjeta de crédito. El sistema utilizado actualmente se denomina RSA y usa congruencias, el pequeño teorema de Fermat y primos muy, muy grandes. Invitamos al estudiante UNA que quiera continuar estudiando este apasionante tema a ir a

http://es.wikipedia.org/wiki/RSA

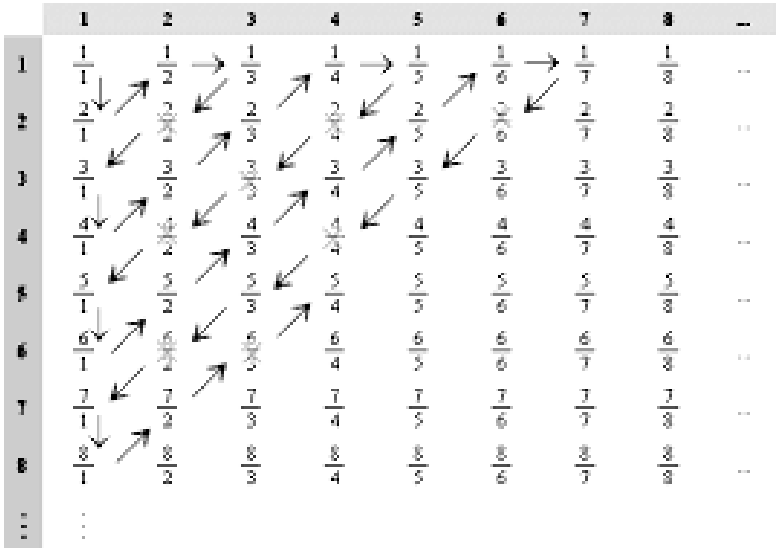
1. Demuestre que $x^2 \equiv x \bmod 2$ para cualquier entero *x*.
2. Busca todas las raíces del polinomio x^2+1 en $\mathbb{Z}_2$.
3. Demuestra que el polinomio x^2+x tiene dos raíces en $\mathbb{Z}_2$.
4. Demuestre que el polinomio x^2+x+1 no tiene raíces en $\mathbb{Z}_2$. ¿Qué ocurre en $\mathbb{Z}_3$?.
5. Demuestre que si x_0 es una raíz de $p(x)=a_0+a_1x+\cdots+a_nx^n$ entonces la clase de x_0 en $\mathbb{Z}_n$ es una raíz del polinomio $\overline{p}(x)=\overline{a}_0+\overline{a}_1x+\cdots+\overline{a}_nx^n$ donde $\overline{a}_i$, para $i=0,1,\cdots,n$ es la clase de a_i, para $i=0,1,\cdots,n$ en $\mathbb{Z}_n$.
6. Calcule $2^5+240+25 \bmod 8$.
7. Construya la tabla completa de la adición y del producto en $\mathbb{Z}_7, \mathbb{Z}_{10}, \mathbb{Z}_{12}$. Indique en cuáles conjuntos aparecen divisores de 0 en el producto. Explique sus resultados de acuerdo a lo estudiado en el texto.
8. Sabemos que $25 \equiv 1 \bmod 3$ y que $4 \equiv 1 \bmod 3$, ¿es cierto que $25^3 \equiv 4 \bmod 3$?. Justifique su respuesta.
9. Demostrar que n^7-n siempre es divisible por 6 para cualquier numero natural *n*.

1. Es claro que el producto de dos enteros consecutivos debe ser par. Así, $x(x-1)$ es siempre par si *x* es un número entero. Además, tenemos que $x^2 \equiv x \bmod 2$ sí y sólo sí 2 divide a $x^2-x=x(x-1)$, lo cual es cierto por nuestra observación inicial.
2. La única raíz en $\mathbb{Z}_2$ del polinomio considerado es la clase del 1.
3. Es claro que tanto la clase del 0, como la clase del 1 son raíces del polinomio considerado.

4. Haga la primera parte sustituyendo las dos clases de $\mathbb{Z}_2$ en el polinomio y observando que no se anula. En $\mathbb{Z}_3$ si existe una raíz, la clase del 1 como podemos observar por sustitución.
5. Este ejercicio es importante. Si x_0 es una raíz de $p(x) = a_0 + a_1 x + \cdots + a_n x^n$ vamos a tener que $p(x_0) = a_0 + a_1 x_0 + \cdots + a_n x_0^{\,n} = 0$, ahora tomemos clase de equivalencia a ambos lados de la igualdad y apliquemos que al tomar la clase de equivalencia se respeta tanto la suma como el producto. Luego, $\overline{a}_0 + \overline{a}_1 \overline{x}_0 + \cdots + \overline{a}_n \overline{x}_0^{\,n} = \overline{0}$ y esto es lo que queríamos demostrar.
6. 240 es 0 módulo 8, ¿por qué? Y 25 equivale a 1. Por otro lado 32 es de nuevo 0, así $2^5 + 240 + 25 \equiv 1 \bmod 8$.
7. Dejamos al estudiante UNA la construcción de las tablas. Debe observar que en $\mathbb{Z}_7$ no hay divisores de 0 pero que en $\mathbb{Z}_{10}, \mathbb{Z}_{12}$ sí los hay. El estudiante UNA debe indicar por qué se obtiene este resultado.
8. Elévese al cubo la primera congruencia y luego multiplíquense lo obtenido con la segunda congruencia dada para obtener que el resultado es cierto.
9. Observamos que $n^7 - n = n\left(n^6 - 1\right)$. Si aplicamos el teorema de Fermat vemos que 7 debe dividir a $n^6 - 1$ y por ende divide también a $n^7 - n = n\left(n^6 - 1\right)$ como deseábamos demostrar.

UNIDAD 6

Los números racionales



Semana 9

Aplicar los números racionales y reales en la resolución de problemas, en el modelado matemático y en la demostración de nuevos resultados

Contenidos a tratar: Construcción de los números racionales. Operaciones aritméticas definidas en el conjunto de los números racionales. Existencia de los números irracionales. Bases y Fracción Generatriz.

8.1 Introducción

Los números racionales capturan la idea de proporción entre números enteros. Los griegos usaban la idea proporción para describir la relación entre magnitudes geométricas como el área entre figuras. Euclides decía que las áreas A_1, A_2 de dos

círculos de diámetro d_1, d_2 están en proporción con los cuadrados de los diámetros. Hoy escribiríamos esto así

$$\frac{A_1}{A_2} = \frac{{d_1}^2}{{d_2}^2}$$

En otras áreas como en Ciencias Sociales la idea de proporción es crucial y permite extrapolar lo que observamos cuando tomamos una muestra y queremos inferir lo que ocurre a nivel nacional. Por ejemplo, si el tamaño de la muestra es de 100 personas y observamos una incidencia de 5 personas con determinada característica entonces esperamos que 5% de la población total tenga la misma característica. Por supuesto, aquí intervienen las leyes de la probabilidad para justificar este salto entre la muestra y la población.

Vamos a realizar nuestra construcción de los números racionales de manera completamente análoga a lo que ya hicimos con los números enteros, es decir, introduciremos una relación de equivalencia en cierto conjunto de forma que las clases de equivalencia obtenidas representan a los números racionales. Posteriormente, introducimos operaciones de suma y producto en las clases de equivalencia, mostrando que las mismas están bien definidas.

Un hecho importante en la matemática es la aparición de los números irracionales, números que no corresponden a fracción alguna, como $\sqrt{2}$. La tradición histórica asocia a Hipaso con este descubrimiento que añadió riqueza al sistema numérico. Vamos a demostrar, debido a la importancia del resultado, de distintas maneras que $\sqrt{2}$ no es un número racional.

Para el docente de educación media, la caracterización de los racionales mediante su expansión decimal vía la fracción generatriz es un tema importante que debe manejar. La misma sirve también para caracterizar los irracionales mediante su expansión decimal, correspondiendo la misma a los números con expansión decimal no periódica. Esto lo trataremos en la última sección.

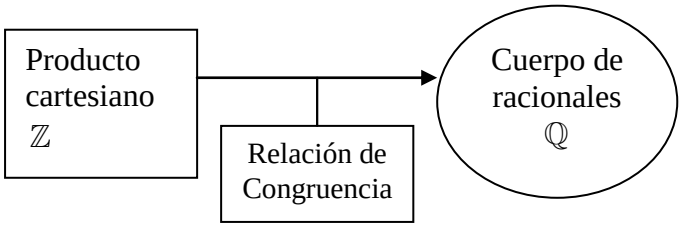
8.2 La construcción de $\mathbb{Q}$

Recordamos al lector que la relación de equivalencia que introducimos para construir los enteros capturaba la idea de "diferencia". En el caso de los racionales vamos a tratar de capturar la idea de proporción. El lector recordará que los pares de números naturales *a:b* y *c:d* están en la misma proporción si y sólo si *ad=bc*, usualmente decimos *a* es a *b* como *c* es a *d.* Por ejemplo, 1:2 es como 3:6 ya que 1.6=2.3. El estudiante que haya seguido este razonamiento habrá vislumbrado nuestra definición de relación de equivalencia.

Consideremos el conjunto $\mathbb{Z}\times\mathbb{Z}^* = \{(a,b) \text{ con } a\in\mathbb{Z}, b\in\mathbb{Z}, b\neq 0\}$. Vamos a establecer nuestra relación de equivalencia en $\mathbb{Z}\times\mathbb{Z}^*$, decimos que

$$(a,b)R(c,d) \Leftrightarrow ad = bc$$

Solicitamos que *b* sea nulo para evitar que las fracciones que vamos a construir tengan denominador nulo.



Teorema 1. La relación $(a,b)R(c,d) \Leftrightarrow ad = bc$ es una relación de equivalencia.

Demostración. La relación es reflexiva ya que $ab = ab \Rightarrow (a,b)R(a,b)$. Por otro lado, la relación es simétrica ya que si $(a,b)R(c,d) \Leftrightarrow ad = bc \Leftrightarrow bc = ad \Leftrightarrow (c,d)R(a,b)$ Por último si $(a,b)R(c,d)$ y $(c,d)R(e,f)$ tenemos que *ad=bc* y *cf=de.* Luego, *adf=bcf=deb* y de aquí *af=be* ya que $d\neq 0$. Luego, $(a,b)R(e,f)$.

Como sabemos, cualquier relación de equivalencia induce una partición del conjunto en clases de equivalencia, veamos algunas de ellas.

1. La clase de equivalencia de (2,1) son los pares (c,d) que verifican que $2d=c$, es decir la primera componente es el doble de la segunda, y esta proporción corresponde a la idea de 2. Por otro lado, la clase de equivalencia de (1,3) son todos los pares (a,b) tales que $3a=b$, es decir b es 3 veces a, esto captura la idea de la fracción $\frac{1}{3}$.

Notación. La fracción $\frac{a}{b}$ representa todos los pares que son equivalentes al par (a,b), es decir a la clase de equivalencia del par ordenado (a,b). No es difícil ver que estos pares son necesariamente de la forma (na,nb) donde n es un entero arbitrario. Esto lleva a la conocida regla de simplificación $\frac{na}{nb} = \frac{a}{b}$.

Nuestra siguiente definición es muy importante.

Definición. El conjunto $\mathbb{Q}$ es el conjunto cociente de todas las clases de equivalencia en $\mathbb{Z}\times\mathbb{Z}^*$ con respecto a la relación R, es decir $\mathbb{Q} = \mathbb{Z}\times\mathbb{Z}^* / R$.

Mucho del trabajo que nos queda es similar a lo que ya hicimos para los números enteros y en buena medida lo vamos a dejar al estudiante UNA. Los términos fracción o número racional van a ser equivalentes para nosotros.

8.3 Las operaciones de suma y producto en $\mathbb{Q}$

8.3.1 Suma de racionales

Es natural definir la suma de fracciones como aprendimos en el colegio.

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

Teorema 2. La definición anterior no depende de los representantes que tomemos.

Demostración. Suponga que sustituimos $\frac{a}{b}$ por $\frac{na}{nb}$ y $\frac{c}{d}$ por $\frac{mc}{md}$ donde *n,m* son enteros arbitrarios. Entonces $\frac{na}{nb} + \frac{mc}{md} = \frac{namd + nbmc}{nbmd} = \frac{ad + bc}{bd}$ por la ley de simplificación.

Hemos justificado que la ley de composición interna suma + está bien definida en el conjunto $\mathbb{Q}$ y que opera como la adición de racionales que conocemos desde primaria.

1. Demuestre que $\frac{a}{b} + \frac{0}{c} = \frac{a}{b}$

El ejercicio anterior demuestra que la fracción $\frac{0}{c}$ se comporta como el elemento neutro para la suma y la denotaremos sencillamente por 0.

2. Demuestre que $\frac{a}{b} + \left(\frac{-a}{b}\right) = 0$

El ejercicio demuestra que toda fracción tiene un opuesto o inverso respecto a la suma antes definida.

3. Demuestre que $\frac{a}{b} + \frac{c}{d} = \frac{c}{d} + \frac{a}{b}$ para fracciones cualesquiera $\frac{c}{d}$ y

$$\frac{a}{b}$$

El ejercicio demuestra que la suma antes definida es conmutativa.

4. Demuestre que $(\frac{a}{b} + \frac{c}{d}) + \frac{e}{f} = \frac{a}{b} + (\frac{c}{d} + \frac{e}{f})$ para fracciones cualesquiera $\frac{c}{d}$, , $\frac{e}{f}$ y $\frac{a}{b}$

Hemos establecido con estos axiomas que los números racionales con al operación de suma constituyen un grupo abeliano. El concepto de grupo lo verá el estudiante en detalle en el módulo III de este curso.

8.3.2 Producto de racionales

Siguiendo la motivación que le hemos dado a nuestra semana dedicada a los racionales vamos a definir el producto de dos racionales $\frac{a}{b}$ y $\frac{c}{d}$ como

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

Nuestro primer ejercicio debería estar claro para el estudiante UNA que ha seguido el razonamiento de nuestra construcción.

1. Demuestre que la operación del producto de dos racionales está bien definida.

Sugerencia: Calcule $\frac{mc}{md}\frac{na}{nb}$

2. Demuestre que $\frac{a}{b}\frac{c}{d} = \frac{c}{d}\frac{a}{b}$

Esto demuestra que la operación producto es conmutativa.

¿Qué pasa con el elemento neutro para el producto? Sabemos que el 1 cumple este rol y lo podemos representar por medio de la fracción $\frac{c}{c}, c \neq 0$, tenemos el siguiente ejercicio que justifica este hecho.

3. $\frac{a}{b}\frac{c}{c} = \frac{a}{b}$ para cualquier fracción $\frac{a}{b}$.

3. Toda fracción no nula $\frac{a}{b}$, a distinto de cero, tiene un inverso respecto a la multiplicación dado por la fracción $\frac{b}{a}$. El estudiante UNA debe verificar que en efecto $\frac{a}{b}\frac{b}{a} = 1$.

1. Enuncie y verifique la propiedad asociativa para la multiplicación de fracciones.

Hemos verificado que los racionales, excluyendo el 0, son un grupo abeliano respecto a la multiplicación que definimos arriba. La noción de grupo abeliano la estudiará el estudiante en el módulo III.

El estudiante recuerda de sus estudios de bachillerato que el producto de racionales es distributivo respecto a la suma. Este es el contenido de nuestro próximo teorema.

Teorema 3.

Si $\frac{a}{b}, \frac{c}{d}$ y $\frac{e}{f}$ son fracciones cualesquiera se tiene que

$$\frac{a}{b}\left(\frac{c}{d} + \frac{e}{f}\right) = \frac{a}{b}\frac{c}{d} + \frac{a}{b}\frac{e}{f}$$

Demostración

$\frac{a}{b}\left(\frac{c}{d}+\frac{e}{f}\right)=\frac{a}{b}\left(\frac{cf+ed}{df}\right)=\frac{acf+aed}{dbf}=\frac{acfb+aebd}{dbfb}$ y luego

$\frac{acfb+aebd}{dbfb}=\frac{ac}{bd}+\frac{ae}{bf}=\frac{a}{b}\frac{c}{d}+\frac{a}{b}\frac{e}{f}$ como deseábamos demostrar. □

El conjunto $\mathbb{Q}$ con la operación de suma y producto antes definida constituye un cuerpo. La noción de cuerpo será estudiada en el módulo III.

Nosotros demostramos, en la semana 9, que dentro del conjunto de los enteros $\mathbb{Z}$ existe una copia de $\mathbb{N}$ el conjunto de los números naturales. Vamos a demostrar de igual manera que dentro del conjunto $\mathbb{Q}$ existe una copia de los enteros. Así tenemos

$$\mathbb{N}\subset\mathbb{Z}\subset\mathbb{Q}$$

Teorema 4. La aplicación $f:\mathbb{Z}\to\mathbb{Q}$ que manda cada entero z en la clase $(z,1)=\frac{z}{1}=f(z)$ es inyectiva, además $f(z+z')=f(z)+f(z'), f(zz')=f(z)f(z').$

Demostración. Tenemos que f es inyectiva ya que si $\frac{z}{1}=f(z)=f(z')=\frac{z'}{1}$ entonces $\frac{z}{1}=\frac{z'}{1}\Leftrightarrow z=z'$. Por otro lado, $f(z+z')=\frac{z+z'}{1}=\frac{z}{1}+\frac{z'}{1}=f(z)+f(z')$. Por último, $f(zz')=\frac{zz'}{1}=\frac{z}{1}\frac{z'}{1}=f(z)f(z').$

La aplicación f se dice que es un homomorfismo inyectivo del anillo $\mathbb{Z}$ en el anillo $\mathbb{Q}$. La noción de homomorfismo será estudiada en el módulo III.

8.4 Los irracionales

8.4.1 Introducción

Existe controversia si el descubrimiento de longitudes que no eran expresables mediante lo que llamamos ahora un racional causó impacto y una crisis en la matemática griega. Muchos autores se refieren a este descubrimiento como el escándalo de los irracionales, aunque autores como Bochner señalan que solamente fue un avance en la matemática griega que llevó a la teoría de la proporción de Eudoxo.

La leyenda cuenta que fue un pitagórico de nombre Hipaso de Metaponte, el que descubrió que la hipotenusa de un triángulo rectángulo de catetos de longitud uno era inconmensurable.

Los números enteros y racionales ocupaban un lugar privilegiado en la escuela Pitagórica. Por ejemplo, la música y el concepto de armonía eran asociados a la idea de proporción ya que sólo al pulsar una cuerda en ciertas posiciones se producía un sonido agradable al oído. La palabra armónico tiene un origen matemático. Hipaso de Metaponto nació alrededor del año 500 A.C. y era un discípulo de Pitágoras. Se le atribuye el descubrimiento de que era imposible establecer una proporción entera entre la hipotenusa y el cateto de un triángulo rectángulo e isósceles. Tal descubrimiento y su revelación se cree le causaron la muerte a Hipaso o al menos su expulsión de la escuela pitagórica ya que demostraba una falla en la fundamentación matemática de la escuela.

Este término lo que significaba es que era imposible establecer una proporción entera entre la longitud de la hipotenusa y un segmento de longitud 1. Posteriormente, Teefeso demostró que lo mismo ocurría para $\sqrt{3}, \sqrt{5}, \sqrt{6}, \sqrt{7}, \sqrt{8}, \sqrt{10}, \sqrt{11}, \sqrt{12}, \sqrt{13}, \sqrt{14}, \sqrt{15}$ y $\sqrt{17}$. Creemos que la razón de parar en la raíz de 17 es geométrica.

Vamos a demostrar que $\sqrt{2}$ es irracional de dos formas distintas. La primera es la demostración que aparece en la mayor parte de los textos. La segunda es muy bonita y

permite ser generalizada a otros naturales. No solo es bonita, la demostración de Hardy captura la condición para poder saber si $\sqrt{n}$ es o no racional, siendo n un entero arbitrario.

Teorema 5. $\sqrt{2}$ no se puede escribir de la forma $\frac{p}{q}$ donde p, q son enteros positivos.

Demostración 1. Supongamos que $\sqrt{2} = \frac{p}{q}$. Simplificando al máximo la fracción $\frac{p}{q}$ *podemos suponer que p y q no poseen divisores comunes.* La ecuación $\sqrt{2} = \frac{p}{q}$ implica que $p^2 = 2q^2$. En particular p^2 debe ser par y luego p también lo es. El estudiante UNA debe decir por qué p debe ser par. Luego, $p=2n$ para un cierto natural n. Luego, $p^2 = 2q^2 \Rightarrow (2n)^2 = 2q^2 \Rightarrow 2n^2 = q^2$. Un razonamiento similar al que hicimos con p demuestra que q es par. Pero nosotros asumimos *que p y q no poseen divisores comunes y vemos que* 2 *es un divisor común*. Hemos hallado una contradicción que concluye la demostración. □

Demostracion 2. Partimos de suponer que $\sqrt{2} = \frac{p}{q}$ y luego

$$p^2 = 2q^2.$$

Aplicando el Teorema Fundamental de la Aritmética (semana 9), sabemos que $p = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ y $q = q_1^{\alpha_1} q_2^{\alpha_2} \cdots q_j^{\alpha_j}$, siendo todos los p_i y los q_r números primos. Pero entonces

$$p^2 = \left(p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} \right)^2 = p_1^{2\alpha_1} p_2^{2\alpha_2} \cdots p_k^{2\alpha_k} = 2q^2 = 2q_1^{2\alpha_1} q_2^{2\alpha_2} \cdots q_j^{2\alpha_j}$$

Observe que todas las potencias en los primos p_i son pares, mientras que del lado izquierdo el primo 2 va a aparecer ¡con una potencia impar!. De nuevo, el Teorema Fundamental de la Aritmética, no permite esta situación, de donde es imposible escribir

$\sqrt{2} = \frac{p}{q}$, lo que concluye la demostración. □

1. Demuestre que $\sqrt{3}$ es irracional.
2. Demuestre que $\sqrt{n}$ es irracional a menos que *n* sea un cuadrado.

Sugerencia: Use la demostración de Hardy.

3. Demuestre que $\sqrt{2}+\sqrt{3}$ es irracional.
4. Demuestre que $\sqrt{2}+\sqrt{3}+\sqrt{5}$ es irracional.
5. ¿Puede Ud. generalizar los dos problemas anteriores?
6. Demuestre que la suma de un racional con un irracional es irracional.
7. ¿Es la suma de dos irracionales un irracional?
8. Recordamos que $\sqrt{2}$ se puede construir con regla y compás. ¿Cómo se construye $\sqrt{3}$?. Suponga que Ud. construyó $\sqrt{n}$, construya $\sqrt{n+1}$.

1. Supongamos que $\sqrt{3}$ es racional, luego $\sqrt{3} = \frac{n}{m} \Rightarrow n = m\sqrt{3} \Rightarrow n^2 = 3m^2$.

   Vemos que 3 debe dividir a *n* ya que 3 es un número primo, pero la potencia de 3 en el lado izquierdo de la igualdad va a ser par mientras que en el lado derecho es impar, esto contradice el teorema fundamental de la aritmética.

2. Indicación: Use el teorema fundamental de la aritmética para demostrar primero que nada que si *n* es un cuadrado entonces $n = p_1^{2\alpha_1} p_2^{2\alpha_2} \cdots p_k^{2\alpha_k}$ y ahora repita el argumento del problema 1.

3. Esto es muy bonito, supongamos que $\sqrt{2}+\sqrt{3}$ es racional y que se escribe como $\sqrt{2}+\sqrt{3} = \frac{n}{m}$, luego $\sqrt{3} = \frac{n}{m} - \sqrt{2}$. Elevando al cuadrado a ambos lados de la igualdad anterior se obtiene $3 = \frac{n^2}{m^2} + 2 - 2\sqrt{2}\frac{n}{m}$. Pero podemos despejar $\sqrt{2}$ de

esta última igualdad y obtendríamos que $\sqrt{2}$ es racional (por favor complete los detalles), lo cual es absurdo.

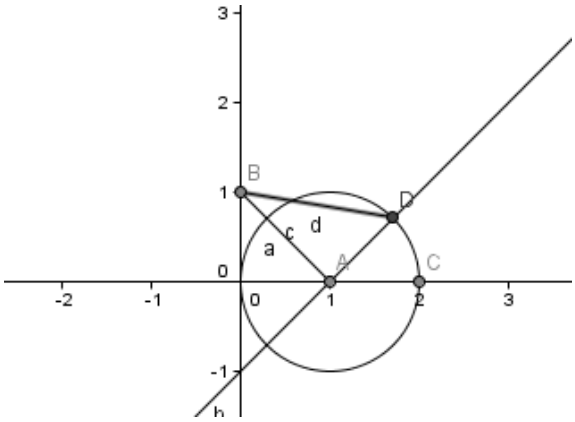
4. Indicación: similar al problema 3, el estudiante UNA debe hacer los cálculos.

5. Una generalización de este resultado es que $\sqrt{2}+\sqrt{3}+\sqrt{5}+\cdots+\sqrt{p}$ con p primo es irracional. Yo encontré una prueba no elemental de este resultado, le dejo al estudiante UNA pensar si es posible hallar una prueba que no use resultados avanzados de álgebra.

6. Vamos a razonar por el absurdo, supongamos que x es irracional y q racional y formemos $x+q=z$. Si z es racional entonces $x=z-q$, pero es claro que $z-q$ es racional, luego x es irracional y racional a la vez, un absurdo. Luego, z debe ser irracional.

7. Una buena pregunta que debe ser respondida cuidadosamente. Observemos que si x es irracional entonces $q-x$ lo es también para cualquier racional q, esto es debido a nuestro ejercicio anterior. Luego, $x+(q-x)=q$ indica que la suma de dos irracionales puede ser racional. El ejercicio 2 nos indica que la suma de irracionales puede ser irracional también, luego no sabemos en principio si al sumar dos irracionales el resultado es irracional o racional.

8. Usando Geogebra hacemos la construcción de raíz de 3,



El segmento BD mide exactamente $\sqrt{3}$, el estudiante UNA debe indicar el por qué. Invitamos a nuestros alumnos a reflexionar cómo continuar la construcción geométrica de longitudes que representen las distintas raíces de *n.*

8.6 Bases, fracción generatriz y representación numérica

8.6.1 Bases

Un proceso que es muy importante en matemática es la representación en la base 10 (o en otra base) de un número y su interpretación geométrica. Cuando decimos que tenemos el número 134, esto significa que

$$134 = 1 \cdot 100 + 3 \cdot 10 + 4$$

Es decir, nos basamos en el hecho de que *cualquier número natural N se pueda escribir de forma única como*

$$N = a_0 + a_1 10 + a_2 10^2 + \cdots + a_n 10^n$$

donde cada $a_i \in \{0,1,2,3,4,5,6,7,8,9\}$.

Es decir, cualquier numero natural N puede ser visto como un polinomio en las potencias de 10 con exponentes naturales y con coeficientes entre 0 y 9. Al ser únicos los coeficientes el número queda caracterizado por ello, lo que permite escribirlo como $a_0 a_1 \cdots a_{n-1} a_n$. Veamos el por qué. Tomemos cualquier número natural N y busquemos el mayor natural n de 10 tal que $10^n \leq N$. Si $N = 10^n$ paramos el procedimiento, de lo contrario escribimos

$$N = a_n 10^n + r_n$$

por el algoritmo de Euclides. Observe que solo tenemos las elecciones 0,1,2,3,4,5,6,7,8,9 para a_n ya que $N = a_n 10^n + r_n \geq a_n 10^n \geq 10^{n+1}$ si $a_n \geq 10$, contrario a lo que supusimos sobre *n.* Por otro lado, el algoritmo de Euclides garantiza que

$0 \le r_n < 10^n$ y si $r = 0$ de nuevo paramos y escribimos $N = a_n 10^n$. Si $0 < r_n < 10^n$, aplicamos el mismo procedimiento a r_k. El procedimiento debe parar en algún momento después de un número finito de pasos, logrando escribir $N = a_0 + a_1 10 + a_2 10^2 + \cdots + a_n 10^n$. La unicidad de la escritura se deriva de que el cociente y el resto son únicos al aplicar el algoritmo de Euclides.

1. Tome 12345. Entonces la mayor potencia de 10 menor que 12345 es 10000. Dividimos ahora 12345 por 10000 y vemos que $12345 = 1 \cdot 10000 + 2345$. La mayor potencia de 10 menor que 2345 es 1000, luego $2345 = 2 \cdot 1000 + 345$. Similarmente $345 = 3 \cdot 100 + 45, 45 = 4 \cdot 10 + 5$ y aquí paramos.

1. **(Base dos)** Demuestre que cualquier número natural N admite una representación única de la forma

$$N = a_0 + a_1 2 + a_2 2^2 + \cdots + a_k 2^k$$

1. Asumimos que Ud. resolvió el ejercicio anterior, si no lo hizo ¡este ejemplo lo va ayudar a resolverlo!. Tomemos el número 134. La mayor potencia de 2 que no excede 134 es $128 = 2^7$, luego $134 = 2^7 + 6$. Pero $6 = 2^2 + 2$ y entonces $134 = 2^7 + 2^2 + 2 = 10000110$

Hemos examinado hasta el momento la representación de un número natural en distintas bases, como la base 2 y la base 10. Pero supongamos que usted considera el número 12,123. ¿Qué ocurre con la parte decimal de un número?¿Qué representa? Para tener una idea fijemos la base 10 para nuestra discusión y empecemos con un caso concreto. Por ejemplo, tomemos el número 0,34567. Para ver que significan los decimales

3,4,5,6,y 7 en este número, procedemos de manera análoga que en nuestra construcción anterior notando que

$$0{,}34567 = 3\times10^{-1} + 4\times10^{-2} + 5\times10^{-3} + 6\times10^{-4} + 7\times10^{-5}$$

Una expresión análoga a lo que hicimos antes pero los exponentes de las potencias de 10 son ahora negativos. ¿Cómo obtener la representación anterior? Hay varias maneras y podemos suponer, sin pérdida de generalidad que $0<x<1$. Suponga que la representación decimal es finita, es decir que $x = 0, a_0 a_1 \cdots a_n$. Podemos multiplicar el número por una potencia de 10, digamos 10^j , de forma de obtener un entero positivo. Tales potencias existen por ser la expresión decimal finita y el número obtenido, por lo que hicimos arriba, lo podemos escribir como

$$10^j x = a_0 + a_1 10 + a_2 10^2 + \cdots + a_k 10^k$$

De donde $x = a_0 + a_1 \frac{10}{10^j} + a_2 \frac{10^2}{10^j} + \cdots + a_k \frac{10^k}{10^j}$, observe que todas los exponentes de 10 son negativos ya que $0<x<1$ y $x \geq a_i 10^{i-j}$.

Para representar este número geométricamente tomemos el intervalo [0,1] y dividámoslo en 10 partes. El número cae en el intervalo [0,3;0,4] ya que su primer decimal es 3. Dividamos ahora el intervalo [0,3;0,4] en 10 partes. El número cae en el intervalo [0,34;0,35] y continuamos de esta manera hasta que ubicamos el punto en la recta después de un número finito de pasos.

2. **(Base 2)** Si usamos la base 2, veamos como representar geométricamente el número 0,111100101. Dividamos el intervalo [0,1] en dos intervalos de igual longitud $[0, \frac{1}{2}]$, $[\frac{1}{2}, 1]$. El primer digito 1 nos indica que nuestro punto esta a la derecha de $\frac{1}{2}$. Dividamos ahora el intervalo $[\frac{1}{2}, 1]$ en los intervalos $[\frac{1}{2}, \frac{3}{4}], \left[\frac{3}{4}, 1\right]$, el dígito 1 nos indica que nuestro número se encuentra a la derecha de $\frac{3}{4}$. Continuamos de esta manera hasta determinar el punto sobre la

recta. Observe que el punto debe coincidir con alguno de los extremos de los intervalos que vamos construyendo.

Hemos manejado la representación de números con partes decimales (o en otra base) **finitas**. Pero el estudiante recuerda que en muchas situaciones aparecen números que admiten una representación decimal infinita pero periódica, por ejemplo

$$0{,}21234565656\cdots$$

Los puntos suspensivos indican que el 56 se repite indefinidamente. Vamos a demostrar que el numero $a=0{,}21234565656\cdots$ representa a un número racional. La técnica para lograr esto la aprendió el estudiante en bachillerato y se llama cálculo de la *fracción generatriz* de una expresión decimal periódica. Procedemos de la siguiente manera: multiplicamos a por 10^5 para obtener

$$10^5 \cdot a = 21234{,}565656\cdots$$

De manera análoga multiplicamos a por 10^7 y obtenemos

$$10^7 \cdot a = 2123456{,}5656\cdots$$

El punto es que los dos números encontrados tienen iguales expresiones decimales y al restarlos

$$10^7 \cdot a - 10^5 \cdot a = 2123456{,}5656\cdots \text{ -}21234{,}565656\cdots =$$

$$=2102222$$

Luego,

$$a = \frac{2102222}{10000000\text{-}100000} = \frac{2102222}{9900000}$$

Tome su calculadora de bolsillo o de su celular y verifique el resultado. Podemos enunciar un teorema, pero no lo haremos, indicando que *cualquier expresión decimal periódica corresponde a un número racional*. La demostración de este resultado es solamente una generalización de lo que hemos expuesto. El algoritmo de Euclides implica que el reciproco es cierto, *dado cualquier número racional su representación*

decimal es periódica, dejamos al lector que reflexione sobre este punto. En resumen: los números racionales corresponden a los números que tienen una expansión decimal periódica.

1. El número $12,12345678910111213\cdots$ no es racional ya que su expansión decimal es claramente no periódica.

Modelando con los números racionales

La base binaria es muy importante en computación ya que los computadores están diseñados para solo detectar dos estados en sus circuitos lógicos: encendido que corresponde al número 1 y apagado que corresponde al número 0. También el lector puede identificar estos estados con Verdad(1) y Falso(0). Los computistas hablan del bit=$\{0,1\}$ como la unidad básica de información. Por ejemplo, el número 15 en base 2 es $8+4+2+1=1111$ y por ende necesitamos 4 bits para poder representarlo. Un byte son 8 bits. El hecho de usar base 2 en computación hace que aparezcan constantemente cantidades expresadas como potencias de 2. Así hablábamos en un pasado cercano de 64 megas de memoria ram o actualmente de 16 gigas de ram.

Cualquier número natural, como ya fue estudiado anteriormente, puede ser representado en base 2 y luego por medio de una cantidad finita de bits. Usando los circuitos lógicos se pueden combinar estos estados para producir la suma y el producto de números naturales. Luego, como cualquier polinomio se basa solo en multiplicaciones y sumas, esto permite evaluar polinomios con computadoras. Es un logro del cálculo diferencial haber demostrado que funciones muy complejas se pueden, usualmente, aproximar por polinomios lo que permite usar computadoras y calculadoras para realizar cálculos complejos con extraordinaria precisión. El estudiante UNA debe observar que cualquier *resultado numérico* que nos dé una calculadora o un computador va a representar un numero racional ya que su expansión decimal se hace 0 a partir de algún momento. Por ejemplo, en mi calculadora aparecen 8 decimales para representar en pantalla un número, obteniendo siempre un número racional.

1. Demostrar que $1+\frac{1}{2}+\cdots+\frac{1}{p}$ no es un entero si p es un número primo.
2. Demuestre que entre dos números racionales $\frac{p}{q},\frac{r}{s}$ distintos siempre encontramos otro número racional. Esto es si $\frac{p}{q}<\frac{r}{s}$ entonces existe un número racional $\frac{x}{y}$ tal que $\frac{p}{q}<\frac{x}{y}<\frac{r}{s}$.
3. Suponga que el polinomio mónico $p(x)$ con coeficientes enteros tiene una raíz racional p/q. Demuestre que de hecho debe ocurrir que p/q es un entero. Encuentre un ejemplo que demuestre que no se puede omitir la hipótesis que $p(x)$ sea mónico en el resultado anterior.
4. Aplique lo demostrado en el ejercicio 3 para demostrar, de una nueva manera, que $\sqrt{2}$ es irracional.
5. Halle la fracción generatriz de $123{,}123412345676767\cdots$
6. ¿Es $\sqrt{3}+\sqrt[3]{2}$ un número racional?.

1. Tomemos $1+\frac{1}{2}+\cdots+\frac{1}{p}$ y supongamos que es un entero n, luego $1+\frac{1}{2}+\cdots+\frac{1}{p}=n.$ Multipliquemos ambos lados por $p!$ entonces $(1+\frac{1}{2}+\cdots+\frac{1}{p})p!=p!n$, pero cada término $\frac{p!}{k}$ es un entero si k es menor o igual a p y es divisible por p si k es menor estricto que p. Pero esto implica que p debe dividir a $(p\text{-}1)!$ Lo cual es absurdo.

2. Tome el promedio de los dos racionales que es un racional que está entre ambos racionales.
3. Se deja al estudiante UNA.
4. Como x^2-2 no tiene raíces enteras se concluye que no puede tener raíces racionales y luego $\sqrt{2}$ es irracional.

5. Muy sencillo y lo dejamos al estudiante UNA.

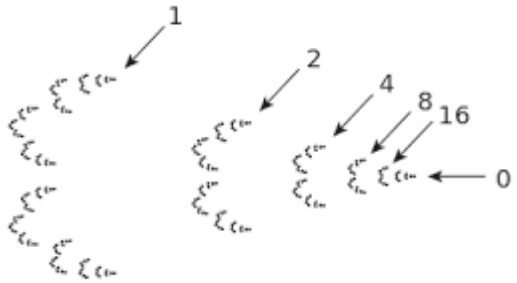
6. Es un número irracional, veamos esto por reducción al absurdo. Si $\sqrt{3}+\sqrt[3]{2}$ fuese racional, entonces

$$\sqrt{3}+\sqrt[3]{2}=\frac{p}{q}\Rightarrow\sqrt[3]{2}=\frac{p}{q}-\sqrt{3}\Rightarrow$$
$$3=\left(\frac{p}{q}-\sqrt{3}\right)^3=\left(\frac{p}{q}\right)^3-3\left(\frac{p}{q}\right)^2\sqrt{3}+9\frac{p}{q}-3\sqrt{3}$$

Afirmamos que la última línea contiene una contradicción que el estudiante UNA debe indicar.

UNIDAD 6

Los números reales



Números *p-adicos*

Semana 10

Aplicar los números racionales y reales en la resolución de problemas, en el modelado matemático y en la demostración de nuevos resultados

Contenidos a tratar: Los axiomas de los números reales. La no numerabilidad de los reales. Números algebraicos y trascendentes.

9.1 Introducción

Los números reales son el resultado de una profunda reflexión de los matemáticos en un período que abarca milenios. Para muchos matemáticos Eudoxo ya tenía una noción clara de ellos y evidentemente el problema de los irracionales surge en el marco de la cultura griega como ya vimos la semana anterior. El lenguaje matemático griego *enmarca lo numérico dentro de lo geométrico* pero al medir longitudes, áreas y volúmenes la noción de número y proporción sobrevive en la matemática griega. Además, los Pitagóricos le habían dado relevancia suficiente al número y sus representaciones físicas y musicales. Sin embargo, es hacia el renacimiento con el uso de expresiones decimales por Stevin (1585) cuando se logre algún avance en la

compresión de la recta numérica y este logro es, en realidad, el fruto de la interacción de muchas culturas. Stevin solo considera expresiones decimales finitas pero advierte que con ellas podemos aproximar con grado de precisión arbitraria otros números. Sin embargo, estábamos lejos de una teoría que explique de manera confiable el sistema numérico más importante. Es con el trabajo de Bolzano, Weierstrass, Cantor y Dedekind que logramos una teoría de los números reales rigurosa, un trabajo que abarca más de 2000 años de matemática si empezamos con Eudoxo.

Nosotros seguiremos a David Hilbert en su aproximación al concepto de número real. Es el enfoque axiomático de Hilbert lo que presentaremos a nuestros estudiantes. Hilbert pensaba que los axiomas, cuidadosamente escogidos, caracterizan a los objetos matemáticos. El lector recordará que los axiomas de Peano nos sirvieron de base para establecer el concepto de número natural. Hilbert escoge el mismo camino de Peano y despliega un conjunto de axiomas donde están involucradas las operaciones aritméticas, la noción de orden y la crucial idea de completitud. Está última es la que le da su base a la noción de "continuo", tan importante en matemática como en las aplicaciones en Física e Ingeniería. Muchas personas piensan que en las aplicaciones siempre lidiamos con números racionales ya que el ser humano y sus instrumentos solo usan un determinado grado de aproximación. Sin embargo, un modelo numérico de ese tipo complicaría las cosas de tal manera que no podríamos garantizar, por ejemplo, que una función continua que cambia de signo se anula en algún punto o que determinado proceso alcanza un máximo. Por eso, los números reales son una necesidad, el lenguaje matemático se empobrecería notablemente si excluimos a los números reales.

Muchos de nuestros resultados se enuncian usualmente dentro de un curso de análisis matemático y este es un curso de álgebra. Esto no debe sorprendernos: los reales son el conjunto numérico necesario para poder hacer análisis matemático. Por otro lado, si no realizamos su construcción el álgebra tendría serias limitaciones ya que resultados como El Teorema Fundamental del Álgebra no podrían ser demostrados. Sin embargo, no haremos un estudio profundo de la topología de los reales ya que eso corresponde a otro curso.

Sigamos a Hilbert en su excursión por el interesante mundo de los números reales, es un conjunto lleno de sorpresas y posibilidades.

9.2 Los axiomas de los números reales

Uno puede construir el sistema numérico de los reales mediante el expediente de las cortaduras de Dedekind. Es una construcción hermosa y nosotros invitamos al estudiante de Educación Matemática y de Matemáticas a ir a la *Guía Instruccional* del curso Historia de la Matemática (760) para que estudien la visión de Dedekind.

Los Matemáticos que contribuyeron a la idea de número real

Bolzano demuestra que sucesiones de Cauchy tienen una menor cota superior

Dedekind elabora la idea de cortadura

Cantor piensa que los números reales son clases de equivalencia en el espacio de las sucesiones de Cauchy

Weierstrass y su discípulo Haenkel establecen la unicidad del sistema de números reales.

Hilbert establece una aproximación axiomática al concepto de número real

Pero, es posible partir de una serie de axiomas que caracterizan a los números reales $\mathbb{R}$. El lector puede pensar en los reales de la siguiente forma: tome una línea recta

cualquiera. Y fije en ella un punto que corresponde al 0 y otro que corresponde a 1 y que determina la unidad de longitud y el sentido de la semirrecta que representa a lo que llamamos números positivos. Cada número real queda representado unívocamente por un punto de esa recta.

