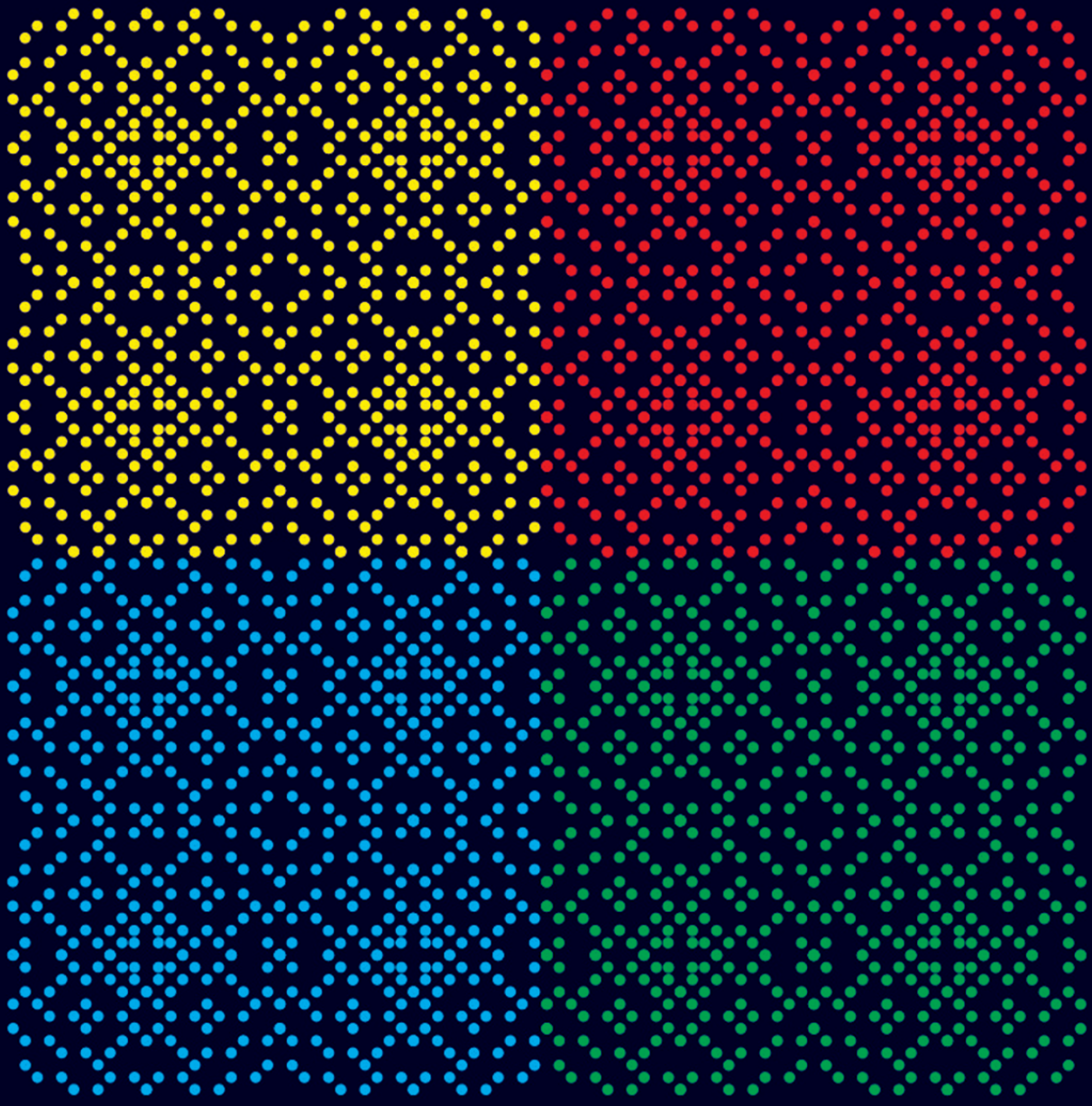
eudem
libros de grado

Temas de Álgebra



Estella Maris Álvarez | María Isabel Oliver | María Susana Vecino

TEMAS DE

ALGEBRA

ESTELLA MARIS ÁLVAREZ

MARÍA ISABEL OLIVER

MARÍA SUSANA VECINO

eudem

Álvarez, Estella Maris
Temas de algebra / Estella Maris Álvarez; María Isabel Oliver; María Susana Vecino. - 1a ed.
Mar del Plata: EUDEM, 2020.

Libro digital; PDF

Archivo digital: descarga y online
ISBN 978-987-4440-79-2

1. Álgebra. I. Oliver, María Isabel II. Vecino, María Susana III. Título
CDD 512

Este libro fue evaluado por la Dra. Elsa Adriana Fernández

Primera edición digital: Mayo 2020

ISBN 978-987-4440-79-2

Editorial de la Universidad Nacional de Mar del Plata
3 de Febrero 2538
Mar del Plata / Argentina

Arte y Diagramación: Luciano Alem

Imagen de tapa: Santiago Rueda

Libro
Universitario
Argentino

Deseamos rendir un homenaje a la memoria del Dr. de Enzo Gentile cuya obra, NOTAS DE ÁLGEBRA I, es nuestra fuente de inspiración y relectura recurrente, y agradecer a las personas que colaboraron con este proyecto, especialmente a:
Dra. Sonia Trepode, por su gestión ante la Facultad de Ciencias Exactas y Naturales de la Universidad Nacional de Mar del Plata para impulsar la edición del libro.
Dra. Elsa Fernández, por sus valiosos aportes en la corrección de la obra.

Las autoras

PRÓLOGO

Este libro surge a partir de apuntes de aula realizados por las autoras que se han desempeñado durante más de 20 años en la asignatura Introducción al Álgebra que se dicta para el Profesorado y Licenciatura en Matemática en la Facultad de Ciencias Exactas y Naturales de la Universidad Nacional de Mar del Plata. Una de las principales motivaciones ha sido la carencia de bibliografía en castellano apropiada a las necesidades del curso.

La temática del libro corresponde a un curso de álgebra elemental con la apropiada rigurosidad de la disciplina. Los conceptos se introducen adecuadamente y la complejidad va creciendo gradualmente. El libro es autocontenido lo que facilita su lectura.

Es bien conocida la aplicabilidad del álgebra a distintas disciplinas como la biología, la física y la química. En este material se dan aplicaciones a la criptografía y a la aritmética del ISBN, y algunas estructuras se introducen sobre cuerpos finitos.

Asimismo se presentan notas históricas y bibliográficas que permiten situar a lector en el contexto en que se desarrollaron las ideas e introducirlo a la historia de la matemática. Todo este marco contribuye a que la lectura del libro sea estimulante y amena.

En todo el texto se desarrollan ejemplos muy adecuados para ilustrar métodos y resultados. Se introduce una variada e interesante ejercitación cuya complejidad se eleva gradualmente.

En cuanto al contenido del libro, se comienza con la noción intuitiva de los números reales, identificándolos con los puntos de una recta, para luego formalizar su definición con los axiomas de cuerpo ordenado, a partir de los cuales se pueden demostrar todas las propiedades bien conocidas. Dentro de este cuerpo se reconoce el conjunto de Números Naturales, con el Principio de Inducción Completa que lo caracteriza. A continuación se extiende el conjunto de Números Naturales al de Números Enteros. El estudio de los Números Enteros es la llamada Aritmética, y es la base de la Teoría de Números. Se desarrolla la teoría de la divisibilidad, hasta demostrar el Teorema Fundamental de la Aritmética, el Algoritmo de la División, y su consecuencia, una aritmética finita introducida por la congruencia módulo n. Por último, se extiende el conjunto de Números Enteros al conjunto de Números Racionales; observando que éste es también un cuerpo ordenado, pero que está contenido propiamente en el conjunto de Números Reales, dado que hay números reales que no son racionales. Esto muestra que los axiomas de cuerpo ordenado no caracterizan al cuerpo de Números Reales, y que para definirlo se necesita un axioma adicional, el axioma de completitud, permitiendo caracterizarlos como un *cuerpo ordenado completo*.

En la segunda parte del libro se introducen las estructuras algebraicas. Se estudia el anillo de polinomios permitiendo que el mismo sea sobre cuerpos finitos, y los números complejos con el grupo de raíces n-ésimas de la unidad. Se estudia la irreductibilidad de polinomios y la factorización de los mismos como productos de irreducibles. Se introducen los grupos, anillos, cuerpos y los homomorfismos entre ellos. Se trabaja sobre grupos cíclicos y el grupo de permutaciones Sn.

Se incorporan dos apéndices al libro, uno de los cuales puede de ser de utilidad para estudiantes de otras áreas universitarias. En el Anexo I se introduce el domino de los enteros de Gauss y los enteros de Eisenstein, con el objetivo de dar a los estudiantes la oportunidad de conocer otros ejemplos diferentes a los números enteros y los polinomios. Esto les muestra que existen muchos ejemplos y por esto surge la necesidad del concepto de estructura y se observa que los teoremas que se demuestran en general tienen su implicancia en cada ejemplo particular. Se incorporan todos los conceptos de anillos necesarios para introducir los mencionados enteros, esto es ideales, dominios principales y euclidianos, elementos primos e irreducibles. En el Anexo II se demuestra la existencia de elementos trascendentes sobre un anillo conmutativo con identidad, con el objetivo de justificar plenamente la construcción dada del anillo de polinomios.

La estructura del libro excede la de un curso básico regular de algebra elemental, en particular por el contenido de los apéndices. Creo que sin duda este material puede ser adaptado al dictado de las asignaturas de álgebra de los primeros años de carreras universitarias seleccionando algunos capítulos. Dada la escasez de bibliografía en castellano, el material podría ser de utilidad para estudiantes de universidades del país y de otros países de habla hispana. Para los estudiantes

de las licenciaturas en matemática aporta conceptos básicos de aritmética que serán muy útiles a lo largo de su carrera. Pienso que el texto puede convertirse en una referencia y volverse material de consulta permanente para estudiantes y egresados de licenciaturas afines, ingenierías, computación e informática. Por otra parte, podría ser utilizado para la implementación de prácticas docentes innovadoras por parte de los estudiantes de los profesorados en matemática. El material resulta también apropiado para complementar la formación de docentes de matemática de los distintos niveles de la enseñanza, de manera que les permita consolidar sus conocimientos y así poder justificar, idear y proponer actividades apropiadas para el nivel en que se desempeñan.

Creo que un amplio espectro de estudiantes, egresados y formadores podrá beneficiarse con la labor realizada por las autoras, la cual pone en evidencia la extensa experiencia docente de las mismas. Estella Maris Álvarez, actualmente jubilada, ha sido docente de la asignatura inicial de Álgebra en mi Facultad por más de 30 años, en particular ha sido mi profesora, y María Isabel Oliver ha sido mi asistente en la mencionada asignatura. Junto a Susana Vecino las tres han sido mis colegas en la Universidad Nacional de Mar del Plata por más de 20 años. Tanto en mis tiempos como estudiante, como en mis tiempos como colega he podido observar su dedicación a la docencia, el entusiasmo y la pasión que han sabido trasmitir a sus estudiantes durante años. Ahora han conseguido plasmar estos elementos en un libro de texto, que espero el lector pueda apreciar y disfrutar. Por todo lo expuesto escribo este prólogo con mucho placer.

Sonia Trepode

INDICE

CAPITULO IV: NUMEROS NATURALES

CAPITULO V: NUMEROS ENTEROS

CAPITULO VI : NUMEROS RACIONALES COMPLETITUD DEL CUERPO DE LOS REALES

CAPITULO VII: ESTRUCTURAS ALGEBRAICAS

CAPITULO VIII: ANILLO DE POLINOMIOS

CAPITULO IX: NUMEROS COMPLEJOS

CAPÍTULO I

INTRODUCCIÓN A LA LÓGICA PROPOSICIONAL

La historia de la lógica se puede dividir, si nos permitimos un pequeño exceso de simplificación, en tres etapas: 1) la lógica griega; 2) la lógica escolástica, y 3) la lógica matemática. En la primera etapa las fórmulas lógicas se enunciaban con palabras del lenguaje ordinario, sujetas naturalmente a las reglas sintácticas usuales. Durante la segunda etapa, la lógica se abstrajo del lenguaje ordinario, caracterizándose por unas reglas sintácticas diferenciadas y unas funciones semánticas especiales. En la tercera etapa la lógica quedó marcada por el uso de un lenguaje artificial en el que los signos y palabras estaban regidos por una sintaxis exacta y tenían una función semántica estrechamente delimitada y definida también exactamente. Mientras que en las dos primeras etapas los teoremas lógicos se derivaban del lenguaje usual, en la tercera etapa la lógica procede al contrario: primero construye un sistema puramente formal, y sólo más tarde busca una interpretación en el lenguaje diario.

("Historia de la Matematica" Carl B. Boyer)

Introducción

En este capítulo, nuestra intención es brindar herramientas del Cálculo Proposicional y el Cálculo de Predicados, enfocándolos desde un punto de vista intuitivo, con un sesgo de formalidad, la necesaria para que se comprendan los fundamentos de la Lógica que sirven de base a todo pensamiento matemático. Este texto es de carácter elemental, y su lectura no requiere conocimientos previos de lógica clásica ni de matemática.

Cálculo proposicional

Proposiciones y valores de verdad

Sin pretender dar una definición, una *proposición* es toda expresión (o más generalmente, toda sucesión de palabras que tenga significado) a la que se le pueda atribuir un *valor de verdad.* Los valores de verdad posibles son: verdadero, V, o falso, F .

Las proposiciones las designaremos con letras minúsculas: p , q , r , s , etc.

Notación:

$\mathcal{V}(p) =$ V (valor de verdad de p, verdadero) o $\mathcal{V}(p) =$ F (valor de verdad de p , falso)

Ejemplos:

Son proposiciones:
p : El perro es un crustáceo
q : La Tierra es un planeta del Sistema Solar
u : 31 es un número primo
s : El otoño precede al invierno
t : Hay $10^{10^{10}} - 2$ estrellas en el universo
r : 102 es un número impar
w : Los grupos abelianos son finitos

$\mathcal{V}(p) = \mathcal{V}(r) =$ F ; $\mathcal{V}(q) = \mathcal{V}(u) = \mathcal{V}(s) =$ V

Desconocemos si $\mathcal{V}(t) =$ V o $\mathcal{V}(t) =$ F , pero ello no significa que no tenga un valor de verdad. Muchas personas pueden desconocer $\mathcal{V}(w)$, y muchas pueden no saber siquiera qué significa esa afirmación, pero ese desconocimiento no impide que $\mathcal{V}(w) =$ F

No son proposiciones:
- $x + 2$ es múltiplo de 5
- ¿qué hora es?
- ¡qué bello día!
- tu cuando mesa ser
- 16
- dos cuadrados y un triángulo

Hay una diferencia entre la primera y las demás expresiones, ninguna tiene un valor de verdad, pero si en la primera le damos valores a x podemos obtener una proposición, que podrá ser verdadera o falsa; por ejemplo, para $x = 3$ es verdadera, para $x = 4$ es falsa. Estas expresiones se denominan *esquemas proposicionales* y volveremos a ellas más adelante.

Conectivos lógicos

Los *conectivos lógicos* son las operaciones entre proposiciones. Así como la suma de números enteros es un número entero, el producto de dos números reales da otro número real, con los distintos conectivos lógicos, a partir de dos proposiciones (en cierto caso, de una) obtenemos una nueva proposición. Para definir cada operación debemos determinar cuál es el valor de verdad de la proposición obtenida, a partir de los respectivos valores de verdad de las proposiciones que intervienen en la operación, por ello las definiremos mediante las *tablas de verdad.*
Los conectivos lógicos son: *conjunción, disyunción, negación*, *condicional.* Todas ellas, excepto la negación, son operaciones *binarias,* porque a partir de dos proposiciones se obtiene una nueva proposición.

Conjunción o producto lógico

***Definición*:** Se llama *conjunción* o *producto lógico* de p y q , y se simboliza $p \wedge q$ (se lee p y q), a la proposición obtenida a partir de p y de q que toma el valor de verdad verdadero si y sólo si los valores de verdad de ambas son verdaderos. Esto se sintetiza en la siguiente *tabla de verdad*:

p	q	$p \wedge q$
V	V	V
V	F	F
F	V	F
F	F	F

La "tabla de verdad" expresa que, para que $p \wedge q$ sea verdadera es necesario y suficiente que ambas, p y q , lo sean.
Veremos algunos ejemplos que nos muestran que esta definición se corresponde con la idea que tenemos de la conjunción "y" en nuestro lenguaje corriente.