La recta numérica

Es una imagen que el lector conoce desde el bachillerato y que puede usar libremente para interpretar los axiomas de los números reales.

Vamos a pensar que es un conjunto que contiene al menos dos elementos 0 y 1, en el cual dos operaciones + y • han sido definidas y una relación de orden < es dada. Las operaciones y la relación de orden verifican los siguientes axiomas:

9.2.1 Primer grupo de axiomas relacionados con la suma +

a. Para cualquier real x se tiene que $x+0=0+x=x$, *es decir el* 0 *es el elemento neutro de la suma*
b. Dado cualquier real x existe un real $(-x)$ tal que $x+(-x)=(-x)+x=0$, *es decir todo número real tiene un inverso respecto a la operación de la suma.*
c. La suma es conmutativa es decir, $x+y=y+x$ para reales cualesquiera x,y
d. La suma es asociativa, es decir, $x+(y+z)=(x+y)+z$ para reales cualesquiera x,y y z

Hemos establecido con estos axiomas que los números reales con al operación de suma constituyen un grupo abeliano. El concepto de grupo lo verá el estudiante en detalle en el módulo III de este curso.

9.2.2 Segundo grupo de axiomas relacionados con el producto

e. Para cualquier real x se tiene que $x1=1x=x$, *es decir el* 1 *es el elemento neutro de la suma*
f. Dado cualquier real x existe un real x^{-1} tal que $x\,x^{-1}= x^{-1}x=1$, *es decir todo número real tiene un inverso respecto a la operación de multiplicación.*
g. La multiplicación es conmutativa, es decir, $xy=yx$ para cualquier par de reales x,y
h. La multiplicación es asociativa, es decir, $x(yz)=(xy)z$ para cualquier trío de reales x,y y z.
i. La multiplicación es distributiva respecto de la suma, es decir $x(y+z)=xy+xz$ para cualquier trío de reales x,y y z.

Hemos establecido con estos axiomas que los números reales con la operación de suma y producto constituyen un cuerpo. El concepto de cuerpo lo verá el estudiante en detalle en el módulo III de este curso.

9.2.3 Tercer grupo de axiomas relacionados con el orden <

j. Dado dos reales x,y cualesquiera debe ocurrir una y sólo una de las tres posibilidades siguientes $x<y$ *o* $x=y$ *o* $y<x$. *Esta propiedad se conoce como propiedad de tricotomía*
k. Si $x<y$ y $y<z$ entonces $x<z$, es decir, la relación < es transitiva.
l. Si $x<y$ entonces $x+s<y+s$, es decir el orden respeta la operación de suma.
m. Si $x<y$ entonces $xs<ys$, para cualquier $s>0$
n. Si $0<a<b$ entonces existe un natural n tal que $b<na$. Esta propiedad se denomina propiedad arquimediana.

Antes de dar el último pero importante axioma de completitud daremos unas definiciones. *Un conjunto A se denomina acotado superiormente si y sólo si existe un* $M>0$ *tal que* $x<M$ *para cualquier x en A.* El número M se denomina cota superior de A. Por supuesto, de existir una cota superior existen muchas más.

o. Si un conjunto de números reales A está acotado superiormente entonces existe una cota superior mínima, es decir existe un *K* tal que $x<K$ para cualquier *x* en *A* y *K* es el menor elemento con esta propiedad. Este axioma se conoce como la propiedad de completitud de los números reales.

9.3 Observaciones y consecuencias de los axiomas

En los cursos de análisis el estudiante UNA profundizará en las ideas que trataremos sobre los números reales, así que solo haremos algunas observaciones y resultados fundamentales.

Los dos primeros grupos de axiomas indican que los reales es un cuerpo conmutativo. El tercer grupo de axiomas está relacionado con las propiedades de orden del *continuo.* **Cruciales son los axiomas que hemos llamado propiedad arquimediana y completitud de los números reales.** Son los que permiten identificar a los números reales con los puntos de una recta y concluir que la recta numérica esta hecha de una sola pieza, es decir que *no tiene huecos.* Una consecuencia muy útil de la propiedad arquimediana es la siguiente.

Teorema 1. Existen números reales arbitrariamente pequeños. Es decir, si $0 < \varepsilon < 1$ entonces existe un real *x* tal que $0 < x < \varepsilon$.

Demostración. Tomemos el número $K = \frac{1}{\varepsilon}$ tenemos que $0<1< K = \frac{1}{\varepsilon}$, luego existe un *d* natural tal que $d> K = \frac{1}{\varepsilon}$, luego $\frac{1}{d} < \varepsilon$ y esto es lo que queríamos demostrar. □

Si *A* está acotado superiormente sabemos por el axioma o. existe una cota superior mínima, ese número es denominado el supremo de *A* y se denota $\sup A$. Siempre es importante establecer la unicidad de un objeto como el supremo.

Teorema 2. Si *A* está acotado superiormente entonces el supremo de *A* está definido de manera unívoca.

Demostración. Si *M* y *K* son cotas superiores cualesquiera y distintas, se debe tener por el axioma de tricotomía que $M < K$ o $K<M$. Luego dos cotas superiores distintas no pueden ser, simultáneamente, la menor cota superior.

El siguiente resultado es una caracterización muy usada del supremo.

Teorema 3. Si *A* está acotado superiormente entonces $x = \sup A$ sí y sólo sí *x* es una cota superior de *A* y para cualquier $\varepsilon > 0$ existe $x_0 \in A$ tal que $x_0 + \varepsilon > x$.

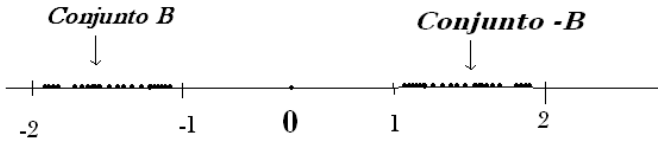
Demostración. Supongamos que $x = \sup A$, entonces si tomo un $\varepsilon > 0$, $x - \varepsilon$ no puede ser cota superior de *A* ya que $x - \varepsilon < x$. Luego debe existir un $x_0 \in A$ tal que $x_0 > x - \varepsilon \Rightarrow x_0 + \varepsilon > x$.

Por otro lado, supongamos que *x* es una cota superior de *A* y para cualquier $\varepsilon > 0$ existe $x_0 \in A$ tal que $x_0 + \varepsilon > x$. Sea *M* otra cota superior de *A* y supongamos que $M<x$ y llamemos $\delta = \frac{x - M}{2} > 0$. Sabemos que existe x_0 tal que $x_0 + \delta > x$

Hay un hecho notable sobre el orden de los números reales y es su simetría. Hemos hablado de supremo de un conjunto acotado superiormente y ¿qué pasa con los conjuntos acotados inferiormente?. Primero definamos los mismos. *Decimos que B está acotado inferiormente si y sólo si existe un M tal que x>M para todo x en B.* Luego, si llamamos –*B* al conjunto

$$-B = \{x \text{ tal que } x = -b \text{ con } b \in B\}$$

Tenemos que *B* esta acotado inferiormente si y sólo si –*B* está acotado superiormente. El siguiente dibujo representa la situación.



Continuamos con una definición. Si *B* está acotado inferiormente definimos el ínfimo de *B* como la mayor de sus cotas superiores y lo denotamos por $\inf B$. Podemos preguntarnos: ¿necesitamos un axioma que garantice la existencia del ínfimo de un conjunto acotado superiormente?. El estudiante UNA que haya estado atento a nuestra exposición afirmará que no es necesario. La razón es que *B* esta acotado inferiormente si y sólo si *–B* está acotado superiormente. Luego, *–B* va a tener un supremo que llamamos *x* y vamos a tener que

$$\inf B = -x$$

1. Demuestre en detalle que $\inf B = -x$.
2. Sea *A* un conjunto acotado inferiormente y *L*=inf *A*. Demuestre que dado cualquier $\varepsilon > 0$ existe un *x* en *A* tal que *x*- $\varepsilon < L$.
3. Dé ejemplo de un conjunto que esté acotado superiormente pero no inferiormente.
4. Sea $A = \left\{ \frac{1}{n} \text{, para } n = 1,2,3,\cdots \right\}$, calcule si existen el supremo y el ínfimo de *A*.

El siguiente resultado es muy importante para dejarlo fuera de nuestra exposición y además lo usaremos más adelante para demostrar que los reales son no numerables.

Teorema 4 (Intervalos encajados de Cantor).

Consideremos una sucesión de intervalos $I_n = [a_n, b_n]$, $n = 1,2,\cdots$ que verifican la condición de encaje $I_n = [a_n, b_n] \supset I_{n+1} = [a_{n+1}, b_{n+1}]$ y cuyas longitudes $l(I_n) = b_n - a_n$ van a 0 cuando *n* tiende a infinito. Entonces

$$\bigcap_{n=1}^{\infty} I_n = \bigcap_{n=1}^{\infty} [a_n, b_n] = \{c\}$$

Es decir, la intersección de todos los intervalos es no vacía y consiste en un solo punto.

Demostración. Examinemos cuidadosamente el conjunto *A* formado por todos los extremos izquierdos de los intervalos I_n, es decir $A=\{a_n, n=1,2,\cdots\}$. Cualquier $a_n \le b_1$ y $a_n \le a_{n+1}$ ¿porqué? Luego el conjunto *A* está acotado superiormente y debe tener un supremo que llamamos $c=\sup A$. Similarmente definimos el conjunto *B* de todos los extremos derechos de los intervalos I_n, es decir $B=\{b_n, n=1,2,\cdots\}$. Tenemos que $a_1 \le b_j$ para $j=1,2,\cdots$ y $b_{j+1} \le b_j$. Luego el conjunto *B* está acotado inferiormente y debe tener un ínfimo que llamamos $d=\inf B$. Como $|d-c| \le b_n - a_n$ concluimos, haciendo *n* tender a infinito, que $c=d$. Como $a_n \le c=d \le b_n$ entonces $c \in \bigcap_{n=1}^{\infty} I_n = \bigcap_{n=1}^{\infty} [a_n, b_n]$ y la demostración concluye al observar que la intersección solo puede tener un punto debido a la condición $l(I_n)=b_n-a_n \to 0$ si $n \to \infty$.□

1. Complete cuidadosamente el último paso de la demostración anterior.

Sugerencia: Suponga que $c' \in \bigcap_{n=1}^{\infty} I_n = \bigcap_{n=1}^{\infty} [a_n, b_n]$ esta en la intersección y pregúntese qué pasa con el intervalo [*c´*, *c*].

9.4 ¡ $\sqrt{2}$ Existe!

Muchos de Uds. dan por garantizado la existencia de $\sqrt{2}$ aunque ya demostramos que no corresponde a ningún número racional. La idea de esta corta sección es usar los axiomas de Hilbert para demostrar que existe un número real positivo que verifica la ecuación

$$x^2 = 2$$

La solución de la anterior ecuación es lo que llamamos $\sqrt{2}$. Vamos a proceder, mediante una serie de pasos sencillos de seguir, a demostrar, a partir de los axiomas de Hilbert, la existencia de $\sqrt{2}$. En primer lugar, definamos el conjunto

$$A=\left\{0\leq y \text{ tales que } (y)^2<2\right\}.$$

Observamos lo siguiente:

a. *A* es no vacío ya que al menos el 0 está en *A.*
b. *A* esta acotado superiormente. En efecto, si *A* no estuviese acotado superiormente podríamos encontrar un *y* en *A* que fuese mayor que 2, pero si $y>2$ entonces $y^2<2$ y $y^2>4$. Lo cual es absurdo.
c. Por el axioma o. el conjunto *A* tiene una cota superior mínima que llamamos *x.*
d. Afirmamos que $x^2=2$. Supongamos que esto no ocurre, entonces por tricotomía $x^2<2$ o $x^2>2$. Vamos a ver la imposibilidad de cada una de estas posibilidades.
e. Suponga que $x^2<2$ entonces $2-x^2>0$ y podemos encontrar por el teorema de la sección anterior un $\varepsilon>0$ tal que $0<2\varepsilon+\varepsilon^2<2-x^2$, luego $(x+\varepsilon)^2<2$ y por ende $x+\varepsilon\in A$ contradiciendo *x* que cota superior mínima.
f. El estudiante UNA debe completar este caso, demostrando que es imposible que $x^2>2$

Luego, solo queda la posibilidad de $x^2=2$ como queríamos demostrar.

1. Demuestre por qué es posible encontrar un $\varepsilon>0$ tal que $0<2\varepsilon+\varepsilon^2<2-x^2$ si suponemos que $x^2<2$.
2. Demuestre la existencia de $\sqrt{3}$
3. Demuestre que si *A* es acotado superiormente y *l* es el supremo de *A* entonces dado cualquier $\varepsilon>0$ entonces existe un *x* en *A* tal que $x+\varepsilon>0>l$.

9.5 La no numerabilidad de los reales y los números trascendentes

Un gran descubrimiento de Cantor fue darse cuenta que no existía un solo tamaño del infinito. Cantor demuestra, mediante su argumento de la diagonal, que los números reales tienen un cardinal mayor que el de los números naturales. Su descubrimiento lo llevó a plantear el primer problema de la lista de Hilbert: ¿Hay algún conjunto de la recta real cuyo cardinal sea intermedio entre el cardinal de los números naturales y el de los reales?. Cantor pensaba que no y esto constituye su famosa *hipótesis del continuo.* El problema es insoluble en la axiomática de Zermelo-Fraenkel como demostraron Godel y Cohen.

Las nociones de conjunto numerable y cardinal fueron estudiadas en el módulo I . Vamos a demostrar de dos maneras distintas que el conjunto de los reales no es numerable. Es, en la opinión de los autores, uno de los resultados más bonitos e importantes en matemática. Vamos a dar dos demostraciones del resultado. La primera es debida a Cantor y constituye su célebre argumento diagonal que ya vio en el módulo I. Debemos señalar que el argumento de Cantor se aplica a una variedad de resultados y se convirtió en una técnica matemática. De acuerdo a Polya *una técnica es un truco que aplicamos muchas veces*. La segunda demostración es muy bonita también y se basa en otro resultado de Cantor que demostramos anteriormente: el teorema de los intervalos encajados.

Teorema 5. Los números reales no son numerables.

Demostración 1. (Diagonal de Cantor)

Vuelva y repase la demostración que aparece en el módulo I.

Demostración 2. Razonaremos por el absurdo y supondremos que los reales son numerables, es decir existe una biyección $f:\mathbb{N}\to\mathbb{R}$. Sea $a_n = f(n)$ con $n = 0,1,2\cdots$. Tomemos un intervalo cerrado $I_0 \subset \mathbb{R}$ tal que la longitud de $I_0 \subset \mathbb{R}$ es 1 y

$$a_0 \notin I_0$$

Dentro de $I_0 \subset \mathbb{R}$ construya un intervalo cerrado I_1 de longitud $\frac{1}{2}$ tal que

$$a_1 \notin I_1$$

Seguimos de esta forma y construimos en el paso *n* un intervalo cerrado I_n de longitud $\frac{1}{2^n}$ y que verifica $I_n \subset I_{n-1}$. Además

$$a_n \notin I_n$$

El principio de Cantor establece que $\bigcap_{n=0}^{\infty} I_n = \{a\}$ pero al ser $f : \mathbb{N} \to \mathbb{R}$ una biyección entonces $a = f(k) = a_k$ para algún *k*. Ahora bien, $a = a_k \notin I_k \Rightarrow a = a_k \notin \bigcap_{n=1}^{\infty} I_n$ una contradicción. □

Una importante consecuencia algebraica de este resultado es la existencia de números trascendentes. Para entender de qué hablamos vamos a dar un par de definiciones.

Un real a se denomina algebraico si y sólo si existe un polinomio no nulo $p(x) = a_0 + a_1 x + \cdots + a_n x^n$ *con coeficientes enteros,* $a_i \in \mathbb{Z}$ *tal que* $p(a) = 0$. Es decir, *a* es algebraico si y sólo si a es raíz de algún polinomio con coeficientes enteros. *Un número real es trascendente si y sólo si no es algebraico.*

1. $\sqrt{2}$ es algebraico ya que el polinomio $q(x) = x^2 - 2$ tiene coeficientes enteros y $q(\sqrt{2}) = \sqrt{2}^2 - 2 = 0$.

2. El número *e* base de los logaritmos neperianos es trascendente. Fue el primer ejemplo de un número importante que fue catalogado como número trascendente. La demostración escapa el alcance de este libro ya que es una demostración analítica, la puede ver en el libro *Calculus* de M. Spivak.

1. Demuestre que $\sqrt{2}+\sqrt{3}$ es algebraico.
2. Demuestre que $\sqrt{2}+\sqrt[3]{3}$ es algebraico.
3. Demuestre que $\sqrt{2}+\sqrt{3}+\sqrt{5}$ es algebraico.
4. Tome el conjunto $\mathbb{Q}$ de los números racionales. Ud. y un amigo van a jugar un juego que $I_n \supset I_{n+1}, n=0,1,2,\cdots$ consiste en escoger cada uno y sucesivamente un intervalo cerrado I_n de la recta real $\mathbb{R}$ con la única condición $I_n \supset I_{n+1}, n=0,1,2,\cdots$. Es decir, Ud. Toma el intervalo cerrado, digamos [0,1] y su amigo toma el intervalo cerrado [0;0,5] y así sucesivamente. Ud. gana el juego si $\bigcap_{i=1}^{\infty} I_i$ no contiene racional alguno. ¿Tiene Ud. Una estrategia ganadora?

Sugerencia: Revise cuidadosamente la segunda demostración de la no numerabilidad de los números reales.

1. Llamemos *x* a $\sqrt{2}+\sqrt{3}$, entonces

$$x=\sqrt{2}+\sqrt{3}\Rightarrow$$
$$x^2=2+3+2\sqrt{6}\Rightarrow$$
$$x^2-5=2\sqrt{6}\Rightarrow$$
$$x^4-10x^2+25=24\Rightarrow$$
$$x^4-10x^2+1=0$$

Lo que demuestra que *x* satisface una ecuación polinómica con coeficientes enteros y luego es un número algebraico.

2. Imite lo hecho en 1.
3. Imite lo hecho en 1.
4. Ud. tiene una estrategia ganadora muy interesante, haga una enumeración $x_1, x_2, \cdots, x_j, x_{j+1}, \cdots$ de los racionales. Tome Ud. el primer intervalo I_1 de forma que x_1 no esté en I_1 , de seguida tome I_2 de forma que x_2 no esté en I_2 y

continuamos este proceso garantizando que en cada paso I_n no contiene a x_n. Claramente $\bigcap_{i=1}^{\infty} I_i$ no contiene a ningún $x_1, x_2, \cdots, x_j, x_{j+1}, \cdots$ y por ende no interseca el conjunto de los racionales.

Los números trascendentes

Un problema importante en matemáticas fue demostrar la existencia de los números trascendentes. El primero que encontró un número trascendente fue el gran matemático francés Joseph Liouville quién demostró que el número

$$0{,}1010010000001000000000000000000000001\cdots$$

es trascendente (la cantidad de ceros entre dos unos consecutivos es 1!,2!,3! y así sucesivamente). Sin embargo, era un número un poco artificial y seguía la interrogante si las constantes importantes en matemática como π o la base de los logaritmos neperianos e eran números trascendentes. Fue Charles Hermite el que realizó el fantástico descubrimiento que e era trascendente. Posteriormente, el maestro de Hilbert, Lindemann demostró que π era trascendente. Con eso quedaba demostrada la imposibilidad de realizar la cuadratura del círculo ya que las construcciones con regla y compás solo determinan números algebraicos. Esto lo veremos en detalle en la Unidad correspondiente al concepto de Cuerpo.

Joseph Liouville

Charles Hermite

Cantor demuestra la existencia de los números trascendentes observando que el conjunto de polinomios con coeficientes enteros es numerable y por ende el conjunto de todas sus raíces lo es también. Pero, los reales no son numerables como ya demostramos, luego deben existir los números trascendentes. Esto es una hermosa prueba no constructiva de la existencia de los números trascendentes. Expliquemos esto en detalle. Liouville demostró que existen números trascendentes mostrando explícitamente uno de ellos. Eso es una demostración de existencia constructiva. Cantor demuestra que existen los números trascendentes comparando el tamaño de dos colecciones infinitas. Pero no encuentra ningún número trascendental en particular.
El siguiente cuadro resume las distintas clasificaciones de los números reales

<table>
<tr><td colspan="2">Números algebraicos</td></tr>
<tr><td>Irracionales</td><td>Racionales</td></tr>
<tr><td colspan="2">Números trascendentes</td></tr>
</table>

Los números reales

1. Se puede demostrar que la suma de dos números algebraicos es algebraicos. Use este resultado para demostrar que la suma de un número algebraico y uno trascendente es trascendente.

2. ¿Es la suma de dos números trascendentes un número trascendente? Si cree que es cierto demuéstrelo, si es falso de un contraejemplo.

1. Supongamos que x es algebraico y z es trascendente. Si $x+z=y$ fuese algebraico entonces $z=x-y$ fuese también algebraico lo cual es una contradicción.

2. La suma de dos trascendentes puede ser algebraico o trascendente. Por ejemplo, $2+\pi, -\pi$ son trascendentes pero su suma es 2 que es algebraico. Es un problema muy difícil determinar si el número $\pi + e$ es algebraico o trascendente, el autor cree que es un problema todavía abierto.

9.6 Modelando con los números reales

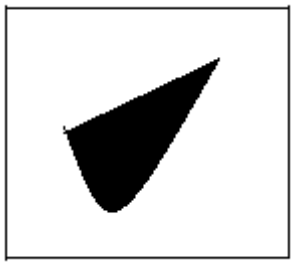
Probabilidad Geométrica: El problema de la aguja de Buffon.

Cuando tiramos un dado legal la probabilidad *P* que caiga en el número *j*, *j* perteneciente al conjunto $M=\{1,2,3,4,5,6\}$ es $P=\frac{1}{6}$. En este caso el espacio muestral *M* es finito y está conformado por 6 eventos, todos equiprobables si usamos un dado que no este cargado. En estos espacios los números racionales $\mathbb{Q}$ usualmente constituyen un lenguaje apropiado para expresar las relaciones probabilísticas pero en muchas situaciones es necesario trabajar con los números reales.

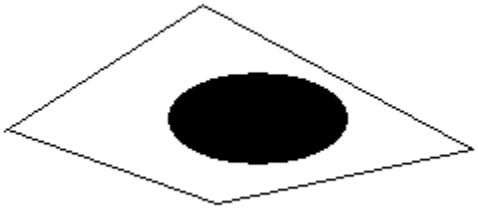
Consideremos el conjunto *P* los habitantes de la República Bolivariana de Venezuela, a un habitante *p* tomado al azar le medimos su altura *X*(*p*) en metros. Note que en este caso la variable *X* toma valores en un intervalo *I* que podemos suponer igual a [0,4], esto es $X(p)\in[0,4]$. Aquí hemos hecho la plausible suposición que toda persona tiene una altura mayor que 0 metros y menor que 4, los aficionados al libro de Record Guiness por favor verifiquen esto. Como se ve es imprescindible usar los reales para expresar la función $X: P \to [0,4]$.

Nuestro siguiente ejemplo, tomado de la Teoría de Probabilidades, es mucho más rico e ilustra la necesidad de trabajar con el cuerpo de los números reales.

Considere la figura siguiente



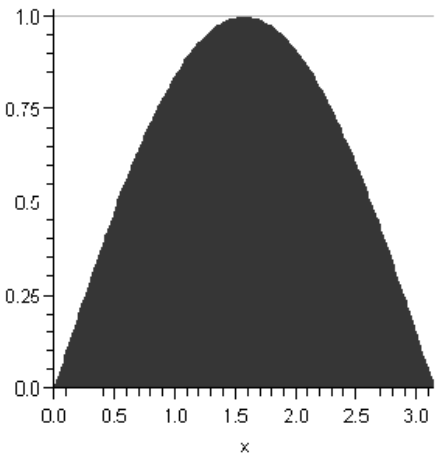
donde el cuadrado tiene lado 1 y por ende área 1. ¿Cuál es la probabilidad que si tomamos un punto al azar dentro del cuadrado que caiga dentro la zona negra?. Una respuesta intuitiva y simple es: la probabilidad *equivale al área de la zona oscura*. Más generalmente, considere la figura de abajo:



La probabilidad geométrica que un punto tomado al azar quede en la zona oscura se define como

Área zona oscura /Área del polígono

Esto tiene muchas bonitas implicaciones. Consideremos la gráfica de la función seno entre 0 y π.

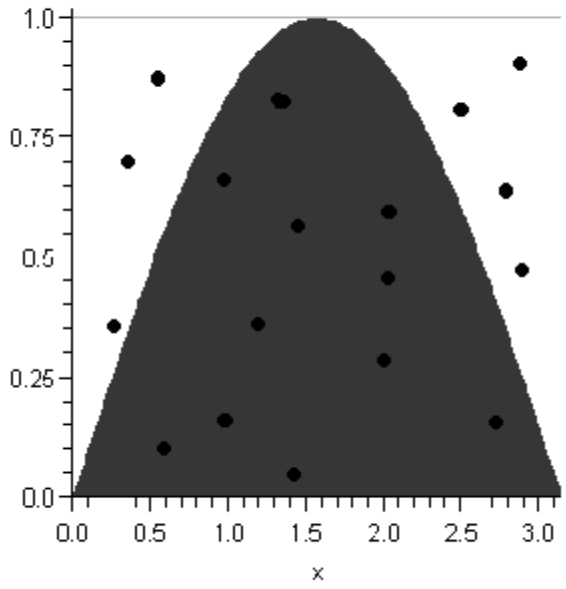


El estudiante UNA ha aprendido a calcular estas áreas en sus cursos de Cálculo. De hecho, el área de la zona gris es $\int_0^{\pi} \sin(x)dx = -\cos x \Big|_{x=0}^{x=\pi} = 1+1 = 2$. Observe que esta área queda encerrada por el rectángulo R conformado por los ejes coordenados, la recta $y=1$ y la recta $x=\pi$. Este rectángulo R tiene área fácilmente calculable, ya que el área de cualquier rectángulo es base por altura, en este caso obtenemos π. ¿Lo ve usted?. Por la fórmula de la probabilidad geométrica tenemos que

$$\frac{\text{área zona roja}}{\pi} = P$$

Donde P es la probabilidad de que si tomamos un punto al azar en el rectángulo este caiga en la zona gris. Supongamos ahora que Ud. hace experimentos con un computador y escoge un punto al azar en el rectángulo R. Esto es sencillo ya que los computadores traen generadores de números aleatorios y basta seleccionar dos números aleatorios consecutivos x,y y pensar que conforman un par (x,y). Una visión pictórica del resultado es que Ud. le dispara al azar al rectángulo R y cuenta cuántos disparos caen la zona roja. Después divide este número por el total de disparos.

$\frac{\text{área zona roja}}{\pi} = P$



Resultados de una serie de “disparos” al azar sobre el rectángulo R.

Note que los puntos (x,y) que caen en la zona gris son precisamente aquellos que están en R y que verifican $y < \sin(x)$. ¿Por qué?. Luego podemos experimentar con una hoja de cálculo o con un programa sencillo hecho en cualquier lenguaje de programación y hacer un montón de disparos al rectángulo R y contar cuántos caen en la zona gris. Esto nos da un estimado de P (probabilidad empírica) con lo cual podemos hallar el área de la zona gris.

La siguiente tabla fue realizada con una hoja de cálculo de manera muy sencilla.

0.94952535	2.9830218	0.813139315	0.57704497	0.23609434
0.1255195	0.39433113	0.125190163	0.25295822	-0.12776805
0.49800039	1.56451433	0.477669756	0.16494108	0.31272867
0.31906367	1.00236807	0.313677627	0.85943698	-0.54575935
0.81583877	2.56303304	0.728300629	0.45710887	0.27119176
0.3049704	0.95809276	0.300264944	0.97862487	-0.67835992
0.69425237	2.1810581	0.639811038	0.29317591	0.34663513
0.59564206	1.87126469	0.561040359	0.80081072	-0.23977036
0.00170087	0.00534345	0.001700872	0.74092256	-0.73922168
0.05082253	0.15966367	0.05080065	0.14579298	-0.09499233
0.62886399	1.97563447	0.588226455	0.13350758	0.45471887
0.55755827	1.75162094	0.529115849	0.85711544	-0.32799959
0.62317302	1.95775574	0.583614681	0.92120099	-0.33758631
0.31935339	1.00327825	0.125190163	0.57335542	-0.44816525
0.43155334	1.35576478	0.477669756	0.42067163	0.05699813
0.36953498	1.16092837	0.313677627	0.37048335	-0.05680573
0.37547415	1.1795868	0.728300629	0.06026522	0.66803541
0.90044758	2.82883946	0.300264944	0.34663092	-0.04636598
0.24940803	0.78353842	0.639811038	0.33076585	0.30904518
0.04560313	0.14326644	0.561040359	0.14945561	0.41158475
0.48763155	1.53193966	0.001700872	0.47799718	-0.47629631
0.25274501	0.79402185	0.05080065	0.90796134	-0.85716069

0.13432992	0.42200989	0.588226455	0.51686207	0.07136438
0.68471722	2.15110255	0.529115849	0.12921314	0.39990271
0.60305455	1.89455171	0.583614681	0.55317182	0.03044286

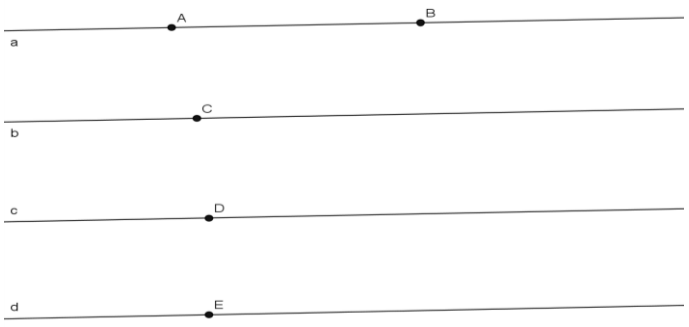
La primera columna es un número aleatorio real entre 0 y 1, en la segunda aparece el mismo número ampliado a la escala entre 0 y π. La tercera columna le aplicamos la función seno al número que tenemos en la segunda columna. Un nuevo número aleatorio entre 0 y 1 aparece en la cuarta columna. Por último, la quinta columna compara para determinar si $y < \sin(x)$. Obtuvimos 26 éxitos sobre 50 disparos, esto es P_e empírica es 0,52, luego

$$\frac{\text{área zona roja}}{\pi} \approx P_e = 0,52 \Rightarrow \text{área zona roja} \approx \pi(0,52) = 1.63$$

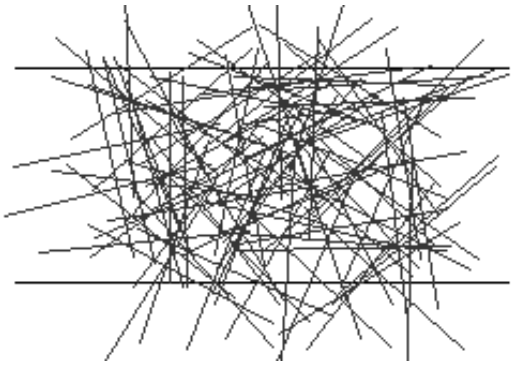
El método de Montecarlo

Similares ideas pueden ser aplicadas para calcular un volumen en el espacio, la densidad de un cuerpo o una distribución de cargas eléctricas. Constituyen una idea importante en análisis numérico denominada el método de Montecarlo, el nombre deriva del uso del azar y la probabilidad para estimar un resultado matemático y del hecho que un famoso casino esté situado en esa ciudad. Fue ideado y aplicado por vez primera por los matemáticos Ulam y Von Neumann durante el famoso proyecto Manhattan para la construcción de la primera bomba atómica durante la segunda guerra mundial (1939-1945).

Ahora le planteamos un problema interesante. Consideremos un conjunto de líneas rectas paralelas y equidistantes con distancia *L*.

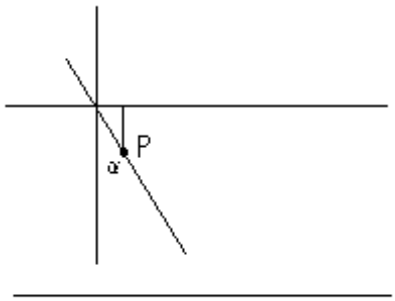


Imagine que el conjunto de rectas se esparce por todo el plano y que Ud. deja caer en el plano una aguja de tamaño *L*. Nos preguntamos: ¿cuál es la probabilidad de que la aguja toque una línea del entramado?. Este problema lo formuló el científico francés Buffon en 1733. Se conoce como el problema de la aguja de Buffon. Su solución es muy interesante.

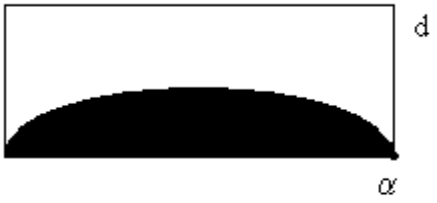


Consideremos una aguja y sea P su punto medio. El ángulo α es el ángulo que forma la aguja con la vertical y *d* es la distancia del punto medio a las líneas paralelas.

Tenemos entonces que $0 < d < \frac{L}{2}$ y que $0 < \alpha < \pi$



La condición de corte es que $\text{sen}(\alpha)(\frac{L}{2}) > d$ (indique el porqué), luego si dibujamos el rectángulo representando las variables α y *d obtenemos un rectángulo de área* $\pi L/2$.



La zona rayada corresponde a la zona de solución del problema. Invitamos al estudiante UNA a determinar el área de la zona oscura en el dibujo anterior para completar el cálculo de la probabilidad buscada.

1. Sean a,b números irracionales. ¿Es siempre a^b un número irracional?.
2. Demuestra que un número real puede aproximarse de manera arbitraria por medio de un número racional.
3. Construye un polinomio $p(x)$ con coeficientes enteros de tal manera que $\sqrt{2}+\sqrt{5}$ sea una raíz del mismo.
4. Dado el intervalo $[0,1)$, ¿cuál es, si existe, el mayor real en este intervalo?, ¿cuál es el supremo del intervalo considerado?.
5. Consideremos el conjunto de los números naturales $\mathbb{N}$. ¿Es $\mathbb{N}$ acotado superiormente?, ¿es $\mathbb{N}$ acotado inferiormente? . ¿Cuál es el ínfimo de $\mathbb{N}$?.
6. Construya un ejemplo de un conjunto *numerable* que no sea acotado.
7. Demuestre que cualquier conjunto finito es un conjunto acotado.

1. El resultado es que no siempre ocurre esto. Tomemos $\left(\sqrt{2}\right)^{\sqrt{2}}$ si este número es racional estamos listos, pero en caso que sea irracional entonces $\left(\left(\sqrt{2}\right)^{\sqrt{2}}\right)^{\sqrt{2}}=\sqrt{2}^{2}=2$, un ejemplo que revela que debemos ser muy cuidadosos con el manejo de los números racionales e irracionales.
2. Sea $a_0,a_1a_2a_3\cdots$ un real cualquiera escrito, por ejemplo, en base 10. Esto es $x=a_0+a_1 10^{-1}+a_2 10^{-2}+\cdots, a_i\in\{0,1,2,\cdots,9\}$ y tomemos la sucesión

$$x_0=a_0$$
$$x_1=a_0+a_1 10^{-1}$$
$$x_2=a_0+a_1 10^{-1}+a_2 10^{-2}$$
$$\vdots$$

Que aproxima el número y cuyos miembros son siempre números racionales.

3. Se deja al estudiante UNA.
4. No hay un mayor elemento en ese intervalo pero si existe el supremo y es 1, note la diferencia entre el máximo elemento y el supremo.
5. El conjunto de los naturales no está acotado superiormente pero si inferiormente, siendo, por ejemplo -1, una cota inferior. El conjunto de los números naturales tiene un mínimo que es 0 que coincide con su ínfimo.
6. Revise los ejemplos anteriores para resolver este problema..
7. Un conjunto finito tiene tanto un menor como un mayor elemento, luego es acotado.

Test de autoevaluación Módulo II

1. Demuestra que para cualquier n natural $1\cdot 2\cdot 3+2\cdot 3\cdot 4+\cdots+n(n+1)(n+2)=\frac{n(n+1)(n+2)(n+3)}{4}$
2. Construye un entero n tal que $n+2, \cdots, n+99$ sean números compuestos.
3. Demuestra que para cualquier a natural $(p+1)^k a^{p-1} \equiv 1 \, mod \, p$.
4. ¿Es $\sqrt{2}+\sqrt[3]{2}+1$ un número racional?.
5. Demuestra que los números reales no son numerables.

1. Tenemos que verificar que $1\cdot 2\cdot 3+2\cdot 3\cdot 4+\cdots+n(n+1)(n+2)=\frac{n(n+1)(n+2)(n+3)}{4}$ para cualquier n natural.

   Este tipo de problemas usualmente se resuelve por inducción matemática. Veamos que es cierto el resultado para n igual a 1, en efecto $1\cdot 2\cdot 3=\frac{1(2)(3)(4)}{4}$ que es una igualdad cierta. Ahora asumimos que el resultado es cierto para $n=k$, esto es $1\cdot 2\cdot 3+2\cdot 3\cdot 4+\cdots+k(k+1)(k+2)=\frac{k(k+1)(k+2)(k+3)}{4}$, lo que constituye la llamada hipótesis inductiva. A partir de la misma demostramos el

resultado para $n=k+1$. Sumemos a ambos lados de la hipótesis inductiva el término $(k+1)(k+2)(k+3)$,obtenemos

$$1\cdot 2\cdot 3+2\cdot 3\cdot 4+\cdots+k(k+1)(k+2)+(k+1)(k+2)(k+3)=\frac{k(k+1)(k+2)(k+3)}{4}+(k+1)(k+2)(k+3)$$

$$\frac{k(k+1)(k+2)(k+3)}{4}+(k+1)(k+2)(k+3)=$$

$$(k+1)(k+2)(k+3)(\frac{k}{4}+1)=\frac{1}{4}(k+1)(k+2)(k+3)(k+4)$$

Ahora, calculemos con cuidado $\frac{k(k+1)(k+2)(k+3)}{4}+(k+1)(k+2)(k+3)$.

Tenemos $\frac{k(k+1)(k+2)(k+3)}{4}+(k+1)(k+2)(k+3)=$

$$(k+1)(k+2)(k+3)(\frac{k}{4}+1)=\frac{1}{4}(k+1)(k+2)(k+3)(k+4)$$

Lo que demuestra el resultado.

Si no pudo resolver el problema vaya de nuevo a la Unidad 5, El Número Natural y repase lo que se discute en inducción matemática.

2. La idea es tomar 99! Que sin duda es un número que cumple con la condición del ejercicio ya que $99!=2\cdot 3\cdot 4\cdots 98\cdot 99$ y luego $k+99!$ Es divisible por k para cualquier k entre 2 y 99. Este ejercicio demuestra que existen lagunas arbitrariamente grandes donde no encontramos primo alguno. Si no pudo resolver el problema vaya a la continuación de la Unidad 5 y repase el concepto de divisibilidad y los ejercicios que aparecen allí.

3. Sabemos que $(p+1)^k \equiv 1 \mod p$ ya que por la fórmula del binomio de Newton se tiene $(p+1)^k = p^k + \binom{k}{1}p^{k-1}+\cdots+\binom{k}{k-1}p+1$. Por otro lado, por el Teorema Pequeño de Fermat siempre $a^{p-1}\equiv 1 \bmod p$ y multiplicando las congruencias se tiene el resultado.

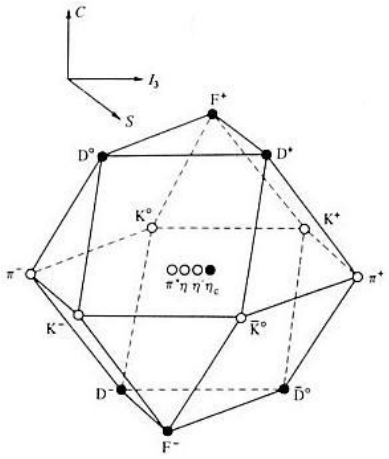
Si no logro resolver el problema repase en Unidad 6 el concepto de congruencia y el Teorema de Fermat.

4. El número es irracional y en la unidad 7 hay ejemplos y ejercicios que indican la forma de demostrarlo, vaya a la misma si no puede hacer usted la demostración y repase el contenido.

5. Vea la demostración en el “medio maestro”, Unidad 7.

UNIDAD 7

La teoría de Grupos



Semana 11

Aplicar el concepto de grupo en la resolución de problemas, en el modelado matemático y en la demostración de nuevos resultados.

Temas a tratar: Ley de composición interna. El concepto de grupo. Ejemplos: grupo de permutaciones. Rotaciones y Simetrías. Orden de un grupo.

10.1. Introducción

Como muchas ideas de la matemática moderna, el concepto de ley de composición interna surge del trabajo de Leonard Euler. Por supuesto que los matemáticos conocían leyes de composición interna sobre distintos conjuntos antes del trabajo de Euler pero este la utiliza en conjuntos bastantes arbitrarios, como los residuos de las potencias de un número módulo *p.* Es un primer movimiento hacia un mayor grado de abstracción. Posteriormente, Gauss escribe su tratado fundamental Disquisiciones Aritméticas donde claramente se expone el concepto de ley de composición interna.

10.2. El concepto de ley de composición interna

En muchos casos dos objetos *x,y* de un conjunto dado *A* **se combinan mediante una operación para formar un nuevo objeto que pertenece a** *A*. Por ejemplo, si tomamos dos matrices *M,N* cuadradas 2x2 las podemos sumar de manera natural , entrada por entrada y obtenemos una nueva matriz.

Definición. Una ley de composición interna en un conjunto *A* es una función

$$f : A \times A \to A$$
$$(x, y) \to f(x, y)$$

que a cada par $(x,y) \in A \times A$ le asocia el elemento $f(x,y) \in A$.