Ejemplos:

p : 3 divide a 15
q : 6 divide a 15
r : 5 divide a 15
s : 10 divide a 15

Claramente $\mathcal{V}(p) = \mathcal{V}(r) =$ V ; $\mathcal{V}(q) = \mathcal{V}(s) =$ F
$p \wedge q$: 3 divide a 15 y 6 divide a 15 (o lo que es equivalente: 3 y 6 dividen a 15)
$p \wedge r$: 3 y 5 dividen a 15
$p \wedge s$: 3 y 10 dividen a 15
$s \wedge q$: 10 y 6 dividen a 15

En estos ejemplos vemos que la única verdadera es $p \wedge r$, donde p y r son verdaderas:
$\mathcal{V}(p \wedge r) =$ V ; $\mathcal{V}(p \wedge q) = \mathcal{V}(p \wedge s) = \mathcal{V}(s \wedge q) =$ F

Disyunción o suma lógica

***Definición*:** Se llama *disyunción* o *suma lógica* de *p* y de *q*, y se simboliza $p \vee q$ (se lee *p* o *q*), a la proposición obtenida a partir de *p* y *q* que toma el valor de verdad falso si y sólo si los valores de verdad de ambas son falsos. Esto se sintetiza en la siguiente *tabla de verdad*:

p	q	$p \vee q$
V	V	V
V	F	V
F	V	V
F	F	F

La "tabla de verdad" expresa que, para que $p \vee q$ sea falsa es necesario y suficiente que ambas, *p* y *q* , sean falsas.
Veremos con los ejemplos dados anteriormente que esta definición se corresponde con la idea que tenemos de la disyunción "o" en nuestro lenguaje corriente.

$p \vee q$: 3 divide a 15 o 6 divide a 15 (o equivalentemente: 3 o 6 dividen a 15)
$p \vee r$: 3 o 5 dividen a 15
$p \vee s$: 3 o 10 dividen a 15
$s \vee q$: 10 o 6 dividen a 15

En estos ejemplos vemos que la única proposición falsa es $s \vee q$, en la cual *s* y *q* son falsas: $\mathcal{V}(p \vee r) = \mathcal{V}(p \vee q) = \mathcal{V}(p \vee s) = \text{V}$; $\mathcal{V}(s \vee q) = \text{F}$

Negación

***Definición*:** La *negación* de una proposición *p*, como la palabra lo indica, es su proposición contraria u opuesta, en el sentido de su valor de verdad. La negación de *p*, que llamaremos *no p* , la simbolizaremos $\sim p$.
La *tabla de verdad* correspondiente a $\sim p$ es la siguiente:

p	$\sim p$
V	F
F	V

Ejemplos:

Para las proposiciones definidas anteriormente

$\sim p$: 3 no divide a 15
$\sim q$: 6 no divide a 15
$\sim r$: 5 no divide a 15
$\sim s$: 10 no divide a 15

$\mathcal{V}(\sim q) = \mathcal{V}(\sim s) = \text{V}$; $\mathcal{V}(\sim p) = \mathcal{V}(\sim r) = \text{F}$

Condicional

***Definición*:** El *condicional* es una operación que conecta dos proposiciones mediante las palabras: *Si …entonces….* Simbolizaremos el condicional entre p y q de la siguiente forma : $p \to q$, y lo leeremos *si p entonces q* .

> *La diversidad del uso de la frase "si ……., entonces….." en el lenguaje ordinario y en la lógica matemática está en la base y hasta apasionadas discusiones en las cuales, dicho sea de paso, los verdaderos lógicos profesionales han tomado poca parte. Es interesante saber que los comienzos de esta discusión se remontan a la Antigüedad. El filósofo griego Filón de Megara (del siglo IV a.J.C), fue probablemente el primero en la historia de la lógica que propagó el uso de la implicación material; esto le oponía al punto de vista de su maestro, Diodoro Crono, el cual proponía usar la implicación en un sentido más estricto, más bien relacionado con lo que hoy consideramos el sentido formal de la implicación. Algo más tarde (en el siglo III a.J.C), y probablemente bajo la influencia de Filón, se discutieron por parte de los filósofos y lógicos griegos de la escuela estoica varias concepciones posibles de la implicación.*
> ("El mundo de las Matemáticas" J.R.Newman)

Definiremos el condicional mediante la siguiente *tabla de verdad*:

p	q	$p \to q$
V	V	V
V	F	F
F	V	V
F	F	V

De acuerdo con lo expresado por la tabla de verdad, un condicional $p \to q$ es falso si y sólo si p es verdadera y q falsa.
p se denomina el *antecedente* y q el *consecuente* de la proposición $p \to q$
La idea intuitiva que representa el condicional es: de una proposición verdadera no podemos concluir una falsa, si queremos que éste sea verdadero, mientras que si el antecedente es falso, el consecuente puede ser verdadero o falso y el condicional seguirá siendo verdadero.

Ejemplos:

p: hoy llueve
q: hoy voy al cine
$p \to q$: si hoy llueve entonces hoy voy al cine
Obsérvese que si "hoy llueve y voy al cine", la proposición $p \to q$ es verdadera; si "hoy llueve y no voy al cine" , la afirmación $p \to q$ resulta falsa; en cambio, si "hoy no llueve, yo puedo ir al cine o no" , y en cualquier caso no varía la veracidad de $p \to q$, porque el condicional dice lo que haré en el caso que llueva, pero no dice nada para el caso que no llueva.

Nota: Hay distintas formas de leer el condicional $p \to q$; ellas son:
Si p entonces q
p, sólo si q
q, si p
p es condición suficiente para q
q es condición necesaria para p

Fórmulas proposicionales

Al igual que ocurre en el Álgebra, a partir de dos proposiciones, y un conectivo lógico (o de una proposición, si el conectivo es la negación) obtenemos una nueva proposición, y por tanto, a ésta y otra proposición, podemos aplicarle un conectivo obteniendo así otra diferente, y así sucesivamente, la cantidad de veces que queramos, obteniendo así una *fórmula lógica o proposicional*, que es la versión lógica de la expresión algebraica.
Simbolizaremos las fórmulas lógicas con las letras $\mathcal{A}$, $\mathcal{B}$, $\mathcal{C}$,$\mathcal{D}$, etc.

Bicondicional

La primera de las fórmulas proposicionales que daremos es el *bicondicional,* que es la conjunción de dos condicionales contrarios.
A la fórmula: $(p \to q) \wedge (q \to p)$ la llamamos el *bicondicional* y la notamos: $p \leftrightarrow q$
Veamos cómo es la *tabla de verdad* del bicondicional.

p	q	$p \to q$	$q \to p$	$(p \to q) \wedge (q \to p)$	$p \leftrightarrow q$
V	V	V	V	V	V
V	F	F	V	F	F
F	V	V	F	F	F
F	F	V	V	V	V

Por lo tanto el bicondicional es verdadero si y sólo si p y q, ambas son verdaderas, o ambas falsas.

Ejemplos: Son fórmulas proposicionales

$\mathcal{A} : \sim [p \wedge (q \to r)]$
$\mathcal{B} : p \wedge (\sim p)$
$\mathcal{C} : p \vee (\sim p)$
$\mathcal{D} : (p \wedge q) \vee (\sim t)$

***Definición*:** Dos fórmulas $\mathcal{A}$ y $\mathcal{B}$ se dicen *lógicamente equivalentes* cuando tienen la misma tabla de verdad, o sea, para cada uno de los posibles valores de verdad de sus componentes o variables primarias, los valores de verdad de ambas fórmulas coinciden.
Cuando $\mathcal{A}$ y $\mathcal{B}$ sean lógicamente equivalentes lo notaremos: $\mathcal{A} \equiv \mathcal{B}$.

Ejemplos:

1) $\sim (\sim p) \equiv p$

Vamos a demostrarlo

p	$\sim p$	$\sim (\sim p)$
V	F	V
F	V	F

Nótese que p y $\sim (\sim p)$ son ambas verdaderas o ambas falsas para cada valor de verdad de p.

2) $\sim(p \wedge q) \equiv (\sim p) \vee (\sim q)$

Haremos las tablas de verdad para demostrarla.

p	q	$\sim p$	$\sim q$	$p \wedge q$	$\sim(p \wedge q)$	$(\sim p) \vee (\sim q)$
V	V	F	F	V	F	F
V	F	F	V	F	V	V
F	V	V	F	F	V	V
F	F	V	V	F	V	V

Vemos que las dos últimas columnas coinciden, luego las dos fórmulas son equivalentes.

3) $\sim(p \vee q) \equiv (\sim p) \wedge (\sim q)$

Comprobémoslo con las tablas de verdad

p	q	$\sim p$	$\sim q$	$p \vee q$	$\sim(p \vee q)$	$(\sim p) \wedge (\sim q)$
V	V	F	F	V	F	F
V	F	F	V	V	F	F
F	V	V	F	V	F	F
F	F	V	V	F	V	V

Vemos que las dos últimas columnas coinciden, luego las dos fórmulas son equivalentes.

4) $p \rightarrow q \equiv (\sim p) \vee q$

p	q	$p \rightarrow q$	$\sim p$	$(\sim p) \vee q$
V	V	V	F	V
V	F	F	F	F
F	V	V	V	V
F	F	V	V	V

Las columnas 3 y 5 coinciden, luego son equivalentes.

5) $(\sim q \wedge p \rightarrow \sim p) \equiv \quad p \rightarrow q$

La demostración de esta equivalencia se deja como ejercicio.

Leyes de De Morgan

En los ejemplos 2) y 3) hemos demostrado las Leyes de De Morgan:

$$\sim(p \wedge q) \equiv (\sim p) \vee (\sim q) \qquad \text{y}$$

$$\sim(p \vee q) \equiv (\sim p) \wedge (\sim q)$$

August De Morgan nació en la actualmente llamada Madurai (India) el 27 de junio de 1806 y falleció en Londres el 18 de marzo de 1871. Siendo, junto a Sir William Hamilton, uno de los principales inspiradores de la Lógica, aportó a la misma una inteligencia más sensible y flexible que la de Hamilton y, además, entrenada en la Matemática. Cuantificó el predicado, dando una detallada tabla de las treinta y dos formas diferentes de proposición que surgen de esa cuantificación, añadió reglas de transformación y anunció equivalencias.

Generalización de las Leyes de De Morgan

$$\sim (p_1 \wedge p_2 \wedge p_3 \wedge ... \wedge p_n) = (\sim p_1) \vee (\sim p_2) \vee (\sim p_3) \vee ... \vee (\sim p_n)$$

$$\sim (p_1 \vee p_2 \vee p_3 \vee ... \vee p_n) = (\sim p_1) \wedge (\sim p_2) \wedge (\sim p_3) \wedge ... \wedge (\sim p_n)$$

Ejemplo: ¿A qué fórmula será equivalente $\sim (p \rightarrow q)$?

por lo visto antes $p \rightarrow q \equiv (\sim p) \vee q$

entonces $\sim (p \rightarrow q) \equiv \sim [(\sim p) \vee q]$

Por las Leyes de De Morgan, $\sim [(\sim p) \vee q] \equiv [\sim (\sim p)] \wedge (\sim q)$

$\sim (\sim p) \equiv p$

Luego $[\sim (\sim p)] \wedge (\sim q) \equiv p \wedge (\sim q)$

Entonces $\sim (p \rightarrow q) \equiv p \wedge (\sim q)$

Verifiquémoslo con las tablas de verdad

p	q	$p \rightarrow q$	$\sim (p \rightarrow q)$	$\sim q$	$p \wedge (\sim q)$
V	V	V	F	F	F
V	F	F	V	V	V
F	V	V	F	F	F
F	F	V	F	V	F

Vemos que las columnas 4 y 6 coinciden, luego las fórmulas son equivalentes.

Tautología y Contradicción

***Definición*:** Una *Tautología* es una fórmula proposicional que toma el valor de verdad verdadero para todos los valores de verdad de sus componentes primarias, y una *Contradicción* es una fórmula que toma el valor de verdad falso para todos los valores de verdad de sus componentes primarias.

Ejemplos:

1) $p \vee (\sim p)$ es una Tautología

Haremos la tabla de verdad para demostrarlo

p	$\sim p$	$p \vee (\sim p)$
V	F	V
F	V	V

2) $p \wedge (\sim p)$ es una Contradicción

Haremos la tabla de verdad para demostrarlo

p	$\sim p$	$p \wedge (\sim p)$
V	F	F
F	V	F

Ejercicios:

1) Demostrar que las siguientes fórmulas proposicionales son tautologías:
i. $\mathcal{A} : \sim (p \vee q) \leftrightarrow (\sim p) \wedge (\sim q)$
ii. $\mathcal{B} : \sim (p \wedge q) \leftrightarrow (\sim p) \vee (\sim q)$

2) Demostrar que, en general, si $\mathcal{A}$ y $\mathcal{B}$ son fórmulas equivalentes, o sea, si $\mathcal{A} \equiv \mathcal{B}$ entonces $\mathcal{A} \leftrightarrow \mathcal{B}$ es una tautología
3) Demostrar que $\mathcal{A}$ es tautología si y sólo si $\sim \mathcal{A}$ es contradicción

Deducciones lógicas

Observemos que en la tabla de verdad del condicional

p	q	$p \rightarrow q$
V	**V**	**V**
V	F	F
F	V	V
F	F	V

Hay una única fila en la que $\mathcal{V}(p) = \mathcal{V}(p \rightarrow q)$ = V , y es aquélla en la que $\mathcal{V}(q)$ = V ; luego podemos afirmar que si $\mathcal{V}(p) = \mathcal{V}(p \rightarrow q)$ = V entonces $\mathcal{V}(q)$ = V . Esta situación se expresa diciendo que *q se deduce lógicamente de p y de* $p \rightarrow q$, y se simboliza : $p \rightarrow q$, $p \Rightarrow q$, y se lee " $p \rightarrow q$ y *p implican q*"

***Definición*:** Sean $\mathcal{A}$, $\mathcal{B}$, $\mathcal{C}$ fórmulas proposicionales. Diremos que $\mathcal{C}$ se *deduce lógicamente* de $\mathcal{A}$ y de $\mathcal{B}$ si cada vez que $\mathcal{V}(\mathcal{A}) = \mathcal{V}(\mathcal{B}) =$ V entonces $\mathcal{V}(\mathcal{C}) =$ V .
Simbolizaremos este hecho con: $\mathcal{A}$, $\mathcal{B} \Rightarrow \mathcal{C}$
En general , si $\mathcal{A}_1$, $\mathcal{A}_2$, $\mathcal{A}_3$, … , $\mathcal{A}_n$, $\mathcal{C}$ son fórmulas proposicionales, diremos que $\mathcal{C}$ se deduce lógicamente de $\mathcal{A}_1$, $\mathcal{A}_2$, $\mathcal{A}_3$, … , $\mathcal{A}_n$ si cada vez que
$\mathcal{V}(\mathcal{A}_1) = \mathcal{V}(\mathcal{A}_2) = \mathcal{V}(\mathcal{A}_3) = \ldots = \mathcal{V}(\mathcal{A}_n) =$ V entonces $\mathcal{V}(\mathcal{C}) =$ V .

Lo simbolizaremos: $\mathcal{A}_1 , \mathcal{A}_2 , \mathcal{A}_3 , \ldots , \mathcal{A}_n \Rightarrow \mathcal{C}$

Ejemplo:
$p \vee q , \sim p \Rightarrow q$

Observemos la tabla de verdad

p	q	$\sim p$	$p \vee q$
V	V	F	V
V	F	F	V
F	**V**	**V**	**V**
F	F	V	F

Veamos que cuando $\mathcal{V}(\sim p) =$ $\mathcal{V}(p \vee q) =$ V también $\mathcal{V}(q) =$ V

Si bien notamos que la confección de una tabla de verdad para verificar una inferencia lógica, es un método extremadamente sencillo, también podemos observar que puede ser largo y tedioso si la cantidad de variables primarias que intervienen en las fórmulas es relativamente grande; por ello es conveniente conocer ciertas deducciones lógicas básicas, que nos permitan realizar las inferencias lógicas sin necesidad de confeccionar la tabla de verdad.

Inferencias lógicas básicas:

1. *modus ponens* (MP): $\mathcal{A} , \mathcal{A} \rightarrow \mathcal{B} \Rightarrow \mathcal{B}$
2. *modus tolens* (MT): $\sim \mathcal{B} , \mathcal{A} \rightarrow \mathcal{B} \Rightarrow \sim \mathcal{A}$
3. *silogismo disyuntivo* (SD): $\mathcal{A} \vee \mathcal{B} , \sim \mathcal{A} \Rightarrow \mathcal{B}$
4. *contrarrecíproco* (CR): $\mathcal{A} \rightarrow \mathcal{B} \Rightarrow \sim \mathcal{B} \rightarrow \sim \mathcal{A}$
5. *simplificación* (S): $\mathcal{A} \wedge \mathcal{B} \Rightarrow \mathcal{A}$ (también $\mathcal{A} \wedge \mathcal{B} \Rightarrow \mathcal{B}$)
6. *adición* (A): $\mathcal{A} \Rightarrow \mathcal{A} \vee \mathcal{B}$ (también $\mathcal{B} \Rightarrow \mathcal{A} \vee \mathcal{B}$)
7. *silogismo hipotético* (SH): $\mathcal{A} \rightarrow \mathcal{B} , \mathcal{B} \rightarrow \mathcal{C} \Rightarrow \mathcal{A} \rightarrow \mathcal{C}$

Nota: de $\mathcal{A} \Rightarrow \mathcal{B}$ y $\mathcal{C} \Rightarrow \mathcal{B}$ tendremos $\mathcal{A} \wedge \mathcal{C} \Rightarrow \mathcal{B}$
de $\mathcal{A} \Rightarrow \mathcal{B}$ obtenemos $\mathcal{A} \vee \mathcal{C} \Rightarrow \mathcal{B}$

***Demostración*:** Demostraremos el 2. (MT) a modo de ejemplo; los demás se dejan como ejercicios.

Partiremos de los distintos valores de verdad de las fórmulas dadas.
Para demostrar que la inferencia es verdadera debemos verificar que cada vez que
$\mathcal{V}(\sim \mathcal{B}) =$ $\mathcal{V}(\mathcal{A} \rightarrow \mathcal{B}) =$ V también es $\mathcal{V}(\sim \mathcal{A}) =$ V , por lo tanto sólo nos interesan las filas correspondiente a $\mathcal{V}(\mathcal{B}) =$ F

$\mathcal{A}$	$\mathcal{B}$	$\sim \mathcal{B}$	$\mathcal{A} \rightarrow \mathcal{B}$	$\sim \mathcal{A}$
V	F	V	F	F
F	F	**V**	**V**	**V**

La tabla de verdad muestra que si $\mathcal{V}(\sim \mathcal{B}) = \mathcal{V}(\mathcal{A} \to \mathcal{B}) = V$ también $\mathcal{V}(\sim \mathcal{A}) = V$, por lo tanto $\sim \mathcal{B}, \mathcal{A} \to \mathcal{B} \Rightarrow \sim \mathcal{A}$.

Métodos de Demostración

Los métodos de demostración que veremos son los recursos que podemos utilizar para demostrar que un condicional es verdadero. Ellos son: el *método directo*, el *método indirecto* o *contrarrecíproco* y el *método por el absurdo*.

Los condicionales asociados a un condicional dado $p \to q$ son:

i. $q \to p$ (recíproco)
ii. $\sim p \to \sim q$ (contrario)
iii. $\sim q \to \sim p$ (contrarrecíproco)

Ejercicio: Demostrar que $p \to q \equiv \sim q \to \sim p$, $q \to p \equiv \sim p \to \sim q$ y que $p \to q \not\equiv q \to p$

Si tenemos un condicional $\mathcal{A} \to \mathcal{B}$ sabemos que de la única forma en que será falso es si $\mathcal{V}(\mathcal{A}) = V$ y $\mathcal{V}(\mathcal{B}) = F$, y en este hecho deberemos basarnos para demostrar que $\mathcal{A} \to \mathcal{B}$ es verdadero.

Método directo

Dadas $\mathcal{A}$ y $\mathcal{B}$ fórmulas proposicionales, el método directo se basa en analizar los posibles valores de verdad de $\mathcal{A}$. Como para $\mathcal{V}(\mathcal{A}) = F$ siempre se cumplirá que $\mathcal{V}(\mathcal{A} \to \mathcal{B}) = V$, sólo nos interesa analizar cuando $\mathcal{V}(\mathcal{A}) = V$, si establecemos que $\mathcal{V}(\mathcal{B}) = V$, habremos demostrado que $\mathcal{V}(\mathcal{A} \to \mathcal{B}) = V$.

Ejemplo:

Vamos a definir algunos conceptos para entender el ejemplo.
Decimos que para a , b números enteros , $a \neq 0$, a "divide a" b si podemos escribir $b = c.a$ para algún entero c .

Notación: escribiremos: $a \mid b$ cuando a divida a b , y $a \nmid b$ cuando a no divida a b .

Queremos demostrar que $a \mid b \wedge b \mid c \to a \mid c$

En este caso $\mathcal{A}$: " $a \mid b \wedge b \mid c$ " , y $\mathcal{B}$: " $a \mid c$ "

Suponiendo $\mathcal{V}(\mathcal{A}) = V$ debemos ver que $\mathcal{V}(\mathcal{B}) = V$.

Si suponemos $\mathcal{V}(\mathcal{A}) = V$, por definición, sabemos que $b = k.a$, y que $c = h.b$, donde k, h son números enteros , entonces reemplazando b en la segunda igualdad, tenemos que $c = k.h.a$ y como $k.h$ es también un número entero , por lo tanto $a \mid c$ y así $\mathcal{V}(\mathcal{B}) = V$. Luego $\mathcal{V}(\mathcal{A} \to \mathcal{B}) = V$

Método indirecto o contrarrecíproco

Dadas $\mathcal{A}$ y $\mathcal{B}$ fórmulas proposicionales, este método se basa en analizar los valores de verdad de $\mathcal{B}$ Para $\mathcal{V}(\mathcal{B})$ = V , siempre resulta $\mathcal{V}(\mathcal{A} \rightarrow \mathcal{B})$ = V (ver tabla de verdad del condicional!) , así que sólo nos interesa establecer qué ocurre cuando $\mathcal{V}(\mathcal{B})$ = F : para que $\mathcal{V}(\mathcal{A} \rightarrow \mathcal{B})$ = V debe ser $\mathcal{V}(\mathcal{A})$ = F .

Ejemplo:

Recordaremos algunas notaciones y propiedades:

- Si a es mayor o igual que b lo escribiremos : $a \geq b$
- Si a y b son distintos, lo escribimos $a \neq b$
- Si a es un número natural , se verifica que $a \geq 1$
- Si a es un número natural o es cero lo escribiremos : $a \in \mathbb{N} \cup \{0\}$
- a es menor o igual que b si y sólo si b es mayor o igual que a ; en símbolos : $a \leq b$ si y sólo si $b \geq a$
- consistencia del orden respecto de la suma : si $a \leq b$ se verifica que $a + c \leq b + c$ cualquiera sea el número c
- Si a es menor que b , lo escribiremos $a < b$, y tenemos que $a < b$ si y sólo si $a \leq b$ y $a \neq b$. Análogamente , a es mayor que b , $a > b$, si y sólo si $a \geq b$ y $a \neq b$

Queremos demostrar que si a , $b \in \mathbb{N} \cup \{0\}$: $a + b = 1 \rightarrow a = 0 \vee b = 0$

$\mathcal{A}$: " $a + b = 1$ " ; $\mathcal{B}$: " $a = 0 \vee b = 0$ " ;
$\sim \mathcal{A}$: " $a + b \neq 1$ " ; $\sim \mathcal{B}$: " $a \neq 0 \wedge b \neq 0$ "

Si $\mathcal{V}(\mathcal{B})$ = F , entonces $\mathcal{V}(\sim \mathcal{B})$ = V ;
Si $\mathcal{V}(\mathcal{B})$ = F (o sea, $\mathcal{V}(\sim \mathcal{B})$ = V) se verifica que $a \neq 0 \wedge b \neq 0$

Como a , $b \in \mathbb{N} \cup \{0\}$, y además $a \neq 0 \wedge b \neq 0$ entonces a , $b \in \mathbb{N}$, por lo tanto $a \geq 1 \wedge b \geq 1$

Por ser $a \geq 1$, se verifica que $a + b \geq 1 + b$, y por ser $b \geq 1$, $1 + b \geq 1 + 1 = 2 > 1$

Luego $a + b > 1$, y por lo tanto $a + b \neq 1$, con lo cual $\mathcal{V}(\sim \mathcal{A})$ = V , y por ende $\mathcal{V}(\mathcal{A})$ = F

Así $\mathcal{V}(\mathcal{A} \rightarrow \mathcal{B})$ = V

Nota: Demostrar $\mathcal{V}(\mathcal{A} \rightarrow \mathcal{B})$ = V por el método indirecto, no es otra cosa que demostrar $\mathcal{V}(\sim \mathcal{B} \rightarrow \sim \mathcal{A})$ = V por el método directo, y esto es válido porque $\mathcal{A} \rightarrow \mathcal{B} \equiv \sim \mathcal{B} \rightarrow \sim \mathcal{A}$

Método por el absurdo

Partimos de la siguiente equivalencia lógica:

$(\sim \mathcal{B} \wedge \mathcal{A} \rightarrow \sim \mathcal{A}) \equiv \mathcal{A} \rightarrow \mathcal{B}$

Luego, si queremos demostrar que el condicional $\mathcal{A} \rightarrow \mathcal{B}$ es verdadero, ello es equivalente a demostrar que es verdadero el condicional $\sim \mathcal{B} \wedge \mathcal{A} \rightarrow \sim \mathcal{A}$; aplicamos el método directo para demostrar este último, para lo cual debemos ver que si

$\mathcal{V}(\sim \mathcal{B} \wedge \mathcal{A}) = \text{V}$ entonces $\mathcal{V}(\sim \mathcal{A}) = \text{V}$

Ejemplo:
Si $0 < x < 1 \rightarrow x^2 < 1$

Notaciones y propiedades previas:

- $\mathbb{R}$ es el conjunto de números reales
- Si $x \in \mathbb{R}$ (si x es un número real) , $x \neq 0$, tiene inverso multiplicativo $x^{-1} = \frac{1}{x}$
- Consistencia del orden respecto del producto por un número positivo:
  si $x, y, z \in \mathbb{R}$, $x \leq y$ y $z > 0$ entonces $x.z \leq y.z$
- Si $x > 0$, entonces $x^{-1} > 0$ y $x^2 > 0$
- x no es menor que y se simboliza: $x \not< y$

$\mathcal{A}$: " $0 < x < 1$ " ; $\mathcal{B}$: " $x^2 < 1$ " ; $\sim \mathcal{B} \wedge \mathcal{A}$: " $x^2 \not< 1 \wedge 0 < x < 1$ "

Demostración: Supongamos que $\mathcal{V}(\sim \mathcal{B} \wedge \mathcal{A}) = \text{V}$, o sea, $0 < x < 1$ y que $x^2 \not< 1$; luego debe ser $x^2 \geq 1$.

$0 < x < 1$ entonces $\frac{1}{x} > 1 > 0$, por consistencia del orden con respecto al producto por números positivos, $x = x^2 . \frac{1}{x} \geq 1 . \frac{1}{x} > 1$, o sea, no se cumple que $0 < x < 1$.

Luego $\mathcal{V}(\sim \mathcal{A}) = \text{V}$, lo que resulta una contradicción ya que supusimos que $\mathcal{V}(\sim \mathcal{B} \wedge \mathcal{A}) = \text{V}$, lo que significa que $\mathcal{V}(\mathcal{A}) = \text{V}$; esto es un absurdo que proviene de suponer $\mathcal{V}(\sim \mathcal{B} \wedge \mathcal{A}) = \text{V}$, con lo cual $\mathcal{V}(\sim \mathcal{B} \wedge \mathcal{A}) = \text{F}$, y así la implicación $\sim \mathcal{B} \wedge \mathcal{A} \rightarrow \sim \mathcal{A}$ resulta verdadera, y con ella también $\mathcal{V}(\mathcal{A} \rightarrow \mathcal{B}) = \text{V}$.

Ejercicios:

1. Sean $p: 1 \leq 10$, $q: 0 \leq 1$.
Determinar el valor de verdad de cada una de las proposiciones siguientes:

a) $\sim p$
b) $p \wedge q$
c) $\sim p \wedge \sim q$
d) $p \vee q$
e) $p \leftrightarrow q$
f) $p \leftrightarrow \sim q$
g) $\sim q$
h) $p \vee \sim q$

2. Hacer las tablas de verdad de las siguientes fórmulas proposicionales:

a) $\sim (p \wedge q)$
b) $\sim p \vee \sim q$
c) $\sim (p \vee q)$
d) $\sim p \wedge \sim q$
e) $p \wedge \sim q$
f) $\sim p \vee q$
g) $\sim q \rightarrow \sim p$
h) $\sim \left[p \wedge (q \rightarrow r) \right]$

3. Simbolizar completamente las proposiciones siguientes, utilizando el símbolo que corresponde a cada término de enlace. Designar con letras minúsculas cada proposición atómica o mínima:

a) El área del triángulo *ABC* es igual que el área del triángulo *DEF*, o el área del triángulo *ABC* es menor que el área del triángulo *DEF*.
b) Tomará parte en el salto de altura y correrá media milla.
c) Si las células de las plantas no tienen clorofila, entonces no pueden sintetizar los alimentos.
d) O tomará parte en la representación o no ayudará en el vestuario.
e) Si *a* no es igual que cinco, entonces o es mayor que cinco o es menor que cinco.
f) Si el Sr. Perez no está enfadado, entonces Luis no ha venido demasiado tarde.
g) O sus deberes están terminados, o si no están terminados tendrá que hacerlos por la noche.
h) Se puede dar el vector por medio de dos componentes, o estamos en tres dimensiones.

4. Demostrar que las siguientes proposiciones son tautologías:

a) $\sim (p \vee q) \leftrightarrow \sim p \wedge \sim q$
b) $\sim (p \wedge q) \leftrightarrow \sim p \vee \sim q$
c) $(p \rightarrow q) \leftrightarrow \sim p \vee q$
d) $(p \rightarrow q) \leftrightarrow (\sim q \rightarrow \sim p)$

5. Dadas *p*, *q* y *r* variables proposicionales, *F* es una contradicción y *T* una tautología. Verificar en cada uno de los siguientes casos si los pares de proposiciones dadas son o no lógicamente equivalentes y cuando no lo sean explicar por qué:

a) $\sim p \vee q$ y $p \rightarrow q$
b) $p \wedge (q \vee T)$ y p
c) $(p \vee q) \wedge (p \wedge q)$ y $\sim (p \wedge q)$
d) $p \leftrightarrow q$ y $(p \wedge q) \vee (\sim p \wedge \sim q)$
e) $(p \rightarrow q) \rightarrow r$ y $p \rightarrow (q \rightarrow r)$

f) p y $q \wedge r$

g) $\sim p \wedge \sim q$ y $\sim (p \vee q)$

h) $(p \wedge \sim q) \vee r$ y $\sim (\sim p \vee q) \rightarrow r$

6. Dadas p, q y r variables proposicionales, F es una contradicción y T una tautología. Verificar cada una de las siguientes Leyes del Álgebra de Proposiciones:

Leyes Idempotentes

1.a) $p \vee p \equiv p$ 1.b) $p \wedge p \equiv p$

Leyes de Asociatividad

2.a) $p \vee (q \vee r) \equiv (p \vee q) \vee r$ 2.b) $p \wedge (q \wedge r) \equiv (p \wedge q) \wedge r$

Leyes Conmutativas

3.a) $p \vee q \equiv q \vee p$ 3.b) $p \wedge q \equiv q \wedge p$

Leyes distributivas

4.a) $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$

4.b) $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$

Leyes de Identidad

5.a) $p \vee F \equiv p$ 5.b) $p \wedge T \equiv p$

6.a) $p \vee T \equiv T$ 6.b) $p \wedge F \equiv F$

Leyes de complementos (o de inversas)

7.a) $p \vee \sim p \equiv T$ 7.b) $p \wedge \sim p \equiv F$

8.a) $\sim (\sim p) \equiv p$ 8.b) $\sim T \equiv F$ y $\sim F \equiv T$

Leyes de De Morgan

9.a) $\sim (p \vee q) \equiv \sim p \wedge \sim q$ 9.b) $\sim (p \wedge q) \equiv \sim p \vee \sim q$

Leyes de Doble Negación o Involución

10. $\sim (\sim p) \equiv p$

7. Demostrar que las siguientes equivalencias lógicas de la implicación y su negación:

a) $(p \rightarrow q) \equiv \sim p \vee q$

b) $(p \rightarrow q) \equiv (\sim q \rightarrow \sim p)$

c) $\sim (p \rightarrow q) \equiv p \wedge \sim q$

8. Demostrar las siguientes inferencias lógicas básicas:

a. *modus ponens* : $\mathcal{A}$, $\mathcal{A} \rightarrow \mathcal{B} \Rightarrow \mathcal{B}$

b. *modus tolens* : $\sim \mathcal{B}$, $\mathcal{A} \rightarrow \mathcal{B} \Rightarrow \sim \mathcal{A}$

c. *silogismo disyuntivo* : $\mathcal{A} \vee \mathcal{B}$, $\sim \mathcal{A} \Rightarrow \mathcal{B}$

d. *contrarrecíproco* : $\mathcal{A} \rightarrow \mathcal{B} \Rightarrow \sim \mathcal{B} \rightarrow \sim \mathcal{A}$

e. *simplificación* (S) : $\mathcal{A} \wedge \mathcal{B} \Rightarrow \mathcal{A}$ (también $\mathcal{A} \wedge \mathcal{B} \Rightarrow \mathcal{B}$)

f. *adición* (A): $\mathcal{A} \Rightarrow \mathcal{A} \vee \mathcal{B}$ (también $\mathcal{B} \Rightarrow \mathcal{A} \vee \mathcal{B}$)

g. *silogismo hipotético* (SH): $\mathcal{A} \rightarrow \mathcal{B}$, $\mathcal{B} \rightarrow \mathcal{C} \Rightarrow \mathcal{A} \rightarrow \mathcal{C}$

h. $\mathcal{A} \rightarrow \mathcal{B}$, $\mathcal{C} \rightarrow \mathcal{B} \Rightarrow \mathcal{A} \wedge \mathcal{C} \rightarrow \mathcal{B}$

i. $\mathcal{A} \rightarrow \mathcal{B} \Rightarrow \mathcal{A} \wedge \mathcal{C} \rightarrow \mathcal{B}$

'Ponens' significa 'que pone' o 'que afirma'; 'tollens', 'que borra' o 'que niega'. Así, 'modus ponendo ponens' puede traducirse 'modo que afirma afirmando'; 'modus tollendo tollens', 'modo que niega negando'; 'modus tollendo ponens', 'modo que afirma negando'; 'modus ponendo tollens', 'modo que niega afirmando. 'Modus ponens' puede traducirse 'modo que afirma' o 'modo afirmativo'; 'modus tollens', 'modo que niega' o 'modo negativo'.
("Diccionario de Filosofía", J. Ferrater Mora)

9. Simplificar cada uno de los siguientes polinomios booleanos o proposiciones (es decir, sustituyendo por expresiones lógicamente equivalentes, tratar de obtener una expresión en $\sim$, $\wedge$ y $\vee$ con un número mínimo de términos):

a) $p \vee (\sim p \vee q)$

b) $(p \vee q) \wedge \sim p$

c) $(p \wedge q) \vee p$

d) $(p \wedge q \wedge r) \vee (p \wedge q \wedge \sim r)$

e) $(p \rightarrow q) \wedge p$

f) $(p \rightarrow r) \wedge (p \rightarrow q)$

g) $(p \vee q) \vee (\sim p \wedge \sim q)$

10. Expresar simbólicamente la siguiente afirmación: "si el cuadrado de un número entero es par, entonces ese número es par".
Enunciar el contrarrecíproco, el contrario y el recíproco.