Notación: Es costumbre en matemática usar, para indicar una ley de composición interna, un símbolo como $*$ entre los elementos *x* e *y*, así escribimos $x * y$ en lugar de *f*(*x*,*y*). También son muy comunes los símbolos $+, \times, \oplus, \odot$ para indicar leyes de composición interna.


Cuando tenemos una ley de composición interna $*$ en *A* es costumbre decir que *A* es *cerrado respecto a* $*$. El estudiante debe saber que usaremos muchas veces esta expresión para indicar que $*$ es una ley de composición interna.

1. Consideremos el conjunto de todos los enteros $\mathbb{Z}$, en ellos se puede definir la ley de composición interna del producto (definido en la Unidad 4) que asocia a cada par (*x*,*y*) el elemento de $\mathbb{Z}$ dado por $x \cdot y$.
2. Consideremos el conjunto de todos los enteros $\mathbb{Z}$ y definamos la ley de composición interna

$$g : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$$
$$g(x, y) = x \oplus y = x + y - xy$$

Observe que $g(x,0) = x \oplus 0 = x + 0 - x0 = x$ y que $0 \oplus x = x$. ¿Por qué?. Más adelante veremos que 0 es un elemento neutro para esta ley.

3. En el conjunto *M* de todas las matrices 2x2 con coeficientes reales se pueden definir distintas operaciones. Pero, primero entendamos bien que es *M*

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}, a_{ij} \in \mathbb{R} \text{ para } i, j \in \{1,2\}$$

La suma + de matrices en *M* se define mediante la asignación:

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} + \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} = \begin{pmatrix} a_{11}+b_{11} & a_{12}+b_{12} \\ a_{21}+b_{21} & a_{22}+b_{22} \end{pmatrix}$$

Es claro que el conjunto *M* es cerrado respecto a la suma antes definida. La suma que hacemos en las entradas es la suma usual de números reales. Desde un punto de vista formal debiéramos usar un símbolo para la suma de matrices y otro para la suma de reales pero esto sólo haría la notación más engorrosa. Una pregunta al estudiante UNA, de acuerdo con la definición de suma de matrices dada arriba, ¿qué pasa si le sumamos a una matriz cualquiera la matriz $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$? Reflexione su respuesta.

4. El estudiante aprendió en bachillerato (segundo año) que si tenemos dos polinomios $p(x)$ y $q(x)$ con coeficientes reales estos se pueden sumar para obtener un nuevo polinomio. Es decir, si denotamos por $\mathbb{R}[x]$ al conjunto de todos los polinomios con coeficientes reales, entonces la adición de polinomios es una ley de composición interna en $\mathbb{R}[x]$. ¿Puede el estudiante UNA decir qué ocurre con el producto de polinomios en $\mathbb{R}[x]$?

5. Consideremos el conjunto $\mathbb{Q}^+$ de los números racionales positivos. Definimos una operación $\otimes$ en $\mathbb{Q}^+$ de la manera siguiente: si *x,y* están en $\mathbb{Q}^+$ entonces $x \otimes y = x + y + \sqrt{x} + \sqrt{y}$. El estudiante UNA debe decir si $\mathbb{Q}^+$ es cerrado respecto a esta operación.

Definición. Sea un conjunto *A* dotado de una ley de composición interna $\bullet$, un elemento e perteneciente a *A* se denomina elemento neutro para $\bullet$ sí y sólo

$$x \bullet e = e \bullet x = x,$$

para cualquier elemento *x* de *A*.

Es decir, al operar *x* con el elemento *e* no se produce cambio alguno y se obtiene *x*.

1. Consideremos el conjunto de todos los enteros $\mathbb{Z}$ respecto a la suma usual. Entonces 0 es un elemento neutro como ya vimos en la unidad correspondiente a los números enteros. Si tomamos ahora la multiplicación en $\mathbb{Z}$ vemos que el 1 es el elemento neutro.
2. Tomemos K el conjunto de todas las matrices 2x2 con entradas reales. Es decir,

$$K=\left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix}, \text{donde } a,b,c,d \text{ son números reales}\right\}$$

Definimos en *K* una ley de composición interna $\times$ por medio de $\begin{pmatrix} a & b \\ c & d \end{pmatrix}\times\begin{pmatrix} e & f \\ g & h \end{pmatrix}=\begin{pmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{pmatrix}$, el estudiante debe verificar que la matriz dada por $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ es un elemento neutro para $\times$.

Hemos hablado de un elemento neutro *e* para una ley de composición interna, una pregunta natural es ¿pueden haber varios elementos neutros para una ley de composición interna definida en un conjunto *A* dado? La respuesta es no como lo demuestra la siguiente proposición.

Proposición 1. Si la ley de composición interna $*$ admite un elemento neutro *e,* este elemento es único.

Demostración. Supongamos que exista otro elemento neutro *e'* y que *e* sea distinto de *e'*. Es decir, razonamos *por reducción al absurdo.* Entonces $e * e' = e'$ por ser *e* un elemento neutro. Por otro lado, $e * e' = e$ ya que *e'* es un elemento también, pero combinando ambas igualdades obtenemos $e = e'$, de donde obtenemos una contradicción y esto implica la unicidad del elemento neutro.

1. Es típico usar reducción al absurdo para demostrar la unicidad de objetos matemáticos. Por ejemplo, en Cálculo I el estudiante demostró la unicidad del límite de manera similar.
2. Observe la importancia de la proposición anterior, cada vez que tenemos una ley de composición interna con un elemento neutro no debemos preocuparnos por la unicidad del mismo. Esto demuestra *la potencia de usar un enfoque abstracto.*

1. Considere el conjunto M de todas las matrices 2x2 (2 filas y dos columnas) con entradas pertenecientes los números reales. Definimos en *M* la ley de composición interna siguiente

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \otimes \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} ae & bf \\ cg & dh \end{pmatrix}$$

Estudie si esta ley de composición tiene un elemento neutro.

2. Considere los números naturales $\mathbb{N}$ y la operación definida entre números naturales por medio de $a \oplus b = a + b + ab$. Diga si esta operación corresponde a una ley de composición interna y determine su elemento neutro en caso de que este exista.

1. La matriz $\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$ es el elemento neutro de la ley de composición interna considerada, el estudiante UNA debe verificar esta afirmación.

2. Para que exista un elemento neutro *e* debe ocurrir que $a \oplus e = a + e + ae = a \Rightarrow e(a+1) = 0$, pero $a+1$ es un natural no nulo, luego se

debe tener que e=0. Es claro que $0 \oplus a = 0$ de donde 0 es el elemento neutro buscado.

Cuando existe un elemento neutro *e* respecto a una ley de composición interna es muy importante estudiar la existencia del *inverso* de un elemento dado. Veamos este concepto en detalle. *Sea A un conjunto con una ley de composición interna* $*$ *y elemento neutro e, decimos que el elemento x admite un inverso o es invertible, y denotamos su inverso por* x^{-1}, *si* $x * x^{-1} = x^{-1} * x = e$ *para* x^{-1} *en A.* [1]

1. En los números naturales $\mathbb{N}$ sabemos que el 0 es el elemento neutro respecto de la ley de composición de suma o adición. Sin embargo, ningún elemento en $\mathbb{N}$ tiene un inverso respecto a la adición ya que si *n* está en $\mathbb{N}$ no podemos encontrar otro natural *k* tal que $n+k=k+n=0$.
2. En los números enteros $\mathbb{Z}$, la adición tiene un elemento neutro que es el 0 y *todo elemento x tiene un inverso que llamamos –x.* Vea la unidad de los números enteros para tan importante propiedad.
3. Consideremos *M* todas las matrices cuadradas 2x2 con coeficientes reales. Es decir, $M = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ con } a,b,c,d \in \mathbb{R} \right\}$. En el ejemplo 2 arriba, definimos en *M* una multiplicación que tiene la matriz *I* como elemento neutro, donde $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. No toda matriz en *M* tiene un inverso respecto a la multiplicación. Por ejemplo, la matriz $A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ no puede tener inverso ya que $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. La condición para que una matriz $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ pueda tener inverso es $ad\text{-}bc \neq 0$. En efecto, si planteamos la

[1] En muchos textos se habla de inverso por la derecha y por la izquierda y de inverso cuando estos dos coinciden, nosotros no estudiaremos esas posibilidades.

ecuación $\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} x & y \\ z & w \end{pmatrix}=\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, ella genera dos sistemas de ecuaciones independientes, precisamente

$$\begin{cases} ax+bz=1 \\ cx+dz=0 \end{cases}$$

$$\begin{cases} ay+bw=0 \\ cy+dw=1 \end{cases}$$

El estudiante UNA debe recordar de su estudios de bachillerato (ver *Matemática y el buen vivir,* Quinto año, Colección Bicentenario), que estos sistemas tienen solución única si el determinante $\begin{vmatrix} a & b \\ c & d \end{vmatrix}=ad-bc\neq 0$. De hecho, aplicando la regla de Cramer obtenemos

$$x=\frac{\begin{vmatrix} 1 & b \\ 0 & d \end{vmatrix}}{\begin{vmatrix} a & b \\ c & d \end{vmatrix}}, z=\frac{\begin{vmatrix} a & 1 \\ c & 0 \end{vmatrix}}{\begin{vmatrix} a & b \\ c & d \end{vmatrix}}, y=\frac{\begin{vmatrix} 0 & b \\ 1 & d \end{vmatrix}}{\begin{vmatrix} a & b \\ c & d \end{vmatrix}}, z=\frac{\begin{vmatrix} a & 0 \\ c & 1 \end{vmatrix}}{\begin{vmatrix} a & b \\ c & d \end{vmatrix}}$$

El estudiante UNA debe verificar que $\begin{pmatrix} x & y \\ z & w \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}=\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

Definición. Una ley de composición $*$ definida en un conjunto *A* se denomina asociativa sí y sólo sí $(a*b)*c=a*(b*c)$ cualesquiera que sean *a,b,c* pertenecientes a *A.*

1. Consideremos *A* el conjunto de las funciones exponenciales, es decir

$$A=\left\{ f:\mathbb{R}\to\mathbb{R} \text{ tales que } f(x)=Ce^{\alpha x} \text{con } \alpha,C \text{ reales arbitrarios}\right\}$$

Vamos a definir una ley de composición interna $\circ$ en *A* de la forma siguiente, para *f,g* pertenecientes a *A* definimos

$$f\circ g=h \text{, donde } h(x)=f(x)g(x)$$

Como $h(x) = f(x)g(x) = Ce^{\alpha x}De^{\beta x} = CDe^{(\alpha+\beta)x}$ entonces *h* está en *A*. Veamos que $\circ$ es asociativa. En efecto, supongamos que $f(x) = Ce^{\alpha x}, g(x) = De^{\beta x}, h(x) = Ee^{\delta x}$. Si llamamos $\big((f \circ g) \circ h\big) = r$ y $f \circ g = m$ entonces

$$(f \circ g)(x) = m(x) = CDe^{(\alpha+\beta)x}$$

Luego, $(m \circ h)(x) = CDe^{(\alpha+\beta)x}Ee^{\delta x} = CDEe^{(\alpha+\beta+\delta)x}$. Invitamos al estudiante UNA a calcular paso a paso $(f \circ (g \circ h))$ y verificar que es igual a $\big((f \circ g) \circ h\big)$.

Este ejemplo es muy importante en la teoría de ecuaciones diferenciales.

2. La adición en los números naturales es una operación asociativa como ya vimos en la Unidad correspondiente.
3. La multiplicación de matrices definida en el ejemplo 2 arriba constituye una ley de composición interna asociativa.

Sea *A* un conjunto cualquiera con una ley de composición interna • definida entre sus elementos. Asuma que en *A* existe un elemento neutro *e* para la ley de composición interna antes definida y que • es asociativa. Demuestre que si *a* en *A* es invertible entonces su inverso a^{-1} es único.

Supongamos que *b* y *c* son inversos de *a* respecto a la operación •, luego $(b \bullet a) \bullet c = e \bullet c = c$. Pero, por otro lado $(b \bullet a) \bullet c = b \bullet (a \bullet c) = b \bullet e = b$, de donde *b*=*c*.

Definición. Una ley de composición interna $\circ$ en un conjunto *A* se denomina conmutativa sí y sólo sí $a \circ b = b \circ a$ para cualesquiera elementos *a*,*b* pertenecientes a *A*.

En matemática es obligatorio después de una definición indicar algún ejemplo.

1. Consideremos el espacio de vectores $\mathbb{R}^3$, donde $\mathbb{R}^3 = \{(x, y, z) \text{ donde } x, y, z \text{ son números reales}\}$. Definimos una ley de composición interna + en $\mathbb{R}^3$, llamada suma de vectores, y dada por

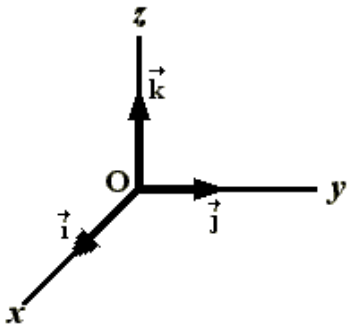
$$(x, y, z) + (x', y', z') = (x + x', y + y', z + z')$$

Como la suma de números reales es conmutativa también lo es la suma de vectores. Es decir, la ley de composición interna en $\mathbb{R}^3$ hereda la propiedad de conmutatividad de lo que ocurre en $\mathbb{R}$.

2. Como ya el lector conoce para dar una función tenemos que dar el conjunto de partida, el de llegada y la regla de transformación. Consideremos el espacio de vectores $\mathbb{R}^3$ y definamos una ley de composición en los vectores de $\mathbb{R}^3$ por medio de

$$\vec{u} \times \vec{v} = \begin{vmatrix} \vec{i} & \vec{j} & \vec{k} \\ u_1 & u_2 & u_3 \\ v_1 & v_2 & v_3 \end{vmatrix}, \vec{u} = (u_1, u_2, u_3) \text{ y } \vec{v} = (v_1, v_2, v_3).$$

Aquí los símbolos $\vec{i}, \vec{j}$ y $\vec{k}$ representan los vectores unitarios $\vec{i} = (1,0,0)$, $\vec{j} = (0,1,0)$ y $\vec{k} = (0,0,1)$ sobre los ejes *x*,*y* y *z*.



Una propiedad básica de los determinantes es que al intercambiar dos filas cambia el signo del resultado, es decir,

$$\vec{u} \times \vec{v} = -\vec{v} \times \vec{u}$$

y concluimos que la ley definida no es conmutativa. Estamos acostumbrados a que las operaciones en matemáticas sean conmutativas pero muchas no lo son.

3. En el conjunto de los enteros $\mathbb{Z}$ la suma y la multiplicación usuales son leyes de composición conmutativas. Vea la semana correspondiente para verificar los detalles.

Sir Rowan Hamilton y las operaciones matemáticas

Hamilton realizó muchos aportes importantes en matemática. Uno de ellos fue descubrir una nueva clase de números llamados *cuaternios o cuaterniones.* Por supuesto es importante en cualquier clase de números *definir operaciones o leyes de composición interna*. Hamilton tardó bastante en encontrar cómo multiplicar los cuaternios. Se cuenta que todas las mañanas al levantarse sus hijos pequeños le preguntaban: ¿ya puedes multiplicar los cuaternios? Hamilton invariablemente contestaba: solo sé como sumarlos y restarlos. Un día estando de paseo en el bosque de su querida Irlanda encontró la solución. La multiplicación de cuaternios no podía ser conmutativa. Hamilton tardó tanto en encontrar la solución porque buscaba una operación que fuese conmutativa. La solución le causó tal impresión que talló en la base de un puente la forma de multiplicar los cuaternios. Actualmente hay una placa conmemorativa en el mismo puente ya que la talla original de Hamilton se perdió,

Placa conmemorativa del descubrimiento de Hamilton

Tomada de : http://es.wikipedia.org/wiki/Cuaterni%C3%B3n

1. Si definimos en los reales $\mathbb{R}$ la ley de composición interna por medio

$$x * y = x^2 - y^2$$

¿Es esta ley conmutativa?. Razone su respuesta.

2. Consideremos el conjunto M_{22} las matrices cuadradas 2x2 con entradas reales, esto es ¨

$$M_{22} = \left\{ \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}, a_{ij} \in \mathbb{R} \text{ con } i, j \in \{1,2\} \right\}$$

Las operaciones de suma y multiplicación fueron definidas anteriormente. Examine si son conmutativas.

3. Consideremos en el conjunto de funciones reales de variable real la ley de composición interna dada por la composición usual de funciones. ¿Es esta ley de composición interna conmutativa?

1. Veamos que la ley de composición interna dada no es conmutativa, en efecto $1*0 = 1^2 - 0^2 = 1$ pero $0*1 = 0^2 - 1^2 = -1$.
2. Al sumarse las matrices entrada por entrada se tiene que la suma de matrices es conmutativa por ser conmutativa la suma usual de números reales. La multiplicación de matrices es más interesante. Tomemos un par de matrices $\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ y efectuemos su multiplicación en los dos órdenes posibles

$$\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 2 & 1 \\ 4 & 3 \end{bmatrix}$$

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}=\begin{bmatrix} 3 & 4 \\ 1 & 2 \end{bmatrix}$$

Lo que indica que la operación de multiplicación de matrices no es conmutativa, al ser las dos matrices distintas.

3. Tomemos dos funciones reales definidas en todos los reales muy conocidas por el estudiante UNA, $f(x)=x^2, g(x)=\cos x$. Invitamos al estudiante UNA a calcular $f(g(x))$ y $g(f(x))$ para que verifique que la operación de composición es no conmutativa.

10.3. El concepto de grupo

En el trabajo de Cauchy y Galois aparece la idea de introducir operaciones o leyes de composición en conjuntos no numéricos. Ellos trabajaron con el conjunto de las *permutaciones de n elementos*. Seguiremos el camino histórico para motivar el concepto de grupo.

En primer lugar, *una permutación de n elementos es una función biyectiva* $\sigma:\{1,2,\cdots,n\}\to\{1,2,\cdots,n\}$. Ud. puede pensar que se toman inicialmente los números 1, 2, ⋯, *n* y se cambian de lugar o se permutan los mismos, manteniendo a todos los números presentes. La forma como se cambian o permutan los números está determinada por una función que llamaremos permutación. Para describir una permutación σ usaremos una notación matricial que describimos a continuación. Colocamos en una matriz de *dos filas* los números de 1 hasta *n* de forma que en la fila superior aparecen en el orden natural 1, 2, 3, ⋯, *n*-1, *n* . *En la fila de abajo a parecen las imágenes de 1, 2, 3,* ⋯, *n-1,n determinadas por la permutación* σ.

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$$

Aclaremos esto con un ejemplo.

Fijamos el conjunto $A=\{1,2,3,4\}$. Consideremos la permutación σ definida en este conjunto y dada por $\sigma(1)=2,\sigma(2)=3,\sigma(3)=1,\sigma(4)=4$. Es claro que σ es

biyectiva. El estudiante UNA debe decir por qué. Usando la notación matricial podemos escribir $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$. Observe que en la fila de arriba aparecen los números 1,2,3 y 4 en su orden natural, mientras que en la fila de abajo aparecen los mismos números permutados. Note que si apareciera, en la fila de abajo, algún número repetido no tendríamos que σ fuera una permutación ya que no sería inyectiva.

1. ¿Cuántas permutaciones tenemos si *n*=1, *n*=2, *n*=3? ¿Puede Ud. generalizar el resultado para un *n* natural cualquiera?.
2. Dada la permutación de tres elementos $\mu = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$. Determine:

a) $\mu(1), \mu(2)$ y $\mu(3)$.

b) $\mu \circ \mu = \mu^{(2)}$ donde $\circ$ representa la composición usual de funciones.

c) Demuestra que $\mu \circ \mu \circ \mu = \mu^{(3)} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$.

Nota: La notación $\mu^{(n)}$ indica que componemos la función μ *n* veces consigo misma.

1. El estudiante debe recordar de sus estudios de bachillerato que el número de permutaciones de *n* elementos es *n*!.
2. a) Por inspección vemos que $\mu(1) = 2, \mu(2) = 3$ y $\mu(3) = 1$

   b) Si volvemos a aplicar la permutación $\mu^2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ obtenemos

   $$\mu \circ \mu = \mu^{(2)} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

   c) Queda para el estudiante UNA.

Para n=3 tenemos, como ya el estudiante UNA verificó, 6 permutaciones, estas son

$$e=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix},\sigma=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix},\delta=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$$
$$\lambda=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix},\theta=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix},\omega=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$$

Observe que si tomo las permutaciones σ,δ las podemos componer de dos maneras, $\sigma\circ\delta$ es una de las formas y la otra es $\delta\circ\sigma$. Al no ser conmutativa la composición de funciones el orden de composición es muy importante.

1. Considere las permutaciones del ejemplo anterior, determine:
   a) $\sigma\circ\theta$ y $\theta\circ\sigma$, ¿son iguales?
   b) Calcule $e\circ\theta$
   c) ¿Qué ocurre cuando componemos cualquier permutación con e?

2. ¿Cuántos elementos tiene S_n?

1. a) $\sigma\circ\theta=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$ y $\theta\circ\sigma=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$ que son distintas, recuerde que el orden es importante en la composición de funciones.
   b) Es igual a θ.
   c) La permutación queda invariante, es decir, e es el elemento neutro para la operación de composición de permutaciones.
2. Como ya hemos visto hay $n!$ permutaciones en S_n.

Definición.

3. Consideremos *el conjunto* $\{1,2,\cdots,n-1,n\}$ *de n elementos. El conjunto de todas las permutaciones actuando sobre el conjunto* $\{1,2,\cdots,n-1,n\}$ *se denomina* S_n.

Como señalamos en la introducción, es importante dotar a los conjuntos relevantes en la matemática de leyes de composición. El estudiante UNA , que haya estado atento a los ejemplos anteriores, puede prever que la ley de composición "natural" para el conjunto de permutaciones S_n *es la composición de funciones*. El resultado fundamental que debe recordar el estudiante de la unidad de Funciones que la composición de dos biyecciones es una biyección. Luego si f y g pertenecen a S_n entonces $f \circ g$ está en S_n ¿Qué propiedades tiene el conjunto S_n dotado de la ley de composición interna definida por la composición de funciones?. Vamos a analizar con detalle este caso que es muy importante en toda nuestra discusión del concepto de grupo. En realidad, el concepto de grupo es una generalización de este ejemplo[2].
En primer lugar enunciemos explícitamente un resultado que comentamos anteriormente.

Teorema 2. La composición de funciones es una ley de composición interna en el conjunto S_n.

Demostración. En la Unidad de Funciones, el estudiante UNA estudió que la composición de la permutación $\sigma:\{1,2,3,\cdots,n\}\to\{1,2,3,\cdots,n\}$, con la permutación $\mu:\{1,2,3,\cdots,n\}\to\{1,2,3,\cdots,n\}$, $\mu\circ\sigma$, está bien definida. El siguiente diagrama explica por qué.

$$\{1,2,\cdots,n-1,n\}\xrightarrow{\sigma}\{1,2,\cdots,n-1,n\}\xrightarrow{\mu}\{1,2,\cdots,n-1,n\}$$

Por otro lado, es un resultado de esa Unidad, que al componer dos biyecciones obtenemos una biyección. Luego $\mu\circ\sigma$ está en S_n . Esto concluye la demostración.

[2] Uno puede pensar que los grupos son casos particulares de ciertos grupos de permutaciones.

Luego el conjunto, S_n tiene una ley de composición interna $\circ$. Como ya señalamos esto lo escribimos $(S_n, \circ)$. Estudiemos qué propiedades tiene $(S_n, \circ)$.

Teorema 3. En $(S_n, \circ)$ existe un elemento neutro dado por la permutación

$$e = \begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{pmatrix}.$$

Es decir, e es la permutación que fija todos los elementos, $e(i)=i$ para todo i en $\{1, 2, 3, \cdots, n\}$.

Demostración. Recordamos que e es un elemento neutro para la ley de composición interna $\circ$ sí y sólo sí $e \circ \sigma = \sigma$ y $\sigma \circ e = \sigma$. Pero, $e \circ \sigma(j) = e(\sigma(j)) = \sigma(j)$ para cualquier j entre 1 y n. Luego, $e \circ \sigma = \sigma$. Similarmente, $\sigma \circ e(j) = \sigma(e(j)) = \sigma(j)$ para cualquier j entre 1 y n. Esto implica, $\sigma \circ e = \sigma$, lo que concluye la demostración.

Recordamos al estudiante UNA (ver Unidad de Funciones) que en la composición de funciones el orden de composición es muy importante. De hecho, es sencillo dar ejemplos de composición de dos funciones que es solo posible en un orden determinado. Aún más, aunque la composición sea posible, en general el orden importa. Luego, en $(S_n, \circ)$ la ley de composición no es conmutativa.

Teorema 4. En $(S_n, \circ)$ la ley de composición es asociativa.

Demostración. La composición de funciones, sean o no permutaciones, *siempre es asociativa*. Esto concluye la demostración.

Vamos a examinar la existencia de un inverso para cada permutación α que consideremos en S_n. Esto es muy sencillo si el estudiante UNA recuerda el concepto de función inversa.

Teorema 5. En $(S_n, \circ)$ cada permutación α tiene un inverso denotado por α^{-1} que verifica $\alpha \circ \alpha^{-1} = \alpha^{-1} \circ \alpha = e$.

Demostración. Como cada α en S_n es una biyección tiene una función inversa (Ver Unidad 3). Denotamos a la misma α^{-1} que esta caracterizada por la relación

$$\alpha(i) = j \Leftrightarrow \alpha^{-1}(j) = i$$

Luego,

$$\alpha(\alpha^{-1}(j)) = \alpha(i) = j$$
$$\alpha^{-1}(\alpha(i)) = \alpha^{-1}(j) = i$$

para i,j arbitrarios. Luego $\alpha \circ \alpha^{-1} = \alpha^{-1} \circ \alpha = e$, como se quería demostrar.

Consideremos S_3 y la permutación $\phi = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$. ¿Cuál es la permutación inversa de ϕ? La función inversa ϕ^{-1} de ϕ debe mandar al 1 en 2, al 2 en 1 y fijar el 3. Observe que desde un punto de vista práctico la propia matriz de ϕ nos da la inversa.

$$\begin{pmatrix} 1 & 2 & 3 \\ \uparrow & \uparrow & \uparrow \\ 2 & 1 & 3 \end{pmatrix}$$

Las flechas indican los valores de ϕ^{-1}

Resumamos lo que hemos encontrado:

Propiedades de (S_n, $\circ$).
1. Existe un elemento neutro dado por la permutación $e = \begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{pmatrix}$
2. La ley de composición interna definida por la composición de permutaciones es asociativa
3. Toda permutación φ tiene una permutación inversa φ^{-1} que verifica $\varphi \circ \varphi^{-1} = \varphi^{-1} \circ \varphi = e$

El genio de Galois caracterizó con el nombre de *grupo a todo conjunto A con una ley de composición interna * donde se verifiquen las tres propiedades siguientes:*

existencia de un elemento neutro, que la ley de composición sea asociativa y que todo elemento tenga un inverso para la ley de composición interna.

Debido a la importancia del concepto, escribiremos esto en detalle en nuestra siguiente definición.

Definición. *Sea A un conjunto cualquiera que posee una ley de composición interna *. Supongamos que:*

1. *Existe un elemento neutro e en A tal que e*a=a*e=a para cualquier elemento a en A.*
2. *Todo elemento a en A tiene un inverso perteneciente a A y denotado por a^{-1} tal que $a* a^{-1} = a^{-1}*a=e$.*
3. *La ley de composición interna * es asociativa.*

Evariste Galois : El creador del álgebra moderna

Matemático francés (25 de octubre de 1811 , 31 de mayo de 1832) que muere a los veinte años de edad dejando un legado muy importante. Los matemáticos italianos Cardano, Tartaglia y Del Ferro habían encontrado fórmulas que permitían resolver las ecuaciones de tercero y cuarto grado. Esas fórmulas involucraban extracciones de raíces cúbicas de cantidades complejas. Una pregunta natural es: ¿existe una fórmula para la ecuación de quinto grado?. Evariste Galois resolvió este problema y caracterizó las ecuaciones que podían ser resueltas por radicales. Debemos señalar el trabajo pionero de Ruffini y Abel en relación a la ecuación de quinto grado pero fue Galois quien sistematizó todas estas ideas, introduciendo los conceptos de grupo, cuerpo y extensión de cuerpo, así como de homomorfismo, lo que da inicio al álgebra moderna. Su muerte ocurrió al recibir un balazo en el estomago en un duelo y fallecer a los dos días en el hospital. La noche antes de morir redactó su memoria sobre la solución de las ecuaciones polinómicas, trabajo que permaneció por mucho tiempo sin ser conocido por la comunidad matemática.

Dentro de los grupos distinguiremos los grupos en los cuales la ley de composición es conmutativa, *un grupo G se dice abeliano o conmutativo si la ley de composición en G es conmutativa.*

Vamos a dar varios ejemplos de este concepto fundamental, por supuesto empezamos con el ejemplo que inició nuestra discusión. En cada ejemplo discutiremos si el grupo dado es abeliano o no.

1. El conjunto de permutaciones de n elementos S_n con la ley de composición dada por la composición de funciones es un grupo, se denomina el grupo simétrico y tiene $n!$ elementos. Es un grupo muy importante en matemáticas. Solo es abeliano en el caso de tener n=1 o 2, el estudiante UNA debe indicar por qué.
2. El conjunto $\mathbb{Z}$ es un grupo respecto a la adición. Vaya a la unidad de los números enteros para los detalles. Es un grupo abeliano con *infinitos* elementos.
3. El conjunto $\mathbb{Z}_n$ de clases de equivalencia módulo n es un grupo respecto a la adición. Es un grupo abeliano que cuenta con n elementos (las n clases de congruencia módulo n) como ya el estudiante UNA estudió.
4. Consideremos el conjunto de todos los racionales $\mathbb{Q}^*$ excepto el 0. Tomemos como ley de composición interna en $\mathbb{Q}^*$ la multiplicación usual de racionales. Vemos que $\mathbb{Q}^*$ es un grupo cuyo elemento neutro es el 1. El inverso del racional $\frac{p}{q}$ es el racional $\frac{q}{p}$. $\mathbb{Q}^*$ es un grupo abeliano con infinitos elementos.
5. Consideremos el conjunto de todos los números reales positivos $\mathbb{R}^*_+ = \{x \in \mathbb{R}, x > 0\}$ con la ley de composición dada por el producto usual de números reales. El estudiante UNA debe verificar que $\mathbb{R}^*_+$ es un grupo.

1. Verificar que $\mathbb{R}^*_+$ es un grupo respecto al producto usual de números reales.

Sugerencia:

1. Trate de responder estas preguntas, ¿es el producto de reales positivos un real positivo?, ¿cuál es el elemento neutro?, ¿cuál es el inverso de un elemento *x* en $\mathbb{R}^*_+$?
2. Definimos en los enteros $\mathbb{Z}$ definimos una ley de composición interna * por medio de $m*n=m+n+1$. Estudie si $(\mathbb{Z},*)$ es un grupo.

Sugerencia:

1. Trate de responder estas preguntas, ¿cuál es el elemento neutro?, ¿cuál es el inverso de un elemento *x* en $\mathbb{Z}$? ¿Es la operación asociativa?

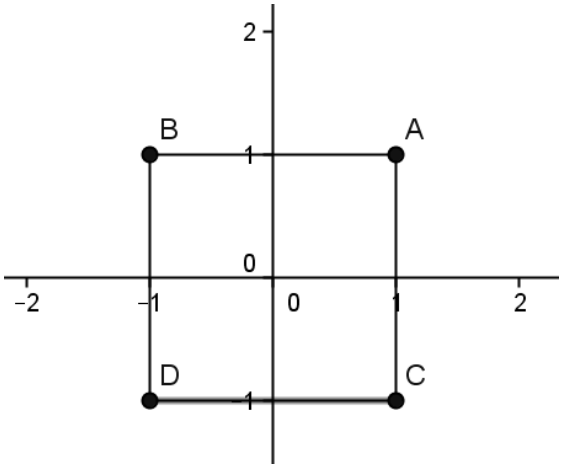
2. Consideremos el conjunto de todos los números reales $\mathbb{R}$ con la ley de composición interna dada por $x*y=xy+x+y$. Estudie si $(\mathbb{R},*)$ es un grupo.

1. El producto de reales positivos es un real positivo, luego la operación definida es, de hecho, una ley de composición interna. Al ser el producto usual de números reales asociativo entonces $\mathbb{R}^*_+$ hereda esta propiedad. Es claro que 1 es el elemento neutro para el producto y como hemos excluido al 0, todo elemento *x* de $\mathbb{R}^*_+$ tiene inverso, en este caso $\frac{1}{x}$. Luego, $\mathbb{R}^*_+$ es un grupo respecto al producto de números reales.
2. La operación definida es una ley de composición interna ya que $m*n=m+n+1$ es un entero siempre que *m,n* sean enteros. Estudiemos la existencia de un elemento neutro *e*. Como $m*e=m+e+1=m\Rightarrow e=-1$ entonces -1 es el elemento neutro buscado. Como la ecuación en *n*,

$m*n=m+n+1=-1$ tiene solución en $\mathbb{Z}$ entonces todo elemento es inversible o invertible. Dejamos al estudiante UNA la verificación de que la propiedad asociativa si se cumple, luego $\mathbb{Z}$ es un grupo respecto a la operación indicada.

3. En este caso falla la existencia del inverso para la operación dada, el estudiante UNA debe suplementar los detalles. Luego, no es un grupo.

Grupo de rotaciones de un cuadrado. Tomemos un cuadrado de vértices A,B,C,D. Sea 0 el centro del cuadrado. Consideremos las rotaciones de centro 0 que llevan el cuadrado en sí mismo. Por ejemplo, una rotación de 90 grados



centrada en 0 y con sentido antihorario (rotación positiva) lleva al cuadrado en el mismo, moviendo el vértice A a B, el vértice B a D el vértice D a C y C va a A. Hay precisamente cuatro rotaciones centradas en 0 que dejan el cuadrado invariante. Estas son:

- La rotación R_1 de 0 grados
- La rotación R_2 de 90 grados
- La rotación R_3 de 180 grados
- La rotación R_4 de 270 grados

Cada uno de estas rotaciones queda caracterizada por su efecto sobre los vértices del cuadrado, note que un vértice debe ir necesariamente en un vértice si la rotación deja al cuadrado en el mismo.

Hagamos una tabla con el efecto sobre los vértices de cada una de las rotaciones R_1, R_2, R_3 y R_4 listadas arriba.

Vértice(posición original)	Rotación	Vértice(posición al rotar)
A	R_1	A
B		B
C		C
D		D

Observe que esta rotación deja fijo a cada vértice. Arriba ya estudiamos la rotación R_2 pero resumamos lo que conocemos en una tabla.

Vértice(posición original)	Rotación	Vértice(posición al rotar)
A	R_2	B
B		D
C		A
D		C

Es el turno de estudiar la acción de R_3.

Vértice(posición original)	Rotación	Vértice(posición al rotar)
A	R_3	D
B		C
C		B
D		A

Sólo falta describir la acción de R_4 para completar el análisis de cada rotación.

Vértice(posición original)	Rotación	Vértice(posición al rotar)
A	R_4	C
B		A
C		D
D		B

Observe que cada rotación *puede ser vista como una permutación en el conjunto de cuatro elementos dados por los vértices del cuadrado.* Denotemos por *A* al conjunto formado por las cuatro rotaciones estudiadas arriba, esto es $A = \{ R_1, R_2, R_3 \text{ y } R_4\}$. Dotemos a *A* de una ley de composición interna bastante natural. Observe que si realizamos en el plano una rotación positiva de ángulo r respecto al origen de coordenadas y después realizamos una rotación positiva de ángulo r´ respecto al origen de coordenadas, estas se pueden combinar en una sola rotación de ángulo r+r´,

donde la suma la realizamos módulo 360. Por ejemplo, si combinamos una rotación antihoraria de ángulo 270 grados centrada en 0 con una de 180 grados igualmente antihoraria y centrada en 0, obtenemos una rotación de 450 grados, que módulo 360, equivale a una rotación de 90 grados. Note también que una rotación de 360 grados en el sentido antihorario y respecto al origen de coordenadas equivale a la rotación de ángulo 0 respecto al mismo origen de coordenadas 0. Luego, es natural dotar al conjunto A= { R_1, R_2, R_3 y R_4} de una ley de composición interna dada por la suma de los ángulos involucrada en cada rotación. Como el efecto de rotar primero un ángulo r y después rotar un ángulo r´ es equivalente a primero rotar un ángulo r' y luego rotar un ángulo un ángulo r, esta operación va a ser conmutativa. El estudiante que prefiere un argumento algebraico ante uno geométrico puede pensar que la suma módulo 360 es conmutativa (vaya a la unidad donde estudiamos $\mathbb{Z}_n$ para los detalles). La siguiente tabla nos indica como opera la ley de composición interna definida en el conjunto A= { R_1, R_2, R_3 y R_4}.

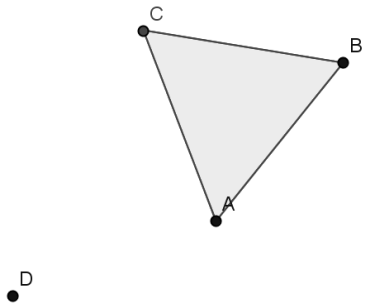
Suma de rotaciones	R_1	R_2	R_3	R_4
R_1	R_1	R_2	R_3	R_4
R_2	R_2	R_3	R_4	R_1
R_3	R_3	R_4	R_1	R_2
R_4	R_4	R_1	R_2	R_3

Observe que al sumarle R_1 a cualquier rotación R_i, i=1,2,3,4, obtenemos la misma rotación R_i. En otras palabras, R_1 es el elemento neutro para la ley de composición interna dada por la suma de rotaciones. Por otro lado, al fijarnos en la tabla vemos que cada elemento tiene un inverso respecto a la ley de composición interna definida. En efecto, la siguiente tabla muestra claramente la situación:

Rotación(ángulo)	Inverso(Angulo)	Suma (módulo 360)
R_1(0 grados)	R_1(0 grados)	0+0=0
R_2(90 grados)	R_4(270 grados)	90+270=0
R_3(180 grados)	R_3(180 grados)	180+180=0
R_4(270 grados)	R_1(90 grados)	270+90=0

Como la suma módulo 360 es asociativa entonces el conjunto A= { R_1, R_2, R_3 y R_4} con la operación suma de rotaciones es un *grupo.* Ya vimos que el grupo es conmutativo o abeliano. Tiene 4 elementos.

1. Tomemos un triángulo equilátero cualquiera.



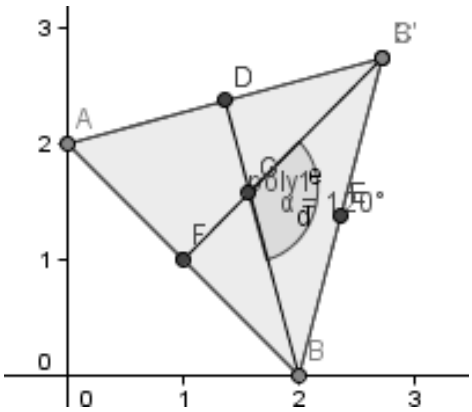
Sea 0 su centro. Le preguntamos

a) Determine las rotaciones centradas en 0 en sentido antihorario que llevan el triángulo en sí mismo. Sugerencia: Estas rotaciones deben llevar los vértices en los vértices.
b) Sean R_1, R_2 y R_3 las rotaciones halladas en a) ¿Cuál ley de composición interna le asociaría Ud. a las mismas?
c) Estudie si ha obtenido un grupo en la parte b) determinando el elemento neutro y la existencia de inverso.
d) ¿Es un grupo abeliano?

2. Complete la siguiente tabla del siguiente grupo conmutativo.

*	S	B	O	A
S	S			
B		S		O
O				
A			B	

1. a) Como el triangulo es equilátero las rotaciones de 120 grados y de 240 grados, llevan al triangulo en sí mismo.



En el dibujo se muestra cómo el vértice B se lleva al vértice B' mediante una rotación de 120 grados.

Es claro que la rotación de 0 grados lleva al triángulo en el miso ya que no modifica absolutamente nada.

b) La ley de composición entre las rotaciones de 0, 120 y 240 grados halladas en la parte a) es la suma de rotaciones. Invitamos al estudiante UNA a hacer la tabla de la ley considerada.

c) La rotación de 0 grados juega el papel del elemento neutro para la ley considerada. Es claro que la ley es asociativa y que el inverso de la rotación de 120 grados es la rotación de 240 grados, luego tenemos una estructura de grupo en este caso.

d) El grupo es abeliano como se puede ver en la tabla que invitamos al estudiante UNA realizar.

2. Este problema es interesante de realizar. Al tener que SS=S y al ser la tabla considerada la de un grupo, se deduce, por medio de la ley de cancelación, que S es elemento neutro del grupo. Esto permite completar sin dificultad la primera fila y la primera columna de la tabla dada. Observe ahora con detenimiento la segunda fila de la tabla, en ella no puede haber ningún elemento repetido, luego BO=A. El mismo argumento nos lleva a garantizar,

usando la tercera columna que OO=S. Como A debe tener un inverso para la operación indicada y este inverso no es ni S, B u O entonces el inverso de A es el mismo A, AA=S. El resto de la tabla se completa sin dificultad usando el mismo tipo de argumento. El estudiante UNA debe obtener

$*$	S	B	O	A
S	S	B	O	A
B	B	S	A	O
O	O	A	S	B
A	A	O	B	S

Es muy importante que en un grupo *G*, con ley de composición interna *, **siempre podemos resolver de manera única la ecuación**

$$a * x = b,$$

donde *x* es la incógnita y *a,b* son elementos dados de *G*. Para ver esto, procedemos como en bachillerato "despejando" la *x*. Multiplicamos a ambos lados y a la izquierda por el inverso de *a*, $\psi(x) = \psi(y) \Rightarrow x = y$. De donde, $x = a^{-1} * b$ ya que $a^{-1} * a = e$.

Definición. *El orden de un grupo G es el número de elementos o cardinal del conjunto G.*

Si *G* tiene infinitos elementos diremos que el orden de *G* es infinito.

1. El grupo $\mathbb{Z}_n$ tiene orden *n*.
2. El grupo R_3 de rotaciones que dejan invariante un triángulo equilatero tiene orden 3.
3. $\mathbb{Z}$ con respecto a la adición usual de enteros es un grupo de orden infinito.