11. Negar las proposiciones compuestas del ejercicio 3, y luego expresarlas en lenguaje coloquial. Emplear equivalencias si fuera necesario.

12. Demostrar que la proposición indicada es consecuencia lógica de las premisas dadas. Deducir la conclusión, escribiendo la abreviatura que corresponde a la regla que permite obtener cada línea, y cuando se empleen líneas deducidas anteriormente, indicar el número de cada línea que ha sido utilizada al aplicar la regla.

i. Demostrar : $\sim q$
$(1)\ p \rightarrow \sim q$
$(2)\ r \rightarrow p$
$(3)\ r$

ii. Demostrar : p
$(1)\ \sim r \rightarrow \sim q$
$(2)\ \sim r$
$(3)\ \sim q \rightarrow p$

iii. Demostrar: $\sim s$
$(1)\ \sim r \wedge t$
$(2)\ s \rightarrow r$

iv. Demostrar : $r \vee s$
$(1)\ \sim p \rightarrow r \vee s$
$(2)\ q \vee t \rightarrow \sim p$
$(3)\ q \vee t$

v. Demostrar : p
$(1)\ \sim p \rightarrow \sim q$
$(2)\ q$

vi. Demostrar: $p \wedge q$
$(1)\ p \wedge r$
$(2)\ p \rightarrow q$

vii. Demostrar : $\sim p$

viii. Demostrar: $p \wedge q$

ix. Demostrar: p

$(1)\ p \to q$
$(2)\ q \to r$
$(3)\ r \to s$
$(4) \sim s$

$(1)\ q$
$(2)\ q \to \sim s$
$(3)\ p \vee s$

$(1) \sim q \vee p$
$(2) \sim q \to s$
$(3) \sim s$

13. Demostrar utilizando el método que crea más conveniente:

a) Si n es impar entonces n^2 es impar, ($n \in \mathbb{Z}$)
b) Si $x = a + b$ entonces $x^2 = a^2 + 2ab + b^2$
c) Si n^2 es impar entonces n es impar, ($n \in \mathbb{Z}$)
d) Si $a \,.\, b$ es par entonces a es par o b es par
e) Si $a, b, c \in \mathbb{R}$, $a + c < b + c$ entonces $a < b$

14) a) Enunciar el contrarrecíproco de las implicaciones del ejercicio 13.
b) Enunciar la implicación recíproca de las implicaciones del ejercicio 13 y analizar la validez de las mismas.

Cálculo de predicados

Esquemas proposicionales

Cuando definimos proposición, hicimos mención de cierto tipo de expresiones en una o varias variables, que por sí mismas no poseen un valor de verdad, pero si se les asignan "valores" a la/las variable/s se transforman en proposiciones, con su correspondiente valor de verdad.

Ejemplos:

i) " x es un número primo "
ii) " x divide a 24 "
iii) " x divide a y "
iv) " x es hijo de Juan "
v) " x es hijo de y "
vi) " 4 divide a x "
vii) " 3^x "
viii) " $x + y$ "

Nótese que ninguna de ellas es proposición, porque no se puede decir que sean verdaderas o falsas. Las expresiones i), ii), iv) y vi) se convierten en proposición en cuanto le damos algún valor apropiado a la variable x ; las iii) y v) requieren que le demos valores apropiados a dos variables : x e y ; y las vii) y viii) no se convierten en proposición aunque le demos valores apropiados a la o las variables.

Las expresiones del tipo i), ii), iii), iv), v), vi) se denominan *esquemas proposicionales* , y ellas pueden ser en una o más variables. El conjunto de objetos sobre el que tomamos los elementos para darle valor a las variables de un esquema, para que éste se transforme en una proposición, lo denominamos ***universo*.**

La notación que corresponde a los esquemas proposicionales es la siguiente:

F[x] : x es un número primo
G[x] : x divide a 24
H[x, y] : x divide a y
T[x] : x es hijo de Juan
L[x, y] : x es hijo de y
N[x] : 4 divide a x

Si $\mathbf{U}$ designa al universo sobre el que se evaluarán determinados esquemas proposicionales, y $a \in \mathbf{U}$ (esto quiere decir que a es un elemento de $\mathbf{U}$) , simbolizaremos con F[a] la proposición que se obtiene del esquema F[x] al reemplazar x por a .

Nota: Dado un esquema proposicional, para transformarlo en una proposición debemos reemplazar la/las variable/s por nombres pertenecientes a cierto "universo" en el cual la expresión tenga sentido; así, para reemplazar x por algún nombre en F[x] , debemos elegir un universo dentro del conjunto de números naturales o enteros, no tiene sentido si el universo está constituido por personas o por cuadriláteros, por dar algunos ejemplos.
Cuando los esquemas son en más de una variable, cada una de ellas debe evaluarse en un universo adecuado para que la expresión tenga sentido. Por ejemplo el esquema proposicional:

S[x, y] : x usa calzado nº y

claramente las dos variables deben evaluarse en universos distintos, porque no tendría sentido evaluar *x* en un universo de números, ni tampoco *y* en uno constituido por personas.

Para el universo $\mathbb{U} = \mathbb{N}$ (conjunto de números naturales),

F[5] : 5 es un número primo
F[56] : 56 es un número primo
H[5, 20] : 5 divide a 20

Las tres son proposiciones, dos de ellas verdaderas y la otra falsa; es más:

$\mathcal{V}$(F[5]) = $\mathcal{V}$(F[19]) = $\mathcal{V}$(F[53]) = V
$\mathcal{V}$(F[25]) = $\mathcal{V}$(F[56]) = $\mathcal{V}$(F[14]) = F
$\mathcal{V}$(G[4]) = $\mathcal{V}$(G[12]) = $\mathcal{V}$(G[1]) = V
$\mathcal{V}$(G[5]) = $\mathcal{V}$(G[25]) = $\mathcal{V}$(G[13]) = F
$\mathcal{V}$(H[12, 36]) = $\mathcal{V}$(H[2, 6]) = $\mathcal{V}$(H[4,12]) = V
$\mathcal{V}$(H[7, 5]) = $\mathcal{V}$(H[5, 16]) = $\mathcal{V}$(H[11, 13]) = F

Para el universo $\mathbb{U}' = \{ Juan, Cristina, Andrés, Mariela, Laura, Esteban \}$

$\mathcal{V}$(T[*Laura*]) = V ; $\mathcal{V}$(T[*Esteban*]) = F

pero no tiene sentido F[*Laura*] , por ello tampoco se le puede asignar un valor de verdad.

Cuantificadores

Reemplazar la o las variables por elementos de un universo conveniente, no es la única forma en que podemos obtener de un esquema proposicional una proposición.
Por ejemplo, si decimos:

i. “Para todo *x* , *x* es un número primo” , o bien

ii. “Existe un *x* tal que *x* es un número primo” , o

iii. “Para todo *x* y para todo *y* , *x* divide a *y* ” , o

iv. “Para todo *x* existe un *y* tal que *x* divide a *y* ” , o

v. “Existe un *x* tal que para todo *y* , *x* divide a *y* ”

todas ellas son proposiciones, y así podríamos construir otras con el esquema H[*x*, *y*] .

Para analizar el valor de verdad de esas expresiones, en primer término hay que estar en un contexto razonable, o sea, pensarlo en un universo adecuado, luego teniendo distintos universos, aunque sean adecuados, el valor de verdad de cada una de ellas podría cambiar. Una vez fijado el universo adecuado, por ejemplo $\mathbb{U} = \mathbb{N}$, podremos decir que i. , iii. son falsas, mientras que las restantes son verdaderas.
Vamos a ocuparnos de esas locuciones que introdujimos : “para todo…” , “existe..” ; ellos se denominan *cuantificadores u operadores* , que al anteponerlos a un esquema proposicional lo transforman en una proposición.

***Cuantificador u Operador Universal para esquemas en una variable*:**

La locución "Para todo *x*… " se denomina *cuantificador u operador universal en x* , y lo simbolizaremos con $\forall x$.
En términos generales, si se tiene un esquema proposicional F[*x*] , se puede obtener de él una proposición mediante la adjunción de un operador universal : $\forall x$: F[*x*]

Ejemplos:

1) " $\forall x$: *x* es un número primo " , o " $\forall x$: F[*x*] "
2) " $\forall x$: *x* divide a 24 " , o " $\forall x$: G[*x*] "

***Cuantificador u Operador Existencial para esquemas en una variable*:**

Llamamos *cuantificador u operador existencial en x* a la locución "existe un *x* tal que…" , y la notaremos : $\exists x$
En general, si se tiene un esquema proposicional F[*x*], se puede obtener de él una proposición mediante la adjunción de un operador existencial : $\exists x$: F[*x*]

Ejemplos:

1) " $\exists x$: *x* es un número primo " , o " $\exists x$: F[*x*] "
2) " $\exists x$: 4 divide a *x* " , o " $\exists x$: N[*x*] "

Reglas de deducción para proposiciones con cuantificadores

Las reglas de deducción para proposiciones con cuantificadores son:

Para $a \in \mathbb{U}$, F[*x*] esquema proposicional
1. $\forall x$: F[*x*] $\Rightarrow$ F[*a*] , cualquiera sea $a \in \mathbb{U}$
2. F[*a*] $\Rightarrow$ $\exists x$: F[*x*]

Ejemplos: 1. "Todos los perros son mamíferos", por lo tanto "Colita es un perro entonces es mamífero"

2. "5 es un número entero primo"
Por lo tanto "existen los números enteros primos"

Negación de los cuantificadores

Dada una proposición, tenemos determinada la proposición contraria, su negación.
Por ejemplo, si tenemos la proposición:
Todo número es primo
su negación será:
No todo número es primo
o bien :
Algunos números no son primos
o también :
Existe un número que no es primo

Estas tres últimas expresiones son equivalentes en el lenguaje coloquial porque expresan el mismo concepto, pero la última podemos traducirla simbólicamente, así que, cuando tengamos: $\sim(\forall x:$ x es primo) estaremos diciendo: $\exists x$: x no es primo

En lenguaje formal: $\sim(\forall x: F[x])$ es $\exists x : \sim \mathrm{F}[x]$

***Definición*:** definiremos $\sim(\forall x: F[x])$ como "$\exists x : \sim \mathrm{F}[x]$"

Ahora, si tenemos la proposición:
Existe un número que es primo
su negación será:
No existe un número que sea primo
o bien:
Ningún número es primo
o también:
Todos los números son no primos

Como antes, las últimas tres expresiones son equivalentes en el lenguaje coloquial, pero sólo la última, quizás la que menos usaríamos, es la que puede simbolizarse lógicamente.
Cuando decimos: $\sim(\exists x:$ x es primo) estamos diciendo: $\forall x$: x no es primo
o sea que: $\sim(\exists x: \mathrm{F}[x])$ es $\forall x: \sim \mathrm{F}[x]$

***Definición*:** definiremos $\sim(\exists x: \mathrm{F}[x])$ como "$\forall x: \sim \mathrm{F}[x]$"

Cuantificadores en esquemas de dos o más variables

Volvamos al esquema

H[x, y] : x divide a y

Si le damos un valor a x o a y , y sólo a uno, no tendremos una proposición, sino un esquema proposicional en una variable:

Q[x] = H[x, 26] : x divide a 26

J[y] = H[13, y] : 13 divide a y

Para obtener una proposición debemos darle valor a ambas variables:

H[12, 35] : 12 divide a 35

Igualmente, no basta con adjuntarle un solo cuantificador para obtener una proposición:

" Para todo x , x divide a y " , o "$\forall x$: x divide a y" , o "$\forall x$: H[x, y]"

" existe un x tal que x divide a y " , o "$\exists x$: x divide a y" , o "$\exists x$: H[x, y]"

" Para todo y , x divide a y " , o "$\forall y$: x divide a y" , o "$\forall y$: H[x, y] "

" existe un y tal que x divide a y " , o "$\exists y$: x divide a y" , o "$\exists y$: H[x, y]"

Ninguna de ellas es proposición, sino esquema proposicional en una variable.
Para obtener una proposición de esos esquemas proposicionales en una variable, podemos darle un valor a la variable, o bien adjuntarle un cuantificador:
Si tenemos el esquema S[y] : $\forall x$: x divide a y

S[45] : $\forall x$: x divide a 45 , es una proposición y es falsa para $\mathrm{U} = \mathbb{N}$

También es proposición:
$\exists y : (\forall x : x \text{ divide a } y)$
que expresa que " existe un número natural que es divisible por todo número natural " , proposición que es falsa, pero es proposición (siempre en el universo $\mathbf{U} = \mathbb{N}$)

Para el esquema T[x] : $\exists y$: x divide a y
T[13] : $\exists y$: 13 divide a y , es proposición y es verdadera, para $\mathbf{U} = \mathbb{N}$
$\forall x : (\exists y : x \text{ divide a } y)$
es una proposición que dice que "cualquiera sea el número natural x siempre existirá un número natural y tal que x divida a y " , proposición que también es verdadera $(\mathbf{U} = \mathbb{N})$.