10.4. Subgrupos

Muchas veces encontramos dentro de un grupo G un subconjunto H que es con derecho propio un grupo *al restringir la ley de composición de G a H.* Vamos a aclarar esto con un ejemplo muy sencillo.

Consideremos el grupo de todos los enteros $\mathbb{Z}$ respecto a la adición usual. Los números pares 0, 2, -2,4,-4,… son un subconjunto de $\mathbb{Z}$. Los números pares están caracterizados por ser de la forma $2k$ con k entero arbitrario. Si sumamos dos números pares cualesquiera $2j$ y $2r$, j y r enteros, obtenemos un número par ya que

$$2j + 2r = 2(j+r)$$

y $2(j+r)$ es un número par. Es decir, si llamamos $2\mathbb{Z}$ al conjunto de todos los números pares, podemos dotar a $2\mathbb{Z}$ de una ley de composición interna por medio de restringir la suma usual de enteros a $2\mathbb{Z}$. Note que 0 está en $2\mathbb{Z}$ ya que 0 es un número par. Por otro lado, si tomo un número par cualquiera $2j$, j entero, entonces $-2j=2(-j)$ es el inverso de $2j$. Por último, la adición es asociativa ya que es asociativa en Z y debe ser asociativa en cualquier subconjunto de este conjunto. Luego $2\mathbb{Z}$ es un grupo. *Diremos que* $2\mathbb{Z}$ *es un subgrupo del grupo* $\mathbb{Z}$.

Definición. Sea G un grupo cualquiera y H un subconjunto de G tal que al restringir la ley de composición interna de G a H obtenemos que H es un grupo. Diremos entonces que H es un subgrupo de G.

Observe que para que un conjunto H sea un subgrupo del grupo G *el elemento neutro debe estar en H.*

1. Si *G* es un grupo cualquiera, entonces los conjuntos $\{e\}$ y el propio *G* son subgrupos de *G*. Son llamados *los subgrupos triviales*. Esto demuestra que el concepto de subgrupo es no vacuo, siempre existen subgrupos en un grupo dado.
2. Tomemos el conjunto de permurtaciones de tres elementos, es decir S_3. Este conjunto está formado por 6 permutaciones que son:

$$e=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}\quad \alpha=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}\quad \beta=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$$
$$\theta=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}\quad \nu=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\quad \sigma=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$$

Tomemos el conjunto *H* formado por la permutación α que fija el 1 y por la permutación *e*. Como $\alpha\circ\alpha=e$ entonces la composición de funciones define una ley de composición interna en $H=\{e,\ \alpha\}$. Por otro lado, *e* pertenece a *H* por definición de este conjunto y como $\alpha\circ\alpha=e$, cada elemento de *H* tiene un inverso. Por último, la operación de composición restringida a *H* es asociativa. Luego, *H* es un subgrupo de S_3. Esto lo denotaremos por $H\prec G$. Observe que el orden de *H* es 2 y que el orden de S_3 es 6 y que 2 divide a 6, esto no es un fenómeno aislado sino una propiedad básica del orden de un subgrupo de un grupo finito.

Consideremos el grupo $\mathbb{Z}_6$ con respecto a la adición. Sea *H el conjunto formado por las clases de* 0, 2 y 4. Como 2+2=4(mod 6), 4+4=2(mod 6) y 2+4=0 mod 6 entonces la ley de composición interna de $\mathbb{Z}_6$ se puede restringir a *H* definiendo un grupo.

Veamos su tabla:

+	$\overline{0}$	$\overline{2}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{2}$	$\overline{4}$
$\overline{2}$	$\overline{2}$	$\overline{4}$	$\overline{0}$
$\overline{4}$	$\overline{4}$	$\overline{0}$	$\overline{2}$

Vemos por inspección de la tabla que el $\overline{0}$ funciona como elemento neutro para la adición definida en *H*. Por otro lado el inverso de $\overline{2}$ es la clase $\overline{4}$, ya que $\overline{2} + \overline{4} = \overline{0}$. Recíprocamente, la misma igualdad anterior implica que el inverso de la clase $\overline{4}$ es la clase del $\overline{2}$. Esto demuestra que *H* es un subgrupo de $\mathbb{Z}_6$.

El siguiente resultado es básico en la teoría de grupos.

Teorema 6. Si *G* es un grupo cualquiera y *H, K* subgrupos de *G* entonces $K \cap H$ es un subgrupo de *G*.

Demostración. Al ser *H,K* subgrupos de *G* tenemos que $e \in H, e \in K$ y por consiguiente $e \in H \cap K$. Por otro lado, si $x \in H \cap K \Rightarrow x \in H$ y $x \in G$. Al ser *H* y *K* subgrupos se debe tener que $x^{-1} \in H$ y $x^{-1} \in K$ y por ende, $x^{-1} \in H \cap K$. Al ser la ley de composición interna en el grupo asociativa, debe serlo en cualquier subconjunto de *G*. Por ello, $K \cap H$ es un subgrupo de *G*.

La relación de inclusión entre subconjuntos es una relación de orden en el conjunto de todos los subgrupos de *G*. Dejamos al estudiante verificar esto (Ejercicio). Luego, tiene sentido decir que un subgrupo es más pequeño que otro.

 Listemos todos los subgrupos de $\mathbb{Z}_6$.

$$\{\overline{0}\} \prec \begin{matrix} \{\overline{0},\overline{2},\overline{4}\} \\ \{\overline{0},\overline{3}\} \end{matrix} \prec \{\overline{0},\overline{1},\overline{2},\overline{3},\overline{4},\overline{5}\}$$

Como puede ver el estudiante, si ordenamos estos subgrupos se obtiene una estructura *reticular* cuando tomamos los subgrupos de un grupo dado. El orden viene dado por la relación de inclusión. Esto implica que no necesariamente un subgrupo puede ser comparado con otro en el orden definido.

Teorema 7. (Condición necesaria y suficiente para ser un subgrupo)

Sea *G* un grupo y *H* un subconjunto no vació de *G*. Entonces *H* es un subgrupo sí y sólo sí para cualquier *x*,*y* en *H* entonces $xy^{-1} \in H$.

Demostración.

Ejercicio.

Demuestre el teorema anterior siguiendo los pasos que siguen:

a) Demuestre que *e* está en *H*.
b) Demuestre que x^{-1} está en *H* si *x* está en *H*.
c) Demuestre que si *x*,*y* están en *H* entonces *xy* está en *H*.
d) Explique por qué la ley de composición al restringirse a *H* necesariamente es asociativa.

Para la parte a) tome cualquier *x* que está en *H*, al tener que $xx^{-1} \in H \Rightarrow e \in H$. Luego, b) sigue de manera similar tomando ahora $ex^{-1} \in H \Rightarrow x^{-1} \in H$. Dejamos al estudiante UNA completar c) y d) que son muy similares a las anteriores.

Teorema 8. (Subgrupo generado por *T*)

Si *G* es un grupo cualquiera y *T* un subconjunto cualquiera de *G*. Entonces existe un subgrupo *H* de *G* que contiene a *T* y es el más pequeño subgrupo de *G* con esta propiedad.

Demostración. Tomemos el conjunto Ω de todos los subgrupos de *G* que contienen a *T*. Observe que Ω es no vacío ya que $G \in \Omega$. El estudiante UNA debe decir por qué. Sea ahora

$$H = \bigcap_{H_\alpha \in \Omega} H_\alpha$$

Es decir, intersecamos todos los subgrupos que están en Ω. Por el teorema anterior *H* es un subgrupo. Como *T* está incluido en cada H_α perteneciente a Ω, entonces *T* está incluido en *H.* Por último, $H \subset H_\alpha$ para cualquier H_α perteneciente a Ω, y debe ser entonces el subgrupo más pequeño con la propiedad deseada.

La existencia del subgrupo generado por *T*

La demostración del teorema anterior es típica e importante en matemáticas. El estudiante debe repasarla con cuidado. La misma se repite de manera completamente análoga en estructuras como anillos, cuerpos, espacios vectoriales y espacios topológicos entre otras estructuras.

1. Consideremos el grupo $\mathbb{Z}_n$ respecto a la adición. ¿Cuál es el subgrupo generado por el conjunto $T = \{\overline{1}\}$? Al contener a la clase del 1 y ser cerrado respecto a la adición, debe contener a la clase del 2, a la del 3, y así sucesivamente. Luego *H* coincide en este caso con *G.*

2. **(Subgrupo cíclico)**

Este ejemplo es muy importante. Sea *G* un grupo finito y *x* un elemento cualquiera. Denotaremos la ley de composición interna del grupo multiplicativamente, esto es, si *x,y* están en *G* entonces *xy* denota el elemento que se obtiene al aplicar al par (*x,y*) la ley de composición interna. Para simplificar la notación, escribiremos $xx=x^2$, $xxx=x^3$, y así sucesivamente.

¿Cuál es el subgrupo *H* que genera el conjunto {*x*}?. Si *x* es el elemento neutro *e* entonces el subgrupo generado por *x* es precisamente el subgrupo trivial {*e*}. Así, podemos suponer sin pérdida de generalidad que $x \neq e$. Con seguridad todas las

potencias x^n , con n natural, están en H. Al ser G finito, el conjunto $\{y = x^n \text{ con } n \text{ natural}\} \subset G$ es también finito. Aún más, la ley de composición interna de G se puede restringir al conjunto $\{y = x^n \text{ con } n \text{ natural}\} \subset G$. Esto se debe a que $x^t x^s = x^{t+s} \in \{y = x^n \text{ con } n \text{ natural}\} \subset G$. Luego, las potencias de x, no pueden ser todas distintas, algunas de ellas deben coincidir por ser G finito. Esto implica, que existen naturales j y r, $j<r$, y

$$x^j = x^r$$

Pero,

$$x^j = x^r = x^j x^{r-j}$$

Luego, $x^{r-j} = x^k = e, k > 0$. De donde, $e \in \{y = x^n \text{ con } n \text{ natural}\} \subset G$. Por el principio de inducción, debe haber un natural k mínimo donde por primera vez ocurre que $x^k = e$. Esto implica, como veremos abajo, que

$$H = \{y = x^n \text{ con } n = 1, 2, \cdots, k\}$$

Observemos que:

1. La ley de composición interna se puede restringir a H.
2. $e \in H$.
3. La ley de composición interna es asociativa en H ya que es asociativa en G.
4. Todo elemento de H tiene un inverso.

Solo nos falta verificar la afirmación 4. Esto es muy sencillo ya que $x^k = e \Rightarrow x^j x^{k-j} = e$ para cualquier j natural entre 1 y k-1. Esto implica que todo elemento de H tiene un inverso y *que H es un subgrupo*. Como cualquier subgrupo que contenga a x debe contener a H entonces H es el subgrupo generado por x. Este subgrupo se denomina grupo cíclico generado por x.

Definición. Un grupo G se denomina cíclico si existe un $x \in G$ tal que $G = \{ y = x^n \text{ con } n \in \mathbb{Z} \}$.

En el caso que el grupo cíclico sea finito, por el ejemplo anterior, sabemos que sólo necesitamos una cantidad finita de potencias positivas. Esto es, $G = \{ e, x, x^2, \cdots, x^{k-1} \}$.

1. El conjunto de rotaciones que dejan invariante un triángulo equilátero forman un grupo cíclico de orden 3 (rotaciones de 0, 120, 240). Está generado, en este caso, por la rotación de 120 grados.
2. El grupo $\mathbb{Z}_n$ es cíclico y tiene como generador a la clase $\overline{1}$. Observe que el generador de un grupo no es único, si k es un número natural coprimo con n entonces $\overline{k}$ genera $\mathbb{Z}_n$. Veamos esto en detalle. Recordamos que al sumar $\overline{k}$ sucesivamente $\overline{k}$, $\overline{k} + \overline{k}$, $\cdots$en algún momento llegamos a la clase del 0. Afirmamos que la primera vez que ocurre es precisamente al sumar n veces $\overline{k}$. De lo contrario, existiría un $j<n$ tal que $\overline{jk} = \overline{0}$, pero esto implica que n divide a jk. A su vez, de aquí se sigue que n divide a j ya que n y k son primos entre si. Luego, la clase $\overline{k}$ también genera al grupo aditivo $\mathbb{Z}_n$. Para ilustrar esto, tomemos $\mathbb{Z}$. Vemos que 5 y 6 son primos entre sí. Entonces

$$\overline{5} + \overline{5} = \overline{4}$$
$$\overline{4} + \overline{5} = \overline{3}$$
$$\overline{3} + \overline{5} = \overline{2}$$
$$\overline{2} + \overline{5} = \overline{1}$$
$$\overline{1} + \overline{5} = \overline{0}$$

3. El conjunto $\mathbb{Z}$ con la adición usual es un grupo cíclico infinito, está generado por el 1.

El siguiente teorema es muy importante, es debido al genio de Lagrange.

Teorema 9. (Lagrange) Sea *G* un grupo finito de orden *n*. El orden de cualquier subgrupo *H* de *G* debe dividir a *n.*

Demostración. Sea *H* un subgrupo de *G* y consideremos la relación de equivalencia en *G* definida por medio de $xRy \Leftrightarrow x = yz$ donde $z \in H$. Verifiquemos que esto es, de hecho, una relación de equivalencia. Como sabemos por el estudio de la Unidad 2, debemos verificar que *R* es reflexiva, simétrica y transitiva. En primer lugar, vemos que *R* es reflexiva ya que $x = xe, e \in H$. Así, *xRx* y *R* es reflexiva. Supongamos ahora *xRy* esto significa que $x = yz$ para algún $z \in H$. Luego,

$$x = yz \Rightarrow xz^{-1} = yzz^{-1} \Rightarrow xz^{-1} = ye = y$$

Como $z^{-1} \in H$ entonces *yRx.* Sólo resta demostrar que *R* es transitiva. Supongamos que *xRy* y que *yRz.* Luego, $x = yz, z \in H$ y $y = wz'$ y $z' \in H$. De donde $x = yz = wz'z, z'z \in H \Rightarrow xRz$ y la relación *R* es transitiva. Luego, *R* es una relación de equivalencia. Una corta reflexión demuestra que las clases de equivalencia son conjuntos de la forma $xH = \{y \text{ tales que } y = xz, z \in H\}$ y que todos estos conjuntos tienen el mismo cardinal que *H*. Sean C_i, con *i* desde 1 hasta *r,* todas las clases de equivalencia. Como ellos forman una partición de *G* (ver la Unidad 2), entonces

$$|G| = \sum_{i=1}^{r} |C_i| = r|H|$$

De donde el orden de *H* debe dividir al de *G.*

Este ejemplo es una bonita aplicación del teorema anterior. Demostraremos que cualquier grupo finito *M* de orden primo *p* es cíclico. En efecto, tomemos un *x distinto del elemento neutro e*. Este elemento genera un subgrupo cíclico *H* de orden *k*>1. Por el teorema de Lagrange, *k* debe dividir a *p*. Pero *p* es primo, luego *p*=*k.* De donde *H*=*M* y *M* es cíclico.

1. Demuestre que un grupo *G* que verifica la condición $x^2 = e$ para cualquier *x* en *G* es conmutativo. Aquí como es usual *e* es el elemento neutro de *G*.
2. Demuestra que todo grupo de orden 4 es conmutativo.
3. Demuestre que si *G* es un grupo conmutativo entonces $(ab)^n = a^n b^n$ para cualesquiera elementos *a, b* y *n* natural. Sugerencia: Use inducción matemática.
4. Sea *G* un grupo no necesariamente conmutativo. Definimos el centro de *G* como $Z(G) = \{x \in G \text{ tales que } xy = yx \text{ para todo } y \in G\}$. Demuestre en detalle que *Z*(*G*) es un subgrupo de *G*.
5. Sea *G* un grupo cíclico finito, ¿es cierto que cualquier subgrupo de *G* es cíclico?
6. Encuentre una permutación σ en S_4 el conjunto de todas las permutaciones de 4 elementos que genere un subgrupo de orden 2.
7. Demuestre que todos los grupos de orden menor o igual que 5 son conmutativos. Liste los mismos.
8. Estudie si es cierto el siguiente enunciado: Si en un grupo *W* se tiene que $(ab)^2 = a^2 b^2$, para elementos cualesquiera *a, b* en *W*, entonces *W* es abeliano.

1. Supongamos que $x^2 = e$ para cualquier *x* en *G*, entonces si *x,y* son elementos arbitrarios de *G* tenemos

$$
\begin{aligned}
&(xy)^2 = e \Rightarrow \\
&(xy)(xy) = e \Rightarrow \\
&x(yx)y = e \Rightarrow \\
&xx(yx)y = xe \Rightarrow \\
&(yx)yy = xy \Rightarrow \\
&yx = xy
\end{aligned}
$$

2. Si el grupo es de orden 4 y cíclico no hay nada que demostrar ya que cualquier grupo cíclico es conmutativo. Luego podemos suponer, sin pérdida de generalidad, que G es de orden 4 y no cíclico. Sean e,x,y,z los elementos de G. Sabemos que x no genera el grupo G, luego se debe tener que $x^2 = e$. De igual forma tenemos que $y^2 = e$. Luego, xy no puede ser e porque aplicando la ley de cancelación llegamos a $x=y$. Luego, $xy=z$ pero de manera similar vemos que $yx=z$. Con esta información el estudiante UNA puede completar la tabla del grupo y verificar que es conmutativo, de hecho se trata del grupo $\mathbb{Z}_2 \times \mathbb{Z}_2$.
3. Use inducción matemática como fue indicado. Observe que $(ab)^{n+1} = (ab)^n (ab)$ y aplique la hipótesis inductiva a esta igualdad, usando posteriormente que el grupo es conmutativo. Complete los detalles que lo van a llevar a la solución del problema.
4. Es claro que $Z(G)$ contiene el elemento neutro e de G ya que $ex=xe$ para cualquier x de G. Supongamos ahora que $x \in G$ como

$$x^{-1}y = x^{-1}\left(y^{-1}\right)^{-1} \Rightarrow$$
$$x^{-1}y = \left(y^{-1}x\right)^{-1} = \left(xy^{-1}\right)^{-1} = yx^{-1}$$

   Concluimos que $x^{-1} \in G$. De manera similar verificamos que si $x,y \in G$ entonces $xy \in G$. Luego el centro es siempre un subgrupo.
5. Sea G un grupo cíclico finito de orden n y x un generador de G. Sea H un subgrupo de G que claramente debe ser finito y que podemos suponer no trivial, esto es, H es distinto de $\{e\}$ y de G. Sea x^j la menor potencia de x en H, $0<j<n$. Queremos ver que H está compuesto por $e,x^j,x^{2j}, \cdots x^{jk}, \cdots$. Es decir, x^j genera a H. Sea y cualquier elemento de H entonces $y=x^m$ para algún m natural. Luego, por el algoritmo de Euclides, $m=cj+r$ donde $r<j$. Luego, $x^m = x^{jc}x^r$ pero esto implica que x^r *pertenece a* H y como x^j era la menor potencia no nula de x en H entonces $r=0$ y esto implica que y es una potencia de x^j y luego H es cíclico.
   a. Se deja al estudiante UNA.
   b. Los grupos cíclicos son siempre conmutativos, luego los grupos de orden primo son siempre conmutativos ya que un grupo de orden primo debe ser

cíclico (ver ejemplo en el texto). Luego, los grupos de orden 2,3 y 5 son conmutativos. Los grupos de orden 4 ya han sido estudiados en un problema anterior y por último el grupo trivial de 1 elemento es claramente conmutativo.

c. Como $(ab)^2 = a^2b^2 \Rightarrow (ab)(ab) = a^2b^2$. Ahora, la propiedad asociativa sirve para agrupar los elementos de distintas maneras cuando entran en un producto. Luego, aplicando la propiedad asociativa $(ab)(ab) = a^2b^2 \Rightarrow a(ba)b = aabb$ y solamente resta multiplicar a la izquierda de la igualdad por a^{-1} y a la derecha por b^{-1} para obtener la igualdad $ba = ab$ que indica que el grupo es conmutativo.

UNIDAD 7

La teoría de Grupos

 **Semana 12**

 *Aplicar el concepto de grupo en la resolución de problemas, en el modelado matemático y en la demostración de nuevos resultados.*

Temas a tratar: Homomorfismos. Isomorfismos. El teorema fundamental de isomorfismo. Uso de software matemático FGB. *Modelando con Grupos*

11.1 ¿Cómo aparecen los subgrupos?: El concepto de homomorfismo

En muchas situaciones nos encontramos con grupos que tienen un comportamiento similar pero difieren en la naturaleza de sus elementos. Por ejemplo, el grupo de 4 elementos formado por las rotaciones que dejan invariante un cuadrado es muy similar al grupo $\mathbb{Z}_4$. Es importante desarrollar un concepto matemático que capture esta semejanza. Las nociones de homomorfismo e isomorfismo son las adecuadas para lograr este objetivo.

Supongamos que *G* y *K* son grupos cualesquiera con leyes de composición $*, \circ$ respectivamente.

Definición. Una función $\psi : G \to K$ con dominio igual a G se denomina homomorfismos de grupo sí y sólo sí $\psi(x * y) = \psi(x) \circ \psi(y)$ para cualquier par de elementos *x,y* de *G*.

Muchas veces decimos que $\psi : G \to K$ respeta las leyes de composición de las estructuras *G* y *K*

1. Consideremos los grupos $\mathbb{Z}$ y $\mathbb{Z}_n$ con la adición como ley de composición interna en cada uno. Sea

$$\phi : \mathbb{Z} \to \mathbb{Z}_n$$
$$\phi(a) = \overline{a}$$

Como $\phi(a+b) = \overline{a+b} = \overline{a} + \overline{b} = \phi(a) + \phi(b)$ entonces ϕ es un homomorfismo. Es llamado el homomorfismo canónico o la proyección canónica.

2. Consideremos el grupo de todos los enteros $\mathbb{Z}$ y el conjunto $2\mathbb{Z}$ de todos los números pares. Sabemos que $2\mathbb{Z}$ es un grupo respecto a la adición. Tomemos la función

$$\phi : \mathbb{Z} \to 2\mathbb{Z}$$
$$\phi(n) = 2n$$

Vemos que $\phi(x+y) = 2(x+y) = 2x + 2y = \phi(x) + \phi(y)$, luego ϕ es un homomorfismo.

3. Sea G un grupo y consideremos la función $\psi_a : G \to T$ donde fijamos $a \in G$ y $\psi_a(z) = a^{-1}za$ es un homomorfismo. El estudiante UNA debe verificar por qué.
4. Consideremos los números reales positivos $\mathbb{R}^*_+ = \{x \in \mathbb{R}, x > 0\}$, ya vimos anteriormente que $\mathbb{R}^*_+ = \{x \in \mathbb{R}, x > 0\}$ es un grupo respecto a la multiplicación usual. Sea el grupo $\mathbb{R}$ con la suma usual de números reales. Definimos

$$\phi : \mathbb{R} \to \mathbb{R}^*_+$$
$$\phi(x) = e^x$$

Como

$$\phi(x+y) = e^{x+y} = e^x e^y = \phi(x)\phi(y)$$

Entonces ϕ es un homomorfismo. Observe que $\phi(0) = e^0 = 1$, es decir el homomorfismo lleva el elemento neutro 0 de la suma en el elemento neutro 1 de la

multiplicación de números reales, esto es una situación general como demuestra el siguiente resultado.

Teorema 1. Sea $\phi: G \to T$ un homomorfismo del grupo *G* en el grupo *T.* Entonces $\phi(e) = e'$ donde *e, e'* son los elementos neutros de *G* y *T* respectivamente.

Demostración. Vemos que $\phi(x) = \phi(xe) = \phi(x)\phi(e) \Rightarrow \phi(e) = e'$ lo que queríamos demostrar. □

Definición. *Sea* $\phi: G \to T$ *un homomorfismo del grupo G en el grupo T. Denotemos por e el elemento neutro de T. El conjunto* $\{x \in G \text{ tal que } \phi(x) = e\}$ *se denomina el núcleo de* ϕ. *El núcleo de* ϕ *será denotado por Ker* ϕ.[3]


Consideremos la proyección canónica

$$\gamma: \mathbb{Z} \to \mathbb{Z}_4$$
$$\gamma(z) = \overline{z}$$

Determinemos su núcleo. Debemos encontrar todos los *z* tales que $\gamma(z) = \overline{z} = \overline{0}$. Esta igualdad implica que *z*=4*k* donde *k* es entero arbitrario. Luego, $Ker\,\gamma = \{0, \pm 4, \pm 8, \cdots\}$. Observe que $Ker\,\gamma = \{0, \pm 4, \pm 8, \cdots\}$ es un subgrupo de $\mathbb{Z}$. Esto es completamente general como indica nuestro resultado siguiente.

Teorema 2. Consideremos el homomorfismo de grupos $\psi: G \to K$, esto es $\psi(x * y) = \psi(x) \circ \psi(y)$ para cualquier par de elementos *x,y* de *G.* Entonces el *Ker* ψ es un subgrupo de *G.*

Demostración. Veamos que si denotamos por *e'* al elemento neutro de *G* entonces *e'* está en *Ker* ψ. Como $\psi(x) = \psi(e' * x) = \psi(e') \circ \psi(x) \Rightarrow \psi(e') = e$. Veamos ahora que podemos restringir la ley de composición interna * al *Ker* ψ. Sean *x, y* en *Ker* ψ, deseamos demostrar que $x * y$ está en *Ker* ψ. Como

[3] Del alemán kernel que significa núcleo. Por el teorema anterior el nucleo es no vacío.

$\psi(x*y)=\psi(x)\circ\psi(x)=e\circ e=e$. Luego, $x*y$ está en *Ker* ψ. Luego basta ver que si *x* está en *Ker* ψ entonces x^{-1} está en *Ker* ψ. Pero, $e=\psi(x*x^{-1})=\psi(x)\circ\psi(x^{-1})=e\circ\psi(x^{-1})=\psi(x^{-1})$, luego $e=\psi(x^{-1})$. Hemos demostrado que *Ker* ψ es un subgrupo. □

Para evitar una notación engorrosa voy a denotar de igual forma las leyes de composición en los grupos que vamos a considerar de ahora en adelante, si *x, y* están en un grupo entonces *xy* es su producto.

Un resultado muy importante y que se repite en distintas estructuras es el siguiente.

Teorema 3. Consideremos el homomorfismo de grupos $\psi:G\to K$ entonces ψ es inyectivo sí y sólo sí *Ker* ψ es el subgrupo trivial {*e'*}.

Demostración. Si ψ es inyectivo claramente *Ker* ψ es el subgrupo trivial {*e'*} ya que $\psi(e')=e$ y *e'* es el único elemento que puede tener esa propiedad ya que ψ es inyectiva. Supongamos ahora que *Ker* ψ es el subgrupo trivial {*e'*}. Para verificar si una función es inyectiva tenemos que ver si $\psi(x)=\psi(y)\Rightarrow x=y$. $\psi(x)=\psi(y)\Rightarrow\psi(x)(\psi(y))^{-1}=e$. Pero, $(\psi(y))^{-1}=\psi(y^{-1})$ (Ejercicio), de donde

$$\psi(x)(\psi(y))^{-1}=\psi(x)\psi(y^{-1})=e\Rightarrow$$
$$\psi(xy^{-1})=e\Rightarrow xy^{-1}\in \mathrm{Ker}\,\psi$$

Pero *Ker* ψ es el subgrupo trivial {*e'*}, luego $xy^{-1}=e'\Rightarrow xy^{-1}y=e'y=y\Rightarrow xe'=y\Rightarrow x=y$ y la aplicación es inyectiva.

Un resultado muy bonito es que los homomorfismos transforman subgrupos en subgrupos. Veamos esto con precisión.

Teorema 4. Consideremos el homomorfismo de grupos $\psi:G\to K$, esto es $\psi(xy)=\psi(x)\psi(y)$ para cualquier par de elementos *x, y* de *G*. Entonces el $\psi(T)$ es un subgrupo de *K* para cualquier subgrupo *T* de *G*.

Demostración. Basta ver por un teorema anterior que si $z, w \in \psi(T)$ entonces $zw^{-1} \in \psi(T)$. Pero, si $z, w \in \psi(T)$ entonces $z = \psi(a), w \in \psi(b)$ con *a,b* miembros de *T.* Luego, $zw^{-1} = \psi(a)\psi(b^{-1}) = \psi(ab^{-1}) \in \psi(T)$ ya que ab^{-1} está en *T.* □

11. 2. El concepto de isomorfismo entre grupos

En el lenguaje matemático, el término isomorfo significa que dos objetos o entes matemáticos tienen la misma estructura, solamente difiriendo, quizás, en la naturaleza de sus elementos. Esta idea se pone de manifiesto en la siguiente definición.

Definición. *Sean G y H dos grupos cualesquiera. Decimos que G y H son isomorfos si existe un homomorfismo biyectivo* $\phi : G \to H$.

Recordamos que para que un homomorfismo $\phi : G \to H$ sea biyectivo debe ser inyectivo y sobreyectivo. Un teorema anterior nos indica que $\phi : G \to H$ es inyectivo sí y sólo sí su núcleo es trivial e igual a $\{e\}$. Por otro lado, sabemos que $\phi(G)$ es un subgrupo de H y para que $\phi : G \to H$ sea sobreyectivo se debe tener $\phi(G) = H$. *Un homomorfismo biyectivo se llama isomorfismo.*

Dos grupos isomorfos *G* y *H* **deben tener la misma cantidad elementos** ya que $\phi : G \to H$ es una biyección. Sin embargo, *hay grupos que tienen la misma cantidad de elementos pero no son isomorfos.* Veremos ejemplos de esto.

1. Consideremos los números reales positivos $\mathbb{R}^*_+ = \{x \in \mathbb{R}, x > 0\}$, ya vimos anteriormente que $\mathbb{R}^*_+ = \{x \in \mathbb{R}, x > 0\}$ es un grupo respecto a la multiplicación usual. Sea el grupo $\mathbb{R}$ con la suma usual de números reales. Definimos

$$\phi : \mathbb{R} \to \mathbb{R}^*_+$$
$$\phi(x) = e^x$$

Como

$$\phi(x+y) = e^{x+y} = e^x e^y = \phi(x)\phi(y)$$

Entonces ϕ es un isomorfismo. Veamos por qué. Primero, $\phi(x) = e^x$ es inyectiva ya que $\phi(x) = e^x = 1 \Rightarrow x = 0$. Además, si y>0 la ecuación $e^x = y$ siempre tiene solución, la cual es $x = \ln y$. De donde ϕ es un isomorfismo. Esta es la gran idea de Napier para introducir los logaritmos, Napier se dio cuenta que la multiplicación podía ser sustituida por la suma, la cual es una operación más sencilla.

2. Consideremos el grupo de todos los enteros $\mathbb{Z}$ y el conjunto $2\mathbb{Z}$ de todos los números pares. Sabemos que $2\mathbb{Z}$ es un grupo respecto a la adición. Tomemos la función

$$\phi : \mathbb{Z} \to 2\mathbb{Z}$$
$$\phi(n) = 2n$$

Vemos que ϕ es un isomorfismo. El estudiante UNA debe verificar todos los detalles.

1. Demuestre que un grupo *G* finito no puede ser isomorfo a un grupo *G* infinito.
2. Demuestre que cualquier grupo *G* es isomorfo a si mismo.
3. Sean *G* y *H* dos grupos isomorfos. Demuestre que si *G* es conmutativo entonces *H* es también conmutativo.
4. Sean *G* y *H* dos grupos finitos isomorfos. Demuestre que $|G| = |H|$.
5. Demuestre que si *G* es un grupo cualquiera y *a* es un elemento fijo de *G* entonces $\theta(x) = a^{-1}xa$ es un isomorfismo.
6. Demuestre que si $\phi : G \to H$ es un isomorfismo entre el grupo *G* y el grupo *H* entonces $\phi^{-1} : H \to G$ es un isomorfismo del grupo *H* en el grupo *G*.

1. Cualquier isomorfismo debe ser en primer lugar una función biyectiva, luego si un conjunto es finito y el otro infinito ya sabemos que tal biyección no puede existir.
2. Considere la función $f:G\to G$ dada por $f(x)=x$ para cualquier *x* en *G*. El estudiante UNA debe verificar los detalles que muestran que f es un isomorfismo.
3. Sea f un isomorfismo entre *G* y *H*, $f:G\to H$. Tomemos *z,w* dos elementos cualesquiera de *H*. Luego, al ser f biyectiva deben existir *x, y* únicos tales que $f(x)=z,\ f(y)=w$. Se tiene

$$zw=f(x)f(y)=f(xy)=f(yx)=f(y)f(x)=wz$$

De donde la ley de composición interna en *H* es conmutativa. El estudiante UNA debe estudiar y justificar cada una de las igualdades anteriores en caso de que no haya resuelto el problema.

4. Si dos grupos son isomorfos, al ser cualquier isomorfismo una biyección, deben ser equipotentes. Vea la Unidad de Conjuntos para cualquier duda al respecto.
5. Veamos en primer lugar que $\theta(x)=a^{-1}xa$ es un homomorfismo, tenemos que

$$\theta(xy)=a^{-1}xya=a^{-1}xeya=\left(a^{-1}xa\right)\left(a^{-1}ya\right)=$$
$$\theta(x)\theta(y)$$

Esto demuestra que $\theta(x)=a^{-1}xa$ es un homomorfismo, falta ver que es una biyección. Calculemos el núcleo o kernel de $\theta(x)=a^{-1}xa$, si

$$\theta(x)=a^{-1}xa=e\Rightarrow a(a^{-1}xa)a^{-1}=aea^{-1}=e$$
$$\Rightarrow\left(aa^{-1}\right)x\left(aa^{-1}\right)=x=e$$

Luego, por nuestro **Teorema 3.** $\theta(x)=a^{-1}xa$ es inyectiva. Por último, se puede ver que la ecuación con incógnita x, $a^{-1}xa=y$ siempre puede ser resuelta para *y*

elemento arbitrario de *G*, esto demuestra que $\theta(x) = a^{-1}xa$ es sobreyectiva y por ende biyectiva.

6. El asunto aquí es escribir con cuidado las cosas pero es una verificación rutinaria que dejamos al estudiante UNA.

El siguiente teorema indica que cualquier grupo finito de orden n es isomorfo a un subgrupo del grupo de permutaciones de n elementos. Es un teorema muy importante en la teoría de grupos.

Teorema 5 (Cayley).

Sea *G* un grupo de *n* elementos. Entonces *G* es isomorfo a un subgrupo *H* de S_n.

Demostración. Primero verificamos que cualquier *x* en *G* determina una biyección de *G* en *G*, es decir una permutación de *n* elementos. La idea es muy sencilla, fijemos *x* en *G* y definamos $f_x : G \to G$ por medio de la regla. $f_x(y) = xy$. Es un ejercicio para el estudiante UNA verificar que cada $f_x : G \to G$ es biyectivo. Es decir, $f_x : G \to G$ es un elemento de S_n. Observe que la operación en S_n es la composición de funciones y $f_x \circ f_y = f_{xy}$ ya que $f_x \circ f_y(z) = f_x(yz) = (xy)z = f_{xy}(z)$. Así,

$\theta : G \to S_n$
$\theta(x) = f_x$
es un homomorfismo. Luego

$$H = \{ f_x : G \to G, x \text{ en } G\}$$

es un subgrupo de S_n por el Teorema 3 anterior. ¿Cuál es el núcleo de $\theta : G \to S_n$? Vemos que $f_x : G \to G$ es identidad sí y sólo sí *x*=*e*. De donde, $\theta : G \to S_n$ es un isomorfismo de *G* en $H = \{ f_x : G \to G, x \text{ en } G\}$. Como queríamos demostrar. □

11.3. El teorema Fundamental de Isomorfismo

Sea $\psi : G \to H$ un homomorfismo sobreyectivo pero no necesariamente inyectivo, es decir, el *Ker* ψ no es el grupo trivial. Vamos a definir una relación de equivalencia $\sim$ en *G* y dotaremos a las clases de equivalencia de una ley de composición interna. Sean *x*, *y* elementos de *G*, decimos que $x \sim y \Leftrightarrow \psi(x) = \psi(y)$. Es decir, *x* esta relacionado con *y* si tienen iguales imágenes. Esto es, sin duda, una relación de

equivalencia. Observe que $x \sim y \Leftrightarrow \psi(x) = \psi(y) \Leftrightarrow \psi(xy^{-1}) = e \Leftrightarrow xy^{-1} \in$ Ker ψ. Esta caracterización de la relación de equivalencia nos permite decir que las clases de equivalencia (en inglés cosets) son de la forma

$$a \, Ker \, \psi$$

donde a es un elemento cualquiera de G y $a\text{Ker}\,\psi = \{z = at \text{ con } t \in \text{Ker } \psi\}$. El conjunto cociente obtenido de G al tomar las clases de equivalencia lo denotaremos por $G/\text{Ker}\,\psi$. Queremos multiplicar las clases de equivalencia y lo haremos de una manera natural. Definimos el producto en las clases de equivalencia de la forma siguiente:

$$(a \, Ker \, \psi)(b \, Ker \, \psi) = ab \, Ker \, \psi$$

Si el estudiante UNA estudió cuidadosamente la construcción de los sistemas numéricos pedirá una explicación en este momento. ¿Cómo uno sabe que esa ley de composición interna está bien definida? Debemos ser cuidadosos y verificar que

$$ab \, Ker \, \psi = a'b' \, Ker \, \psi$$

si $a \sim a'$ y $b \sim b'$.

Lema 6. Si T es un subgrupo de G y x está en T entonces $xT=T$.

Demostración. Al ser T un subgrupo si x está en T entonces $xT = \{xt \text{ con } t \in T\}$ está contenido en T. Pero, si tomamos un elemento cualquiera t en T la ecuación, de incógnita y, dada por $xy=t$ admite solución en T. Luego T está contenido en xT y tenemos la igualdad de los dos conjuntos. □

Volvamos a nuestro problema que es demostrar $ab \, Ker \, \psi = a'b' \, Ker \, \psi$ si $a \sim a'$ y $b \sim b'$. Pero $a \sim a'$ y $b \sim b'$ implica que $(b')^{-1}(a')^{-1} ab \in$ Ker ψ y luego, aplicando el lema anterior, $(b')^{-1}(a')^{-1} abT = T \Rightarrow abT = a'b'T$. Esto indica que la ley de composición interna está bien definida en el conjunto cociente $G/\text{Ker}\,\psi$. Aún más, tenemos el importante resultado que sigue.

Teorema 7. $G/\mathrm{Ker}\,\psi$ es un grupo.

Demostración. Vemos que *Ker* ψ juega el papel de elemento neutro ya que *e Ker* ψ = *Ker* ψ y por ende (*e Ker* ψ) (*b Ker* ψ)=*eb Ker* ψ = *b Ker* ψ. Al ser la multiplicación en *G* asociativa, entonces la multiplicación que hemos definido en $G/\mathrm{Ker}\,\psi$ es de nuevo asociativa. Luego, como (b^{-1} *Ker* ψ) (*b Ker* ψ)=b^{-1} *b Ker* ψ =*e Ker* ψ .□

Por último, el resultado que habíamos anunciado.

Teorema 8. Si $\psi : G \to H$ es un homomorfismo sobreyectivo entonces *H* es isomorfo al grupo cociente $G/\mathrm{Ker}\,\psi$.

Demostración. Tenemos que construir un isomorfismo de $G/\mathrm{Ker}\,\psi$ en *H*. Basta tomar el homomorfismo $\bar{\psi} : G/\mathrm{Ker}\,\psi \to H$ donde $\bar{\psi}(x\mathrm{Ker}\,\psi) = \psi(x)$ el cual está bien definido ya que todos los elementos de la clase $x\mathrm{Ker}\,\psi$ tienen igual imagen por medio de ψ. Que $\bar{\psi} : G/\mathrm{Ker}\,\psi \to H$ es un homomorfismo se verifica de manera directa. Igualmente vemos que $\bar{\psi}$ es sobreyectivo ya que ψ lo es. Basta ver que $\bar{\psi} : G/\mathrm{Ker}\,\psi \to H$ es inyectivo para demostrar el resultado. Pero por la construcción de $\bar{\psi} : G/\mathrm{Ker}\,\psi \to H$ vemos que $\bar{\psi}(x\mathrm{Ker}\,\psi) = \psi(x) = e$ sí y sólo sí *x* esta en *Ker* ψ y luego *x Ker* ψ = *Ker* ψ . Lo que concluye la demostración. □

1. Consideremos el grupo $\mathbb{Z}$ con respecto a la adición usual y el grupo de los enteros múltiplos de 3, $3\mathbb{Z} = \{0, \pm 3, \pm 6, \cdots\}$. Definamos la aplicación, $\theta : \mathbb{Z} \to 3\mathbb{Z}$, $\theta(z) = 3z$ que es obviamente sobreyectiva. Aún más, $\theta : \mathbb{Z} \to 3\mathbb{Z}$ es un

homomorfismo. Su núcleo es trivial, luego el Teorema Fundamental del Isomorfismo dice que $\mathbb{Z}$ es isomorfo a $3\mathbb{Z} = \{0, \pm 3, \pm 6, \cdots\}$.