Volvamos al esquema H[x, y] ; por adición de dos cuantificadores podemos obtener las siguientes proposiciones:
i. $\forall x : (\exists y : \text{H}[x, y])$
ii. $\exists y : (\forall x : \text{H}[x, y])$
iii. $\forall x : (\forall y : \text{H}[x, y])$
iv. $\exists y : (\exists x : \text{H}[x, y])$
v. $\forall y : (\exists x : \text{H}[x, y])$
vi. $\exists x : (\forall y : \text{H}[x, y])$

Vamos a traducir al lenguaje coloquial lo que expresamos en cada una de las proposiciones:
i. " Para todo número natural x existe un número natural y tal que x divide a y " .
ii. " Existe un número natural y tal que para todo número natural x se verifica que x divide a y " .
iii. " Para todo número natural x y todo número natural y , x divide a y " .
iv. " Existe un número natural y , y existe un número natural x, tal que x divide a y "
v. " Para todo número natural y existe un número natural x tal que x divide a y "
vi. " Existe un número natural x tal que para todo número natural y , x divide a y "
Todas esas proposiciones son diferentes pues todas ellas expresan conceptos distintos.
(para $\mathbf{U} = \mathbb{N}$) :

i. es verdadera pues todo número divide a algún número, en particular se divide a sí mismo.
ii. es falsa porque no hay ningún número que sea divisible por todos los números
iii. es falsa porque no es cierto que todos los números sean divisibles por todos los números
iv. es verdadera porque hay un número para el cual existe un número que lo divida.
v. es verdadera porque cualquiera sea el número natural elegido siempre hay un número natural que lo divida.
vi. es verdadera porque hay un número natural, el 1, que divide a todo número natural

También observamos que los cuantificadores **no** son intercambiables:
i. $\forall x : (\exists y : \text{H}[x, y])$ y ii. $\exists y : (\forall x : \text{H}[x, y])$
expresan conceptos muy diferentes; y tampoco son intercambiables, en general, las variables:
i. $\forall x : (\exists y : \text{H}[x, y])$ y v. $\forall y : (\exists x : \text{H}[x, y])$

Solamente podemos intercambiar, y por lo tanto no nos interesará en qué orden los pongamos, en el caso en que los cuantificadores en ambas variables sean del mismo tipo, o ambos universales o ambos existenciales:

$\forall x : (\forall y : H[x, y])$, dice que todo número natural es divisible por todo número natural, lo mismo que dice $\forall y : (\forall x : H[x, y])$, por ello lo escribimos generalmente

$$\forall x , \forall y : H[x, y]$$

Análogamente con $\exists y : (\exists x : H[x, y])$, que dice que existen números x e y tales que x divide a y , por lo cual es equivalente a escribir $\exists x : (\exists y : H[x, y])$, por lo que lo escribiremos:

$$\exists y , \exists x : H[x, y]$$

Si tenemos un esquema en tres variables, por ejemplo:

$Q[x, y, z]$: x es máximo común divisor de y y z

Podemos reflexionar como antes; si evaluamos el esquema en una de las variables, tendremos un esquema en dos variables:

$P[y, z] = Q[2, y, z]$: 2 es máximo común divisor de y y z

$R[x, z] = Q[x, 6, z]$: x es máximo común divisor de 6 y z

$M[x, y] = Q[x, y, 13]$: x es máximo común divisor de y y 13

Si lo evaluamos en dos variables, tendremos un esquema en una:

$S[z] = Q[10, 4, z]$: 10 es máximo común divisor de 4 y z

$L[x] = Q[x, 3, 7]$: x es máximo común divisor de 3 y 7

$N[y] = Q[5, y, 8]$: 5 es máximo común divisor de y y 8

y si lo evaluamos en tres variables, tendremos una proposición:

$Q[4, 12, 16]$: 4 es máximo común divisor de 12 y 16

También podemos usar los cuantificadores para los esquemas de una variable:

$\forall x : L[x]$; $\forall y : N[y]$; $\forall z : S[z]$

$\exists x : L[x]$; $\exists y : N[y]$; $\exists z : S[z]$

y dos cuantificadores para los de dos variables:

$\forall x : (\exists z : R[x, z])$; $\exists y : (\forall x : M[x, y])$; $\forall z : (\exists y : P[y, z])$, etc.

Si adjuntamos cuantificadores al esquema en tres variables $Q[x, y, z]$:

$\forall x : Q[x, y, z]$; $\forall y : Q[x, y, z]$; $\forall z : Q[x, y, z]$

$\exists x : Q[x, y, z]$; $\exists y : Q[x, y, z]$; $\exists z : Q[x, y, z]$

obtenemos, en todos los casos, esquemas en dos variables.

Si ahora adjuntamos dos cuantificadores:

$O[z] : \forall x : (\forall y : Q[x, y, z])$; $V[z] : \forall x : (\exists y : Q[x, y, z])$;

$B[x] : \exists z : (\forall y : Q[x, y, z])$; $U[y] : \exists z : (\forall x : Q[x, y, z])$; etc.

Obtenemos esquemas proposicionales en una variable, que, como dijimos para cualquier esquema, podemos transformarlo en una proposición dándole valores a la variable o adjuntándole un cuantificador:

$\exists z : [\forall x : (\forall y : Q[x, y, z])]$; $\forall z : [\forall x : (\exists y : Q[x, y, z])]$;

$\forall x : [\exists z : (\forall y : Q[x, y, z])]$; $\exists y : [\exists z : (\forall x : Q[x, y, z])]$; etc.

Todas ellas son proposiciones.

De forma análoga podemos transformar en proposición, esquemas proposicionales en cualquier cantidad finita de variables.

Negación de los cuantificadores en esquema de más de una variable

Si tenemos un esquema en dos variables $M[x, y]$, y le adjuntamos un cuantificador obtenemos un esquema en una variable :

i. $L[x] : \forall y : M[x, y]$ ii. $S[x] : \exists y : M[x, y]$

iii. $Q[y] : \forall x : M[x, y]$ iv. $R[y] : \exists x : M[x, y]$

Por ser todos ellos esquemas en una variable, al adjuntarle un cuantificador lo transformamos en una proposición:

i. $\forall x : (\forall y : M[x, y])$ ii. $\forall x : (\exists y : M[x, y])$ iii. $\exists x : (\forall y : M[x, y])$

iv. $\exists x : (\exists y : M[x, y])$ v. $\forall y : (\forall x : M[x, y])$ vi. $\forall y : (\exists x : M[x, y])$

vii. $\exists y : (\exists x : M[x, y])$ viii. $\exists y : (\forall x : M[x, y])$

Por lo que ya vimos, los cuantificadores no son intercambiables a menos que sean del mismo tipo, por lo tanto $\forall x : (\forall y : M[x, y])$ es equivalente a $\forall y : (\forall x : M[x, y])$,
como así también lo son $\exists x : (\exists y : M[x, y])$ y $\exists y : (\exists x : M[x, y])$.

Para negar aquellas proposiciones debemos aplicar, en cada caso, la definición de la negación de cuantificadores. Veámoslo en los casos anteriores (eliminamos los casos v. y vii. por ser coincidentes con el i. y el iv. respectivamente):

i. $\sim [\forall x : (\forall y : M[x, y])] \equiv \exists x : \sim (\forall y : M[x, y]) \equiv \exists x : (\exists y : \sim M[x, y])$

ii. $\sim [\forall x : (\exists y : M[x, y])] \equiv \exists x : \sim (\exists y : M[x, y])] \equiv \exists x : (\forall y : \sim M[x, y])$

iii. $\sim [\exists x : (\forall y : M[x, y])] \equiv \forall x : \sim (\forall y : M[x, y]) \equiv \forall x : (\exists y : \sim M[x, y])$

iv. $\sim [\exists x : (\exists y : M[x, y])] \equiv \forall x : \sim (\exists y : M[x, y]) \equiv \forall x : (\forall y : \sim M[x, y])$

vi. $\sim [\forall y : (\exists x : M[x, y])] \equiv \exists y : \sim (\exists x : M[x, y]) \equiv \exists y : (\forall x : \sim M[x, y])$

viii. $\sim [\exists y : (\forall x : M[x, y])] \equiv \forall y : \sim (\forall x : M[x, y]) \equiv \forall y : (\exists x : \sim M[x, y])$

Si el esquema es de más variables, el razonamiento que se emplea para su negación es el mismo que el que aplicamos en dos variables, pero repetido tantas veces cuanta sea la cantidad de variables.

Ejemplo:

$P[x, y] : x < y$

i. $\forall x\ ,\ \forall y\ : P[x, y]$ o $\forall x\ ,\ \forall y : x < y$

"Cualesquiera sean los números x e y se verifica que $x < y$ "

Negación: $\exists x\ ,\ \exists y\ : \sim P[x, y]$ o $\exists x\ , \exists y : x \not< y$
"Existen números x e y tales que $x \not< y$ "

ii. $\forall x : (\exists y : P[x, y])$ o $\forall x : (\exists y : x < y)$

"Para todo número x existe un número y tal que $x < y$ "

Negación: $\exists x : (\forall y : \sim P[x, y])$ o $\exists x\ : (\forall y : x \not< y)$
"Existe un número x tal que para todo número y , $x \not< y$ "

iii. $\forall y : (\exists x : P[x, y])$ o $\forall y\ : (\exists x\ : x < y)$

"Para todo número y existe un número x tal que $x < y$ "

Negación: $\exists y : (\forall x\ : \sim\ P[x, y])$ o $\exists y : (\forall x\ : x \not< y)$

"Existe un número y tal que para todo número x , $x \not< y$ "

Observación: Nótese la diferencia de las afirmaciones ii. e iii. que se obtienen al intercambiar las variables en los cuantificadores.
Si el universo es $\mathbf{U} = \mathbb{N}$, ii. es verdadera e iii. es falsa , si el universo es $\mathbf{U} = \mathbb{R}$ o $\mathbf{U} = \mathbb{Z}$ ambas son verdaderas, pero dicen cosas diferentes.

iv. $\exists y : (\forall x : P[x, y])$ o $\exists y : (\forall x\ : x < y)$

"Existe un número y tal que para todo número x se verifica que $x < y$ "

Negación: $\forall y : (\exists x\ : \sim P[x, y])$ o $\forall y : (\exists x : x \not< y)$

"Para todo número y existe un número x tal que $x \not< y$ "

Observación: Aquí también se percibe la diferencia entre ii. e iv. que tienen intercambiados los cuantificadores. En este caso, cualquiera sea el universo $\mathbf{U} = \mathbb{N}$, $\mathbf{U} = \mathbb{Z}$ o $\mathbf{U} = \mathbb{R}$, iv. es falsa.

v. $\exists x : (\forall y : P[x, y])$ o $\exists x : (\forall y : x < y)$

"Existe un número x tal que para todo número y se verifica que $x < y$ "

Negación: $\forall x : (\exists y : \sim P[x, y])$ o $\forall x : (\exists y : x \not< y)$

"Para todo número x existe un número y tal que $x \not< y$ "

Ejercicio: Analizar la veracidad o falsedad de esta proposición en los universos:

$\mathbf{U} = \mathbb{N}$, $\mathbf{U} = \mathbb{Z}$, $\mathbf{U} = \mathbb{R}$

vi. $\exists x, \exists y : \mathrm{P}[x, y]$ o $\exists x, \exists y : x < y$

"Existen números x e y tales que $x < y$"
Negación: $\forall x, \forall y : \sim \mathrm{P}[x, y]$ o $\forall x, \forall y : x \not< y$
"Para todos x e y se verifica que $x \not< y$"

Ejercicio: Analizar la veracidad o falsedad de esta proposición en los universos:
$\mathbf{U} = \mathbb{N}$, $\mathbf{U} = \mathbb{Z}$ o $\mathbf{U} = \mathbb{R}$

***Aplicación*:** Daremos un ejemplo de cómo demostrar, con los elementos de la lógica dados, que un razonamiento es verdadero.

Sea el siguiente razonamiento:

A ningún pescador le gustan los inspectores.
A todos los habitantes del pueblo les gustan los inspectores.
Juan es pescador.
Juan no es habitante del pueblo.

Definamos los esquemas proposicionales involucrados en el razonamiento.
P[x] : x es pescador
Q[x] : a x le gustan los inspectores
R[x] : x es habitante del pueblo

Expresemos en lenguaje lógico el razonamiento dado.

1. $\forall x : \mathrm{P}[x] \rightarrow \sim \mathrm{Q}[x]$
2. $\forall x : \mathrm{R}[x] \rightarrow \mathrm{Q}[x]$
3. P[*Juan*]
   por lo tanto $\sim$ R[*Juan*]

Justifiquemos la validez del razonamiento:

4. P[*Juan*] $\rightarrow \sim$ Q[*Juan*] (regla de deducción del cuantificador existencial aplicado a 1.)
5. R[*Juan*] $\rightarrow$ Q[*Juan*] (regla de deducción del cuantificador existencial aplicado a 2.)
6. $\sim$ Q[*Juan*] (MP , modus ponens, aplicado a 3. y 4.)
7. $\sim$ R[*Juan*] (MT , modus tolens, aplicado a 5. y 6.)

Ejercicios:

1. Simbolizar utilizando las siguientes letras de predicados o esquemas proposicionales:
$P[x , y] : x > y$; $Q[x , y] : x = y$; $H[x, y , z] : x = y + z$; $S[x , y] : x + y = 3$
$T[x, y , z] : x + z > y$

a) $x > y$ entonces $x = 3$
b) $x \leq y$ entonces $y = 1$
c) $x \leq 2$ o $x + 3 \leq 0$ entonces $x > 1$
d) $x + y > 5$ entonces $y + x > 5$
e) $x + y = 3$ entonces $y + x \neq 3$
f) $x + 2 > y$ y $y > 1$
g) $x = y + z$ o $x + 7 > y$
h) $x \leq y$ y $y \leq z$ entonces $x = z$
i) $x = y + z$ y $z > 1$ entonces $x = y + 1$
j) $x \leq 1$ entonces $x \leq 1$ y $x \leq 2$

2. Simbolizar empleando el cuantificador universal:
a) Todos los perros son mamíferos
b) No todo asiático es chino
c) Cada niño es bueno
d) Todos los hombres son mortales
e) Cada cuadrado es rombo

3. Simbolizar empleando el cuantificador existencial:
a) Existe un felino manso
b) Ningún número entero es primo
c) Hay plantas que viven en el agua
d) No existe un número real cuyo cuadrado sea 1
e) No hay aves cuadrúpedas

4. Negar las proposiciones de los ejercicios 2. y 3. en forma simbólica y coloquial, sin usar el conectivo $\sim$ precediendo al cuantificador.

5. Negar las siguientes proposiciones sin que la negación quede precediendo al cuantificador:
a) $\forall x : \ R[x] \rightarrow S[x]$
b) $\exists x : P[x] \vee Q[x]$
c) $\forall x : (\exists y : P[x , y] \wedge Q[x , y])$
d) $\forall x, \forall y : \ (R[x] \wedge S[y] \rightarrow Q[x , y] \vee H[x , y])$
e) $\exists x : (\forall y : P[x , y] \rightarrow \sim S[y])$

6. Simbolizar las proposiciones siguientes:

En el universo de discurso de los números reales ($\mathbb{R}$), considerar:
$P[x , y] : x > y$; $Q[x , y] : x \leq y$; $R[x] : x - 7 = 2$; $S[x] : x > 9$
$H[x, y , z] : x = y + z$; $T[x, y , z] : x + z > y$

Expresar formalmente la negación de:
a) $\exists x : R[x]$
b) $\forall y : \sim S[y]$
c) $\forall x : (\exists y : \ P[x , y])$
d) $\exists y : (\forall x : Q[x , y])$
f) $\forall x , \forall y : (P[x , y] \vee Q[x , y])$
g) $\exists y : (\forall x : P[x , y] \wedge Q[x , y])$
h) $\forall x, \forall y : \ (R[x] \wedge S[y] \rightarrow Q[x , y])$
i) $\exists x : (\forall y : P[x , y] \rightarrow \sim S[y])$

e) $\forall x : [\exists y : (\forall z : \mathrm{H}[x, y, z])]$ j) $\exists x, \exists y : (\forall z : \mathrm{Q}[x, y] \rightarrow \mathrm{T}[x, y, z])$

7. Negar cada una de las siguientes proposiciones:

a) $\exists x : (\forall y : \mathrm{P}[x, y])$
b) $\forall x : (\exists y : \mathrm{P}[x, y])$
c) $\forall x : (\exists y : (\mathrm{P}[x] \vee \mathrm{Q}[y])$
d) $\exists y, \exists x : [\forall z : (\mathrm{P}[x, y] \rightarrow \mathrm{Q}[z])]$
e) $\exists x : [\forall y : (\mathrm{P}[x] \rightarrow \mathrm{Q}[y])]$
f) $\exists x, \exists y : (\mathrm{P}[x] \leftrightarrow \mathrm{Q}[y])$
g) $\exists y : [\forall x : (\exists x : \mathrm{P}[x] \vee \mathrm{S}[y] \rightarrow \mathrm{T}[x, y, z]))$

8. Analizar el valor de verdad de cada una de las proposiciones del ejercicio 6.

9. Sea $A = \{1, 2, 3, 4, 5\}$. Determinar el valor de verdad de cada una de las siguientes proposiciones. Cuando sea falsa exhibir un contraejemplo o mostrar que su negación es verdadera.

a) $\exists x \in A : \quad x + 1 = 3$
b) $\forall x \in A : \; x + 3 < 10$
c) $\forall x \in A : \; x + 3 \geq 6$
d) $\exists x \in A : \; x.2 < 1$
e) $\exists x : (\forall y : \; x \mid y)$
f) $\forall x : (\exists y : \; y \mid x)$
g) $\forall x : (\exists y : \; y \mid x \wedge x \neq y)$
h) $\forall x, \forall y : \; x^2 + y^2 \leq 49$
i) $\forall x, \forall y : (\exists z : \; x^2 + y^2 < z^2)$

10. Definiendo el universo conveniente en cada caso, utilizar cuantificadores para convertir los siguientes esquemas proposicionales en proposiciones verdaderas:

a) $x + 3 = 3 + x$
b) $x.y > 0$
c) $x + y < 5$
d) $x^2 < 0$
e) $(x + y)^2 = x^2 + y^2$
f) $6x - 4 = 5$
g) $x > 0 \vee x < 0$
h) $x + 1/x > 2$

11. Cambiar, cuando sea posible, el universo de cada uno de los incisos del ejercicio anterior para obtener proposiciones falsas.

12. Sean $\mathbb{N} = \{1, 2, 3, ...\}$ es el conjunto de los números naturales, $\mathbb{Z}$ el de los enteros, $\mathbb{Q}$ el de los racionales, y $\mathbb{R}$ el de los números reales. En cada caso, para el conjunto universal U que se indica, probar que las proposiciones dadas son falsas exhibiendo un contraejemplo o mostrando que su negación es verdadera.

a) $\mathrm{U} = \mathbb{R}$, $\forall z : [\,|z| > 0\,]$
b) $\mathrm{U} = \mathbb{Q}$, $\forall x : (\sqrt{x} \in \mathbb{Q})$

c) $\mathbf{U} = \mathbb{Z}$, $\forall x : (\exists z : \ [xz < 0])$

d) $\mathbf{U} = \mathbb{N}$, $\forall z : (z + 1 < 2)$

e) $\mathbf{U} = \mathbb{Z}$, $\forall x, \forall y : \quad \frac{x}{y} \in \mathbb{Q}$

f) $\mathbf{U} = \mathbb{N}$, $\forall x : (\exists z : \ x - z \in \mathbb{N})$

g) $\mathbf{U} = \mathbb{N}$, $\forall n : \left[\ n > 2^n \right]$

h) $\mathbf{U} = \mathbb{R}$, $\forall x : (\exists z : \ z^2 = x)$

13. Simbolizar los siguientes razonamientos utilizando los símbolos lógicos, y los símbolos típicos de la Aritmética. Después escribir una deducción completa de la conclusión, aclarando las inferencias lógicas y equivalencias que se utilizan en cada paso.

a. Para cada y , y es par si y sólo si $y + 1$ es impar.
Para cada x , si x es igual a $5 + 1$ entonces x es par.
$5 + 1$ no es impar.
Por tanto, 15 es impar.

b. Para todo x , si $12 = x + 4$ o $x = 5.3$, entonces x no es par.
Para cada y, y es par o y es impar.
$15 = 3.5$
Por tanto, 15 es impar.

c. Para todo z , si z es mayor que $3 + 4$, entonces z es mayor que cero.
Cada y es positivo si y sólo si es mayor que cero.
Tres más cinco es mayor que tres más cuatro.
Por tanto, tres más cinco es positivo.

14. Simbolizar los siguientes razonamientos utilizando los símbolos lógicos. Después escribir una deducción completa de la conclusión, aclarando las inferencias lógicas y equivalencias que se utilizan en cada paso.

a. Todo aquél que no está loco puede aprender matemática. Ninguno de los hijos de Domingo es capaz de entender matemática. Ningún loco está habilitado para votar. Pedro es hijo de Domingo.
Por lo tanto, Pedro no está habilitado para votar

b. Ningún caballo sabe silbar.
Ningún cerdo tiene alas.
Todos los que no saben silbar tienen alas.
Por consiguiente, ningún caballo es cerdo.

c. Todos lo niños son traviesos.
Ningún ser es travieso y no es adorable.
Guillermo es un niño.
Por lo tanto, Guillermo es adorable.

d. Todos los grandes compositores son genios.
No hay nadie que no sea compositor y no sea temperamental.
María es genio. Por lo tanto, María es temperamental.

CAPÍTULO II

CONJUNTOS, RELACIONES Y FUNCIONES

“Algunas cantidades en verdad dependen de otras, si al ser combinadas las últimas, las primeras también sufren cambio, y entonces las primeras se llaman funciones de las últimas”. (Euler, 1755)

“Un conjunto es una colección en un todo de determinados y distintos objetos de nuestra percepción o nuestro pensamiento, llamados los elementos del conjunto”.
(Cantor, siglo XIX)

PRIMERA PARTE:

INTRODUCCIÓN A LA TEORÍA DE CONJUNTOS

Georg Cantor- (1845- 1918)

Cantor definió la idea de conjunto como "agrupamiento en un todo de objetos bien definidos, de nuestra intuición o de nuestro pensamiento"…
Cantor es quien dará vida estable y rigurosa a la "teoría de conjuntos". ..Esta teoría original, pero audaz y revolucionaria para la época encontró oposición en especial entre matemáticos influyentes de Alemania; esta circunstancia, unida a las dificultades que presentaba la teoría y los nuevos problemas que planteaba, llevó tal vez a su autor a una enfermedad nerviosa que lo mantuvo alejado de la ciencia durante unos años, volviendo a ocuparse de la teoría de conjuntos en el decenio 1887-1897
("Historia de la Matemática", vol 2 J. Rey Pastor y J. Babini)

Conjuntos

Conceptos básicos

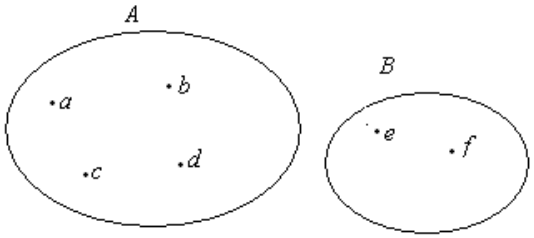
Llamaremos ***conjunto*** a un objeto matemático que no definiremos pero que utilizaremos con la noción intuitiva que la misma palabra nos precisa, como colección de objetos que pueden ser de carácter abstracto o concreto. Dichos objetos constitutivos del conjunto serán denominados ***elementos.***
Para definir un conjunto hay que precisar cuáles son los elementos que lo componen, y ello puede ser hecho en forma explícita, o sea enumerando cada uno de ellos, o bien enunciando la o las propiedades que deben cumplir; en el primer caso los conjuntos se dicen definidos por ***extensión***, y en el segundo, por ***comprensión*** o ***propiedad***. Si un elemento está en un determinado conjunto diremos que ***pertenece*** a dicho conjunto, en caso contrario, cuando no está en el conjunto, diremos que ***no pertenece*** a él.
Designaremos a los conjuntos con letras de imprenta mayúsculas: *A , B, C, D, E, N, R*, etc., y a los elementos con letras minúsculas: *a, b ,c ,d ,e, j, x, y*, etc.
Para indicar que un determinado elemento *a* pertenece a un conjunto ***B,*** escribiremos $a \in B$, y para decir que *a* no pertenece al conjunto ***B,*** escribiremos $a \notin B$.
Al conjunto que no contiene ningún elemento lo llamaremos ***conjunto vacío***, y lo designaremos con el símbolo ϕ .

Ejemplos:

1) $A = \{ x / x \text{ es un número natural par} \}$, conjunto definido por comprensión.
2) $B = \{ 2, 4, 6, 8, 10, 12 \}$, conjunto definido por extensión.
3) $C = \{ x / x \text{ es ciudad de la Argentina} \}$, conjunto definido por comprensión.
4) $D = \{$ *La Plata, Bariloche, Santa Rosa, Posadas, Mar del Plata, San Rafael* $\}$, conjunto definido por extensión.
5) $6 \in A$, $6 \in B$, $24 \in A$, $18 \notin B$, $7 \notin A$, $7 \notin B$
6) *Buenos Aires* $\in C$, *Buenos Aires* $\notin D$, *Bariloche* $\in C$, *Bariloche* $\in D$.

Nota: Para poder definir un conjunto por extensión es necesario que tenga una cantidad finita de elementos, y, aunque teóricamente sea posible para cualquier cantidad finita, desde un punto de vista práctico también se necesita que la cantidad de elementos sea razonablemente chica.

Con frecuencia, representamos gráficamente los conjuntos por los llamados ***Diagramas de Venn.***



$a \in A$, $b \in A$, $f \notin A$, $e \in B$

… al convertir la noción de conjunto en una noción básica de la matemática, se hizo indispensable su introducción en la enseñanza general y se creó, en forma elemental, un "álgebra de conjuntos", en la que desempeñan eficaz papel didáctico los llamados "diagramas de Venn", que el lógico inglés John Venn propuso en 1880, modificando diagramas semejantes que en 1770 había utilizado Euler para representar los silogismos.
("Historia de la Matemática", vol 2 J. Rey Pastor y J. Babini)

VENN (JOHN) (1834-1923) nació en Drypool (Hull) y fue profesor en la Universidad de Cambridge. Incluido por Hamilton y John Stuart Mill, Venn se destacó por sus trabajos en lógica inductiva. Como Hamilton, además, proporcionó en el curso de sus investigaciones lógicas sistemáticas muchos datos para el estudio de la historia de la lógica.
("Diccionario de Filosofía", J. Ferrater Mora)

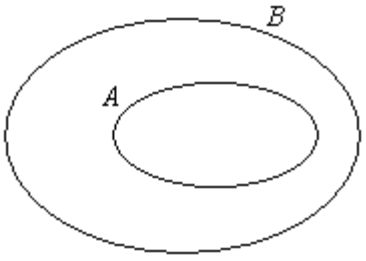
Inclusión

La ***inclusión*** es una relación entre dos conjuntos; dos conjuntos cualesquiera pueden o no estar relacionados por inclusión.

***Definición*:** Diremos que el conjunto *A* está *incluido* (*contenido, es parte de*) en el conjunto *B* si todo elemento de *A* es también elemento de *B*.

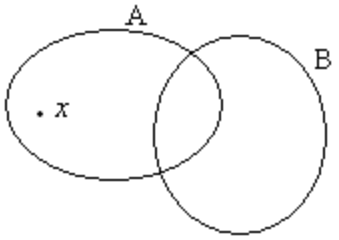
En símbolos: $A \subset B$ *si y sólo si* $\forall x / x \in A \Rightarrow x \in B$

También se utiliza la expresión: *B incluye* o *contiene* al conjunto *A*, en símbolos $B \supset A$.



Entonces, si *A no está contenido* en *B*, significa que **no** todo elemento de *A* es elemento de *B*, o sea, que hay un elemento, al menos, de *A* que no es elemento de *B*., así

$A \not\subset B$ *si y sólo si* $\exists x \ / \ x \in A \ \wedge \ x \notin B$



Ejemplos:
En los conjuntos de los ejemplos 1), 2), 3) y 4) citados anteriormente:

$$B \subset A, \ D \subset C, \ A \not\subset B, \ C \not\subset D$$

Generalmente, cuando definimos un conjunto por comprensión, indicamos la o las propiedades que deben cumplir los elementos que están en el conjunto, y esos elementos los presuponemos en un conjunto referencial *mayor,* un conjunto que contiene a todos los conjuntos de los que hablamos, a ese conjunto lo denominamos ***universal***, y lo designaremos **U**

***Igualdad entre conjuntos*:** Dos conjuntos *A* y *B* son *iguales* si tienen los mismos elementos, o sea, si todo elemento de *A* lo es de *B*, y recíprocamente, todo elemento de *B* lo es también de *A.*

$$A = B \quad \text{si y sólo si} \quad A \subset B \ \wedge \ B \subset A$$

Luego *A* es *distinto* de *B* , o *A* no es igual que *B*, si existe un elemento en *A* que no es elemento de *B* o algún elemento de *B* que no lo es de *A.*

$$A \neq B \quad \text{si y sólo si} \quad A \not\subset B \ \vee \ B \not\subset A$$

***Propiedades de la inclusión*:**

i) *reflexiva*: $\forall A, \quad A \subset A$
ii) *antisimétrica*: $A \subset B \ \wedge \ B \subset A \ \Rightarrow \ A = B$
iii) *transitiva*: $A \subset B \ \wedge \ B \subset C \ \Rightarrow \ A \subset C$
iv) $\phi \subset A \ \forall A$

Demostraremos, a modo de ejemplo, las propiedades, iii) y iv)

Demostración:
iii) Hipótesis: $A \subset B \ \wedge \ B \subset C$,
debemos demostrar que $A \subset C$, por lo tanto , tenemos que ver que todo elemento de *A* es elemento de *C.*
Sea, entonces, $x \in A$, como $A \subset B$, entonces $x \in B$,
pero $B \subset C$, luego si $x \in B$ entonces $x \in C$,
así $x \in A \ \Rightarrow \ x \in C$, luego $A \subset C$, como queríamos demostrar.

iv) Para ver que $\phi \subset A$, cualquiera sea el conjunto *A*, debemos preguntarnos qué pasaría si hubiera un conjunto *A* que no contuviera al conjunto ϕ.
Por definición, si eso ocurriera, deberíamos encontrar algún elemento *x* tal que $x \in \phi \wedge x \notin A$, pero eso es imposible porque no hay ningún $x \in \phi$, luego no ocurre jamás que haya algún elemento en el conjunto vacío que no esté en *A*, simplemente porque no hay ningún elemento en el vacío, por lo tanto la condición para que $\phi \not\subset A$ no se verifica, luego se cumple su negación, y $\phi \subset A$, y esto es sea cual fuere el conjunto *A*.
Si queremos analizar la veracidad de la afirmación $\phi \subset A$ desde el punto de vista lógico, tenemos que estudiar la veracidad de la proposición:

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

la que es trivialmente verdadera ya que el antecedente es falso, o bien que su negación:

$$\exists x: \quad x \in \phi \wedge x \notin A \text{ es falsa.}$$

Operaciones entre conjuntos

Las operaciones *binarias* entre conjuntos nos permiten definir un nuevo conjunto a partir de otros dos. Ellas son ***unión, intersección, diferencia y diferencia simétrica.***
Existe otra operación, a veces llamada *unaria,* que nos define un conjunto a partir de otro; éste es el caso del ***complemento.***

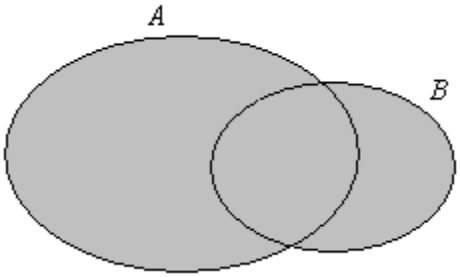
Unión

Dados dos conjuntos *A* y *B*, llamamos $A \cup B$ (*A unión B*) al conjunto que tiene como elementos los elementos de *A* y los elementos de *B*.

En símbolo $A \cup B = \{ x / x \in A \vee x \in B \}$

Así tenemos que $x \in A \cup B \Leftrightarrow x \in A \vee x \in B$.
Luego $x \notin A \cup B \Leftrightarrow x \notin A \wedge x \notin B$

Diagrama de Venn de $A \cup B$:



Ejemplos: $\mathbf{U}$ *es el conjunto de números naturales*, $\mathbf{U} = \mathbb{N}$

1) $A = \{ x / x \leq 6 \}$
$B = \{ 1, 3, 5, 7, 9 \}$
$A \cup B = \{ 1, 2, 3, 4, 5, 6, 7, 9 \}$

2) $C = \{\ x / x \text{ es múltiplo de } 5\ \}$
$D = \{\ x / x \text{ es divisible por } 3\ \}$
$C \cup D = \{\ x / x \text{ es divisible por } 5 \text{ o es divisible por } 3\ \}$

3) $E = \{\ x / x \text{ divide a } 100\ \}$
$F = \{\ x / x \text{ es par } \wedge\ x \leq 10\ \}$
$E \cup F = \{\ 1, 2, 4, 5, 6, 8, 10, 20, 25, 50, 100\ \}$

Propiedades de la unión

i) *asociativa*: $A \cup (B \cup C) = (A \cup B) \cup C$
ii) *conmutativa*: $A \cup B = B \cup A$
iii) $A \subset A \cup B$ y $B \subset A \cup B$
iv) $A \cup B = B$ *si y sólo si* $A \subset B$
en particular: $A \cup A = A$, $A \cup \phi = A$, $A \cup \mathbf{U} = \mathbf{U}$, $\forall A$

***Demostración*:** Se deja como ejercicio

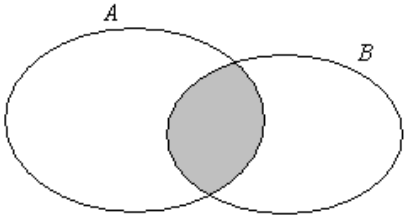
Intersección

Dados dos conjuntos *A* y *B*, llamamos $A \cap B$ (*A intersección B*), al conjunto de los elementos que están simultáneamente en *A* y en *B*.