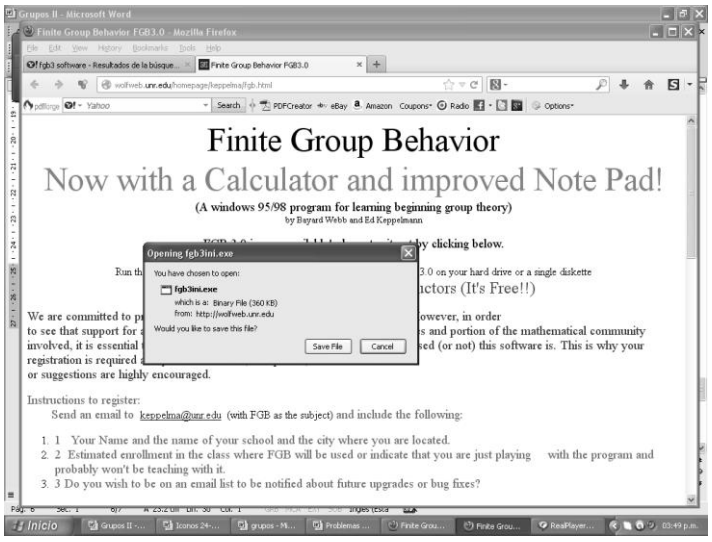
2. Tomemos de nuevo $\mathbb{Z}$ con la adición usual de enteros y consideremos los enteros módulo 5, $\mathbb{Z}_5$. Ya estudiamos el homomorfismo representado por la proyección canónica

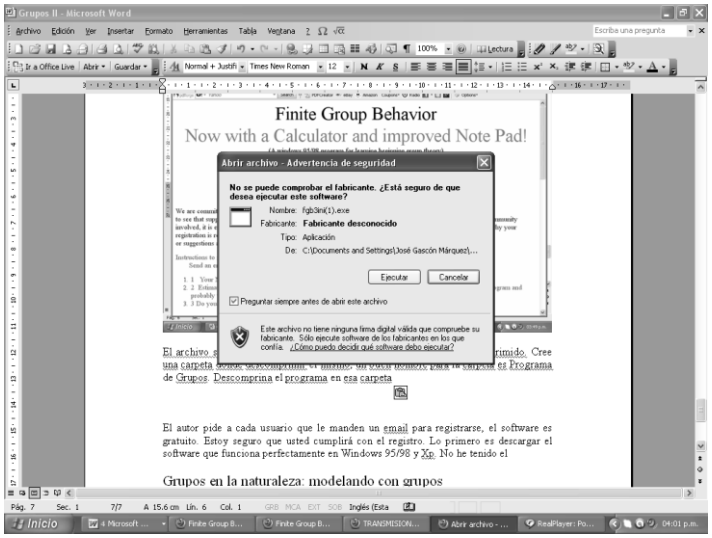
$$\pi : \mathbb{Z} \to \mathbb{Z}_5$$
$$\pi(z) = \overline{z}$$

Su núcleo es el subgrupo de $\mathbb{Z}$ dado por los múltiplos de 5, denotado por $5\mathbb{Z}$. Por el teorema anterior vemos que $\mathbb{Z}_5$ es isomorfo a $\mathbb{Z}_5 \approx \mathbb{Z}/5\mathbb{Z}$.

11.4. Estudiando los Grupos: el software FGB

Vamos a usar un paquete muy sencillo para explorar los grupos: FGB 3.0. FGB son las siglas de Finite Group Behavior, es decir comportamiento de grupos finitos. El mismo se puede descargar desde http://wolfweb.unr.edu/homepage/keppelma/fgb.html. Aquí también encuentran información general sobre el software FGB 3 y cómo registrarse. El software es gratuito pero el matemático que lo desarrolló pide que se registre. Al pulsar el enlace de descarga debe aparecer la pantalla que aparece abajo. Presionen la opción **Save File.** El archivo se descargará a su computador, el archivo que bajó está comprimido. Cree una carpeta donde descomprimir el mismo, un buen nombre para la carpeta es Programa de Grupos. Descomprima el programa en esa carpeta haciendo doble click en el archivo que descargó, haciendo luego click en la opción ejecutar.

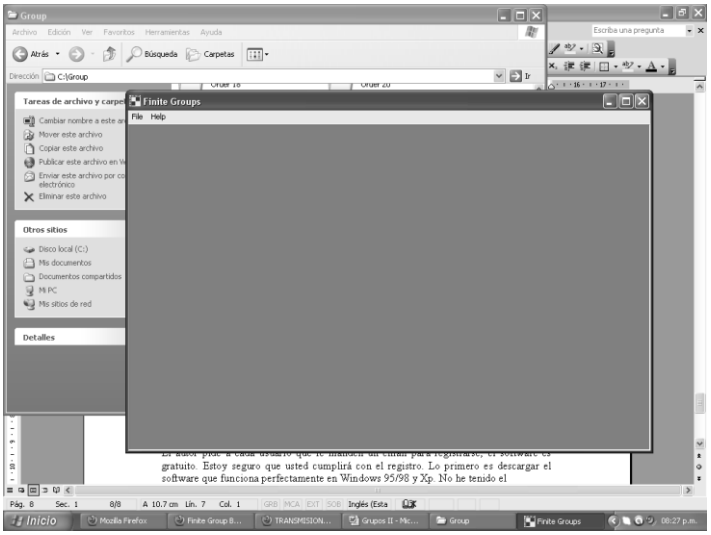




Aparecerá entonces el siguiente cuadro

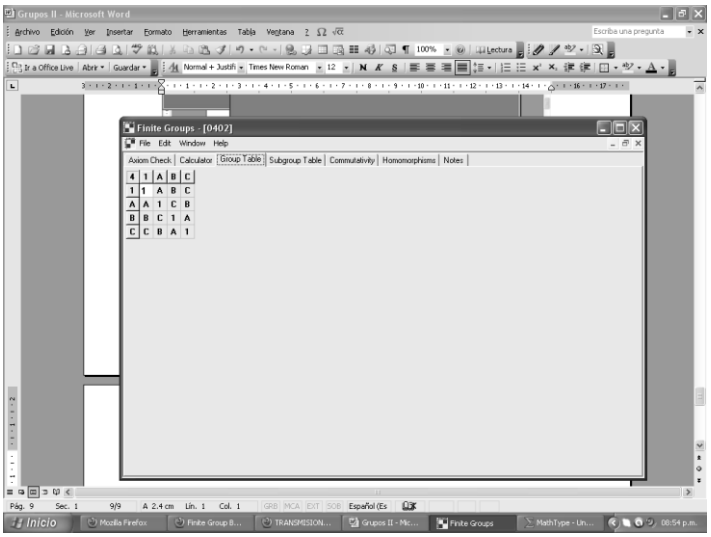
Coloque en la parte a rellenar la dirección de la carpeta donde quiere descomprimir el programa y ¡listo! Ya completó la instalación. En la carpeta donde instaló el programa debe tener el ícono

Haga doble click en el mismo para iniciar la ventana principal del programa.



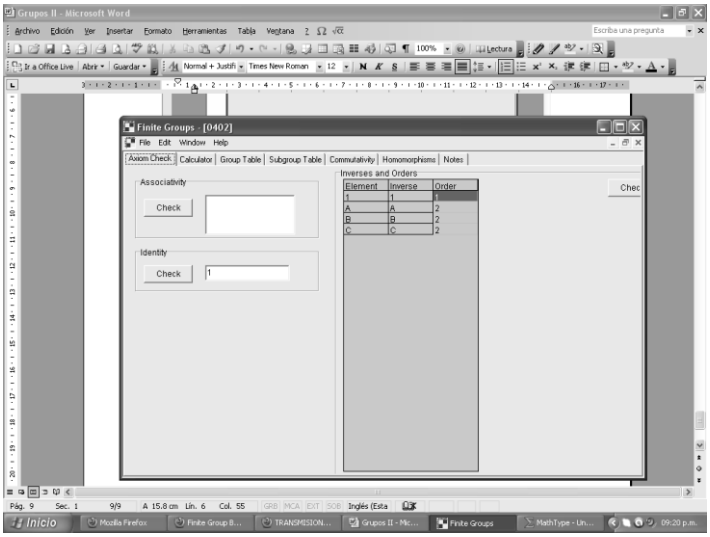
Ahora Ud. puede cargar un grupo finito de orden pequeño y empezar su estudio haciendo click en File y buscando, mediante la selección de Open en el menú contextual, un grupo en las carpetas que se abren.

Vamos a desarrollar un ejemplo abriendo el archivo 0402 de la carpeta Small Groups. El 04 significa que es un grupo de cuatro elementos. Solo hay dos grupos de cuatro elementos, uno es el grupo cíclico $\mathbb{Z}_4$ y el otro es $\mathbb{Z}_2 \times \mathbb{Z}_2$. Veamos la tabla del grupo:

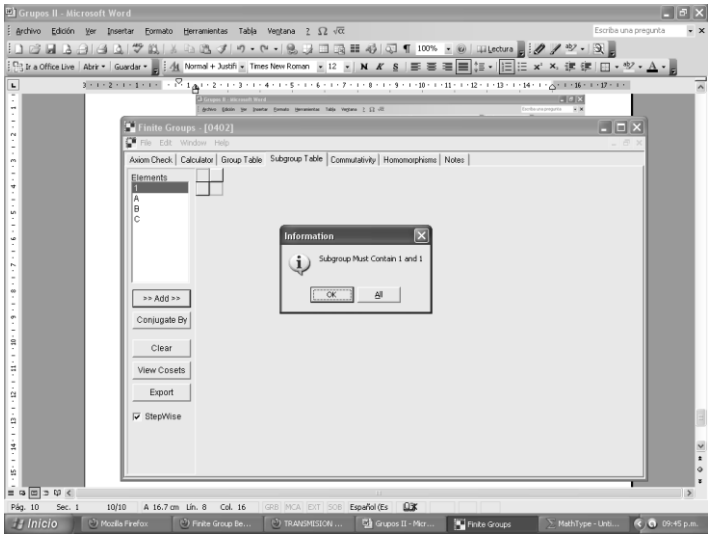


Por inspección de la tabla vemos que todos los elementos distintos al elemento neutro tienen orden 2. Luego el grupo no puede ser cíclico y es $\mathbb{Z}_2 \times \mathbb{Z}_2$. Vamos a ver algunas de las funcionalidades del programa.

1. *Verificación de los axiomas de grupo de la tabla presentada*. Haga click en la pestaña **Axiom Check**. Usted verá la siguiente pantalla de abajo. Usted puede chequear la asociatividad, existencia de elemento neutro y la existencia de un inverso para cada elemento. Explore cada posibilidad, por ejemplo si hacemos click en el botón Asociativity Check, comprobamos si la ley de composición dada es asociativa o no. Al hacer click aparecerá Yes.

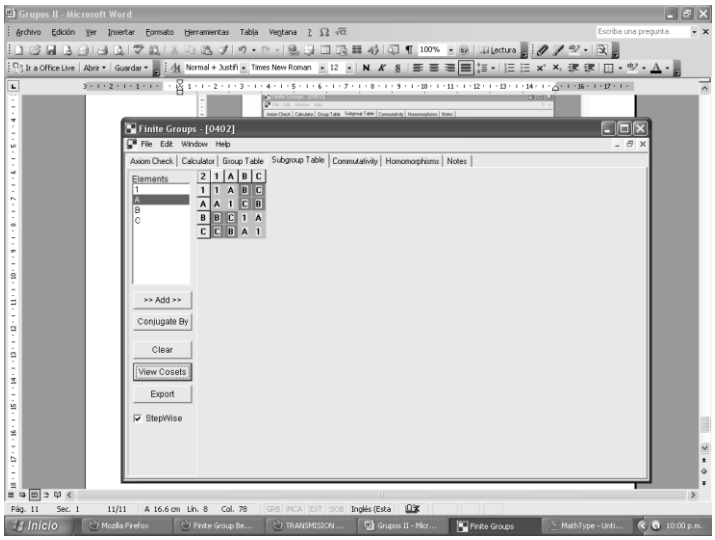


2. En la pestaña **Notes** vemos que el grupo es el grupo de Klein $\mathbb{Z}_2 \times \mathbb{Z}_2$.
3. En la pestaña Subgroups podemos construir un subgrupo generado por una familia de elementos del grupo que estamos estudiando. Haga click para explorar esta actividad del software. Añadimos el 1 ya que sabemos que cualquier grupo debe contener la identidad. Aparece el cuadro de información



La cual nos dice exactamente esto, el subgrupo debe contener el

1. Añadimos un elemento seleccionando el mismo y oprimiendo el botón de Add, en este ejemplo añadimos el elemento A. Vemos que al añadir A se obtiene un subgrupo de orden
2. Si Usted le da al botón de View Cosets aparecen las clases de equivalencia asociadas al subgrupo {1,A}, en este caso son solo dos clases que aparecen resaltadas.



Las clases aparecen resaltadas en gris claro y oscuro en la pantalla arriba.

3. En la pestaña de Conmutatividad tenemos la posibilidad de encontrar el centro de un elemento cualquiera. El centro de un elemento cualquiera x son todos los elementos que conmutan con x. Esto es un subgrupo que denotaremos por $C(x)$.
4. En la pestaña Calculator podemos multiplicar diversos elementos del grupo estudiado, ver su orden, su inverso entre otras cosas. El estudiante UNA va a continuar descubriendo las posibilidades a medida que use el programa.

1. Sea G un grupo cualquiera y $x \in G$. Demuestre que el centro de un elemento x es siempre un subgrupo de G.
2. Estudie cuidadosamente con el software FGB el grupo de permutaciones S_3 de 3 elementos. Siga el siguiente esquema: a) Abra el archivo 0602. b) Verifique

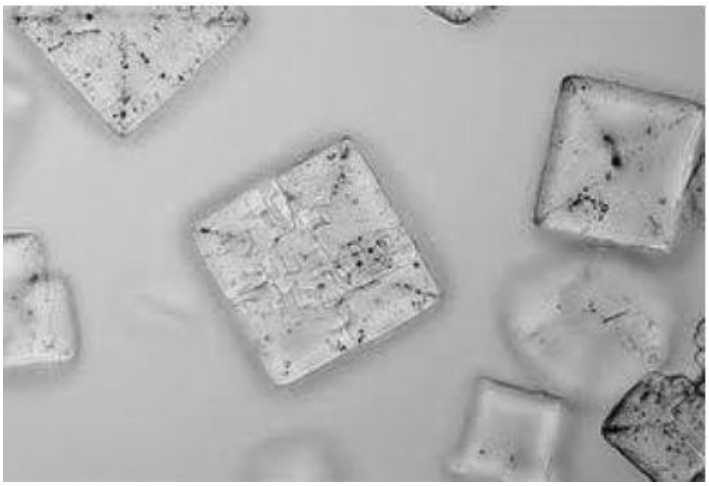
los axiomas de grupos. c) Busque todos los subgrupos de S_3. d) Halle las clases de equivalencias (cosets). e) Lea la información en notes.

3. Demuestre que el grupo S_3 coincide con el grupo de simetrías y rotaciones que llevan un triángulo equilátero en el mismo. Sugerencia: ¿Cuántas simetrías y rotaciones dejan invariante un triángulo equilátero?

1. Por definición, el centro de x son todos los elementos que conmutan con x. Este conjunto que denotaremos por $C(x)$ es no vacío ya que al menos el elemento neutro e del grupo está en él ya que $ex=xe=x$. Supongamos ahora que w,y pertenecen a $C(x)$, entonces $(wy)x = w(yx) = w(xy) = (wx)y = (xw)y = x(wy)$ de donde wy pertenece a $C(x)$. Si w pertenece a $C(x)$ entonces $ex = w^{-1}wx = w^{-1}xw \Rightarrow xw^{-1} = w^{-1}x$, luego w^{-1} pertenece a $C(x)$. Luego, $C(x)$ es un grupo denominado el centro de x.
2. Es un problema que requiere el paquete FGB y lo dejamos al estudiante UNA.
3. Hay tres rotaciones, la de 0 grados (que es la identidad), la de 120 grados y la de 240 grados. Las simetrías corresponden a las reflexiones respecto a las tres medianas del triángulo equilátero. Cada una de estas medianas fija un vértice e intercambia los otros dos. Luego, tenemos 6 permutaciones de los tres vértices de un triángulo equilátero y esto es el mayor número que podemos tener, luego es el grupo S_3.

11.5. Grupos en la naturaleza: modelando con grupos

La sal que usamos en la mesa es un cristal cuya fórmula es NaCl (cloruro de sodio). El cristal tiene forma cúbica.



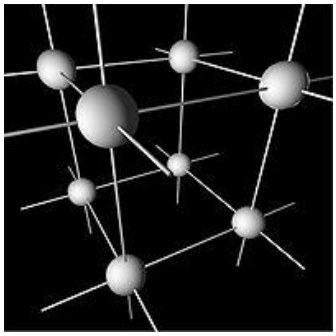
Cristales de Sal

Usted puede hacer estos cristales de sal mediante este procedimiento:

Para empezar, cogemos un recipiente y llenamos **un tercio de su contenido de agua**. A continuación, echamos **tres cucharaditas de sal** en el mismo y removemos bien. Una parte de esta sal se **disolverá**, mientras que otra quedará **depositada** en el fondo del recipiente. Para conseguir nuestros cristales caseros necesitaremos **separar** la sal que no se ha disuelto. Para ello llevaremos a cabo un proceso llamado **decantación**. Es muy simple. Tan solo tenemos que dejar la mezcla en reposo durante toda **una noche**, con lo que la sal no disuelta se quedará claramente en el fondo, y después verter el agua en otro recipiente, con mucho cuidado de no arrastrar también la sal del fondo. Una vez hecho esto, lo único que queda es dejar **reposar** la disolución sin tapar durante **unos días**. Poco a poco irán apareciendo unas **partículas sólidas** en el fondo de la disolución. Con ayuda de la lupa, podremos observarlas mejor y apreciar la forma que van tomando. También podemos **centrarnos en una** haciendo, por ejemplo, un círculo en un trozo de papel que colocaremos debajo del vaso justo en el lugar donde se encuentre. A lo largo de los días veremos cómo va **creciendo** nuestro pequeño cristal elegido. Lo verdaderamente impresionante de este experimento es comprobar que todos los cristales de sal forman **cuadrados** o **rectángulos**.

Tomado de http://www.experimentoscaseros.info/2012/12/como-hacer-cristales-de-sal.html

Existen otros tipos de sales distintas al cloruro de sodio o sal de formas exactamente similares. *Esto permite a la teoría de grupos establecer una correspondencia matemática entre distintos cristales y sus simetrías.*



Red de cristales

Usamos esto para predecir propiedades de difracción por rayos X o polarización de la luz en medios cristalinos. Estos experimentos permiten dilucidar la estructura de los cristales.

Invitamos al estudiante UNA a leer el siguiente texto tomado de *La Vida de Pasteur* por Vallery Radot http://www.librosmaravillosos.com/lavidadepasteur/capitulo02.html. En él encontrará la solución de este gran químico francés al problema de polarización que presentaba el espato de Islandia. El libro completo está en línea, es un gran libro que le recomiendo leer. En su solución Pasteur utiliza el concepto de simetría de manera brillante para dilucidar por qué existía polarización a la derecha o la izquierda en los cristales de este compuesto.

Espato de Islandia

Louis Pasteur

1. ¿Cuáles son los subgrupos del grupo de los enteros módulo 10, $\mathbb{Z}_{10}$? Lístelos todos y verifique su análisis con el software FGB 3.

2. Demuestre que dos grupos cíclicos finitos son isomorfos si y sólo si tienen el mismo número de elementos.

3. Demuestre que cualquier grupo de orden 9 debe tener un subgrupo de orden 3.

4. Demuestre que si $\phi: G \to H, \chi: H \to K$ son isomorfismos del grupo *G* en el grupo *H* y del grupo *H* en el grupo *K* respectivamente, entonces se puede construir un isomorfismo del grupo *G* en el grupo *K*.
5. Demuestre que si dos grupos son isomorfos y uno de ellos es conmutativo entonces el otro es conmutativo.
6. Demuestre que el concepto de grupos isomorfos es una relación de equivalencia.
7. Considere el grupo cíclico $\mathbb{Z}_{12}$. ¿Cuáles son sus subgrupos de orden 6? Verifique su trabajo con el software FGB 3.0. Sugerencia: Establece con cuidado cuál es el orden de cada elemento del grupo.

8. Usando el software FGB 3.0 verifique que todo grupo de orden menor o igual que 5 es conmutativo.
9. Demuestre que el conjunto $k\mathbb{Z}$ de todos los múltiplos de un entero fijo *k*, *k* no nulo, dado es un subgrupo de $\mathbb{Z}$. Demuestre que $\mathbb{Z}$ y $k\mathbb{Z}$ son isomorfos.
10. Demuestra que el grupo S_3 no es isomorfo al grupo cíclico de 6 elementos. Sugerencia: ¿Es S_3 conmutativo?.
11. Supongamos que *x* es un elemento de orden 3 en el grupo *G*. Sea $\phi: G \to H$ un isomorfismo de grupos. ¿Cuál es el orden de $\phi(x)$ en *H*?.

1. 10 sólo tiene dos divisores no triviales: 2 y 5. Así que los subgrupos deben tener precisamente ese orden. El único elemento que genera un grupo de orden 2 es la clase del 5, todos los demás elementos generan grupos de orden 5 o el grupo entero. Dejamos al estudiante UNA que haga la lista completa de los subgrupos.

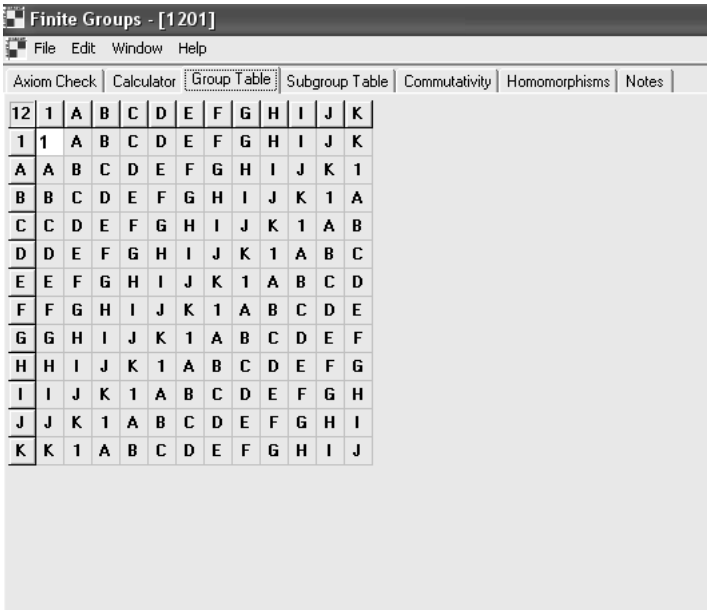
   Para usar el software FGB usamos la pestaña de Subgroup Table y la opción Add que permite ir incluyendo elementos del grupo en el subgrupo. Abra en

primer lugar de la carpeta de grupos cíclicos el archivo 1001. Luego haga click en la pestaña Subgroup Table. Añada los elementos 1 y B (el uno siempre debe estar en el grupo), dele OK cada vez que sale un aviso del programa, ¿qué observa? Vea que ha generado un grupo de orden 5. El elemento B corresponde a la clase del 2, luego es razonable lo que obtuvimos. Siga experimentando con FGB y verificando su trabajo.

2. Para que dos grupos sean isomorfos debe haber una biyección entre ellos y por ende deben tener la misma cantidad de elementos. Así es claro que es una condición necesaria que los dos grupos deben tener la misma cantidad de elementos. Veamos que es también suficiente. Sea *G* un grupo cíclico de orden *n* generado por *x*. Sea *H* un grupo cíclico de orden *n* generado por *y*. Definimos $\phi: G \to H$ por medio de $\phi(x) = y, \phi(x^2) = y^2, \cdots \phi(x^{n-1}) = y^{n-1}, \phi(e) = e'$. Claramente, $\phi: G \to H$ es sobreyectiva y por ende biyectiva al ser *G*,*H* conjuntos finitos de igual número de elementos. Por otro lado, la construcción de $\phi: G \to H$ implica que esta transformación es un homomorfismo. Luego, $\phi: G \to H$ es un isomorfismo y esto concluye el ejercicio.
3. Tomemos un grupo cualquiera de orden 9. Si el grupo es cíclico y generado por *x* estamos listos ya que x^3 debe tener orden 3. El estudiante UNA debe decir por qué. Si suponemos que *G* no es cíclico vemos que cualquier elemento distinto del elemento neutro *e* debe generar un subgrupo propio de *G*. Pero, este subgrupo, por el teorema de Lagrange, debe tener un orden que divida a 9, es decir debe ser de orden 1, 3 o 9. No puede ser de orden 1 ya que nuestro elemento no es el elemento neutro. No puede ser 9 ya que el grupo no es cíclico, luego el orden del subgrupo (y de su generador) debe ser tres.
4. Esto es bastante sencillo y muchas veces en la formulación de resultados de álgebra abstracta las cosas tienen un carácter automático. Esto significa que hacemos las cosas prácticamente de la única forma que podemos hacerlas. Si $\phi: G \to H, \chi: H \to K$ son isomorfismos del grupo *G* en el grupo *H* y del grupo *H* en el grupo *K* respectivamente, entonces consideramos la función compuesta $\chi \circ \phi: G \to K$. Vemos que esta función es un isomorfismo ya que $\chi \circ \phi(xy) = \chi(\phi(xy)) = \chi(\phi(x)\phi(y)) = \chi(\phi(x))\chi(\phi(y))$ y además al ser una

composición de biyecciones $\chi \circ \phi : G \to K$ es una biyección. Esto concluye el problema.

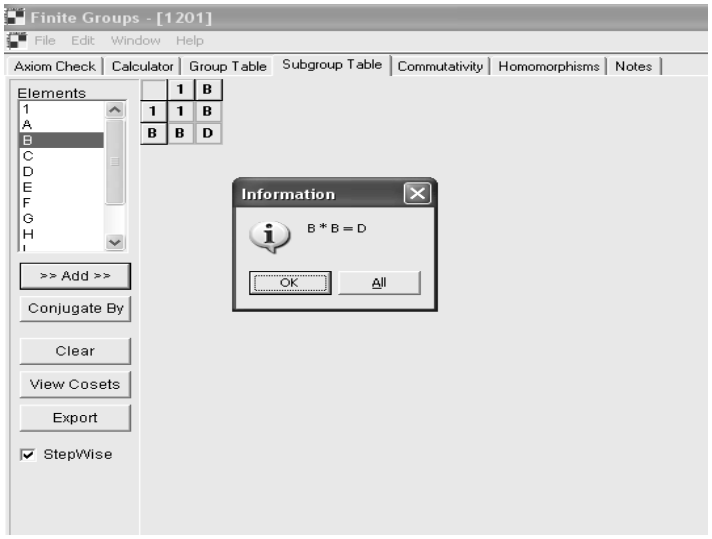
5. Supongamos que $\phi : G \to H$ es un isomorfismo y G es conmutativo. Supongamos que H no fuese conmutativo, entonces deben existir z,w en H tales que zw es distinto de wz pero $\phi^{-1}(zw) = \phi^{-1}(z)\phi^{-1}(w) = \phi^{-1}(w)\phi^{-1}(z) = \phi^{-1}(wz)$ y al ser ϕ^{-1} una biyección debe ocurrir que $\phi^{-1}(wz) \neq \phi^{-1}(zw)$, una contradicción.
6. El estudiante UNA solo debe relacionar algunos resultados que ya demostró para resolver este problema. Recuerde que cualquier grupo es isomorfo a el mismo. Luego la relación es reflexiva. Por otro lado, si $\phi : G \to H$ es un isomorfismo, entonces $\phi^{-1} : H \to G$ es de nuevo un isomorfismo. Luego, la relación es simétrica. El problema 4 demuestra que la relación es transita. Indique por qué. Luego, tenemos una relación de equivalencia.
7. Sabemos que el grupo cíclico de orden 12 es isomorfo al grupo $\mathbb{Z}_{12}$. Todos sus subgrupos son cíclicos. El elemento $\overline{2}$ genera un grupo de orden 6, $\left\{\overline{2}, \overline{4}, \overline{6}, \overline{8}, \overline{10}, \overline{0}\right\}$. Vemos esto con el software FGB 3.0. Vaya al programa y abra el archivo 1201 que encuentra en la carpeta de los grupos cíclicos.



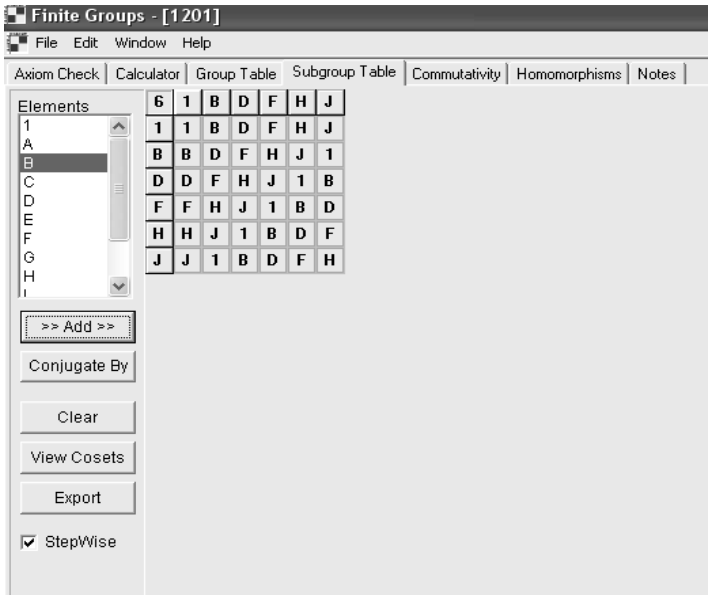
12	1	A	B	C	D	E	F	G	H	I	J	K
1	1	A	B	C	D	E	F	G	H	I	J	K
A	A	B	C	D	E	F	G	H	I	J	K	1
B	B	C	D	E	F	G	H	I	J	K	1	A
C	C	D	E	F	G	H	I	J	K	1	A	B
D	D	E	F	G	H	I	J	K	1	A	B	C
E	E	F	G	H	I	J	K	1	A	B	C	D
F	F	G	H	I	J	K	1	A	B	C	D	E
G	G	H	I	J	K	1	A	B	C	D	E	F
H	H	I	J	K	1	A	B	C	D	E	F	G
I	I	J	K	1	A	B	C	D	E	F	G	H
J	J	K	1	A	B	C	D	E	F	G	H	I
K	K	1	A	B	C	D	E	F	G	H	I	J

Observe que 1 corresponde al elemento neutro ya que están usando la notación multiplicativa. Por otro lado, al revisar la tabla vemos que A es un generador del

grupo, ¿por qué?. Como A+A=B examinemos el grupo que genera B con el paquete FGB. Vamos a la pestaña Subgroup Table.



Agregamos el 1(que debe estar en cualquier subgrupo y el B para empezar. Enseguida el programa indica que como B*B=D debe estar en el subgrupo. Sigamos de esta manera y después de una serie de adiciones obligatorias el programa no agrega ningún elemento más completando el subgrupo que vemos a continuación.



La tabla nos indica que tenemos un grupo de orden 6.

Volvamos a los cálculos personales antes de usar el paquete. El elemento $\overline{3}$ genera un grupo de orden 4 como se puede ver. Este grupo está formado por los elementos $\{\overline{3},\overline{6},\overline{9},\overline{0}\}$. El estudiante UNA debe usar el software FGB para verificar esto. Para

hacer esto pregúntese, ¿qué elemento de la tabla corresponde al elemento $\overline{3}$? ¿Qué pasa con la clase del 4? Vea que esto genera un grupo de orden 3. Al ser 5 primo con 12, debe generar un grupo de orden 12, es decir, el grupo completo. Realice esto con el software FGB. La clase del 6 genera un grupo de orden 2 ya que 6+6=0 modulo 12. El 7 es coprimo con el 12 y debe generar un subgrupo de orden 12, es decir genera a $\mathbb{Z}_{12}$. En el software G corresponde a la clase del 7. Verifique lo que afirmamos usando FGB. Veamos qué ocurre con la clase del 8. Como 8+8=4 módulo 12 y 4+8=0 módulo 12 entonces la clase del 8 genera un subgrupo de orden 3. Aquí está la tabla generada por el software

3	1	D	H
1	1	D	H
D	D	H	1
H	H	1	D

El estudiante UNA debe entender que la única manera de familiarizarse con un software es usarlo mucho. Estoy seguro que finalmente Ud. manejará este programa mejor que yo.

¿Qué podemos decir de la clase del 9?. Hagamos unas cuentas. 9+9=18=6 módulo 12. Luego, 9+6=15=3 módulo 12. Así, por último 3+9=12=0 módulo 12. Es decir, tenemos un grupo de orden 4. El 11 lo dejamos completamente al estudiante UNA ya que hemos tratado casos similares arriba. ¿Qué ocurre con el 10? Aquí está la tabla que genera el software FGB 3.0

6	1	B	D	F	H	J
1	1	B	D	F	H	J
B	B	D	F	H	J	1
D	D	F	H	J	1	B
F	F	H	J	1	B	D
H	H	J	1	B	D	F
J	J	1	B	D	F	H

Es un grupo de orden 6, de hecho es el grupo generado por la clase del 2 (el elemento B). Aquí concluye nuestro análisis ya que hemos examinado todos los subgrupos generados por cada elemento.

9. Fijemos un entero *k.* Tomemos el conjunto $k\mathbb{Z} = \{kn \text{ tal que } n \in \mathbb{Z}\}$ donde *k* es un entero fijo. Demostremos, en primer lugar, que al restringir la suma de los

enteros obtenemos un grupo. Vemos que 0 está en $k\mathbb{Z} = \{kn \text{ tal que } n \in \mathbb{Z}\}$ ya que 0=0*k*. Además, la suma de los enteros se puede restringir al conjunto $k\mathbb{Z} = \{kn \text{ tal que } n \in \mathbb{Z}\}$. Para ver esto, tomemos dos elementos cualesquiera *kn* y *km* en $k\mathbb{Z} = \{kn \text{ tal que } n \in \mathbb{Z}\}$. Como $km+kn=k(m+n)$ esto pertenece a $k\mathbb{Z} = \{kn \text{ tal que } n \in \mathbb{Z}\}$, Por supuesto que la suma, restringida al conjunto $k\mathbb{Z} = \{kn \text{ tal que } n \in \mathbb{Z}\}$ es asociativa, ya que una violación de la asociatividad para la suma implicaría que esta no se cumple en los enteros, lo cual es absurdo. Así, solo resta verificar que un elemento cualquiera *km* tiene un inverso, pero $km+(-km)=0$ y $-km=k(-m)$ está en $k\mathbb{Z} = \{kn \text{ tal que } n \in \mathbb{Z}\}$. Hemos concluido demostración que $k\mathbb{Z} = \{kn \text{ tal que } n \in \mathbb{Z}\}$ es un subgrupo de $\mathbb{Z}$.

Para verificar que los grupos son isomorfos construimos un isomorfismo de $\mathbb{Z}$ a $k\mathbb{Z}$ de manera natural. Consideremos la función $\phi : \mathbb{Z} \to k\mathbb{Z}$ que asigna a cada entero *z* el valor $\phi(z) = kz \in k\mathbb{Z}$. Como

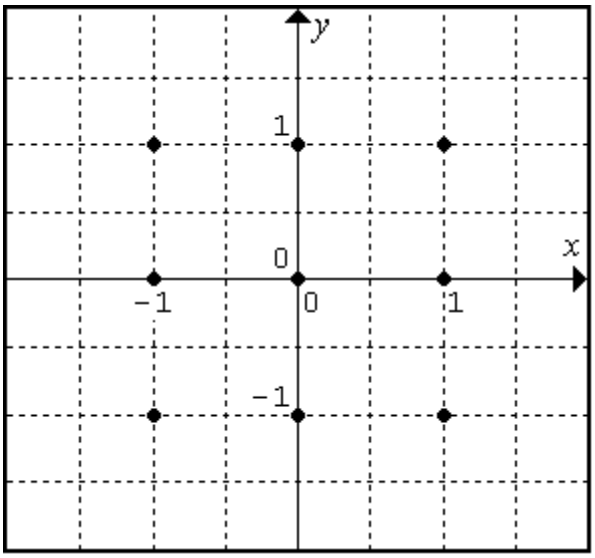
$$\phi(z+w) = k(z+w) = kz + kw = \phi(z) + \phi(w)$$

Luego, $\phi : \mathbb{Z} \to k\mathbb{Z}$ es un homomorfismo. Claramente, $\phi : \mathbb{Z} \to k\mathbb{Z}$ es sobreyectiva. Por otro lado, $\phi(z) = kz = kz' = \phi(z') \Rightarrow k(z-z') = 0 \Rightarrow z = z'$. Aquí usamos que *k* es no nulo. Esto indica que la aplicación $\phi : \mathbb{Z} \to k\mathbb{Z}$ es un isomorfismo. ¿Puede usted pensar qué pasaría si *k* fuese nulo?

10. Sabemos que dos grupos isomorfos deben ser simultáneamente conmutativos, pero S_3 es no conmutativo y cualquier grupo cíclico es conmutativo. Por ende, no pueden ser isomorfos.

11. El orden es 3 como veremos en un momento. En primer lugar observe que $\phi(x)^3 = \phi(x^3) = \phi(e) = e'$ donde *e* y *e'* son los elementos neutros de los grupos *G* y *H*. Como *x* genera un subgrupo *K* cíclico de orden 3 en *G* su imagen debe ser un subgrupo de *H*, en este caso isomorfo *K*. Luego debe ser cíclico de orden 3, luego $\phi(x)$ tiene orden 3.

UNIDAD 8



Anillos

Semana 13,14

Aplicar el concepto de anillo y sus propiedades en la resolución de problemas, en el modelado matemático y en la demostración de nuevos resultados.

Contenidos a tratar: Anillos con identidad y sus propiedades. Subanillos e ideales. Homomorfismos. Polinomios.

12.1. La noción de anillo

Desde la *Educación Media* hemos estudiado distintos conjuntos y operaciones con sus elementos, tal es el caso de los *enteros*, *racionales*, *reales* y *complejos*, así como los *polinomios*, las *matrices* (cuadradas) y las *funciones reales de variable real*, que aunque distintos, en realidad comparten propiedades comunes; de hecho, poseen una misma **estructura**. Por ejemplo, observemos que en los conjuntos antes citados, la ley

aditiva allí definida es interna, es decir, al sumar dos elementos cualesquiera de ese conjunto se obtiene un elemento de ese mismo conjunto. Además, existe un elemento neutro, llamado cero que, aunque tenga una simbología particular dependiendo del conjunto y la naturaleza de sus elementos, *se comporta de la misma manera*. En el caso de $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ y en el conjunto de los polinomios $P[x]$, este cero se escribe simplemente como

$$0$$

En el caso de conjunto de las matrices cuadradas, el cero tiene la forma

$$\begin{bmatrix} 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 0 \end{bmatrix}_{n\times n} \text{ o bien } [0]_{n\times n}$$

Y en el de las funciones reales de variable real definidas de un conjunto $[a,b]$ en $\mathbb{R}$:

$$f(x) = 0, \text{ para cualquier } x \in [a,b]$$

La ley aditiva es asociativa y conmutativa en todos los casos que citamos antes. Y, para cada elemento existe su opuesto aditivo o simétrico. Por otra parte, en estos conjuntos (por sólo citar algunos ejemplos) está definida una multiplicación que verifica la propiedad asociativa y, posiblemente, la existencia de elemento identidad. Notemos que tal identidad sí existe en $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ y $P[x]$, y se simboliza de la misma manera:

$$1$$

En el caso de las matrices es

$$\begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 1 \end{bmatrix}_{n\times n} \quad \text{o bien } I_{n\times n}$$

Y en el de las funciones reales de variable real con el producto usual:

$$f(x)=1$$

Además, se cumplen las dos leyes distributivas (a izquierda y a derecha) de la multiplicación con respecto a la adición.

El conjunto de los *enteros módulo n*, que estudiamos semanas atrás, tiene un comportamiento (estructura) similar.

Tal estructura es medular para las matemáticas en la actualidad, así como para sus aplicaciones en otras disciplinas, áreas y en la realidad. Esta semana se ocupa, precisamente, del estudio de la estructura denominada **anillo** y de algunas de sus propiedades. Una nota: al comienzo hablamos del conjunto de las matrices cuadradas para que de esta forma esté definida la adición y la multiplicación de cualesquiera matrices en dicho conjunto.

12.2. Anillos y Anillos con identidad

Definición. Un conjunto no vacío *A* es un **anillo** si en *A* están definidas dos leyes internas, una aditiva "+" y otra multiplicativa "$\cdot$", que verifican las condiciones que siguen:

(i) *A* es un grupo abeliano con respecto a la ley aditiva.

(ii) La multiplicación es asociativa: $a\cdot(b\cdot c)=(a\cdot b)\cdot c$, $\forall a,b,c\in A$.

(iii) La multiplicación es distributiva, a izquierda y a derecha, con respecto a la adición: $(a+b)\cdot c=a\cdot c+b\cdot c$ y $c\cdot(a+b)=c\cdot a+c\cdot b$. $\forall a,b,c\in A$.

Si adicionalmente se verifica la propiedad (iv), entonces A es un **anillo con identidad**.

(iv) Existe un elemento identidad para la multiplicación: $\exists 1 \in A: 1 \cdot a = a \cdot 1 = a$, $\forall a \in A$.

Además,

(v) Si $ab = ba,\ \forall a,b \in A$, entonces A es un **anillo conmutativo**.

(vi) Si A es un anillo conmutativo con identidad, en el que $ab = 0 \Rightarrow a = 0\ \acute{o}\ b = 0$, es un **dominio entero**.

(vii) Si A es un anillo en el que existen $a \neq 0$ y $b \neq 0$ tales que $ab = 0$, entonces a y b se llaman **divisores de cero**.

El anillo A se representa formalmente con la terna $(A,+,\cdot)$. En $(A,+)$ el *neutro* se denota usualmente con 0, y se le denomina el *cero del anillo*. En $(A,\cdot)$ la *identidad* se denota comúnmente con 1 y se denomina *uno del anillo*. Además, tan como en el caso de los grupos, el inverso aditivo de a se escribe $-a$ y la multiplicación $a \cdot b$ puede escribirse simplemente como ab (sobreentendiendo el signo para esta ley).

1. Si A es un grupo abeliano cualquiera y definimos en A una ley multiplicativa de la siguiente forma: $ab = 0,\ \forall a,b \in A$, entonces $(A,+,\cdot)$ es un anillo (denominado **anillo trivial** sobre A). Observemos que la condición (i) de la definición de Anillo se verifica de inmediato. Y como

$$a \cdot (b \cdot c) = a \cdot 0 = 0 = 0 \cdot c = (a \cdot b) \cdot c$$

entonces se verifica (ii).

Además, de las igualdades

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

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

se tiene (iii).

2. Los conjuntos $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ y $\mathbb{C}$, con la adición y la multiplicación usual, son anillos con identidad.
3. El conjunto de todos los polinomios en $\mathbb{R}$, el de las matrices cuadradas sobre $\mathbb{R}$, y de las funciones reales de variable real son anillos con identidad. (La multiplicación, en el caso de las funciones, está dada por el producto usual de funciones).
4. El conjunto de los enteros módulo 2, $\mathbb{Z}_2$, con la adición y la multiplicación dadas por las tablas:

+	$\bar{0}$	$\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{1}$
$\bar{1}$	$\bar{1}$	$\bar{0}$

y

·	$\bar{0}$	$\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$

es un anillo con identidad. La identidad es

$$\bar{1} = \{x \in \mathbb{Z}:\ x \equiv 1 (mód\ 2)\} = \{\ldots, -3, -1, 1, 3, 5, \ldots\}$$

En $\mathbb{Z}_2$ no hay divisores de cero.

5. Notemos que existen matrices distintas a la matriz cero cuyo producto es la matriz cero; tal es el caso de:

$$\begin{bmatrix} 1 & 0 \\ -1 & 0 \end{bmatrix} \text{ y } \begin{bmatrix} 0 & 0 \\ -1 & \sqrt{2} \end{bmatrix}$$

Aquí,

$$\begin{bmatrix} 1 & 0 \\ -1 & 0 \end{bmatrix}\begin{bmatrix} 0 & 0 \\ -1 & \sqrt{2} \end{bmatrix}=\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}.$$

Es decir, ¡en el anillo de las matrices de orden 2×2, hay divisores de cero! ¿Hay divisores de cero en el anillo de las matrices de orden 3×3?

6. En $\mathbb{Z}_6$ se tiene que $\bar{2}$ y $\bar{3}$ son divisores de cero, ya que $\bar{2}\cdot\bar{3}=\bar{0}$. Además, $\bar{3}$ y $\bar{4}$ también lo son. De seguidas exponemos su tabla multiplicativa.

·	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{0}$	$\bar{2}$	$\bar{4}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{2}$	$\bar{0}$	$\bar{4}$	$\bar{2}$
$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

En efecto, sabemos que

$$\bar{2}=\{x\in\mathbb{Z}:\ x\equiv 2\,(\textit{mód}\ 6)\}=\{x\in\mathbb{Z}:\ 6\mid x-2\}=\{\ldots,-4,2,8,14,20,\ldots\}.$$
$$\bar{3}=\{x\in\mathbb{Z}:\ x\equiv 3\,(\textit{mód}\ 6)\}=\{x\in\mathbb{Z}:\ 6\mid x-3\}=\{\ldots,-3,3,9,15,21,\ldots\}$$

En $\bar{2}$ están los enteros que dan resto 2 al dividir por 6, y en $\bar{3}$ están los enteros que dan resto 3 al dividir por 6. Es decir, cualquier elemento de $\bar{2}$ y $\bar{3}$ tiene la forma $6c+2$ y $6c^*+2$, respectivamente (de acuerdo con el *algoritmo de la división*). Así,

$$(6c+2)(6c^*+3)=36cc^*+18c+12c^*+6=6(6cc^*+2c+2c^*+1)\in\bar{0}$$

Los lectores pueden comprobar, de forma similar, que $\bar{3}\cdot\bar{4}=\bar{0}$.

7. El conjunto $\{x,y,z\}$ con la adición y la multiplicación dadas por las tablas:

+	x	y	z
x	y	z	x
y	z	x	y
z	x	y	z

y

·	x	y	z
x	x	y	z
y	y	x	z
z	z	z	z

es un anillo con identidad. Aquí la identidad es *x*. Este anillo tiene la misma forma (es *isomorfo*) que $\mathbb{Z}_3$.

8. El conjunto de partes de $\mathbb{N}$, esto es $P(\mathbb{N})$, con la adición y multiplicación definidas como sigue, es un anillo conmutativo con elemento identidad.

$$A+B=(A\cup B)-(A\cap B)=A\Delta B$$
$$A\cdot B=A\cap B$$

Para cualesquiera $A,B\in P(\mathbb{N})$.

 Demuestre en detalle lo afirmado en el ejemplo 8.

 **(El anillo de los enteros módulo *n*).** En la unidad 5 estudiamos en detalle el conjunto de de las clases residuales módulo *n*. Aquí veremos que, en general, $\mathbb{Z}_n$ es un anillo conmutativo para cualquier entero positivo *n*. Para ello, notemos que al dividir un entero cualquiera *x* entre *n*, tenemos que

$$x=nc+r,\ 0\le r<n$$

Donde *c* es el cociente y *r* el resto. Es decir, $r = 0, 1, 2, 3, \ldots, n-1$ (sólo existen *n* posibles restos al dividir *x* entre *n*). Además, sabemos que la clase residual $\bar{a}$ consta de todos los enteros que dan el mismo resto que *a* al dividir por *n*. Esto es, $\bar{a} = \{v \in \mathbb{Z} :\ v \equiv a \ (mód\ n)\} = \{v \in \mathbb{Z} :\ n \mid\ a - v\}$. Así, $\mathbb{Z}_n = \{\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{n-1}\}$. Recordemos, además, que $\bar{a} = \{\ldots, a-2n, a-n, a, a+n, a+2n, \ldots\}$.

En $\mathbb{Z}_n$ definimos una adición y una multiplicación como sigue:

$$\bar{a} + \bar{b} = \overline{a+b}$$
$$\bar{a} \cdot \bar{b} = \overline{a \cdot b}$$

Estas leyes son internas pues el resto de la división por *n* de cualquier entero es alguno de los enteros $0, 1, 2, 3, \ldots, n-1$, los cuales se asocian con alguna de las clases de $\mathbb{Z}_n$. Resulta inmediato que la adición es *conmutativa* pues si *r* es el resto de dividir *x* por *n*, y *r** es el resto de dividir *x** por *n*, entonces podemos escribir que $x = nc + r,\ 0 \le r < n$ y $x^* = nc^* + r^*,\ 0 \le r^* < n$; con lo cual

$$x + x^* = n(c + c^*) + (r + r^*)$$

Aquí hay dos posibilidades: (Caso 1) Si $r + r^* < n$, entonces $r + r^*$ es el resto de dividir $x + x^*$ por *n*. (Caso 2) Si $r + r^* \ge n$, simplemente escribimos $r + r^* = n + j < 2n$ (ya que tanto *n* como *n** son menos que *n*), donde $0 \le j < n$. Por lo tanto, $x + x^* = n(c + c^*) + (r + r^*) = n(c + c^*) + (n + j) = n(c + c^* + 1) + j$. Observe que $\overline{a+b} = \bar{j}$. Llegamos a las mismas expresiones si dividimos $x^* + x$ por *n*.

Veamos que la adición es *asociativa*. Sean *x*, *y*, *z* enteros. Probaremos que $(x + y) + z = x + (y + z)$.

¿Cuál es el resto de dividir $(x + y) + z$ por *n*? Para obtenerlo, primero debemos dividir $x + y$ entre *n*. por el algoritmo de la división podemos escribir que

$$x+y=nc+r \qquad (1)$$

Ahora, el resto que resulta de dividir $(x+y)+z$ por *n* es el mismo resto que resulta de dividir $r+z$ por *n*. Aplicando el algoritmo de la división tenemos que

$$r+z=nc^*+r^* \qquad (2)$$

Sumando las expresiones (1) y (2): $x+y+r+z=nc+r+nc^*+r^*$. Por tanto,

$$x+y+z=n(c+c^*)+r^*$$

Y como $0\le r^*<n$, entonces r^* es el resto de dividir $(x+y)+z$ por *n*. A la misma conclusión se llega si calculamos el resto de dividir $x+(y+z)$ por *n*.

Existe neutro en $\mathbb{Z}_n$: el $\bar{0}$. Para ver esto consideremos una clase cualquiera de $\mathbb{Z}_n$, llamémosla $\bar{i}$. Sean $x\in\bar{i}$, $y\in\bar{0}$; en tal caso, por el algoritmo de la división:

$$x=nc+i$$
$$y=nc^*+0$$

Con lo cual

$$x+y=n(c+c^*)+i\in\bar{i}$$

Por tanto, $\bar{i}+\bar{0}=\bar{i}$.

Para cada $\bar{i}\in\mathbb{Z}_n$ existe su simétrico. Si $\bar{i}=\bar{0}$ su simétrico es él mismo (por la propiedad anterior). Ahora, si $\bar{i}=\bar{1},\bar{2},\bar{3},...,\overline{n-1}$, su simétrico es $\overline{n-i}$. En efecto, en la clase $\bar{i}$ están enteros de la forma $nc+i$; y en la clase $\overline{n-i}$ están enteros de la forma $nc^*+(n-i)$. Ahora,

$$nc+i+nc^*+(n-i)=n(c+c^*+1)+i-i=n(c+c^*+1)\in\bar{0}$$

Con todo lo anterior $\mathbb{Z}_n$ es un grupo abeliano (verificándose la condición i de la definición de anillo).

Las condiciones ii y iii (referidas a la asociatividad de la multiplicación y a la distributividad de la multiplicación con respecto a la adición) se prueban de forma similar.

$\mathbb{Z}_n$ *tiene identidad.* La clase $\bar{1}$ tiene enteros de la forma $nc+1$. Una clase $\bar{i}$ tiene elementos de la forma nc^*+i, $0\le i<n$. Así, los elementos de $\bar{1}\cdot\bar{i}$ tienen la forma

$$(nc+1)(nc^*+i)=n^2cc^*+nci+nc^*+i=n(ncc^*+ci+c^*)+i\in\bar{i}$$

Por tanto, $\bar{1}$ es la identidad de $\mathbb{Z}_n$.

Además, *la multiplicación es conmutativa en* $\mathbb{Z}_n$: esto se deriva del hecho de que el resto que resulta de dividir *ij* por *n* es el mismo resto que resulta de dividir *ji* por *n*.
En resumen, $\mathbb{Z}_n$ es un anillo conmutativo con elemento identidad.

Ahora bien, si *n* es compuesto, existen enteros positivos a_1 y a_2, tales que $n=a_1a_2$. Esto implica que, en tal caso, $\mathbb{Z}_n$ tenga divisores de cero (como en el ejemplo que refiere a $\mathbb{Z}_6$). Pero si *n* es primo, no existe tal posibilidad; así que $\mathbb{Z}_n$ sería un dominio entero (como $\mathbb{Z}_3$, por ejemplo).

(Los enteros gaussianos)

Un conjunto muy especial es el de los **enteros gaussianos**, el cual consta de los números de la forma $a+bi$ donde *a* y *b* son enteros.

$$\mathbb{Z}[i] = \{a + bi : \ \ a, b \in \mathbb{Z}\}$$

Donde la adición y la multiplicación se definen tal como en el conjunto de los números complejos:

$$(a + bi) + (c + di) = (a + c) + (b + d)i$$
$$(a + bi)(c + di) = (ac - bd) + (bc + ad)i$$

$\mathbb{Z}[i]$ es un dominio entero.

En efecto, es claro(¡verifique!) que ambas leyes son internas. Por otra parte, la adición es asociativa, pues

$$\begin{aligned}
\big[(a + bi) + (c + di)\big] + (e + fi) &= \big[(a + c) + (b + d)i\big] + (e + fi) \\
&= \big((a + c) + e\big) + \big((b + d) + e\big)i \\
&= \big(a + (c + e)\big) + \big(b + (d + f)\big)i \\
&= (a + bi) + \big[(c + e) + (d + f)i\big] \\
&= (a + bi) + \big[(c + di) + (e + fi)\big]
\end{aligned}$$

Aquí aplicamos la definición de adición, la asociatividad de la adición de enteros, y nuevamente la definición de adición.

La conmutatividad de la adición se sigue de

$$\begin{aligned}
(a + bi) + (c + di) &= (a + c) + (b + d)i \\
&= (c + a) + (d + b)i \\
&= (c + di) + (a + bi)
\end{aligned}$$

Aquí nos basamos en la definición de la adición y en la conmutatividad de la adición en $\mathbb{Z}$, y nuevamente la definición de adición.

Como $(a+bi)+(0+0i)=(0+0i)+(a+bi)=a+bi$, entonces $0+0i=0$ es el neutro aditivo en $\mathbb{Z}[i]$. Dado el entero gaussiano $a+bi$, existe su opuesto $-a-bi$, ya que $(a+bi)+(-a-bi)=(a-a)+(b-d)i=0+0i=0$. Con todo esto, $\mathbb{Z}[i]$ es un grupo abeliano (verificándose la condición i de la definición de anillo).

Por otra parte, como

$$\begin{aligned}
\left[(a+bi)(c+di)\right](e+fi) &= \left[(ac-bd)+(bc+ad)i\right](e+fi) \\
&= \left((ac-bd)e-(bc+ad)f\right)+\left((bc+ad)e+(ac-bd)f\right)i \\
&= (ace-bde-bcf-adf)+(bce+ade+acf-bdf)i \\
&= \left(a(ce-df)-b(de+cf)\right)+\left(b(ce-df)+a(de+cf)\right)i \\
&= (a+bi)\left[(ce-df)+(de+cf)i\right] \\
&= (a+bi)\left[(c+di)(e+fi)\right]
\end{aligned}$$

Entonces, la multiplicación es asociativa (verificándose ii).

Además, la multiplicación es distributiva con respecto a la adición (iii), pues

$$\begin{aligned}
\left[(a+bi)+(c+di)\right](e+fi) &= \left[(a+c)+(b+d)i\right](e+fi) \\
&= \left((a+c)e-(b+d)f\right)+\left((b+d)e+(a+c)f\right)i \\
&= ae+ce-bf-df+bei+dei+afi+cfi \\
&= (ae-bf)+(be+af)i+(ce-df)+(de+cf)i \\
&= (a+bi)(e+fi)+(c+di)(e+fi)
\end{aligned}$$

La identidad es, precisamente, $1+0i$. Observemos que

$$(1+0i)(a+bi)=(1a-0b)+(0a+1b)i=a+bi\,.$$

Y como

$$(a+bi)(c+di)=(ac-bd)+(bc+ad)i=(ca-db)+(da+cb)i=(c+di)(a+bi)$$

entonces se verifica la conmutatividad de la multiplicación.

12.2 Propiedades generales de los anillos

Proposición 1. En cualquier anillo se cumple que $0a = a0 = 0,\ \forall a \in A$.

Demostración. Sea *A* un anillo y $a \in A$, entonces

$$a = 0 + a$$

pues 0 es el neutro aditivo en *A*.

Luego,

$$aa = a(0 + a) \quad \text{multiplicando por } a$$
$$= a0 + aa$$

por una de las leyes distributivas.

Y, de acuerdo con las leyes de cancelación que se verifican en *A*, lo anterior garantiza que $a0 = 0$. Del mismo modo se prueba que $0a = 0$. Por tanto, $a0 = 0a = 0$. ■

Proposición 2. En todo anillo se cumple que:

(i) $-(-a) = a$.

(ii) $-(a + b) = -a - b$.

(iii) $-(a - b) = -a + b$.

(iv) $-ab = (-a)b = a(-b)$.

(v) $(-a)(-b) = ab$.

Demostración. Sean *a* y *b* elementos de *A*. (i) Como $a+(-a)=0$, entonces $-a$ es el opuesto de *a*, y recíprocamente. Esto es, $-(-a)=a$. (ii) Para probar esta parte basta sumar $a+b$ y $-a-b$, y apoyarnos en las propiedades asociativa, conmutativa, existencia de opuesto y neutro en *A*:

$$\begin{aligned}(a+b)+(-a-b) &= a+b+(-a)+(-b)\\ &= a+(-a)+b+(-b)\\ &= 0+0\\ &= 0\end{aligned}$$

Lo anterior garantiza que $-(a+b)=-a-b$. La prueba de (iii) es similar a esta.

(iv) Sabemos que $a+(-a)=0$, pues *A* es un grupo. Ahora, multiplicando por *b* a la derecha y apoyándonos en una de las leyes distributivas, tenemos que: $(a+(-a))b=ab+(-a)b=0$. Y por la unicidad del opuesto aditivo concluimos que $-ab=(-a)b$. De forma similar, de $b+(-b)=0$, tenemos que $a(b+(-b))=ab+a(-b)=0$. Es decir, $-ab=a(-b)$.

Para ver (v) escribimos:

$$\begin{aligned}(-a)(-b) &= (-a)(-b)+0\\ &= (-a)(-b)+a0\\ &= (-a)(-b)+a(b+(-b))\\ &= (-a)(-b)+ab+a(-b)\\ &= (-a)(-b)+a(-b)+ab\\ &= ((-a)+a)(-b)+ab\\ &= 0(-b)+ab\\ &= 0+ab\\ &= ab\end{aligned}$$

Para verificar esto nos apoyamos en la existencia de neutro aditivo en *A*, en que $a0=0$ (propiedad 1), en la existencia de opuesto aditivo en *A*, en una de las leyes distributivas, en el hecho de que la adición en *A* es conmutativa y asociativa, nuevamente en una de las leyes distributivas, en la existencia de opuesto aditivo, en la propiedad 1, y en la existencia de neutro. ■

Proposición 3. En cualquier anillo se cumple que:

(i) $a(b-c)=ab-ac$.

(ii) $(b-c)a=ba-ca$.

Estas propiedades se siguen de manera inmediata (con base en la propiedad distributiva de la multiplicación con respecto a la adición y por la parte iv de la propiedad anterior).

Proposición 4. Sean $a,b\in A$ y $n\in\mathbb{Z}$, entonces $n(ab)=(na)b=a(nb)$.

Proposición 5. Sean $a,b\in A$ y $m,n\in\mathbb{Z}^+$, entonces

(i) $a^{m+n}=a^m a^n$

(ii) Si $ab=ba$, entonces $(ab)^m=a^m b^m$

(iii) $(a^m)^n=a^{mn}$

(iv) $a^1=a$

Dejamos las pruebas de las proposiciones 4 y 5 como ejercicios.

Definición. Sea *A* un anillo con identidad 1. Se dice que $a\in A$ es **inversible o invertible** si existe un $b\in A$ tal que $ab=ba=1$. En tal caso, se conviene en escribir $b=a^{-1}$.

Proposición 6. Si A es un anillo con identidad, entonces el conjunto de todos los elementos inversibles es un grupo.

Demostración. Sea $U(A)=\{a\in A:\ a\ es\ inversible\}$. Es claro que $U(A)\subset A$ y $U(A)\neq\varnothing$, esto último se deriva de que $1\cdot 1=1$, así que la identidad de A está en $U(A)$. Veamos que $U(A)$ es cerrado: si $x,y\in U(A)$, entonces deben ser inversibles, por tanto existen $x^{-1},y^{-1}\in A$. Luego, $(xy)(y^{-1}x^{-1})=x(yy-1)x^{-1}=x\cdot 1\cdot x^{-1}=1$. Entonces, xy también es inversible: $xy\in U(A)$. Veamos ahora que si $x\in U(A)$ entonces $x^{-1}\in U(A)$: como $(x^{-1})^{-1}=x\in A$, entonces x^{-1} es inversible, es decir, $x^{-1}\in U(A)$. ■

Proposición 7. Si A es un anillo en el que se verifican las leyes de cancelación, entonces tal anillo no tiene divisores de cero.

Demostración. Supongamos que $xy=0$ y además que $x\neq 0$, entonces

$$xy=0=x0\Rightarrow y=0$$

Lo anterior garantiza que $y=0$. Esto es, en A no hay divisores de cero. ■

Proposición 8. Si A es un dominio entero, entonces las leyes de cancelación se verifican.

Demostración. Supongamos que $x\neq 0$ y que $xy=xz$. Esto implica que

$$xy-xz=0=x(y-z)$$

Con lo cual, $y-z=0$, puesto que A es un dominio entero. Y con ello $y=z$. De forma similar, si $x\neq 0$ y $yx=zx$, entonces $yx-zx=0=(y-z)x\ \Rightarrow\ y-z=0$. Y con esto concluimos que $y=z$. ■

12.3. Subanillos e ideales

Las subestructuras desempeñan un papel importante en el estudio de los grupos y de los anillos, tal como los subconjuntos en el caso de los conjuntos.

Definición. Dado un anillo *A*, un subconjunto *S* de *A* es un subanillo de *A* si *S* es él mismo un anillo con las mismas operaciones definidas en *A*.

La propiedad 9 es fundamental para estudiar las subestructuras de un anillo.

Proposición 9. Sea *A* un anillo y *S* un subconjunto no vacío de *A*. *S* es un subanillo de *A* si y sólo si:

$$\text{(i)} \qquad x - y \in S$$

$$\text{(ii)} \qquad xy \in S$$

$\forall x, y \in S$.

Prueba. $(\Rightarrow)$ Si *S* es un subanillo de *A*, entonces es inmediato que $x - y, xy \in S$, pues ambas leyes son internas en *A*. $(\Leftarrow)$ Recíprocamente, de $x - y \in S,\ \forall x, y \in S$ se tiene que *S* es un subgrupo de *A*. Además, como el anillo *A* es, por definición, un grupo abeliano, los elementos de *S* también conmutan, así que *S* es un grupo abeliano. Como $xy \in S,\ \forall x, y \in S$ entonces la ley multiplicativa es interna en *S*. Por último, la asociatividad de la multiplicación y las leyes distributivas en *A* garantizan que estas propiedades también se verifiquen en *S*. ■

1. El anillo *A* es un subanillo de sí mismo.
2. Un subanillo de $\mathbb{Z}_6$ es $S = \left(\left\{\bar{0}, \bar{3}\right\}, +, \cdot\right)$. Observe que

$$\bar{0}-\bar{0},\bar{0}-\bar{3},\bar{3}-\bar{0},\bar{3}-\bar{3}\in S.$$

$$\bar{0}\cdot\bar{0}=\bar{0}\cdot\bar{3}=\bar{3}\cdot\bar{0},\bar{3}\cdot\bar{3}\in S$$

Entonces, por la propiedad que acabamos de probar, *S* es un subanillo de $\mathbb{Z}_6$.

3. Un subanillo de $(\mathbb{Z},+,\cdot)$ es $(2\mathbb{Z},+,\cdot)$, donde $2\mathbb{Z}=\{2x:\ x\in\mathbb{Z}\}$. (puesto que suma y el producto de números pares es un número par).
4. El conjunto, $S[x]$, de los polinomios de grado par es un subanillo de $P[x]$ sobre $\mathbb{R}$. Es claro que tal conjunto es un subconjunto no vacío de $P[x]$. Note que dados los polinomios $p,q\in S[x]$, tales que grado $p=2n\geq 2n^*=$ grado q, entonces el grado de $p-q$ es $2n$ y el grado de pq es $2n+2n^*=2(n+n^*)$. Así que tanto $p-q$ como pq están en $S[x]$. Y en virtud de la propiedad 9, $S[x]$ es un subanillo de $P[x]$.
5. El conjunto

$$S=\{M_{2\times 2}:\ m_{21}=0\}$$

es un subanillo del anillo de las matrices 2×2 sobre $\mathbb{C}$.

Esto se basa en el hecho de que la suma y el producto de *matrices triangulares superiores* es también una matriz triangular superior (los elementos "por debajo" de la diagonal principal son todos cero).
En efecto (para el caso 2×2):

$$\begin{bmatrix}a & b\\ 0 & c\end{bmatrix}+\begin{bmatrix}d & e\\ 0 & f\end{bmatrix}=\begin{bmatrix}a+d & b+e\\ 0 & c+f\end{bmatrix}\in S$$

$$\begin{bmatrix}a & b\\ 0 & c\end{bmatrix}\begin{bmatrix}d & e\\ 0 & f\end{bmatrix}=\begin{bmatrix}ad & ae+bf\\ 0 & cf\end{bmatrix}\in S$$

6. El conjunto S de números reales de la forma $a+b\sqrt{2}$, donde a y b son enteros, es un subanillo del anillo $\mathbb{R}$ con las operaciones usuales. De hecho,

$$a+b\sqrt{2}+c+d\sqrt{2}=(a+c)+(b+d)\sqrt{2}\in S$$
$$\left(a+b\sqrt{2}\right)\left(c+d\sqrt{2}\right)=(ac+2bd)+(ad+bc)\sqrt{2}\in S$$

Definición. Sea A un anillo.

(i) Si $x^2=x$, el elemento x se dice **idempotente**.

(ii) Si $x^2=x,\ \forall x\in A$, el anillo A es **booleano**.

(iii) Si $x^n=0$ para algún entero positivo n, el elemento x se dice **nilpotente**.

Definición. Sea A un anillo, un subanillo I es un ideal si y sólo si para cualquier x en A y cualquier y en I se tiene que xy y yx están en I.

1. Consideremos el anillo de los números enteros y sea P el subanillo de los números pares, es decir $P=\{n\in\mathbb{Z} \text{ tales que } n=2k, k\in\mathbb{Z}\}$. Observe que al multiplicar un entero par por *cualquier entero* se obtiene de nuevo un entero par, luego P es un ideal.

2. Los polinomios con coeficientes reales forman un anillo con respecto a la suma y productos usuales (lo veremos en detalle abajo). Consideremos el subanillo I de los polinomios que tiene a 1 como raíz, esto es

   $I=\{p(x), p \text{ polinomio con coeficientes reales tal que } p(1)=0\}$. El estudiante UNA debe verificar (ejercicio) que I verifica la condición de ideal.

3. En cualquier anillo R el conjunto definido por medio de $\{ax \text{ o } xa \text{ donde } a \text{ es un elemento fijo de } R\}$ es un ideal. Este ideal será

denotado por (a). Observe que el ideal de los números pares en el anillo de los enteros es sencillamente (2).

4. En el anillo de partes de un conjunto *X* todos los elementos son idempotentes respecto a la operación de intersección.

5. Construya matrices nilpotentes de 2 filas y dos columnas.

Los ideales surgen de manera natural a partir de los homomorfismos de anillo. Veamos esta definición.

Definición. Sean *R* y *J* dos anillos cualesquiera**.** Una función $\phi: R \to J$ es un homomorfismo si y sólo si

$$\phi(x+y) = \phi(x) + \phi(y)$$
$$\phi(xy) = \phi(x)\phi(y)$$

Para cualesquiera *x,y* en *R.*

Como el estudiante UNA puede ver el concepto es análogo al concepto de homomorfismo de grupos. La noción de núcleo del homomorfismo se define de manera similar. Definimos el núcleo del homomorfismo $\phi: R \to J$, denotado como $Ker\,\phi: R$, como $Ker\phi = \{x \in R \text{ tales que } \phi(x) = 0\}$.

Teorema 9. El $Ker\phi = \{x \in R \text{ tales que } \phi(x) = 0\}$ es un ideal del anillo *R.*

Demostración. Observe que $Ker\phi = \{x \in R \text{ tales que } \phi(x) = 0\}$ es un subanillo ya que si *x,y* están en $Ker\phi = \{x \in R \text{ tales que } \phi(x) = 0\}$ entonces $\phi(x+y) = \phi(x) + \phi(y) = 0 + 0 = 0$ y $\phi(xy) = \phi(x)\phi(y) = 0.0 = 0$. El estudiante UNA debe entender ahora por qué $Ker\phi = \{x \in R \text{ tales que } \phi(x) = 0\}$ es un ideal. Tomemos un elemento arbitrario *y* de *R* y un elemento *x* en $Ker\phi = \{x \in R \text{ tales que } \phi(x) = 0\}$. Como $\phi(xy) = \phi(x)\phi(y) = 0 \cdot \phi(y) = 0$ entonces *xy* está en $Ker\phi = \{x \in R \text{ tales que } \phi(x) = 0\}$, luego demostramos que $Ker\,\phi$ es un ideal. ■

12.4. Un anillo importante: Los polinomios

Si *A* es un anillo cualquiera podemos considerar el anillo $A[x]$ en la indeterminada *x* cuyos elementos son expresiones de la forma

$$p = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n, a_i \in A, i \in \{1, 2, \cdots, n\}$$

Muchas veces escribimos $p(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$ para denotar un polinomio.

 Cualquier polinomio induce una función

$$p : A \to A$$
$$p(x_0) = a_0 + a_1 x_0 + a_2 {x_0}^2 + \cdots + a_n {x_0}^n, a_i \in A, i \in \{1, 2, \cdots, n\}$$

El polinomio p no debe confundirse con la función polinómica asociada. Por ejemplo, consideremos los polinomios en $\mathbb{Z}_2$, esto es $\mathbb{Z}_2[x]$. La función polinómica

$$p : \mathbb{Z}_2 \to \mathbb{Z}_2$$
$$p(x) = x + 1$$

Es exactamente igual a la función polinómica

$$q : \mathbb{Z}_2 \to \mathbb{Z}_2$$
$$q(x) = x^2 + 1$$

Esto se ve fácilmente ya que $p(0) = q(0) = 1, p(1) = q(1) = 0$ y $\mathbb{Z}_2$ sólo tiene 2 elementos: 0 y 1. Sin embargo, los polinomios *p* y *q* son completamente distintos. El estudiante debe leer esta advertencia con cuidado y de ser necesario discutirla con su asesor.

Dos elementos *p* y *q* de $A[x]$,

$$p = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n, q = b_0 + b_1 x + b_2 x^2 + \cdots + b_m x^m$$

se identifican si y sólo si $m=n$ y cada a_i coincide con b_i para cualquier natural *i entre* 1 y *n.* El estudiante recuerda que las expresiones de $A[x]$ son denominadas

polinomios con coeficientes en el anillo *A.* El término polinomio deriva de "poli"(muchos) y "nomos"(reglas).

El mayor exponente de la indeterminada x que aparece en el polinomio p se denomina el grado del polinomio p y lo denotamos por deg(p). El estudiante UNA podría señalar que necesitamos definir dos leyes de composición para poder tener la estructura de anillo en $A[x]$. Esto lo hacemos tal como el estudiante lo realizó en bachillerato, en primer lugar definimos la suma de polinomios *p,q* por medio de

$$p+q=\left(a_0+a_1x+a_2x^2+\cdots+a_nx^n\right)+\left(b_0+b_1x+b_2x^2+\cdots+b_mx^m\right)=$$
$$\left(a_0+b_0\right)+\left(a_1+b_1\right)x+\cdots+\left(a_n+b_n\right)x^n$$

Aquí supusimos que *n>m* y completamos las potencias de *q* hasta *n* por medio de términos de coeficiente 0.

1. Demuestre que $A[x]$ con esta operación es un grupo abeliano.

   Igualmente se define la multiplicación de dos polinomios como lo hicimos en bachillerato. En efecto sean $p=a_0+a_1x+a_2x^2+\cdots+a_nx^n, q=b_0+b_1x+b_2x^2+\cdots+b_mx^m$ dos polinomios cualesquiera. Entonces su producto *m* es el polinomio dado por

$$c_0+c_1x+c_2x^2+\cdots+c_ix^i+\cdots+c_{n+m}x^{n+m}, c_i\in A$$
$$c_i=\sum_{j+r=i}a_jb_r$$

1. Demuestre que $A[x]$ es un anillo con las operaciones antes definidas y que el polinomio 1 es el elemento neutro para la multiplicación definida.

2. Demuestre que $A[x]$ es un dominio de integridad si *A* lo es.

El resto de esta sección nos restringiremos a considerar polinomios sobre anillos muy conocidos: $\mathbb{Z}, \mathbb{Q}$ y $\mathbb{R}$.

Es muy importante recordar cómo dividimos, cuando es posible, polinomios. El comportamiento de la división de polinomios es similar al de los números enteros y vale una versión del algoritmo de Euclides. Es conocido como el algoritmo de Euclides para polinomios. Veamos su enunciado con precisión. Si tenemos dos polinomios *p* y *q, con el grado de p mayor o igual al de q,* entonces existen dos polinomios *únicos c* y *r* tales que

$$p(x) = q(x)c(x) + r(x)$$

Donde el grado de *r es menor que el grado de q. Los polinomios c y r se denominan, respectivamente, cociente y resto de la división de p por el polinomio q.*

La unicidad debe ser clara ya que si existiese otra descomposición $p(x) = q(x)c_1(x) + r_1(x)$ verificando que el grado de r_1 es menor que el grado de *q* entonces, igualando $p(x) = q(x)c(x) + r(x) = c(x)(x-a) + r(x)$ vemos que

$$r_1(x) - r(x) = q(x)(c_1(x) - c(x))$$

Pero el lado izquierdo es un polinomio de grado menor que el de *q*. El estudiante UNA debe decir por qué. Así, $(c_1(x) - c(x))$ debe ser el polinomio nulo y por ende $c_1(x) - c(x) = 0$ y $r_1(x) - r(x) = 0$. La forma de obtener los polinomios *c* y *r* se basa en el procedimiento estudiado en el bachillerato y que se conoce como división larga. Recomendamos al estudiante UNA que no recuerde este proceso que debe repasarlo (puede ver el libro de Matemática y el buen vivir, Quinto año, Colección Bicentenario).

1. Hallar el cociente y el resto de dividir $p(x) = x^3 - x^2 + x - 1$ por $q(x) = x - 1$. En este caso podemos aplicar el Teorema de Ruffini(ver texto Matemática y el buen vivir, quinto año, colección Bicentenario). Este indica que *c*(*x*)= $x^2 + 1$ y

el resto es 0. Como práctica adicional invitamos al estudiante a calcular el resultado mediante una división larga.

Definición. Un polinomio $p(x) \in K[x]$ se denomina divisible por el polinomio $q(x)$, donde el grado de q es menor o igual que el grado de p, si y sólo si $p(x) = q(x)\, c(x)$.

1. Definimos un orden < en los polinomios mediante $q<p$ si y sólo si q divide a p. Demuestra que < es de hecho una relación de orden.

Recordamos el siguiente resultado por ser básico en Álgebra.

Teorema (del resto). El resto de dividir un polinomio $p(x)$ por el polinomio $x-a$ es $p(a)$.

Demostración. Por el algoritmo de Euclides se tiene que $p(x) = c(x)(x-a)+r(x)$ donde $r(x)$ debe ser constante y denotaremos $r(x)$ por su valor constante r. Luego, especializando la variable x por a entonces $p(a) = c(a)(a-a)+r(a) = r$. Esto concluye la demostración.

Un elemento a del anillo A se denomina una raíz del polinomio p en $A[x]$ si y solamente si $p(a)=0$. □

1. El polinomio x^2+1 no tiene raíces en el anillo $\mathbb{R}$ pero si en el anillo $\mathbb{C}$. El estudiante UNA debe explicar las razones que justifican lo afirmado.

2. El polinomio $p(x) = x^3 - 2x - 4$ admite a 2 como raíz.

Así, un polinomio p es divisible por $x-a$ si y sólo si *a es una raíz del polinomio p.*

Un concepto importante es el de polinomio irreducible en un cierto anillo. Tomemos el polinomio x^2-2. Este polinomio no se puede descomponer en $\mathbb{Q}[x]$ como un producto de polinomios de grado 1 ya que las raíces de x^2-2 son $\pm\sqrt{2} \notin \mathbb{Q}$. Sin

embargo, en el anillo de polinomios $\mathbb{R}[x]$ se tiene que $x^2-2=\left(x-\sqrt{2}\right)\left(x+\sqrt{2}\right)$. Vamos a la definición de polinomio irreducible después de esta breve discusión la definición de polinomio irreducible.

Definición. Un polinomio $p(x) \in K[x]$ es irreducible *en el anillo* $K[x]$ si y sólo si no se pueden encontrar dos polinomios no constantes $p_1(x)$, $p_2(x)$ tales que $p(x)= p_1(x)p_2(x)$.

Debe ser claro por nuestra discusión que el concepto de irreducibilidad depende del anillo en que estemos trabajando.

1. El polinomio $m(x)=x^2+1$ es irreducible en el anillo $\mathbb{R}[x]$ pero no lo es en el anillo $\mathbb{C}[x]$ ya que $m(x)=x^2+1=(x-i)(x+i)$.

En el anillo $K[x]$ los polinomios irreducibles juegan el mismo papel que los números primos en los enteros $\mathbb{Z}$.

El siguiente teorema lo usaremos en la unidad siguiente sobre la teoría de cuerpos y proporciona un criterio importante para determinar si un polinomio es irreducible en el anillo $\mathbb{Z}[x]$.

Teorema. (Criterio de Eisenstein) Sea $q(x)=a_0+a_1x+a_2x^2+\cdots+a_nx^n$ un polinomio con coeficientes enteros y supongamos que exista un número primo p que verifica: p/a_i para cualquier $i \neq n$ y p^2 no divide a a_0 entonces $q(x)=a_0+a_1x+a_2x^2+\cdots+a_nx^n$ es irreducible en $\mathbb{Z}[x]$.

Demostración. Vamos a usar cosas elementales de la *aritmética módulo p* y razonaremos por reducción al absurdo. Supongamos que q se descompone como

$$q(x)=g(x)h(x), g \in \mathbb{Z}[x], h \in \mathbb{Z}[x]$$

donde los polinomios $g(x), h(x)$ son no constantes, es decir suponemos que el polinomio $q(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$ es reducible. Considere ahora a cada polinomio $g(x), h(x)$ módulo p, es decir tomamos los polinomios $\bar{q}(x) = \bar{a}_0 + \bar{a}_1 x + \bar{a}_2 x^2 + \cdots + \bar{a}_n x^n$ donde cada coeficiente es un residuo módulo p del correspondiente coeficiente del polinomio original. Es claro que

$$\bar{q}(x) = \bar{g}(x)\bar{h}(x), g \in \mathbb{Z}_p[x], h \in \mathbb{Z}_p[x]$$

Por hipótesis del teorema, todos los coeficientes de $\bar{q}(x) = \bar{a}_0 + \bar{a}_1 x + \bar{a}_2 x^2 + \cdots + \bar{a}_n x^n$, salvo el coeficiente principal $\bar{a}_n$, se anulan módulo p ya que p / a_i para cualquier $i \neq n$, luego $\bar{q}(x) = \bar{a}_n x^n$. Pero esto implica que tanto $\bar{g}(x) = \bar{a} x^r$ como $\bar{h}(x) = \bar{b} x^t, r + t = n$. Luego, los términos independientes de ambos polinomios $\bar{g}(x), \bar{h}(x)$ deben ser 0 módulo p. Si llamamos $\bar{b}_0, \bar{c}_0$ estos términos independientes entonces p divide a b_0 y p divide a c_0. Pero esto implica que p^2 divide a a_0 ya que $a_0 = b_0 c_0$, un absurdo que concluye la demostración. □

Se puede demostrar de manera sencilla y análoga el *lema de Gauss* que afirma que si un polinomio con coeficientes enteros se factoriza de manera no trivial en el anillo $\mathbb{Q}[x]$ entonces admite una factorización no trivial en $\mathbb{Z}[x]$. No demostraremos este teorema que se puede encontrar en el libro Herstein, *Álgebra Moderna.*

1. El polinomio $P(x) = x^2 - 2$ es irreducible en $\mathbb{Q}[x]$. Apliquemos el criterio de Eisenstein para ver esto. En efecto, como 2 divide a -2, 2 divide a 0, 2 no divide a 1 y 4 =2^2 no divide a -2, el criterio de Einsenstein indica que no podemos factorizar $P(x) = x^2 - 2$ en $\mathbb{Z}[x]$ pero el lema de Gauss implica que la factorización no se puede hacer, de manera no trivial, en $\mathbb{Q}[x]$.

2. El polinomio $q(x) = x^2 + x + 1$ es irreducible en $\mathbb{Z}[x]$. En este ejemplo no podemos aplicar directamente el Teorema de Eisenstein y usaremos un bonito

truco. Consideremos el polinomio p en la indeterminada t definido por $p(t)=q(t+1)=(t+1)^2+t+1+1=t^2+3t+3$. El estudiante UNA debe aplicar el criterio de Eisenstein para demostrar que $p(t)$ es irreducible. Concluya a partir de aquí que $q(x)=x^2+x+1$ debe ser también irreducible.

1. Demuestre que el polinomio $R(x)=3x^4+10x-15$ es irreducible en $\mathbb{Z}[x]$.
2. Use el criterio de Eisenstein para demostrar que $\sqrt{2}$ es irracional. Sugerencia: ¿Cómo se puede interpretar lo hecho en el ejemplo 1. arriba?.
3. Use el criterio de Eisenstein para demostrar que $\sqrt{n}$ es irracional para cualquier n natural que se escribe como producto de *p,q* primos distintos.
4. Demuestre que si *a* es una raíz de *p* donde *p* es un polinomio con coeficientes enteros, es decir *p* pertenece a $\mathbb{Z}[x]$ entonces *a* divide al termino independiente de *p* si este es no nulo.
5. Indique las posibles raíces enteras del polinomio $P=12-x^2-x^3$. Encuentre cuales efectivamente son raíces.

1. Vemos que 5 divide a -15 y a 10, además no divide a 3. Por otro lado 25 =5^2 , luego podemos aplicar el criterio de Eisenstein para concluir que $R(x)=3x^4+10x-15$ es irreducible en $\mathbb{Z}[x]$.
2. El polinomio $P(x)=x^2-2$ es irreducible en $\mathbb{Q}[x]$ como ya vimos, luego no puede tener raíces racionales, de donde $\sqrt{2}$ es irracional.
3. Al ser n un natural que se escribe como pq con primos distintos, podemos considerar el polinomio $P(x)=x^2-pq$ que es irreducible por el criterio de Eisenstein, el estudiante UNA debe suplir los detalles que corroboran esta

afirmación. Luego, $\sqrt{n}$ es irracional ya que $P(x)=x^2-pq$ no puede tener una raíz racional ya que, de lo contrario, se factorizaría en $\mathbb{Q}[x]$.

4. Observe que *p* se escribe como $b_0+b_1x+b_2x^2+\cdots+b_nx^n$ donde todos los coeficientes de *p* son números enteros. Como *a* es una raíz de *p* tenemos $b_0+b_1a+b_2a^2+\cdots+b_na^n=0$ y de acá, factorizando *a* se tiene $b_0=-a(b_1+b_2a+\cdots+b_na^{n-1})$ que nos dice que *a* divide al termino independiente de *p* como afirmamos.
5. Se lo dejamos al estudiante UNA ya que solamente debe aplicar el problema 4 y realizar unos cálculos muy simples.

Es un hecho muy importante que cualquier polinomio con coeficientes en los números complejos se puede factorizar completamente en factores lineales. Esto es una consecuencia del Teorema Fundamental del Álgebra que enunciamos pero cuya demostración la estudiará el alumno de la Licenciatura en Matemáticas en su curso de Análisis II (766). Luego en los complejos los únicos polinomios irreducibles son los de grado menor o igual a 1.

Teorema (Fundamental del Álgebra). Todo polinomio no constante con coeficientes complejos posee al menos una raíz compleja.