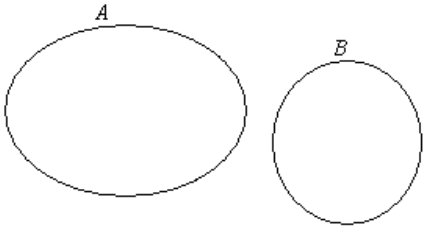
En símbolos: $A \cap B = \{\ x / x \in A \wedge x \in B\ \}$

Así tenemos que $x \in A \cap B \Leftrightarrow x \in A \wedge x \in B$
Luego $x \notin A \cap B \Leftrightarrow x \notin A \vee x \notin B$

Diagrama de Venn de $A \cap B$:



Dos conjuntos *A* y *B* se dicen *disjuntos* si $A \cap B = \phi$



Ejemplos: Para los conjuntos dados antes

1) $A \cap B = \{ 1, 3, 5 \}$
2) $C \cap D = \{ x / x \text{ es divisible por } 15 \}$
3) $E \cap F = \{ 2, 4, 10 \}$

Propiedades de la intersección

i) *asociativa*: $A \cap (B \cap C) = (A \cap B) \cap C$
ii) *conmutativa*: $A \cap B = B \cap A$
iii) $A \cap B \subset A \wedge A \cap B \subset B$
iv) $A \cap B = A$ *si y sólo si* $A \subset B$
en particular: $A \cap A = A$, $A \cap \phi = \phi$, $A \cap \mathbf{U} = A$, $\forall A$

***Demostración*:** Demostraremos, a modo de ejemplo, la iv)

Esta propiedad afirma que son equivalentes dos proposiciones: $A \cap B = A \wedge A \subset B$, por lo tanto debemos demostrar dos implicaciones:

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

y la recíproca:

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

$\Rightarrow$) Comencemos con la primera. Debemos demostrar que $A \subset B$ con la hipótesis $A \cap B = A$.
Para demostrar esta inclusión hay que tomar un elemento genérico de A y ver si también está en B.
Sea entonces $x \in A$, como $A \cap B = A$, entonces $x \in A \cap B$, luego $x \in A \wedge x \in B$, así $x \in B$, que es lo que queríamos probar. Luego $A \subset B$.

$\Leftarrow$) Demostremos la segunda implicación. Ahora nuestra hipótesis es que $A \subset B$, y con ella debemos ver que se verifica la igualdad de los conjuntos A y $A \cap B$.
Para demostrar una igualdad entre dos conjuntos debemos probar que cada uno de ellos está incluido en el otro.
La inclusión $A \cap B \subset A$ se verifica siempre por iii), así que aquí no hay nada para demostrar.
Veamos que $A \subset A \cap B$, ahora sí usando la hipótesis:
Sea $x \in A$, como $A \subset B$, entonces $x \in B$, luego $x \in A \wedge x \in B$, así $x \in A \cap B$, por lo tanto $A \subset A \cap B$.

Los casos particulares provienen de las relaciones $A \subset A$, $\phi \subset A$ y $A \subset \mathbf{U}$ respectivamente.

Tenemos, además, una propiedad que vincula ambas operaciones: *la distributividad*.
La unión es distributiva respecto de la intersección, y la intersección es distributiva respecto de la unión; en símbolos:

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

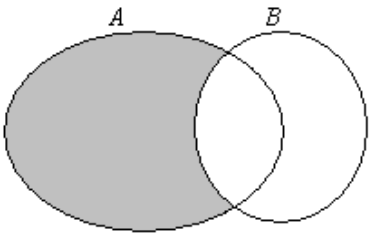
Diferencia

Dados dos conjuntos A y B, llamamos $A - B$ (*A menos B*) al conjunto:

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

Así tenemos que $x \in A - B \Leftrightarrow x \in A \wedge x \notin B$,
Luego $x \notin A - B \Leftrightarrow x \notin A \vee x \in B$

Diagrama de Venn de $A - B$:



Ejemplos: *Para los conjuntos dados más arriba*

1) $A - B = \{\ 2, 4, 6\ \}$
2) $A - B = \{\ x / x$ *es divisible por* 5 *pero no por* 3 $\}$
3) $A - B = \{\ x / x$ *divide a* 100 *y además x es impar o* $x > 10\ \} = \{\ 1, 5, 20, 25, 50, 100\ \}$

Propiedades de la diferencia

i) $A - B = A \Leftrightarrow A \cap B = \phi$ **,** en particular $A - \phi = A$
ii) $A - B = \phi \Leftrightarrow A \subset B$ **,** en particular **:** $\phi - A = \phi$, $A - A = \phi$

***Demostración*:** Se deja como ejercicio

Nota: La diferencia **no** es una operación asociativa:

$A - (B - C) \neq (A - B) - C$ (en general)

ni conmutativa: (en general) $A - B \neq B - A$,

se puede afirmar más, $A - B$ y $B - A$ son conjuntos disjuntos.

Para demostrar las dos primeras afirmaciones, sólo debemos buscar ejemplos de conjuntos *A, B, C*, en el primer caso, y *A , B* en el segundo para los cuales no se verifiquen las igualdades.

Ejemplos: Sean
$A = \{\ 1, 2, 4, 7, 9, 12, 18, 23\ \}$
$B = \{\ x / x$ *es par* $\wedge\ x < 30\ \}$
$C = \{\ x / x \in \mathbb{N}\ \wedge\ 7 < x < 36\ \}$
$A - B = \{\ 1, 7, 9, 23\ \}$
$B - C = \{\ 2, 4, 6\ \}$
$A - (B - C) = \{\ 1, 7, 9, 12, 18, 23\ \}$
$(A - B) - C = \{\ 1, 7\ \}$

Claramente se observa que: $A - (\ B - C\ ) \neq (\ A - B\ ) - C$

Ejercicio para pensar: ¿se verifica siempre alguna de las dos inclusiones?, ¿o nunca?, ¿o a veces ?. Cualquiera sea la respuesta que dé, justifíquela.

Para la segunda afirmación calculamos $B - A$

$B - A = \{\ 6, 8, 10, 14, 16, 20, 22, 24, 26, 28\ \}$

Aquí también se observa que: $A - B \neq B - A$

Ahora debemos demostrar que $(A - B) \cap (B - A) = \phi$

Si no fuese así, existiría un elemento $x \in (A - B) \cap (B - A)$,
Luego $x \in A - B \wedge x \in B - A$
Así $x \in A \wedge x \notin B \wedge x \in B \wedge x \notin A$,
Lo que claramente es una contradicción, que provino de la suposición: $(A - B) \cap (B - A) \neq \phi$,
por lo tanto $(A - B) \cap (B - A) = \phi$.

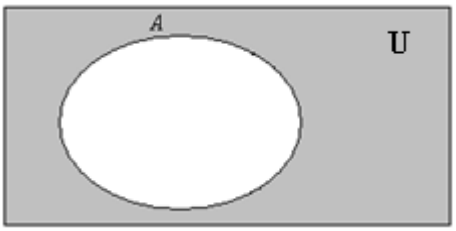
Complemento

Esta operación es llamada *unaria* porque, a diferencia de las anteriores, no se obtiene un nuevo conjunto a partir de otros dos, sino de uno solo.

Dado un conjunto *A*, se llama $\overline{A}$ (*complemento de A*), al conjunto formado por todos los elementos que no están en *A* (considerados éstos en un conjunto Universal predeterminado).

$\overline{A} = \{ x / x \notin A \}$

Diagrama de Venn de $\overline{A}$:



Claramente se observa que el complemento de *A* se puede pensar como una diferencia, puesto que:
$\overline{A} = \mathrm{U} - A$

Ejemplos:

Sean $\mathrm{U} = \mathbb{N}$ (conjunto de números naturales)
$A = \{ x / x \text{ es múltiplo de } 6 \}$
$B = \{ x / x \text{ es par} \}$
$C = \{ 1, 2, 3, 4, 6, 7 \}$
$\overline{A} = \{ x / x \text{ no es divisible por } 2 \vee x \text{ no es divisible por } 3 \}$
$\overline{B} = \{ x / x \text{ es impar} \}$
$\overline{C} = \{ x / x > 7 \vee x = 5 \}$

Propiedades del complemento

i) $\overline{\overline{A}} = A$
ii) $\overline{\phi} = \mathrm{U} \wedge \overline{\mathrm{U}} = \phi$

iii) Leyes de De Morgan: $\overline{A \cup B} = \overline{A} \cap \overline{B}$
$\overline{A \cap B} = \overline{A} \cup \overline{B}$

iv) $A \subset B \Leftrightarrow \overline{B} \subset \overline{A}$

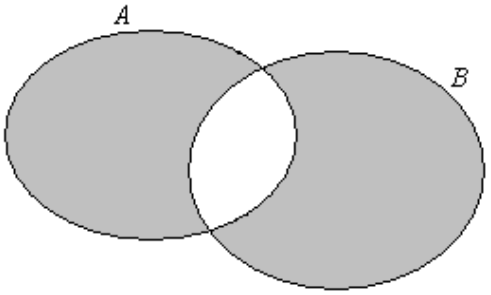
***Demostración*:** Se deja como ejercicio

Diferencia simétrica

Esta operación se define a partir de otras anteriores: $A \Delta B = (A \cup B) - (A \cap B)$

Luego un elemento pertenece a la *diferencia simétrica de A* y *B* ($A \Delta B$) si pertenece a uno de ellos, pero no a ambos.

Diagrama de Venn de $A \Delta B$:



Ejemplos:

1) $A = \{ x / x \leq 6 \}$ $B = \{ 1, 3, 5, 7, 9 \}$
$A \Delta B = \{ 2, 4, 6, 7, 9 \}$

2) $C = \{ x$ */ x es múltiplo de* 5 $\}$ $D = \{ x$ */ x es divisible por* 3 $\}$
$C \Delta D = \{ x$ */ x es múltiplo de* 3 *o de* 5*, pero no de* 15 $\}$

3) $E = \{ x$ */ x divide a* 100 $\}$ $F = \{ x / x$ *es par* $\wedge\ x \leq 10 \}$
$E \Delta F = \{ 1, 5, 6, 8, 20, 25, 50, 100 \}$

Propiedades de la diferencia simétrica

i) *Asociativa*: $A \Delta (B \Delta C) = (A \Delta B) \Delta C$
ii) *Conmutativa*: $A \Delta B = B \Delta A$
iii) $A \Delta A = \phi$, $A \Delta \phi = A$
iv) *Distributiva respecto de la intersección*: $(A \Delta B) \cap C = (A \cap C) \Delta (B \cap C)$

***Demostración*:** Se deja como ejercicio

***Ejercicio para pensar*:** ¿Se verifica la propiedad distributiva de la diferencia simétrica respecto de la unión?, o sea, ¿es verdadero o falso que: $(A \Delta B) \cup C = (A \cup C) \Delta (B \cup C)$?

Justificar la respuesta.
Teorema: Cualesquiera sean los conjuntos A y B, se verifica:

i) $A \Delta B = (A - B) \cup (B - A)$

ii) $A \Delta B = (A \cap \overline{B}) \cup (B \cap \overline{A})$

Demostraremos i) a modo de ejemplo

***Demostración*:**

Como debemos demostrar una igualdad entre dos conjuntos, debemos probar dos inclusiones:

$$A \Delta B \subset (A - B) \cup (B - A) \wedge (A - B) \cup (B - A) \subset A \Delta B.$$

Para la primera, sea $x \in A \Delta B$, entonces $x \in A \cup B \wedge x \notin A \cap B$.
Como $x \in A \cup B$, entonces $x \in A \vee x \in B$.
Si $x \in A$ entonces $x \notin B$, pues $x \notin A \cap B$, $\Rightarrow x \in A - B$
Si $x \in B$ entonces $x \notin A$, por la misma razón, $\Rightarrow x \in B - A$.
Luego $x \in A - B \vee x \in B - A \Rightarrow x \in (A - B) \cup (B - A)$.
Por lo tanto $A \Delta B \subset (A - B) \cup (B - A)$.

Para la segunda inclusión, sea $x \in (A - B) \cup (B - A)$,
entonces $x \in A - B \vee x \in B - A$,
luego $(x \in A \wedge x \notin B) \vee (x \in B \wedge x \notin A)$,
así $(x \in A \vee x \in B) \wedge (x \notin A \vee x \notin B)$.
Luego $x \in (A \cup B) - (A \cap B)$
y como $(A \cup B) - (A \cap B) = A \Delta B$
tenemos que $x \in A \Delta B$
Por lo tanto $(A - B) \cup (B - A) \subset A \Delta B$.

Como hemos demostrado ambas inclusiones, podemos afirmar que:

$$A \Delta B = (A - B) \cup (B - A)$$

Conjunto de partes de un conjunto

Definición*:** Llamaremos ***conjunto de partes de un conjunto A, al conjunto cuyos elementos son los subconjuntos de A.
En símbolos $\mathcal{P}(A) = \{ X / X \subset A \}$

***Observación*:** $\phi \subset A$ y $A \subset A \ \forall A$, por lo tanto $\phi \in \mathcal{P}(A) \wedge A \in \mathcal{P}(A) \ \forall A$.
Por consiguiente, excepto en el caso en que $A = \phi$, $\mathcal{P}(A)$ tiene, al menos, dos elementos; en particular ***siempre*** es $\mathcal{P}(A) \neq \phi$.
$\mathcal{P}(\phi) = \{\phi\}$, conjunto de un solo elemento, o ***unitario,*** puesto que el único subconjunto del conjunto ϕ, es él mismo.

Ejemplos:

1) $A = \{1, 2, 3\}$, $\mathcal{P}(A) = \{\phi, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$

2) $B = \{a\}$, $\mathcal{P}(B) = \{\{a\}, \phi\}$

3) $C = \{\phi\}$, $\mathcal{P}(C) = \{\phi, \{\phi\}\}$

Obsérvese que el conjunto *C* del ejemplo *3)* **no** es el conjunto vacío, es el conjunto ***unitario*** (como lo es también *B* del ejemplo *2*) cuyo único elemento es el ***conjunto vacío,*** y por ello $\mathcal{P}(C)$ tiene dos elementos, como $\mathcal{P}(B)$, y no uno solo como $\mathcal{P}(\phi)$.

Propiedades

i) Si $A \subset B \Rightarrow \mathcal{P}(A) \subset \mathcal{P}(B)$

ii) $\mathcal{P}(A) \cup \mathcal{P}(B) \subset \mathcal{P}(A \cup B)$, ¿se verifica la igualdad? Justifique.

iii) $\mathcal{P}(A) \cap \mathcal{P}(B) = \mathcal{P}(A \cap B)$

iv) ¿Es verdadero o falso que $\mathcal{P}(A - B) \subset \mathcal{P}(A) - \mathcal{P}(B)$? ¿y la inclusión recíproca? Justifique las respuestas.

***Demostración*:** Se deja como ejercicio.

Uniones e intersecciones generalizadas

Así como hemos definido la unión y la intersección entre dos conjuntos, podemos extender estas definiciones a cualquier familia finita de conjuntos, e incluso, a cualquier familia infinita.

Por ejemplo si tenemos tres conjuntos *A, B, C* :

$$A \cup B \cup C = \{\, x / x \in A \vee x \in B \vee x \in C \,\}$$
$$A \cap B \cap C = \{\, x / x \in A \wedge x \in B \wedge x \in C \,\}$$

Si tenemos una sucesión finita de conjuntos A_1 , A_2 , A_3 , …..,A_n , donde *n* es cualquier número natural:

$$A_1 \cup A_2 \cup A_3 \cup A_4 \cup \ldots\ldots \cup A_n = \bigcup_{i=1}^{n} A_i = \{\, x / \exists\, i,\ i = 1,\ldots,n \text{ tal que } x \in A_i \,\}$$

En otras palabras, $\bigcup_{i=1}^{n} A_i$ es el conjuntos de los elementos que están en cada uno de los A_i .

$$A_1 \cap A_2 \cap A_3 \cap A_4 \cap \ldots\ldots \cap A_n = \bigcap_{i=1}^{n} A_i = \{\, x / x \in A_i \ \forall\, i ,\ i = 1,\ldots, n \,\}.$$

Luego $\bigcap_{i=1}^{n} A_i$ está constituido por los elementos que pertenecen simultáneamente a todos los A_i .

Si tenemos una familia cualquiera de conjuntos $(A_i)_{i \in I}$, donde *I* es un *conjunto de índices* (*I* podría ser el conjunto de Números Naturales, un conjunto finito, o cualquier otro conjunto infinito), definimos:

$$\bigcup_{i \in I} A_i = \{\, x / x \in A_i \text{ para algún } i \in I \,\} = \{\, x / \exists\, i \in I \text{ tal que } x \in A_i \,\}$$
$$\bigcap_{i \in I} A_i = \{\, x / x \in A_i \ \forall\, i \in I \,\}.$$

Ejemplos:

$A_i = [\, i,\ i+1\,]$ (intervalo real) , $i = 1,\ldots,n$, $n > 3$

$\bigcup_{i=1}^{n} A_i = [\, 1,\ n+1\,]$, $\quad \bigcap_{i=1}^{n} A_i = \phi$ ¿ y si $n = 1 \vee n = 2$?