Así, si tenemos el polinomio, no constante de grado *n*, *p* con coeficientes complejos entonces $p=a_n(z-z_0)(z-z_1)\cdots(z-z_n)$. Puede ocurrir que algunos z_i coincidan y en este caso tenemos una raíz múltiple.

Es un hecho muy importante en las aplicaciones que si un polinomio $p(x)=a_0+a_1x+a_2x^2+\cdots+a_nx^n$ con coeficientes reales admite una raíz compleja *a*+*ib* debe entonces admitir como raíz el conjugado de *a*+*ib*, esto es, *a*-*ib*. Esto se deduce de que $p(a+ib)=a_0+a_1(a+ib)+a_2(a+ib)^2+\cdots+a_n(a+ib)^n=0.$ Luego, tomando conjugados a ambos lados se tiene que

$$a_0+a_1(a-ib)+a_2(a-ib)^2+\cdots+a_n(a-ib)^n=0.$$

Esto es consecuencia que la operación de conjugado no afecta a los números reales.

1. Suponga que tiene un polinomio *p* mónico de tercer grado con coeficientes reales que admite a 1 y 1-*i* como raíces, ¿puede usted escribir el polinomio *p*?.
2. Factorice el polinomio x^5-1 en $\mathbb{C}[x]$.

1. Al tener el polinomio coeficientes reales y admitir la raíz compleja 1-i debe tener a 1+i raíz , luego $(x-(1+i))(x-(1-i))$ divide a *p*. Como $(x-1)$ divide a *p* y este polinomio es mónico entonces
   $p=(x-(1+i))(x-(1-i))(x-1)$
   $=((x-1)^2+1)(x-1)=(x-1)^3+(x-1)$
2. Lo dejamos al estudiante UNA ya que es un ejercicio de cuarto año de bachillerato.

1. ¿Qué otros ejemplos de anillo puede dar?
2. ¿Es $(\mathbb{Z}^+,+,\cdot)$ un anillo? ¿Y $(n\mathbb{Z},+,\cdot)$? (en ambos la adición y la multiplicación son las usuales).
3. Pruebe que el conjunto $A=\{f:[0,1]\to\mathbb{R}:\ f\ es\ una\ función\ continua\}$ es un anillo conmutativo con identidad respecto a la suma y productos usuales de funciones.
4. Considere el anillo $P(\mathbb{N})$, con la adición y multiplicación definidas como sigue:

$$A+B=(A\cup B)-(A\cap B)=A\Delta B$$

$$A\cdot B=A\cap B$$

Ud. no tiene que demostrar que $P(\mathbb{N})$ es un anillo. ¿Tiene $P(\mathbb{N})$ divisores de cero?

5. Pruebe la propiedad asociativa de la multiplicación en $\mathbb{Z}_n$.
6. Para cada uno de los siguientes anillos determine el grupo que consta de sus elementos inversibles.

   (a) $(\mathbb{Z},+,\cdot)$

   (b) $(\mathbb{R},+,\cdot)$

   (c) $(\mathbb{Z}_{12},+,\cdot)$

   (d) $\mathbb{Z}[i]=\{a+bi:\ a,b\in\mathbb{Z}\}$ con la adición y la multiplicación usuales en $\mathbb{C}$.

7. El subanillo $S=\left(\{\bar{0},\bar{3}\},+,\cdot\right)$ de $\mathbb{Z}_6$, ¿tiene identidad? ¿tiene elementos inversibles?
8. ¿Tiene $\mathbb{Z}[i]$ elementos inversibles?
9. ¿Cuáles son todos los subanillos de $\mathbb{Z}_6$? ¿Y los de $\mathbb{Z}_9$? (De seguidas mostramos la tabla multiplicativa de $\mathbb{Z}_9$).

·	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	$\bar{8}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	$\bar{8}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{6}$	$\bar{8}$	$\bar{1}$	$\bar{3}$	$\bar{5}$	$\bar{7}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{6}$	$\bar{0}$	$\bar{3}$	$\bar{6}$	$\bar{0}$	$\bar{3}$	$\bar{6}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{8}$	$\bar{3}$	$\bar{7}$	$\bar{2}$	$\bar{6}$	$\bar{1}$	$\bar{5}$
$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{1}$	$\bar{6}$	$\bar{2}$	$\bar{7}$	$\bar{3}$	$\bar{8}$	$\bar{4}$
$\bar{6}$	$\bar{0}$	$\bar{6}$	$\bar{3}$	$\bar{0}$	$\bar{6}$	$\bar{3}$	$\bar{0}$	$\bar{6}$	$\bar{3}$
$\bar{7}$	$\bar{0}$	$\bar{7}$	$\bar{5}$	$\bar{3}$	$\bar{1}$	$\bar{8}$	$\bar{6}$	$\bar{4}$	$\bar{2}$
$\bar{8}$	$\bar{0}$	$\bar{8}$	$\bar{7}$	$\bar{6}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

10. Muestre un ejemplo de un anillo *A* con identidad y de un subanillo *S* de éste cuya identidad sea distinta a la identidad de *A*.
11. Pruebe las propiedades 4 y 5 del texto.
12. Sea *A* un anillo. Demuestre que $S = \{x \in A : ax = xa\}$ para un elemento *a* fijo es un subanillo de *A*.
13. ¿Tiene $(\mathbb{R}, +, \cdot)$ elementos idempotentes? ¿Tiene elementos nilpotentes?
14. Dé ejemplos o construye anillos booleanos.
15. Sean *S* y *T* subanillos de *A*. Muestre que no es cierto en todos los casos que $S \cup T$ es un subanillo de *A*. ¿En qué casos es cierto?
16. Fijemos un elemento *j* en el anillo *A*.

    (a) ¿Es $jA = \{jx : x \in A\}$ un subanillo de *A*?

    (b) ¿Es $A_j = \{x : xj = 0\}$ un subanillo de *A*?

17. Sean *S* y *T* subanillos de de *A*. Sea además el **conjunto suma**

$$S + T = \{s + t : s \in S, t \in T\}$$

que consta de los elementos de *A* que se puedes escribir como la suma de un elemento de *S* con un elemento de *T*. ¿es $S + T$ un subanillo de *A*?

18. El conjunto

$$S = \{M_{2\times 2} : m_{11} = m_{22} = 0\}$$

¿Es un subanillo del anillo de las matrices 2×2 sobre $\mathbb{C}$?

19. Demuestre que el polinomio $p(x) = x^3 - 2$ es irreducible en $\mathbb{Q}[x]$.
20. Construya un polinomio que sea irreducible en $\mathbb{Q}[x]$ pero que no lo sea en $\mathbb{R}[x]$.

21. Determine la estructura de los ideales de $\mathbb{Z}$.
22. Demuestre que cualquier polinomio de coeficientes reales y de grado 3 es reducible en $\mathbb{R}[x]$.
23. Factorice, si es posible, en $\mathbb{R}[x]$ el polinomio $p(x) = x^4 + 1$.
24. Generalice el resultado del problema 23. a cualquier polinomio de grado impar mayor o igual que 3.

1. Consideremos el conjunto *R*[x] de todas las funciones racionales $\frac{p(x)}{q(x)}$ donde *p*,*q* son polinomios y *q* no es el polinomio nulo. Si definimos la suma y producto usual de funciones entonces *R*[x] es otro ejemplo de anillo.
2. En este caso los conjuntos considerados no son grupos abelianos respecto a la suma, luego no pueden ser anillos.
3. Recordamos al estudiante UNA un resultado básico de Cálculo Diferencial, la suma y producto usuales de funciones continuas es una función continua. Luego, las leyes de composición interna consideradas están bien definidas. Es claro que estas leyes de composición interna verifican las propiedades algebraicas usuales como la propiedad asociativa para la suma, ya que esta propiedad se verifica en general y estamos trabajando con una parte de las funciones de [0,1] en los reales.

Por favor reflexione sobre esta última afirmación que le puede ayudar a simplificar su trabajo en otros problemas.

La función idénticamente 0 en el intervalo [0,1] juega el papel del elemento neutro para la suma. Si *f* es una función continua es claro que –*f* es de nuevo continua y que *f*+(-*f*)=0, luego toda función admite un inverso para la suma. Luego, el conjunto considerado con respecto a la suma definida es un grupo abeliano. Dejamos al estudiante UNA demostrar, de manera similar, las

propiedades respecto al producto usual de funciones que se necesiten para completar el problema.

4. El conjunto $P(\mathbb{N})$ es el conjunto de todas las partes de los números naturales $\mathbb{N}$, es decir los elementos de $P(\mathbb{N})$ son conjuntos de números naturales como, por ejemplo, {0}, {0,2,3} o el conjunto de todos los números pares. Es claro que el conjunto vacío ϕ es el elemento neutro para la suma definida ya que $A+\phi=(A\cup\phi)-(A\cap\phi)=A-\phi=A$. Observe que si A es un subconjunto no vacío cualquiera de $\mathbb{N}$ que no sea el propio $\mathbb{N}$ entonces su complemento A^c no es ni el ϕ ni $\mathbb{N}$, además $AA^c=\phi$, de donde concluimos que si existen divisores de 0.
5. Se lo dejamos al estudiante UNA.
6. Ya sabemos por la **Proposición 6**. demostrada en esta Unidad que el conjunto de todos los elementos invertibles de un anillos dado es un grupo multiplicativo. Consideremos algunos de los conjuntos propuestos.
   a) En $(\mathbb{Z},+,\cdot)$ el único elemento invertible es la propia unidad 1, luego el grupo es el grupo trivial {1}. El estudiante UNA debe indicar claramente por qué no hay otros elementos invertibles en $\mathbb{Z}$.
   b) En $(\mathbb{R},+,\cdot)$ la situación es mucho más interesante, en los reales si x no es 0 entonces siempre existe $1/x$, luego el grupo de los elementos invertibles es $(\mathbb{R}^*,\cdot)$.
   c) Veamos el caso $\mathbb{Z}_{12}$, se puede verificar sin problemas que cualquier elemento que sea coprimo con 12 genera una clase invertible.
   d) Los únicos elementos invertibles en los enteros gaussianos son el conjunto formado por {1,-1,i,-i}, el estudiante UNA debe hacer la tabla multiplicativa de este grupo como ejercicio adicional.

7. El subanillo $S=(\{\bar{0},\bar{3}\},+,\cdot)$ de $\mathbb{Z}_6$ verifica algo muy interesante, tenemos que $\bar{3}\bar{3}=\bar{3}$ luego la clase del 3 funciona como una identidad y por la ecuación anterior la clase del 3 es invertible. Observe que en el anillo $\mathbb{Z}_6$ la identidad es

la clase del 1, luego puede ocurrir que en un subanillo se tenga otra identidad, distinta a la del anillo original.

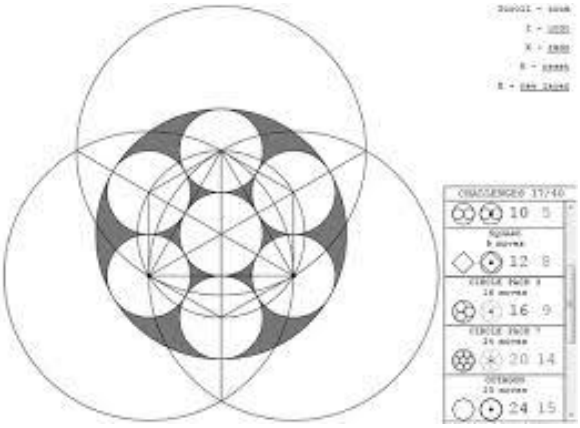
8. Los elementos 1,-1,i,-i son todos invertibles.
9. Vamos a hacer en detalle el caso de $\mathbb{Z}_6$ dejando al estudiante UNA el caso de $\mathbb{Z}_9$. Cualquier subanillo debe ser en primer lugar un subgrupo respecto a la suma definida, y como $\mathbb{Z}_6$ es un grupo cíclico, entonces el subanillo es un subgrupo cíclico (ver Unidad de Grupos para los detalles). Es claro que la clase de 0 genera un subanillo trivial, el {0}. Lo mismo ocurre para la clase del 1 que genera todo el anillo $\mathbb{Z}_6$. Son los subanillos triviales de $\mathbb{Z}_6$. Veamos qué ocurre con el grupo generado por la clase de 2, $\overline{2}$. Un corto cálculo nos dice que es el grupo cíclico $\{\overline{0},\overline{2},\overline{4}\}$. Es claro que tal grupo es cerrado respecto a la multiplicación y que constituye un subanillo de $\mathbb{Z}_6$. La clase del 3 fue estudiada en el ejercicio 7. Una corta reflexión del estudiante UNA lo convencerá de que el subanillo que genera la clase del 4 es el mismo $\{\overline{0},\overline{2},\overline{4}\}$. Al ser 5 coprimo con 6 entonces la clase del 5 genera de nuevo todo el anillo.
10. Revise lo hecho en el ejercicio 7, después puede pensar en algún otro ejemplo.
11. Esto le fue dejado como ejercicio y Ud. debe hacerlo
12. El conjunto en cuestión está formado por todos los elementos que conmutan con *a*. Por los ejercicios de la Unidad de Grupos ya el estudiante conoce que esto es un subgrupo del anillo (es el centro de *a* que denotamos *C*(*a*), vea la Unidad de Grupos si tiene alguna duda). Veamos ahora que *C*(*a*) es cerrado respecto a la multiplicación, sean *x,y* en *C*(*a*) entonces $(xy)a = x(ya) = x(ay) = (xa)y = a(xy)$, de donde *xy* esta en *C*(*a*) y se tiene el resultado deseado por la Propiedad 9 de esta Unidad.
13. El elemento identidad de cualquier anillo, si existe, es idempotente. Luego, 1 es un real idempotente. La ecuación x^2 =1 indica que -1 es también un elemento idempotente, estos son los dos únicos elementos idempotentes de $\mathbb{R}$. No hay elementos nilpotentes no nulos ya que $\mathbb{R}$ es un dominio de integridad.
14. Un ejemplo de anillo boleano es el conjunto de partes $P(X)$ de cualquier conjunto X con las operaciones $A+B = A\cup B-(A\cap B) = A\triangle B$ y

$A \bullet B = A \cap B$. Como $A \bullet A = A \cap A = A$ el anillo es boleano. Otro ejemplo, muy importante en las aplicaciones en computación, es el anillo $\mathbb{Z}_2$. Complete los detalles en este caso para demostrar que este anillo es boleano.

15. Sean *S* y *T* subanillos del anillo de los números enteros. Por ejemplo, *S* es el anillo de los números pares y *T* es el anillo de todos los múltiplos de 3. Es claro que si unimos estos conjuntos esto no es un subanillo ya que 2+3=5 que no se encuentra ni en *S* ni en *T.* Debe ser claro para el estudiante UNA que si *S* está incluido en *T* si se tiene que su unión, que es *T*, si es un subanillo.
16. a) Si es un subanillo que podemos llamar el subanillo de los múltiplos de *j*. Observe que *jA* es cerrado si tomamos la diferencia de dos elementos y también cerrado por el producto. Por favor, demuestre estos hechos. Una reflexión adicional indica que *jA* es de hecho un ideal. La respuesta de b) es negativa, piense la razón.
17. Tenemos que verificar que si *x,y* están en *S+T* entonces *x-y* y *xy* están en *S+T*. Si *x,y* están en *S+T* entonces *x=s+t, y=u+v* donde *s* y *u* están en *S* y *t* y *v* están en *T.* Luego, *x-y*=(*s*+*t*)-(*u*+*v*)=(*s*-*u*)+(*t*-*v*) que está en *S+T* ya que *s-u* es un elemento de *S* y *t-v* es un elemento de *T.* Lo que no es cierto es que *S+T* sea cerrado para el producto. Invitamos al estudiante UNA encontrar un ejemplo. Lo que sí es cierto y se deja como un ejercicio adicional al estudiante UNA es que si *S,T* son ideales entonces *S+T* es un ideal.
18. Este atento con este ejemplo, por ejemplo consideremos la matriz $J = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$ entonces $J \cdot J = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$ que no pertenece al conjunto considerado.
19. Se aplica directamente el criterio de Einsenstein. Este resultado tiene implicaciones importantes en el problema clásico de la duplicación del cubo.
20. Sea *I* cualquier ideal de los enteros $\mathbb{Z}$ y sea *p* el menor entero positivo en *I.* Es claro que, por propiedades de anillo, cualquier múltiplo de *p* se encuentra en *I.* Ahora si *m* pertenece a *I* y *m* es positivo, el algoritmo de Euclides implica que *m=cp+r* donde *r* es positivo y *r<p* pero *r=m-cp* y de aquí se deduce que *r* debe estar en *I.* Pero, por definición de *p* como el menor entero positivo de *I*, entonces *r*=0, es decir *todo elemento de I es un múltiplo de p,* es decir, $I=(np)_n$ entero ▪

21. Basta ver que todo polinomio de grado 3 con coeficientes reales tiene una raíz real x_0. El estudiante UNA debe calcular los límites del polinomio en ∞ y en $-\infty$ y observar que son de signos distintos, de donde aplicando el teorema del valor medio del cálculo diferencial se obtiene el resultado.
22. El hecho de cualquier polinomio con coeficientes reales que admita una raíz compleja z deba admitir como raíz la conjugada $\overline{z}$ implica que el polinomio considerado admite factores cuadráticos. En efecto, el teorema fundamental del álgebra implica que cualquier polinomio con coeficientes reales, no constante, tiene al menos una raíz compleja, digamos $z = a + ib$ implica que $\overline{z} = a - ib$ es también raíz. Luego, $\big(x-(a+ib)\big)(x-(a-ib))$ divide al polinomio considerado, si b es no nulo. Pero $\big(x-(a+ib)\big)(x-(a-ib)) = \big(x-a\big)^2 + b^2$ que es un polinomio cuadrático con coeficientes reales.
23. Queda como ejercicio para el estudiante UNA, piense en lo que hizo en el problema 21 y como trasladarlo a este caso.

UNIDAD 9



Cuerpos

Semana 15,16

Aplicar el concepto de cuerpo en la resolución de problemas, en el modelado matemático y en la demostración de nuevos resultados.

Contenidos a tratar: El concepto de cuerpo, ejemplos de cuerpos. Cuerpos finitos. Extensiones y subcuerpos. Números constructibles. Construcción canónica de un cuerpo a partir de una anillo.

13.1. Introducción

El concepto de cuerpo generaliza la idea de conjunto de “fracciones”generado por un anillo dado. Como el estudiante UNA recordará el conjunto $\mathbb{Q}$ se obtenía a partir del anillo de los enteros $\mathbb{Z}$ de forma de lograr que $\mathbb{Q}$ sea un grupo tanto para la adición como para el producto (al eliminarle el 0). Luego, un cuerpo es una estructura más rica que un anillo ya que en un cuerpo *podemos dividir elementos arbitrarios*. El concepto de cuerpo permitió resolver uno de los problemas más importantes del

mundo antiguo: el de las construcciones con reglas y compás. Además, fue fundamental en la Teoría de Galois[1]. Además, los conjuntos fundamentales del análisis matemático son los números reales y complejos y ambos tienen la estructura de cuerpo. Todo ello indica que el concepto de cuerpo y su construcción es fundamental en el estudio de la matemática y sus aplicaciones. Es el tema que pasamos a estudiar en nuestro curso Álgebra I.

13.2. El concepto de Cuerpo

Vamos a dar la definición central en este capítulo.

Definición. Sea K un conjunto dotado de dos leyes de composición, una adición + y un producto $\cdot$ tales que se verifican las condiciones siguientes:

1. K es un grupo abeliano o conmutativo respecto a la adición +.
2. $K-\{0\}=K^*$ es un grupo respecto al producto $\cdot$.
3. El producto $\cdot$ verifica la ley distributiva respecto a la adición: $a\cdot(b+c)=a\cdot b+a\cdot c$ para elementos cualesquiera de K.

 En muchos textos se asume que el producto en el cuerpo debe ser conmutativo. Nosotros no hemos hecho esa suposición. De esa manera podemos incluir el importante ejemplo de los cuaternios de Hamilton como un cuerpo.

 Muchas veces escribiremos ab en lugar de $a\cdot b$ para indicar el producto de dos elementos a y b de K.

Como siempre indicamos que una definición debe venir acompañada de ejemplos.

---

[1] Se pronuncia galuá

[2] Una demostración de este hecho importante puede ser encontrada en el libro *Calculus* de M. Spivak.

1. El conjunto $\mathbb{Q}$ con respecto a la adición y producto usual de racionales es un cuerpo. Recomendamos al estudiante ir a la unidad de los números racionales para los detalles.

2. Los números reales $\mathbb{R}$ son un cuerpo con respecto a la adición y producto usual de reales. Vaya a la unidad de los números reales si tiene que aclarar algún punto sobre esta afirmación.

3. El conjunto de los enteros $\mathbb{Z}$ no es un cuerpo respecto a la adición y producto usual de enteros. Recuerde que en $\mathbb{Z}$ no es cierto que cualquier elemento tenga un inverso multiplicativo, por ejemplo, usted no puede resolver la ecuación $2x=1$ en $\mathbb{Z}$.

4. El conjunto $\mathbb{Z}_p$ con p primo es un cuerpo. A diferencia de los dos primeros ejemplos arriba, $\mathbb{Z}_p$ es un cuerpo finito. Recordamos que es fundamental que tomemos los enteros módulo p con p primo ya que no es cierto que el anillo $\mathbb{Z}_n$ sea un cuerpo para n natural arbitrario.

5. El conjunto de los números complejos $\mathbb{C}$ es un cuerpo. Recordamos que un número complejo z es un número de la forma $a+bi$. El estudiante de matemática estudiará los complejos en detalle en su curso Análisis II, cod. 766. Antes de pasar al siguiente ejemplo, quiero calcular el inverso multiplicativo de un complejo cualquiera no nulo, $z=a+bi$, es decir, queremos calcular $\frac{1}{a+bi}$. Esto lo hacemos como en bachillerato multiplicando, el numerador y denominador, por el conjugado de z, $\overline{z}=a-bi$. Obtenemos $\frac{1}{a+bi}\frac{a-bi}{a-bi}=\frac{a-bi}{a^2-(bi)^2}=\frac{a-bi}{a^2+b^2}$. Repetiremos este tipo de idea cuando tratemos el ejemplo de los cuaternios.

6. Consideremos el conjunto $\mathbb{Q}\left[\sqrt{2}\right]$ definido mediante

$$\mathbb{Q}\left[\sqrt{2}\right]=\left\{a+b\sqrt{2}\text{ donde } a,b\in\mathbb{Q}\right\}$$

Luego, $1+\sqrt{2}$, 3 y $2\sqrt{2}$ son algunos elementos de $\mathbb{Q}\left[\sqrt{2}\right]$. Dos elementos $a+b\sqrt{2},a_1+b_1\sqrt{2}\in\mathbb{Q}\left[\sqrt{2}\right]$ se identifican si y sólo si $a=a_1,b=b_1$. Esto se debe a que si $a+b\sqrt{2}=a_1+b_1\sqrt{2}\Rightarrow a-a_1=\sqrt{2}(b_1-b).$ Luego, $b_1-b=0$ ya que de lo contrario $\sqrt{2}=\dfrac{a-a_1}{b_1-b}\in\mathbb{Q}$ lo cual es absurdo. Pero si $b_1-b=0$, como $a-a_1=\sqrt{2}(b_1-b)$ entonces $a-a_1=0$. Así, $a=a_1,b=b_1$ como afirmamos.

Vamos a definir en $\mathbb{Q}\left[\sqrt{2}\right]$ una operación de adición y una multiplicación de manera natural y estudiaremos si $\mathbb{Q}\left[\sqrt{2}\right]$ con estas operaciones es un cuerpo. La adición se define por medio de

$$\left(a+b\sqrt{2}\right)+\left(a_1+b_1\sqrt{2}\right)=\left(a+a_1\right)+(b+b_1)\sqrt{2},$$

donde $a+b\sqrt{2},a_1+b_1\sqrt{2}\in\mathbb{Q}\left[\sqrt{2}\right]$. Demostremos que $\mathbb{Q}\left[\sqrt{2}\right]$ con esta adición es un grupo abeliano. En primer lugar, la adición es una ley de composición interna ya que $\left(a+a_1\right)+(b+b_1)\sqrt{2}$ está en $\mathbb{Q}\left[\sqrt{2}\right]$ si $a+b\sqrt{2},a_1+b_1\sqrt{2}$ están en $\mathbb{Q}\left[\sqrt{2}\right]$. El elemento $0+0\sqrt{2}$ está en $\mathbb{Q}\left[\sqrt{2}\right]$ y verifica

$$(0+0\sqrt{2})+(a+b\sqrt{2})=\left(0+a\right)+\left(0+b\sqrt{2}\right)=a+b\sqrt{2}$$

para cualquier elemento $a+b\sqrt{2}$ en $\mathbb{Q}\left[\sqrt{2}\right]$. Luego, $0+0\sqrt{2}$ es el elemento neutro para la adición en $\mathbb{Q}\left[\sqrt{2}\right]$. De ahora en adelante, lo denotaremos por 0 en lugar de $0+0\sqrt{2}$. Observe que cualquier elemento $a+b\sqrt{2}$ tiene un inverso aditivo dado por $-a-b\sqrt{2}$ ya que $(a+b\sqrt{2})+(-a-b\sqrt{2})=(a-a)+(b-b)\sqrt{2}=0+0\sqrt{2}=0$. Que la

suma es conmutativa y asociativa lo dejamos como ejercicio al estudiante UNA. Hemos demostrado que $\mathbb{Q}\left[\sqrt{2}\right]$ es un grupo abeliano respecto a la multiplicación.

El producto lo definimos por medio de

$$\left(a+b\sqrt{2}\right)\left(a_1+b_1\sqrt{2}\right)=aa_1+2bb_1+\left(ab_1+a_1b\right)\sqrt{2}$$

El estudiante UNA debe observar que el producto se define aplicando las reglas usuales de la aritmética de los números reales y usando que $\left(\sqrt{2}\right)^2=2$. Por favor, verifique esta afirmación usted mismo. Observe que $\left(a+b\sqrt{2}\right)\left(a_1+b_1\sqrt{2}\right)=aa_1+2bb_1+\left(ab_1+a_1b\right)\sqrt{2}$ está en $\mathbb{Q}\left[\sqrt{2}\right]$, luego el producto que hemos definido, es una ley de composición interna. Si pensamos que $\mathbb{Q}\left[\sqrt{2}\right]$ es un subconjunto de los números reales $\mathbb{R}$ y al coincidir el producto definido en $\mathbb{Q}\left[\sqrt{2}\right]$ con el usual de los números reales $\mathbb{R}$, se tiene que este producto debe ser conmutativo y asociativo. Note que $1+0\sqrt{2}$ está en $\mathbb{Q}\left[\sqrt{2}\right]$ y que

$$\left(1+0\sqrt{2}\right)\left(a+b\sqrt{2}\right)=\left(1\cdot a+0\cdot b\cdot 2\right)+\left(1\cdot b+0\cdot a\right)\sqrt{2}=a+b\sqrt{2}$$

Así, $1+0\sqrt{2}$ juega el papel de elemento neutro o identidad para el producto definido en $\mathbb{Q}\left[\sqrt{2}\right]$. Veamos la existencia de un inverso para los elementos no nulos de $\mathbb{Q}\left[\sqrt{2}\right]$. Supongamos que $a+b\sqrt{2}$ es no nulo, entonces $a\neq 0$ o $b\neq 0$. La idea es encontrar $\dfrac{1}{a+b\sqrt{2}}$. El estudiante recordará que en bachillerato realizaba este cálculo mediante un procedimiento llamado racionalización, multiplicando por la conjugada $a-b\sqrt{2}$ en el numerador y denominador de la expresión. Lo hacemos de esta manera para que la fracción no cambie y poder eliminar la raíz cuadrada que aparece en el denominador. En efecto,

$\frac{1}{a+b\sqrt{2}}\frac{a-b\sqrt{2}}{a-b\sqrt{2}}=\frac{a-b\sqrt{2}}{a^2-2b^2}=\frac{a}{a^2-2b^2}-\frac{b}{a^2-2b^2}\sqrt{2}$. Observe que $\frac{a}{a^2-2b^2}-\frac{b}{a^2-2b^2}\sqrt{2}$ está en $\mathbb{Q}\left[\sqrt{2}\right]$ ya que a^2-2b^2 no es nulo y con seguridad está en $\mathbb{Q}$. Para ver que a^2-2b^2 no es nulo razonamos por reducción al absurdo. Si

$$a^2-2b^2=0\Rightarrow\sqrt{2}=\frac{a}{b}\in\mathbb{Q}$$

lo cual es absurdo.

Luego, todo elemento no nulo es invertible o inversible. Por último, al ser la multiplicación usual de reales distributiva respecto a la sima, lo mismo debe ocurrir en $\mathbb{Q}\left[\sqrt{2}\right]$. Esto demuestra que $\mathbb{Q}\left[\sqrt{2}\right]$ con las leyes de composición internas definidas arriba es un cuerpo.

Veamos qué entendemos por el cuerpo de los cuaternios o cuaterniones *K*. Este ejemplo lo debemos a Hamilton. Un cuaternio es un número de la forma $a+bi+cj+dk$, donde $a,b,c,d\in\mathbb{R}$. Identificamos dos cuaternios $a+bi+cj+dk$, $a=a_1,b=b_1,c=c_1,d=d_1$ si y sólo si $a=a_1,b=b_1,c=c_1,d=d_1$.

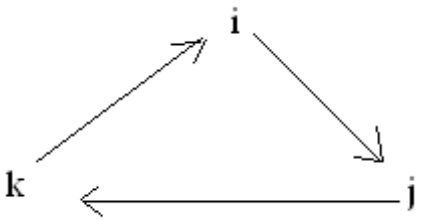
Una adición se define de manera natural, sumando términos semejantes. Por ejemplo, $(1-i+2j)+(i+\sqrt{2}k)=1+0i+2j+\sqrt{2}k$. En general,

$$\left(a+bi+cj+dk\right)+\left(a_1+b_1i+c_1j+d_1k\right)=$$
$$\left(a+a_1\right)+(b+b_1)i+\left(c+c_1\right)j+\left(d+d_1\right)k$$

Es una actividad para el estudiante UNA verificar que *K* es un grupo abeliano respecto a la adición definida. ¿Qué ocurre con la multiplicación?. La tabla de multiplicación que tenemos abajo indica cómo multiplicar los símbolos *i*, *j*, *k*. Esa tabla fue un gran descubrimiento de Hamilton.

	1	i	j	k
1	1	i	j	k
i	i	-1	k	-j
j	j	-k	-1	i
k	k	j	-i	-1

Una manera más sencilla de recordar la tabla anterior es el diagrama que vemos abajo, donde unimos los elementos a multiplicar por una flecha y luego seguimos la flecha ubicada en el segundo elemento de la multiplicación.



Así, $i.j = k$, $j.k = i$ y $k.i = j$ (si va en el sentido contrario de las flechas debe cambiar el signo). La multiplicación no es conmutativa como ya señalamos en una nota histórica en la unidad de grupos. Observe, que si queremos multiplicar $(1-i+2j)(i+\sqrt{2}k)$ aplicamos sencillamente las leyes usuales de la aritmética, obteniendo

$$(1-i+2j)(i+\sqrt{2}k) = i+\sqrt{2}k-i.i-i.k\sqrt{2}+2j.i+2\sqrt{2}j.k =$$
$$i+\sqrt{2}k+1+j\sqrt{2}-2k+2\sqrt{2}i$$

No vamos a escribir la forma general del producto de dos cuaternios, es mucho mejor usar la propiedad distributiva cuando tengamos que multiplicar un par de cuaternios. Es sencillo verificar que $1+0i+0j+0k$ es el elemento neutro para el producto. ¿Es todo elemento no nulo del cuerpo de cuaternios inversible?. Para un elemento $z = a+bi+cj+dk$ cualquiera de los cuaternios definimos su conjugado por medio de

$$\overline{z} = a-bi-cj-dk\,.$$

Entonces tenemos que

$$z\bar{z} = (a+bi+cj+dk)(a-bi-cj-dk) =$$
$$a^2 - abi - acj - adk + abi + b^2 - bck - dbj + acj + bck + c^2 - cdi + adk + dbj$$
$$+cdi + d^2$$

Luego, $z\bar{z} = a^2 + b^2 + c^2 + d^2 \in \mathbb{R}$. Este resultado permite demostrar que cualquier elemento no nulo en los cuaternios es inversible. En efecto, $\frac{1}{a+bi+cj+dk}\frac{a-bi-cj-dk}{a-bi-cj-dk} = \frac{a-bi-cj-dk}{a^2+b^2+c^2+d^2}$. Esto demuestra que los cuaternios forman un cuerpo. La operación de conjugación es muy importante, ella permite definir el módulo o tamaño de un cuaternio $z = a+bi+cj+dk$. El módulo de $z = a+bi+cj+dk$, denotado por $|z|$, se define como $|z| = \sqrt{z\bar{z}} = \sqrt{a^2+b^2+c^2+d^2}$.

El siguiente resultado resume las propiedades de la conjugación en los cuaternios. Lo dejamos como una actividad propuesta al estudiante UNA.

 Demuestre las siguientes propiedades de la operación de conjugación:

1. Para cualquier cuaternio z se tiene $\bar{\bar{z}} = z$
2. Un cuaternio representa un número real si y sólo si $z = \bar{z}$
3. Para cualquier par de cuaternios z, z_1 se tiene $\overline{z + z_1} = \bar{z} + \bar{z}_1$
4. Para cualquier par de cuaternios z, z_1 se tiene $\overline{zz_1} = \bar{z} + \bar{z}_1$

 En este ejemplo desarrollamos el cuerpo de las funciones racionales. Sabemos que los polinomios reales $\mathbb{R}[x]$ es un anillo pero no un cuerpo. Sin embargo, si consideramos las "fracciones" cuyos numeradores y denominadores son polinomios reales, obtenemos un cuerpo que denotaremos por $F[x]$. Los elementos de $F[x]$ son de la forma $\frac{p(x)}{q(x)} = \frac{a_0 + a_1x + a_2x^2 + \cdots a_nx^n}{b_0 + b_1x + b_2x^2 + \cdots b_mx^m}$.

 Demuestre en detalle que $F[x]$ es un cuerpo.

Sugerencia: Establezca la adición y multiplicación en $F[x]$ de manera natural. Investigue las propiedades de estas operaciones: existencia de elemento neutro, inverso, entre otras. ¡Sea sistemático!

Teorema 1. En un cuerpo cualquiera *K* se tienen las siguientes propiedades:

1. $a0 = 0a = 0$ para cualquier *a* en *K*, donde 0 es el elemento neutro para la adición.
2. Si $ab=0$ entonces $a=0$ o $b=0$
3. $a(b-c) = ab - ac$ para cualesquiera elementos *a*, *b* y *c*.

Demostración.

1. Como $a0 = a(0+0) = a0 + a0 \Rightarrow a0 = 0$.
2. Si *a* es no nulo entonces a^{-1} existe. Si multiplicamos a^{-1} a la igualdad $ab=0$ por la izquierda, obtenemos $a^{-1}ab=0$, luego $b=0$ como queríamos demostrar.
3. Muy similar a lo hecho en la Unidad de Anillos, recomendamos al estudiante UNA hacer la demostración como ejercicio.

 La parte 2. del teorema anterior indica que todo cuerpo *es un dominio de integridad.* Esto es, si un producto vale 0 alguno de los factores del producto vale 0 también. Esta propiedad no es cierta en ciertos anillos donde aparecen divisores de 0.

Teorema 2. En un cuerpo cualquiera *K* si $ab = ac$ con $a \neq 0$ entonces $b = c$. Es decir, en un cuerpo cualquiera vale la ley de cancelación respecto al producto.

Demostración. En efecto, si $ab = ac$ con $a \neq 0$ y restamos *ac* a ambos lados de la igualdad, obtenemos que $a(b-c) = 0$. Al ser *a* no nulo, debe tener un inverso multiplicativo que llamamos a^{-1}. Multiplicando, por la izquierda, ambos lados de la

igualdad por a^{-1} se tiene $a^{-1}a(b-c)=a^{-1}0=0$ pero $a^{-1}a(b-c)=1(b-c)=b-c=0\Rightarrow b=c$.

Teorema 3. Sea *K* un cuerpo cualquiera. Entonces la ecuación $ax+b=c$ donde *x* es la incógnita y *a,b* y *c* son elementos de *K*, con $a\neq 0$ tiene solución única.

Demostración. Procedemos a "despejar" la *x.* Como *K* es un grupo aditivo, podemos sumar a ambos lados de la igualdad $ax+b=c$ el inverso aditivo de *b*, esto es *–b.* Obtenemos $ax+b+(-b)=c+(-b)\Rightarrow ax+0=c+(-b)$. Luego, $ax=c+(-b)$ y como *a* es no nulo, *a* es invertible respecto al producto, llamemos su inverso a^{-1}. Multiplicando por este inverso, por la izquierda de la igualdad $ax=c+(-b)$ obtenemos

$$a^{-1}ax=a^{-1}\left(c+(-b)\right)\Rightarrow 1x=a^{-1}\left(c+(-b)\right)\Rightarrow$$
$$x=a^{-1}\left(c+(-b)\right)$$

La unicidad de la solución se obtiene de la ley de cancelación ya que si tenemos que $ax_1+b=c$, entonces $ax_1+b=ax+b\Rightarrow ax_1=ax\Rightarrow x_1=x$.

13.3. Característica de un cuerpo

Como ya hemos visto existen cuerpos *finitos* como $\mathbb{Z}_p$ con *p* primo. Supongamos que *K* es un cuerpo finito y sea 1 el elemento neutro para la multiplicación en *K*. Consideremos la sucesión 1,1+1, $\cdots$. Al ser *K* un cuerpo finito, algunos elementos de esta sucesión deben repetirse. Es decir, existen naturales *n* y *m* con $n<m$ tales que

$$\overbrace{1+1+\cdots 1}^{\text{n veces}}=\overbrace{1+1+\cdots 1}^{\text{m veces}}$$

Luego, $(m-n)1=0$. Así, el conjunto $a1\,o\,b1$ es no vacío y debe tener un menor elemento.

Teorema 4. Sea K un cuerpo finito y consideremos el conjunto $A=\{n\in\mathbb{N} \text{ tales que } n1=0\}$. Entonces el menor elemento de A es primo.

Demostración. Sea p el menor elemento de A vamos a ver que p es primo. Razonemos por el absurdo, supongamos que p no es primo, $p=ab, 1<a<p, 1<b<p$. Luego,

$$0=p1=(ab)1=(a1)(1b)$$

Pero esto es absurdo ya que ni $a1$ o $b1$ son 0 y K es un cuerpo, luego un dominio de integridad. Esta contradicción indica que p debe ser primo.

Definición. *La característica de un cuerpo finito K es el menor primo p tal que 1p=0.*

 El cuerpo $\mathbb{Z}_p$ con p primo tiene característica p.

Teorema 5. Sea R un anillo conmutativo finito con elemento neutro 1 para el producto. Si R es un dominio de integridad entonces R es un cuerpo.

Demostración. Basta ver que cualquier elemento x tiene un inverso multiplicativo. Consideremos la función $\begin{matrix} f:R\to R \\ f(y)=xy \end{matrix}$. Esta función es inyectiva por ser R un dominio de integridad. Al ser R finito entonces f debe ser sobreyectiva también. Luego, f debe tomar el valor 1 para algún y_0, esto es $f(y_0)=xy_0=1$, de donde x es inversible y esto concluye la demostración.

Un cuerpo K que no tenga característica finita se dice de característica 0.

 El cuerpo $\mathbb{Q}$ tiene característica 0 ya que nunca obtenemos 0 al sumar reiteradamente 1, 1+1,1+1+1, $\cdots$

13.4. Extensión de un cuerpo y subcuerpos

Supongamos que tenemos dos cuerpos *K* y *Q* tales que $K \subset Q$ y donde las leyes de composición interna de *K* son la restricción de las leyes de composición de *Q* a *K*. En este caso decimos que *K es un subcuerpo de Q o que Q es una extensión de K.*

1. Este es un ejemplo muy importante ya que $\mathbb{Q}, \mathbb{R}$ y $\mathbb{C}$ son tres cuerpos básicos para la matemática.

$$\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$$

   Así, $\mathbb{R}$ es una extensión de $\mathbb{Q}$ y $\mathbb{C}$ es una extensión de $\mathbb{R}$. También podemos decir que $\mathbb{Q}$ es un subcuerpo de $\mathbb{R}$. Observe que podemos pensar que obtenemos el cuerpo $\mathbb{C}$ del cuerpo $\mathbb{R}$ añadiéndole a $\mathbb{R}$ el elemento *i* y usar el hecho que $i^2 = -1$. Así, $\mathbb{R}[i] = \mathbb{C}$.

2. $\mathbb{Q}[\sqrt{2}]$ es una extensión de $\mathbb{Q}$. Podemos también decir que $\mathbb{Q}$ es un subcuerpo de $\mathbb{Q}[\sqrt{2}]$.

   Los dos siguientes teoremas son muy similares a los teoremas ya demostrado para subgrupos generados. Para que el estudiante UNA fije estas importantes ideas la demostración de los dos resultados las dejaremos como ejercicio.

Teorema 6. Si $(H_\alpha)_{\alpha \in I}$ es una familia de subcuerpos del cuerpo *K* entonces $\bigcap_{\alpha \in I} (H_\alpha)_{\alpha \in I}$ es un subcuerpo.

Demostración: La dejamos como ejercicio.

Teorema 7. Sea *K* un cuerpo y *T* un subconjunto de *K*. Entonces existe un subcuerpo minimal que contiene a *T.*

Demostración La dejamos como ejercicio.

 Demuestre los dos teoremas anteriores.

Sugerencia: El primer teorema es necesario para demostrar el segundo. Vaya a la unidad de grupos para refrescar las ideas involucradas en esta demostración, repase en particular lo relacionado al subgrupo generado por un conjunto.

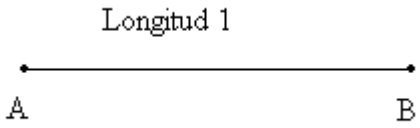
 Sea $\mathbb{Q} \subset \mathbb{R}$. ¿Qué subcuerpo *K* de $\mathbb{R}$ se obtiene al agregar a $\mathbb{Q}$ el real $\sqrt[3]{2}$?. Vamos a aclarar cuidadosamente esta pregunta. En primer lugar estamos pensando que el subcuerpo *K* que buscamos es un subcuerpo de los reales. Es decir, *en este caso buscamos el subcuerpo K de* $\mathbb{R}$ *generado por* $\mathbb{Q} \cup \left\{\sqrt[3]{2}\right\}$. Vemos que $\sqrt[3]{2}\sqrt[3]{2} = \sqrt[3]{4}$ y esto implica que $\sqrt[3]{4} \in K$. Luego *K* debe contener al conjunto *F* de todos los elementos de la forma $a + b\sqrt[3]{2} + c\sqrt[3]{4} \in \mathbb{R}$ con $a, b, c \in \mathbb{Q}$. Observamos que *F* es cerrado bajo la adición y producto usuales en $\mathbb{R}$. Verifiquemos esto en detalle. Si sumamos dos elementos de *F* debe ser claro que obtenemos de nuevo un elemento de *F.* El estudiante UNA debe completar los detalles de esta demostración. Que *F* es cerrado bajo el producto no es tan claro. Como $\sqrt[3]{4}\sqrt[3]{4} = \sqrt[3]{16} = \sqrt[3]{2^3 2} = 2\sqrt[3]{2}$ el resultado es cierto: al multiplicar dos elementos de *A* obtenemos un elemento de *A.*

¿Será cualquier elemento no nulo de *F* invertible? Esto equivale a la pregunta, ¿puede usted racionalizar $\frac{1}{a + b\sqrt[3]{2} + c\sqrt[3]{4}}$ y obtener un elemento de *F*? Esta parte la dejamos al estudiante UNA como una actividad pero es cierto que todo elemento no nulo tiene un inverso multiplicativo. Luego *F* es un subcuerpo y como cualquier subcuerpo de $\mathbb{R}$ que contenga a $\mathbb{Q} \cup \left\{\sqrt[3]{2}\right\}$ *debe contener a F entonces F=K.* El estudiante UNA debe indicar por qué.

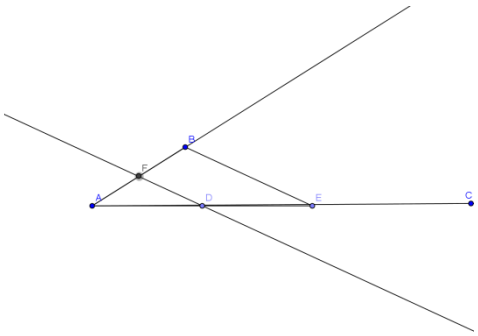
Demuestre que $(a+b)(a^2-ab+b^2)=a^3+b^3$. Use esta identidad para racionalizar $\dfrac{1}{a+b\sqrt[3]{2}+c\sqrt[3]{4}}$.

1.3.5 El cuerpo de los números constructibles Ω

Tomemos un segmento AB de longitud 1 (ver dibujo abajo), ¿qué longitudes pueden ser construidas a partir de AB solo usando una regla y un compás?. La regla no la suponemos graduada (con escala). El conjunto de las longitudes constructibles lo denotaremos por *C*. Así C es un subconjunto de los números reales, $C \subset \mathbb{R}$. Es claro que podemos construir segmentos de longitudes 2, 3,4 y así sucesivamente. Para hacer esto prolongamos con la regla el segmento AB y llevamos sobre esta prolongación, con el compás, el segmento AB las veces requeridas. Luego, $\mathbb{N} \subset C \subset \mathbb{R}$.



Pero cosas más interesantes pueden ser construidas. ¿Cómo construimos un segmento de longitud $\dfrac{1}{2}$? ¿Recuerda usted su curso Geometría, cod.754? La base de tal construcción descansa en el celebrado teorema de Tales. Tomemos dos semirrectas cualesquiera con un origen común (Ver dibujo abajo).



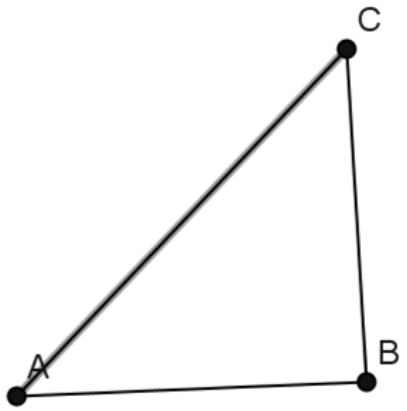
Sobre la semirrecta AC hemos llevado dos veces la longitud del segmento AB dos veces consecutivas determinando los segmentos AD y DE. Unimos ahora los puntos BE por un segmento y trazamos por D una paralela al segmento BE. Todas las

construcciones efectuadas son legítimas si sólo disponemos de una regla y un compás. Indiquemos la longitud del segmento AB por $|AB|$. El teorema de Tales indica que

$\frac{|AF|}{|AB|} = \frac{|AD|}{|AE|} = \frac{1}{2}$ pero $|AB| = 1 \Rightarrow |AF| = \frac{1}{2}$.

Una aplicación análoga del teorema de Tales nos lleva a afirmar que cualquier racional positivo $\frac{a}{b}$ puede ser construido. El estudiante UNA debe indicar cómo. Luego, $\mathbb{Q}_+ \subset C$.

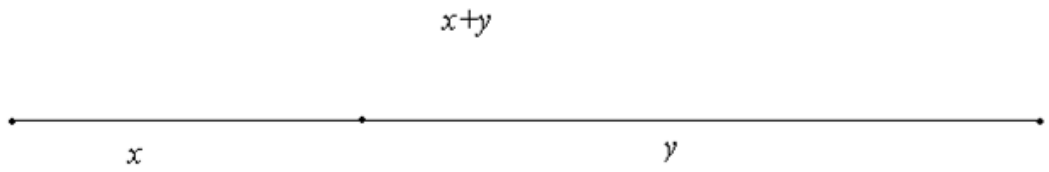
Después de obtener el resultado que todos los racionales positivos $\frac{x}{y} = \frac{x}{|AE|} \Rightarrow |AE| = xy$ están en *C*, uno se puede preguntar, ¿podremos construir algunas longitudes irracionales? El estudiante UNA debe saber la respuesta: ¡claro que sí! Recordarán que los irracionales fueron descubiertos por los matemáticos griegos como longitudes de algunos segmentos. El más conocido es el irracional $\sqrt{2}$. Su construcción es sencilla y transparente, solo necesitamos el Teorema de Pitágoras.



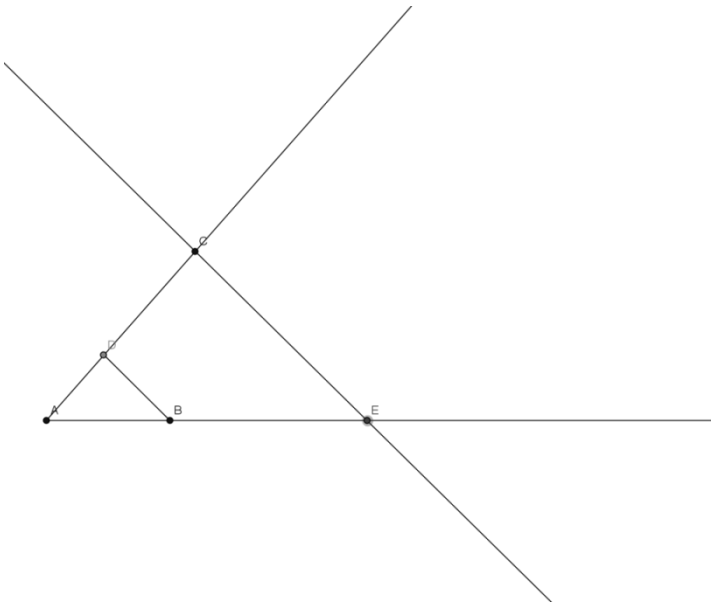
Si el segmento AB tiene longitud 1 y el segmento BC tiene igual longitud, la hipotenusa del triángulo rectángulo $\triangle$ABC mide exactamente $\sqrt{2}$. Invitamos al estudiante UNA a recordar cómo construir un triángulo rectángulo con regla y compás. De igual manera se pueden construir $\sqrt{3}, \sqrt{5}, \sqrt{6}, \cdots, \sqrt{n}, \sqrt{n+1}, \cdots$ Lo proponemos como actividad para el estudiante UNA.

Vemos así que el conjunto *C* es muy rico ya que además de contener a los racionales positivos existen irracionales en el mismo.

Vamos a demostrar a continuación que la adición, multiplicación y división usuales de los números reales al ser restringidas a C son leyes de composición internas en este conjunto. Es claro que si *x, y* están en *C* su suma pertenece a *C*. (ver dibujo abajo)



Para demostrar que el producto es cerrado en *C* necesitamos el teorema de Tales como ya el estudiante debe suponer.



Supongamos que el segmento AB tiene longitud *x*, el segmento AD tiene longitud 1 y el segmento AC tiene longitud *y*. El teorema de Tales dice que

$$\frac{1}{y} = \frac{x}{|AE|} \Rightarrow |AE| = xy$$

Queda como actividad al estudiante UNA indicar cómo se construye la longitud $\frac{x}{y}$.

Ahora bien, si colocamos ahora una recta y un punto 0 en ella, y dejamos que el segmento AB determine el 1 sobre la recta en la dirección que usualmente llamamos positiva, podemos determinar para cada longitud constructible un punto sobre la recta real. El estudiante UNA debe notar que esto se puede hacer hacia el lado negativo también, este conjunto ampliado es lo que llamamos el cuerpo de los números constructibles Ω, es decir $\Omega = \{x \in \mathbb{R} \text{ tales que } x = \pm c \in C\}$. Esto es un cuerpo porque acabamos de demostrar que *C* es cerrado bajo la adición, producto y división.

En nuestra última sección trataremos los problemas clásicos de la geometría griega en este contexto de la teoría de cuerpos.

1. Indique cómo se construyen $\sqrt{3}, \sqrt{5}, \sqrt{6}, \cdots, \sqrt{n}, \sqrt{n+1}, \cdots$. Sugerencia: Use reiteradamente el Teorema de Pitágoras.
2. Explique con claridad cómo, si damos segmentos de longitudes estrictamente positivas *x*, *y*, construir un segmento de longitud $\frac{x}{y}$.

1.3.6 Extensiones algebraicas y trascendentes de un cuerpo

Es conveniente que repase los conceptos de número algebraico y trascendentes vistos en la Unidad 6 del número real.

Consideremos una extensión *F* del cuerpo *K*, es decir $K \subset F$. Esta extensión se denomina algebraica *si cada elemento de F es raíz de un polinomio* $p(x)$ *con coeficientes en K.*

1. Consideremos la extensión $\mathbb{Q}\left[\sqrt{2}\right]$ de $\mathbb{Q}$. Veamos que $\mathbb{Q}\left[\sqrt{2}\right]$ es una extensión algebraica de $=F\left[\alpha\right]$. Primero que todo cualquier elemento de $\mathbb{Q}\left[\sqrt{2}\right]$ es de la forma $a+b\sqrt{2}$,con *a* y *b* racionales. Note que $a+b\sqrt{2}$ es una raíz del polinomio

$$p(x)=(x-(a+b\sqrt{2}))(x-(a-b\sqrt{2}))$$

Observe que además que

$$p(x)=(x-(a+b\sqrt{2}))(x-(a-b\sqrt{2}))=(x-a)^2-(b\sqrt{2})^2=$$
$$=(x-a)^2-2b^2=x^2-2ax+a^2-2b^2$$

Luego, $p(x)$ es un polinomio con coeficientes en $\mathbb{Q}$ y esto concluye la afirmación que $\mathbb{Q}\left[\sqrt{2}\right]$ es una extensión algebraica de $\mathbb{Q}$.

2. El cuerpo $\mathbb{C}$ es una extensión algebraica de los números reales $\mathbb{R}$ ya que la unidad imaginaria *i* satisface la ecuación polinómica real $x^2+1=0$.

3. Asuma que *e* el número base de los logaritmos neperianos es trascendente.[2] El subcuerpo de los reales que genera $\mathbb{Q}\cup\{e\}$ lo denotaremos por $\mathbb{Q}[e]$. Entonces $\mathbb{Q}[e]$ es una extensión trascendente de $\mathbb{Q}$ ya que por definición de número trascendente *e* no puede ser raíz de polinomio alguno con coeficientes racionales. Los de $\mathbb{Q}[e]$ son números reales de la forma

$$\frac{a_0+a_1e+a_2e^2+\cdots+a_ne^n}{b_0+b_1e+b_2e^2+\cdots+b_me^m},\ a_i,b_j\in\mathbb{Q},\ i\in\{1,2,\cdots,n\},\ j\in\{1,2,\cdots,m\}$$

[2] Una demostración de este hecho importante puede ser encontrada en el libro *Calculus* de M. Spivak.

Observe que el denominador de estas fracciones no se puede anular. El estudiante UNA debe decir por qué.

 Demuestre, en detalle, que los números reales de la forma

$\frac{a_0+a_1e+a_2e^2+\cdots+a_ne^n}{b_0+b_1e+b_2e^2+\cdots+b_me^m}, a_i,b_j\in\mathbb{Q}, i\in\{1,2,\cdots,n\}, j\in\{1,2,\cdots,m\}$ forman un subcuerpo *K* de los números reales. A partir de esto concluya que $\mathbb{Q}[e]$=*K*.

Sugerencia: Pruebe la primera afirmación y después observe que cualquier número de la forma $\frac{a_0+a_1e+a_2e^2+\cdots+a_ne^n}{b_0+b_1e+b_2e^2+\cdots+b_me^m}, a_i,b_j\in\mathbb{Q}, i\in\{1,2,\cdots,n\}, j\in\{1,2,\cdots,m\}$ debe estar en cualquier cuerpo que contenga a *e*.

Sea un cuerpo *K* que es una extensión del cuerpo *F*, *decimos que K es una extensión simple si y sólo si K se obtiene como el cuerpo generado por F y un elemento* α. Esto se escribe como $K=F[\alpha]$ y decimos que *K* se obtiene del cuerpo *F adjuntándole el elemento* α.

1. Los ejemplos 1. y 2. anteriores ilustran el concepto de extensión simple.

 Aunque $\mathbb{Q}[\sqrt{2}]$ son los números reales de la forma $a+b\sqrt{2}$,con *a* y *b* racionales y $\mathbb{C}=\mathbb{R}[i]$ son los números de la forma $z=x+iy$ con *x*,*y* números reales no debe suponer el estudiante una que el cuerpo $K=F[\alpha]$ siempre está compuesto únicamente por los elementos de la forma $p+q\alpha$ donde *p*,*q* están en *F*. Por ejemplo, $\mathbb{Q}[\sqrt[3]{3}]$ debe contener el elemento $\sqrt[3]{9}$ que *no es de la forma* $a+b\sqrt[3]{3}, a,b\in\mathbb{Q}$.

1. Demuestre que es imposible hallar racionales *a* y *b* tales que $a+b\sqrt[3]{3}=\sqrt[3]{9}$.

Sugerencia: Use el método de reducción al absurdo.

2. Consideremos el conjunto $F \subset \mathbb{R}$ dado por

$$F=\left\{a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6} \text{ donde } a,b,c,d \in \mathbb{Q}\right\}.$$

Estudie si *F* es un cuerpo y en caso afirmativo si es una extensión simple de $\mathbb{Q}\left[\sqrt{2}\right]$. ¿Es una extensión simple de $\mathbb{Q}$?

Nuestro próximo teorema se puede demostrar en un contexto más amplio pero por las aplicaciones que tenemos nos limitamos a este caso.

Teorema 8. Consideremos una extensión $\mathbb{Q}[\alpha]$ simple y algebraica de $\mathbb{Q}$. Entonces existe un único polinomio *p*(*x*) mónico y de grado *mínimo* con coeficientes racionales tal que $p(\alpha)=0.$

Demostración: Sea conjunto *M* de polinomios *q* con coeficiente racionales tales que $q(\alpha)=0.$ Como la extensión $\mathbb{Q}[\alpha]$ es algebraica entonces *M* es no vacío. Luego, por el principio de inducción, deben existir en *M* polinomios de grado mínimo, digamos *k*. Podemos suponer, sin pérdida de generalidad que estos polinomios son cónicos (de lo contrario divida el polinomio por el coeficiente de x^k , su término líder). Veamos que solo puede existir un polinomio mónico de grado *k* que tenga como raíz α. Supongamos que existan dos polinomios *p* y *m* tales que $m(\alpha)=p(\alpha)=0.$ Además, supongamos que el grado de *p* y *m* es *k* y que los dos son mónicos. Observe que $m(\alpha)=p(\alpha)=0 \Rightarrow (m-p)(\alpha)=0.$ Pero *m-p* es un polinomio de grado menor que *k* ya que los polinomios *m,p* son mónicos y al restarlos se anula el coeficiente de x^k . Luego $(m-p)\equiv 0$, por la escogencia de *k* como el grado mínimo para el cual debe ocurrir que α sea raíz de un polinomio con

coeficientes racionales. De aquí se deduce que el polinomio es único ya que $(m-p)\equiv 0$ implica que *m*=*p*.

El estudiante UNA debe repasar cuidadosamente el último paso de la demostración.
El polinomio p(x) que obtenemos en el teorema anterior se denomina el polinomio minimal de α.

 Consideremos el cuerpo $\mathbb{Q}\left[\sqrt{2}\right]$ como una extensión del cuerpo de los racionales $\mathbb{Q}$. Sabemos que el polinomio x^2-2 es el polinomio minimal de $\sqrt{2}$, si tiene alguna duda complete los detalles.

1. Sabemos que $\mathbb{C}=\mathbb{R}[i]$ ¿Cuál es el polinomio minimal de *i*?.
2. Halle un polinomio con coeficientes racionales que tenga a $\sqrt{2}+\sqrt{3}$ como raíz.
3. Explique con claridad por qué el polinomio minimal es único (ultima parte de la demostración del teorema anterior)

 Una observación elemental pero importante en relación al concepto de polinomio minimal *p*(*x*) de α es que este debe ser *irreducible* en el anillo de los polinomios con coeficientes racionales. Si no lo fuera, existirían polinomios *m, q* con coeficientes racionales tales que $p(x)=q(x)m(x)$ donde ni *q* ni *m* representan polinomios constantes y **sus grados son estrictamente menores** que el de *p*. Pero, $0=p(\alpha)=q(\alpha)m(\alpha)\Rightarrow m(\alpha)=0$ o $q(\alpha)=0$ y esto contradice que *p* es el polinomio minimal de α.

Teorema 9. Consideremos una extensión $\mathbb{Q}[\alpha]$ simple y algebraica de $\mathbb{Q}$. Supongamos que su polinomio *p* minimal tiene grado *m*. Entonces todo elemento *w* de

$\mathbb{Q}[\alpha]$ se puede escribir como $w = a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{m-1}\alpha^{m-1}$ donde los coeficientes a_i son racionales. Aún más, esta escritura es única.

Demostración. Vamos a empezar por la última afirmación, observe que si algún elemento *w* admitiese dos representaciones $w = a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{m-1}\alpha^{m-1}$ y $w = b_0 + b_1\alpha + b_2\alpha^2 + \cdots + b_{m-1}\alpha^{m-1}$,

igualando las dos representaciones tenemos

$$b_0 + b_1\alpha + b_2\alpha^2 + \cdots + b_{m-1}\alpha^{m-1} = a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{m-1}\alpha^{m-1} \Rightarrow$$
$$(b_0 - a_0) + (b_1 - a_1)\alpha + (b_2 - a_2)\alpha^2 + \cdots + (b_{m-1} - a_{m-1})\alpha^{m-1} = 0$$

Y esto contradice que el grado del polinomio minimal *p* es *m*.

El plan para demostrar es el siguiente: primero demostramos que si *K* es el conjunto $\{w \in \mathbb{R} \text{ tal que } w = a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{m-1}\alpha^{m-1}, a_i \in \mathbb{Q}\}$ entonces *K* es un cuerpo. Segundo como *K* es un subconjunto de $\mathbb{Q}[\alpha]$ debe necesariamente coincidir con este, ¿por qué? (piense que $\mathbb{Q}[\alpha]$ es el menor cuerpo que contiene a $\mathbb{Q} \cup \{\alpha\}$).

Demostremos que *K* es un cuerpo. Observe que *K* es cerrado respecto a la adición en los reales. ¿Qué pasa con respecto con la multiplicación?. Esto se aclara de inmediato si consideramos la expresión $a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{m-1}\alpha^{m-1} + a_m\alpha^m + \cdots a_n\alpha^n = c(\alpha)$ con *c* un polinomio de coeficientes racionales de grado *n* y *n>m.* Dividamos *c* por *p* aplicando el algoritmo de Euclides. Tenemos $c(x) = p(x)q(x) + r(x)$ con el grado de *r* *menor que el grado de p.* Luego, especializando el valor de la indeterminada *x* por α se tiene $c(\alpha) = p(\alpha)q(\alpha) + r(\alpha) = r(\alpha)$ ya que $p(\alpha) = 0$. Es decir, $a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{m-1}\alpha^{m-1} + a_m\alpha^m + \cdots a_n\alpha^n = c(\alpha)$ se puede escribir de manera más compacta, no necesitamos sobrepasar el grado *m*-1. Así, al multiplicar dos elementos en *K* volvemos a obtener un miembro del conjunto *K.* Esto demuestra que *K* es un anillo conmutativo con identidad. ¿Serán los elementos no nulos de *K* invertibles? Veamos que sí, tomemos un elemento genérico de *K,*

$w = a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{m-1}\alpha^{m-1}$ que no sea nulo. Esto implica que alguno de sus coeficientes es no nulo. Llamemos *m* al polinomio $a_0 + a_1x + a_2x^2 + \cdots + a_{m-1}x^{m-1}$, claramente $m(\alpha) = w$. Como el polinomio minimal *p* es irreducible y el grado de *m* es menor que el de *p* entonces *p* y *m* deben ser primos entre si. Luego existen polinomios *q* y *g* tales que

$$1 = p(x)q(x) + m(x)g(x)$$

Pero esto implica, especializando la variable *x* por α , que

$$1 = p(\alpha)q(\alpha) + m(\alpha)g(\alpha) = m(\alpha)g(\alpha)$$

De donde cualquier elemento $m(\alpha) = w$ es invertible y *K* es un cuerpo.

Definición. *Sea K[α] una extensión simple y algebraica del cuerpo K. El grado de la extensión se define como el grado del polinomio minimal de α y se denota por* $\left[K[\alpha]:K\right]$.

Esto se puede hacer con más generalidad si tuviésemos a disposición el concepto de espacio vectorial. El estudiante estudiará esta idea en su curso de Álgebra II. El grado de una extensión *F* del cuerpo *K* se define en general como la dimensión del espacio vectorial *F* sobre el cuerpo *K.* Le recomendamos el excelente libro de Herstein, *Algebra Moderna,* Editorial Trillas para los detalles.

1. La extensión $\mathbb{Q}\left[\sqrt{2}\right]$ de $\mathbb{Q}$ es de grado 2.
2. Este ejemplo es importante en relación al problema griego de la duplicación del cubo. Consideremos la extensión $\mathbb{Q}\left[\sqrt[3]{2}\right]$ de $\mathbb{Q}$. Claramente esto es una

extensión simple y algebraica de $\mathbb{Q}$ ya que $\sqrt[3]{2}$ es raíz del polinomio $p(x) = x^3 - 2$. Este polinomio *p* es irreducible en el anillo de los polinomios con coeficientes racionales por el Criterio de Eisenstein. Luego $\left[\mathbb{Q}\left[\sqrt[3]{2}\right]:\mathbb{Q}\right] = 3$.

1.3.7 Aplicación a los problemas clásicos de la geometría griega

Los griegos plantearon tres problemas en Geometría cuya solución esperó siglos. Los problemas son:

- *Duplicación del cubo*: Construir, usando solo regla y compás, un cubo cuyo volumen sea el doble de un cubo dado.
- *Trisección del ángulo*: Dado un ángulo cualquiera, usando solo regla y compás, trisecarlo.
- *Cuadratura del círculo:* Dado un círculo cualquiera, usando solo regla y compás, construir un cuadrado de similar área.

Tesoro de Atenas construido por la victoria en Maratón

Expliquemos brevemente cada uno de estos problemas. Se dice que el problema de la duplicación del cubo surgió durante una epidemia de peste que azotó Delfos. Al consultarse al oráculo de Apolo la sacerdotisa solicitó la duplicación del ara que era de forma cúbica. *Duplicar significa en este caso no duplicar la arista sino el volumen.* Es por ello que este problema se denomina también el problema de Delos.

El problema de trisección del ángulo no tiene una historia tan llamativa y su enunciado es bastante comprensible. Se trata de dado un ángulo *arbitrario* dividirlo en tres partes iguales. Esta trisección es posible para algunos ángulos como el ángulo recto pero no se puede realizar en general.

Los problemas de cuadraturas son muy importantes en la geometría griega. Los pitagóricos conocían cómo construir un cuadrado de área equivalente al área de un polígono dado. Posteriormente, Hipócrates de Quíos logra resolver el problema de la cuadratura de las lúnulas. Sin embargo, el problema de construir un cuadrado cuya área fuese la misma que la de un círculo dado permanecía imposible de atacar.

Algunos intentos de solución involucraban curvas mecánicas pero no satisfacían el requerimiento de usar solo regla y compás. No sabemos quién impuso el canon de construir los objetos geométricos con regla y compás, se cree que fue Platón.

Nos proponemos a continuación resolver los tres problemas más importantes de la geometría griega. La geometría analítica es una herramienta valiosa ya que permite traducir al lenguaje del álgebra proposiciones geométricas. Empezamos observando, como ya vimos, que todos los racionales son constructibles, esto implica que todos los puntos de $\mathbb{R}^2$ de coordenadas racionales se pueden construir, este conjunto es $\mathbb{Q}\times\mathbb{Q}$. Luego iniciamos con los puntos $\mathbb{Q}\times\mathbb{Q}$ y consideramos rectas, trazadas por nuestra regla y determinadas por dos puntos de $\mathbb{Q}\times\mathbb{Q}$. Podemos también considerar círculos de centro un punto en $\mathbb{Q}\times\mathbb{Q}$ y radio racional. El estudiante UNA debe hacer el conjunto de actividades propuestas para continuar la discusión.

1. Demuestre que una recta L: $qy = mx + n$ determinada por los puntos $(a,b),(c,d) \in \mathbb{Q}\times\mathbb{Q}$ tiene todos sus parámetros *q, m* y *n* racionales.
2. Demuestre que un círculo de radio *r* racional y centro (x_0, y_0) en $\mathbb{Q}\times\mathbb{Q}$ se escribe como $x^2 + ax + y^2 + bx = c$ y todos los coeficientes *a, b* y *c* son racionales. Sugerencia: Expanda $\left(x - x_0\right)^2 + \left(y - y_0\right)^2 = r^2$.
3. Demuestre que la intersección, si existe, de dos rectas L y L' con parámetros racionales determina un punto en $\mathbb{Q}\times\mathbb{Q}$.
4. Demuestre que la intersección, si existe, de una recta con parámetros racionales y un círculo de radio *r* y centro (x_0, y_0) en $\mathbb{Q}\times\mathbb{Q}$ determina uno o dos puntos con coordenadas en $\mathbb{Q}$ o en *una extensión algebraica* $\mathbb{Q}[\alpha]$ *de*

grado 2 . Lo mismo ocurre al intersecar dos círculos de radios racionales y centros en $\mathbb{Q}\times\mathbb{Q}$.

1. Use la fórmula de la pendiente y observe que el resultado debe ser un número racional. Haga lo mismo para determinar la ordenada en el origen.
2. Use lo sugerido en la actividad.
3. Resuelva, aplicando cualquier método estudiado en bachillerato (puede usar la regla de Cramer), el sistema de dos ecuaciones y dos incógnitas que determinan las dos rectas.
4. Use la fórmula de la ecuación cuadrática para obtener el resultado.

Las actividades anteriores demuestran que partiendo de los puntos de $\mathbb{Q}\times\mathbb{Q}$ y usando regla y compás extendemos los elementos de $\mathbb{Q}$ a extensiones del tipo $\mathbb{Q}[\alpha]$ de grado 2 sobre los racionales.

Si ahora usamos rectas con puntos de coordenadas en $\mathbb{Q}[\alpha]$(alguna coordenada puede estar en $\mathbb{Q}$) y círculos con centros en puntos de $\mathbb{Q}[\alpha]\times\mathbb{Q}[\alpha]$(alguna coordenada del centro puede estar en $\mathbb{Q}$) y radio en $\mathbb{Q}[\alpha]$, vemos que los puntos de intersección de rectas y círculos de nuevo determinan reales que están en una extensión algebraica $\mathbb{Q}[\alpha,\beta]$ de grado de 2 de $\mathbb{Q}[\alpha]$. Esto se logra como usted lo hizo en las actividades anteriores resolviendo sistemas de ecuaciones de primero o segundo grado con coeficientes en $\mathbb{Q}[\alpha]$. Continuando este proceso vemos que un número real es constructible si y sólo si podemos encontrar una *sucesión finita de cuerpos*

$$\mathbb{Q}\supset\mathbb{Q}[\alpha]\supset\mathbb{Q}[\alpha,\beta]\supset\cdots\supset F_i\supset F_{i+1}\supset\cdots\supset F_n$$

Donde el grado de F_{i+1} como extensión del cuerpo F_i es 1 o 2, esto es $\left[F_{i+1}:F_i\right]=1$ o 2 . La extensión F_n tiene grado 2^k ya que su grado es el producto de los grados $\left[\mathbb{Q}[\alpha]:\mathbb{Q}\right]\cdot\left[\mathbb{Q}[\alpha,\beta]:\mathbb{Q}[\alpha]\right]\cdots\left[F_{i+1}:F_i\right]\cdot\cdots\cdot\left[F_n:F_{n-1}\right]$

Esto implica (ver el libro de Herstein para una prueba) que: *si el número L es constructible debe existir un polinomio irreducible de grado* 2^k *sobre los racionales tal que L es su raíz y su grado es precisamente L*. En particular cualquier número L constructible es algebraico.

Solución al problema de la duplicación del cubo

Duplicar el cubo implica ser capaz de construir el número $\sqrt[3]{2}$. Para ver esto partimos de un cubo de arista 1, su volumen es la arista al cubo, esto es 1 de nuevo. Un cubo de volumen doble tendrá entonces volumen 2, si *a* es su arista entonces debe ocurrir que $a^3=2\Rightarrow a=\sqrt[3]{2}$. Pero el polinomio minimal de $\sqrt[3]{2}$ es $p(x)=x^3-2$ que tiene grado 3 que no es potencia de 2, luego ¡es imposible duplicar el cubo!

Solución al problema de la cuadratura del círculo

El matemático alemán Lindemann demostró que el número π es trascendente. Es decir, π **no es algebraico.** Esta demostración es propia del análisis matemático y escapa del alcance de esta obra. El hecho que π sea trascendente implica que es imposible cuadrar el círculo. Veamos por qué. Tomemos un círculo de radio 1, su área es igual a π ya que el área del círculo de radio *r* es πr^2. Construir un cuadrado área igual a π equivale a construir el lado L de ese cuadrado. Pero $L^2=\pi$ implica que L= $\sqrt{\pi}$.

Lema. Si π es trascendente entonces $\sqrt{\pi}$ es trascendente.

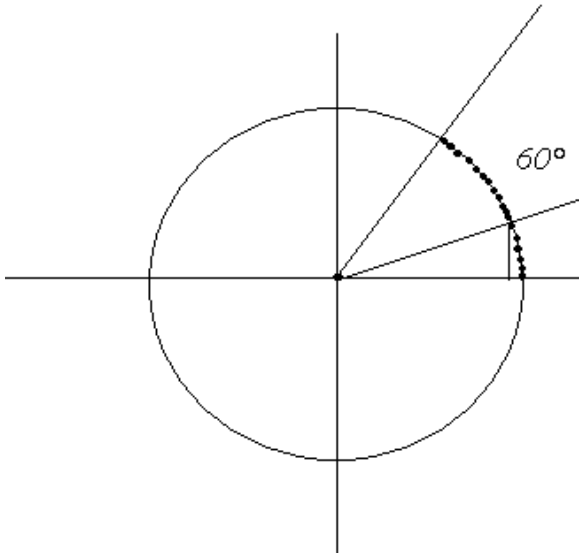
Demostración. Supongamos que $\sqrt{\pi}$ es algebraico y consideramos la extensión de grado *finito* $\mathbb{Q}\left[\sqrt{\pi}\right]$ de $\mathbb{Q}$. Como $\mathbb{Q}\left[\sqrt{\pi}\right]$ es un cuerpo y claramente $\sqrt{\pi}$ está en

$\mathbb{Q}\left[\sqrt{\pi}\right]$ entonces $\sqrt{\pi}\,\sqrt{\pi}=\pi$ está en $\mathbb{Q}\left[\sqrt{\pi}\right]$ lo cual es absurdo por ser π trascendente.

Luego, L=$\sqrt{\pi}$ no es algebraico lo que implica que es imposible construir con regla y compás L=$\sqrt{\pi}$. Así, es imposible cuadrar el círculo.

Solución al problema de la trisección del ángulo

Tomemos un ángulo de 60° y supongamos que se pueda trisecar. Esto equivale a poder construir un segmento de longitud $\cos 20°$. ¿Es esto claro?. Vea el dibujo abajo abajo para aclarar las ideas.



 Demuestre la identidad trigonométrica $\cos 3\alpha = 4\cos^3\alpha - 3\cos\alpha$ (ejercicio de cuarto año de bachillerato).

Si hacemos $\alpha = 20°$ en la identidad que usted acaba de demostrar vemos que $\cos 60° = 4\cos^3 20° - 3\cos 20° \Rightarrow \frac{1}{2} = 4\cos^3 20° - 3\cos 20°$, luego $\cos 20°$ es una raíz raíz o cero del polinomio $\frac{1}{2} = 4x^3 - 3x$. Preferimos multiplicar a ambos lados por 2 y

2 y trabajar con el polinomio $1=8x^3-6x$. Haciendo el cambio $2x=y$, vemos que $\cos 20°$ debe ser una raíz del polinomio $q(y)=y^3-3y-1$.

1. Demuestre que $q(y+1)=y^3+3y^2-3$.
2. Aplique el criterio de Eisenstein para concluir que el polinomio $q(x)$ es irreducible

1. Es un cálculo algebraico elemental que debe realizar el estudiante UNA. Para la parte 2. Aplique el criterio de Eisenstein ya que 3 divide a los coeficientes del polinomio considerado (salvo al coeficiente líder) pero nueve no divide a -3, luego por Eisenstein el polinomio es irreducible.

Aplicando la parte 2. de la actividad anterior concluimos que el polinomio minimal de $\cos 20°$ tiene grado 3 y por ende no es constructible con regla y compás. De esto se deduce que es imposible trisecar un ángulo cualquiera.

 Estudie si es posible trisecar el ángulo de 90°.

Sugerencia: Como lo hecho en el texto, estudie si es posible construir cos30°.

 Recordamos de cuarto año de bachillerato que $\cos 30=\frac{\sqrt{3}}{2}$ y este número es constructible con regla y compás ya que es solución de una ecuación cuadrática.

1. Encuentre un polinomio $p(x)$ con coeficientes racionales tal que $\sqrt{2}+\sqrt[3]{3}$ sea una raíz de $p(x)$.

2. Describe los elementos del cuerpo $\mathbb{Q}\left[\sqrt[3]{5}\right]$.
3. Un isomorfismo del cuerpo *K* al cuerpo *F* es una biyección $\psi : K \to F$ tal que $\psi(x+y) = \psi(x) + \psi(y)$ y $\psi(x \cdot y) = \psi(x)\psi(y)$. Dos cuerpos se denominan isomorfos si existe un isomorfismo entre ellos. Demuestre que si $\psi : K \to F$ es un isomorfismo entonces $\psi^{-1} : F \to K$ es un isomorfismo.
4. Demuestre que si $\psi : K \to F$ es un isomorfismo del cuerpo *K* al cuerpo *F* y $\chi : F \to M$ es un isomorfismo del cuerpo *F* al cuerpo *M* entonces la composición $\chi \circ \psi : K \to M$ es un isomorfismo.
5. ¿Puede ser el cuerpo $\mathbb{Q}\left[\sqrt[3]{5}\right]$ isomorfo al cuerpo $\mathbb{Q}\left[\sqrt{2}\right]$?

Sugerencia: Analice qué pasa con la identidad bajo el isomorfismo.

6. Demuestre que los cuerpos $\mathbb{Q}\left[\sqrt{2}\right]$ y $\mathbb{Q}\left[\sqrt{3}\right]$ son isomorfos**.**

Sugerencia: Defina $\psi(a+b\sqrt{2}) = a+b\sqrt{3}$ y demuestre las propiedades que caracterizan el concepto de isomorfismo.

7. Demuestra que el conjunto de todos los isomorfismos de un cuerpo en sí mismo es un grupo respecto a la composición de funciones.

1. Llamemos $\alpha = \sqrt{2} + \sqrt[3]{3}$, luego

$$\alpha = \sqrt{2} + \sqrt[3]{3} \Rightarrow \alpha - \sqrt{2} = \sqrt[3]{3} \Rightarrow$$
$$\left(\alpha - \sqrt{2}\right)^3 = 3 \Rightarrow \alpha^3 - 3\alpha^2\sqrt{2} + 6\alpha - 2\sqrt{2} = 3$$
$$\left(-3\alpha^2 - 2\right)\sqrt{2} = -\alpha^3 - 6\alpha + 3$$

Ahora, $\alpha^3 - 3\alpha^2\sqrt{2} + 6\alpha - 2\sqrt{2} = 3$ de donde $\left(-3\alpha^2 - 2\right)\sqrt{2} = -\alpha^3 - 6\alpha + 3$. Elevando al cuadrado ambos lados de la igualdad obtenemos la ecuación deseada.

2. Aplicando el criterio de Einsenstein podemos demostrar que x^3-5 es irreducible en los polinomios con coeficientes reales. Luego, los elementos de $\mathbb{Q}\left[\sqrt[3]{5}\right]$ son de la forma $a+b\sqrt[3]{5}+c\sqrt[3]{25}, a,b$ y $c\in\mathbb{Q}$.

$$\begin{array}{l}\psi(x)=f,\psi(y)=g\\ \psi(x+y)=\psi(x)+\psi(y)=f+g\\ \psi^{-1}(f+g)=\psi^{-1}(f)+\psi^{-1}(g)\end{array}$$

3. Un isomorfismo del cuerpo *K* al cuerpo *F* es una biyección $\psi:K\to F$ tal que $\psi(x+y)=\psi(x)+\psi(y)$ y $\psi(x\cdot y)=\psi(x)\psi(y)$. Intuitivamente, entre dos cuerpos se puede establecer un isomorfismo si y solamente si ellos son indistinguibles desde el punto de vista algebraico. Al ser $\psi:K\to F$ una biyección es claro que $\psi^{-1}:F\to K$ existe. Sean *f, g* dos elementos arbitrarios de *F,* luego $\psi(x)=f,\psi(y)=g$ para ciertos elementos *x, y* de *K*. De aquí se tiene que $\psi(x+y)=\psi(x)+\psi(y)=f+g$ aplicando propiedades de isomorfismo. Pero, $x=\psi^{-1}(f), y=\psi^{-1}(g)$ luego $\psi^{-1}(f+g)=\psi^{-1}(f)+\psi^{-1}(g)$. De manera análoga se demuestra la propiedad para el producto, luego $\psi^{-1}:F\to K$ es un isomorfismo.

4. Lo dejamos al estudiante UNA ya que es un ejercicio básico que debe realizar.

5. Sugerencia: plantee un supuesto isomorfismo, y vea que pasa con la imagen de $\sqrt{2}$.

6. Definimos $\psi:\mathbb{Q}\left[\sqrt{2}\right]\to\mathbb{Q}\left[\sqrt{3}\right]$ por medio de $\psi(a+b\sqrt{2})=a+b\sqrt{3}$. Tenemos por ejemplo que

$$\psi(\left(a+b\sqrt{2}\right)+\left(a'+b'\sqrt{2}\right))=\psi((a+a')+(b+b')\sqrt{2})=$$
$$a+a'+(b+b')\sqrt{3}=a+b\sqrt{3}+a'+b'\sqrt{3}=\psi\left(a+b\sqrt{2}\right)+\psi\left(a'+b'\sqrt{2}\right)$$

El estudiante UNA debe mostrar de manera similar que $\psi((a+b\sqrt{2})(a'+b'\sqrt{2}))=\psi(a+b\sqrt{2})\psi(a'+b'\sqrt{2})$ lo que demuestra que la función definida es un homomorfismo. Es claro que $\psi:\mathbb{Q}[\sqrt{2}] \rightarrow \mathbb{Q}[\sqrt{3}]$ es sobreyectiva y la inyectividad se deduce de la manera siguiente: supongamos que $\psi(a+b\sqrt{2})=a+b\sqrt{3}=0$ esto implica que $b\sqrt{3}=-a$ pero como $\sqrt{3}$ es irracional se debe tener que tanto *a* como *b* son 0.

7. Es un ejercicio importante que el estudiante UNA debe realizar, la clave es ser sistemático.

Bibliografía

Cotlar, M., Sadowsky, C. (1966). *Introducción al Álgebra. Nociones de Álgebra Lineal.* Buenos Aires: Eudeba.

Herstein, I.N. (1980). Á*lgebra Moderna.* México: Trillas.

Nachbin, L. (1986). *Álgebra Elemental.* Washington D.C.: Ediciones de la OEA

Orellana, M., Rivas, S., Monagas, O., (1987)**.** *Álgebra I.* Caracas: Universidad Nacional Abierta.

Rivaud, J.(1968) *Ejercicios de Álgebra.* Madrid: Aguilar.

Rojo, A. (1996). *Álgebra I.* Buenos Aires: El Ateneo.

Serrano, W. (2004). *Elementos de Á*lgebra. Caracas: Retos y Logros, Instituto Pedagógico de Miranda José Manuel Siso Martínez.

Trejo, C. (1978). El Concepto de Número. Washington D.C.: Ediciones de la OEA

Zaldivar, F. (2005). *Fundamentos de álgebra*. México: Fondo de Cultura Económica.