$B_n = \left[-\frac{1}{n},\ \frac{1}{n} \right]$, $n \in \mathbb{N}$

$\bigcup_{i\in\mathbb{N}} B_i = [-1,\ 1]$, $\quad \bigcap_{i\in\mathbb{N}} B_i = \{0\}$

$C_n = \left[-1+\frac{1}{n},\ 1-\frac{1}{n} \right]$, $n \in \mathbb{N}$, $\quad \bigcup_{i\in\mathbb{N}} C_i = (-1,\ 1)$, $\quad \bigcap_{i\in\mathbb{N}} C_i = \{0\}$

Producto cartesiano

Sean *a* y *b* dos elementos (del mismo conjunto o no), se puede formar el conjunto $\{a, b\}$ que los tiene a ambos como elementos; en este conjunto importan los elementos *a* y *b* pero no el orden en que éstos figuren, puesto que $\{a, b\} = \{b, a\}$. Si nosotros necesitamos, no sólo especificar los elementos, sino también el orden en que aparecen, debemos definir otro conjunto que dependa de los elementos *a* y *b* y también del orden en que sean tomados.

***Definición*:** dados dos elementos *a* y *b* , llamaremos *par ordenado ab* (de primer elemento *a* y de segundo elemento *b*) al conjunto $\{\{a\}, \{a, b\}\}$.
Designaremos al par ordenado *ab* con el símbolo (*a, b*)

Claramente $(a, b) \neq (b, a)$ puesto que los conjuntos $\{\{a\}, \{a, b\}\}$ y $\{\{b\}, \{a, b\}\}$ son distintos ya que $\{a\} \in \{\{a\}, \{a, b\}\}$ y $\{a\} \notin \{\{b\}, \{a, b\}\}$, cuando $a \neq b$, como así también $\{b\} \in \{\{b\}, \{a, b\}\}$ y $\{b\} \notin \{\{a\}, \{a, b\}\}$.

Por la definición anterior $(a, a) = \{\{a\}, \{a, a\}\} = \{\{a\}\}$.
En el par ordenado (*a*, *b*), *a* se denomina *primera coordenada* y *b segunda coordenada* del par.

***Observación importante*:** A partir de la definición podemos establecer las condiciones necesarias y suficientes para la igualdad entre pares ordenados:

$$(a, b) = (c, d) \quad \textit{si y sólo si} \quad a = c \wedge b = d$$

***Demostración*:**

$\Rightarrow$) Supongamos que $(a, b) = (c, d)$, por definición de par ordenado, esto significa que: $\{\{a\},\{a, b\}\} = \{\{c\},\{c, d\}\}$.

Si $a = b$ entonces $\{\{a\},\{a, b\}\} = \{\{a\}\}$, o sea un conjunto unitario, de donde, por la igualdad supuesta, $\{\{c\},\{c, d\}\}$ también debe ser unitario, luego $\{c\} = \{c, d\}$, lo que implica que $c = d$. Como $(a, a) = \{\{a\}\}$, $(c, c) = \{\{c\}\}$, $(a, a) = (c, c)$ por hipótesis, tenemos que $\{\{a\}\} = \{\{c\}\}$, de donde $\{a\} = \{c\}$, y así $a = c$, como queríamos probar.

Sea ahora $a \neq b$, como $\{\{a\},\{a, b\}\}$ tiene dos elementos, por la igualdad supuesta, $\{\{c\},\{c, d\}\}$ también debe tener dos elementos, luego $\{c, d\} \neq \{c\}$ entonces $c \neq d$.

De la igualdad $\{\{a\},\{a, b\}\} = \{\{c\},\{c, d\}\}$ sabemos que $\{a\} \in \{\{c\},\{c, d\}\}$, y como este conjunto tiene dos elementos, debe ser $\{a\} = \{c\}$ o $\{a\} = \{c, d\}$. Como ya vimos que $\{c, d\}$ tiene dos elementos entonces $\{a\} = \{c, d\}$ es imposible, luego $\{a\} = \{c\}$, de donde $a = c$. Por otra parte, de la igualdad afirmada en la hipótesis, tenemos que $\{a,b\} \in \{\{c\},\{c, d\}\} = \{\{a\},\{a, b\}\}$, y por ser $\{a,b\}$ un conjunto de dos elementos y $\{a\}$ uno unitario, no pueden ser iguales, luego $\{a,b\} = \{a, d\}$, y como $b \neq a$, debe ser $b = d$, como queríamos demostrar.

$\Leftarrow$) Esta implicación es trivial, pues si $a = c$ y $b = d$, se verifica que $\{a\} = \{c\}$ y $\{a,b\} = \{c, d\}$, luego $\{\{a\},\{a, b\}\} = \{\{c\},\{c, d\}\}$, o lo que es lo mismo $(a, b) = (c, d)$.

Así podemos afirmar que: $(a, b) \neq (c, d)$ *si y sólo si* $a \neq c \vee b \neq d$.

***Definición*:** Sean los conjuntos A y B, llamamos *producto cartesiano* de A por B , al conjunto:

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

Ejemplos:

1) $A = \{a,b\}$; $B = \{1, 2, 3\}$
   $A \times B = \{(a, 1), (a, 2), (a, 3), (b, 1), (b, 2), (b ,3)\}$
   $B \times A = \{(1 , a), (2, a), (3, a), (1, b), (2, b), (3, b)\}$

2) $C = \{1\}$; $D = \{1, 5\}$
   $C \times D = \{(1, 1), (1, 5)\}$
   $D \times C = \{(1, 1), (5, 1)\}$

Propiedades

i) $A \times B = \phi \Leftrightarrow A = \phi \vee B = \phi$
ii) $A' \subset A \wedge B' \subset B \Leftrightarrow A' \times B' \subset A \times B$
iii) $(A \cup B) \times C = (A \times C) \cup (B \times C)$
iv) $(A \cap B) \times C = (A \times C) \cap (B \times C)$

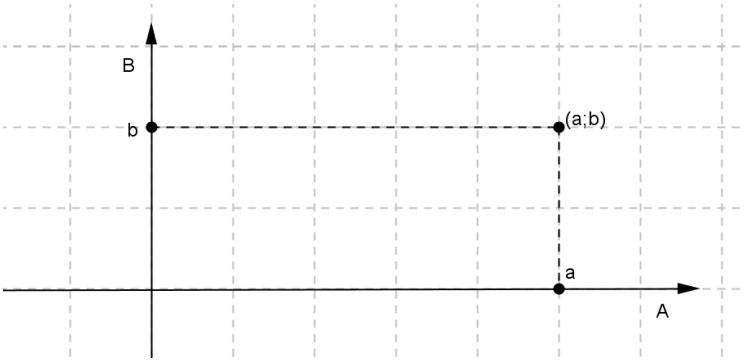
v) $(A - B) \times C = (A \times C) - (B \times C)$

vi) $\overline{A \times B} = (\overline{A} \times \overline{B}) \cup (\overline{A} \times B) \cup (A \times \overline{B})$

***Demostración*:** Se deja como ejercicio.

***Representación gráfica*:**

Usualmente se representa el producto cartesiano de dos conjuntos $A \times B$ en un *sistema de dos ejes cartesianos,* en el cual el eje horizontal, o de las *abscisas* se utiliza para indicar los elementos de *A,* y el vertical, o de *ordenadas,* los de *B*.



Ejercicios

1.- Dado el conjunto $A=\{1, 2, \{3\}, \{1, 2\}, -1\}$, determinar cuáles de las siguientes afirmaciones son verdaderas. Justificar.

i) $3 \in A$ ii) $\{1, 2\} \subset A$ iii) $\{1, 2\} \in A$

iv) $\{3\} \subset A$ v) $\{\{3\}\} \subset A$ vi) $\phi \in$ A

vii) $\phi \subset A$ viii) $\{1, 2, -1\} \in A$ ix) $\{-1, 2\} \subset A$

2.- Determinar si $A \subset B$ en cada uno de los siguientes casos. Justificar.

i) $A=\{1, 2, \sqrt{9}\}$ $B=\{1, 2, \{3\}, -3\}$

ii) $A=\{1, 2, 0, -1, -2\}$ $B=\{x \in \mathbb{R} / \ |x+3| \leq 1\}$

iii) $A=\{1, 2, \sqrt{9}\}$ $B=\{1, 2, 3, 4, 5\}$

iv) $A=\{\phi\}$ $B=\phi$

v) $A=\{x \in \mathbb{R} / \quad 2<|x|<3\}$ $B=\{x \in \mathbb{R} / \quad x^2<3\}$

3.- Dados los conjuntos:

$A=\{n \in \mathbb{N} / \quad n \text{ es par}\}$, $B=\{n \in \mathbb{N} / \quad n \text{ es impar}\}$,

$C=\{x \in \mathbb{R} / \quad 0 \leq x \leq 1\}$, $D=\{n \in \mathbb{N} / \ n \text{ es impar} \wedge \ n<10\}$,

$$E=\left\{q \in \mathbb{Q} / \quad q=\frac{n}{m} \text{ con } m \in \{1, 2\} \wedge n \in \{0, 1, 2\}\right\}$$

a) ¿Cuáles de ellos pueden ser definidos por extensión?

b) Realizar las siguientes operaciones describiendo, cuando sea posible, la solución por extensión:

i) $A \cap B$ ii) $A \cup B$ iii) $A \cap E$ iv) $E \cap C$

v) $\mathbb{Q} \ \Delta \ E$ vi) $\mathbb{R}-C$ vii) $A \ \Delta \ B$ viii) $C \Delta \ E$

4.- Dados A, B y C conjuntos de un conjunto universal $\mathbf{U}$, demostrar cada una de las siguientes Leyes del Álgebra de Conjuntos:

Leyes idempotentes

i-a) $A \cup A = A$ i-b) $A \cap A = A$

Leyes de asociatividad

ii-a) $A \cup (B \cup C) = (A \cup B) \cup C$ ii-b) $A \cap (B \cap C) = (A \cap B) \cap C$

Leyes conmutativas

iii-a) $A \cup B = B \cup A$ iii-b) $A \cap B = B \cap A$

Leyes distributivas

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

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

Leyes de identidad

v-a) $A \cup \phi = A$ v-b) $A \cap \mathbf{U} = A$ vi-a) $A \cup \mathbf{U} = \mathbf{U}$ vi-b) $A \cap \phi = \phi$

Leyes de complementos

vii-a) $A \cup \overline{A} = \mathbf{U}$ vii-b) $A \cap \overline{A} = \phi$ viii-a) $\overline{\overline{A}} = A$ viii-b) $\overline{\mathbf{U}} = \phi \ \wedge \ \overline{\phi} = \mathbf{U}$

Leyes de De Morgan:

ix-a) $\overline{(A \cup B)} = \overline{A} \cap \overline{B}$ ix-b) $\overline{(A \cap B)} = \overline{A} \cup \overline{B}$

5.- Sean A, B conjuntos, probar que:

i) $A \cup B \supset A \ \wedge \ A \cup B \supset B$ ii) $A \cap B \subset A \ \wedge \ A \cap B \subset B$

iii) $A \cap \overline{B} = \phi \Leftrightarrow A \subset B$ iv) $A \Delta B = (A - B) \cup (B - A)$

v) $A \subset B \Leftrightarrow A \cap B = A \Leftrightarrow A \cup B = B \Leftrightarrow \overline{B} \subset \overline{A}$

vi) $A \cap B = \phi \Leftrightarrow \overline{A \Delta B} = \overline{A \cup B}$

vii) $A \Delta B = \phi \Leftrightarrow A = B$ viii) $A \cap (B \Delta C) = (A \cap B) \Delta (A \cap C)$

6.- Usando diagramas de Venn, conjeturar cuáles de las siguientes afirmaciones pueden ser verdaderas y demostrarlas. En los casos que se consideren falsas, verificarlo con algún ejemplo:

i) $(A \cup B) - C = (A - C) \cup (B - C)$ ii) $\begin{cases} A-(B-C) \subset (A-B)-C \\ A-(B-C) \supset (A-B)-C \\ A-(B-C) = (A-B)-C \end{cases}$

iii) $A - B = A \Leftrightarrow B = \phi$

iv) $A \Delta B \subset \left(A \cap \overline{B}\right) \cup \left(\overline{A} \cap B\right)$, $A \Delta B \supset \left(A \cap \overline{B}\right) \cup \left(\overline{A} \cap B\right)$,

$A \Delta B = \left(A \cap \overline{B}\right) \cup \left(\overline{A} \cap B\right)$

v) $A \Delta B = A - B \Leftrightarrow B \subset A$ vi) $A \cup B \cup C = B \cup C \Leftrightarrow A \subset B \ \vee \ A \subset C$

7.- Realizar las siguientes operaciones para los conjuntos A, B , C, D y E del ejercicio 3, haciéndolo por extensión cuando sea posible, y realizar un gráfico también cuando sea posible:

i) $D \times \mathbb{N}$ ii) $C \times C$ iii) $C \times \mathbb{R}$ iv) $E \times E$

v) $B \times B$ vi) $C \times \{0, 1\}$ vii) $A \times \{0\}$

8.- Probar que, para A, B y C conjuntos:

i) $(A \cup B) \times C = A \times C \cup B \times C$ ii) $(A \cap B) \times C = A \times C \cap B \times C$

iii) $(A - B) \times C = (A \times C) - (B \times C)$ iv) $A \times (B \Delta C) = (A \times B) \Delta (A \times C)$

v) $A \times B = \phi \Leftrightarrow A = \phi \ \vee \ B = \phi$ vi) $A' \subset A$, $B' \subset B \Rightarrow A' \times B' \subset A \times B$

vii) $A \neq \phi$, $B \neq \phi$, $A \neq B \Rightarrow A \times B \neq B \times A$; ¿cuándo es $(A \times B) \cap (B \times A) \neq \phi$?

9.- Para los conjuntos $\mathbb{U} = \{ A_i \ / \ i \in I \}$ que se indican, calcular:

$\bigcup_{A_i \in U} A_i = \bigcup_{i \in I} A_i = \{ x \ / \ \exists i \in I : \ x \in A_i \}$ y $\bigcap_{A_i \in U} A_i = \bigcap_{i \in I} A_i = \{ x \ / \ x \in A_i \ \forall i \in I \}$

i) $I = \{4, 5, 6, 10\}$, $A_i = \{ d \in \mathbb{N} \ / \ d \ \textit{divide a} \ i \}$

ii) $I = \mathbb{N}$, $A_i = \{1, 2, ..., i\}$ iii) $I = \mathbb{Q}$, $A_i = \{0, 2i\}$

10.- Hallar los conjuntos de partes de los siguientes conjuntos:

i) $A = \{2, 3, 4\}$ ii) $B = \{a, b\}$ iii) $B \times B$ iv) ϕ v) $\mathcal{P}(\phi)$ vi) $\mathcal{P}(B)$

11.- Demostrar que $A \subset B \Rightarrow \mathcal{P}(A) \subset \mathcal{P}(B)$

12.- Analizar la veracidad o falsedad de:

i) $\mathcal{P}(A \cup B) = \mathcal{P}(A) \cup \mathcal{P}(B)$ ii) $\mathcal{P}(A \cap B) = \mathcal{P}(A) \cap \mathcal{P}(B)$

iii) $A \cap B = \phi \Rightarrow \mathcal{P}(A) \cap \mathcal{P}(B) = \phi$ iv) $\mathcal{P}(\phi) = \phi$

v) $\mathcal{P}(A) \neq \phi \ \forall A \subset \cup$ ($\cup$ universo dado) vi) $\mathcal{P}(A - B) = \mathcal{P}(A) - \mathcal{P}(B)$

13.- Demostrar las siguientes propiedades del producto cartesiano de conjuntos:

i) $A \times B = \phi \Leftrightarrow A = \phi \vee B = \phi$

ii) $A' \subset A \wedge B' \subset B \Leftrightarrow A' \times B' \subset A \times B$

iii) $(A \cup B) \times C = (A \times C) \cup (B \times C)$

iv) $(A \cap B) \times C = (A \times C) \cap (B \times C)$

v) $(A - B) \times C = (A \times C) - (B \times C)$

vi) $\overline{A \times B} = (\overline{A} \times \overline{B}) \cup (\overline{A} \times B) \cup A \times \overline{B})$

Hilbert contribuyó, con su gran autoridad, a difundir las ideas de Cantor, en especial en Alemania, y puede decirse que la teoría de conjuntos recibió consagración oficial en el Congreso de Zurich de 1897.
Esa teoría trajo aparejado el hallazgo de algunos "conjuntos paradójicos", que dieron base a una polémica acerca de los fundamentos de la matemática que se mantuvo durante los primeros decenios de este siglo (XX) y cuya reseña tiene ya cabida en una historia de la matemática.
Algunas de estas paradojas, que se deben al uso indebido del concepto "todos", venían de lejos. Recuérdese la del cretense mentiroso que puede sintetizarse en la expresión "yo miento", que implica contradicción pues si digo la verdad miento y si miento digo la verdad. Este tipo de sofisma, con ropaje variado, está muy difundido; una versión por ejemplo, se enuncia en el Quijote:

***La paradoja del Quijote**: Aparece entre las cuestiones sometidas al juicio de Sancho Panza, como gobernador de la ínsula de Barataria. En resumen es la siguiente: El dueño de un río había impuesto como condición a quien quisiera pasar un puente que lo cruzaba, que debía "jurar primero a dónde y a qué va; y si jurase verdad, déjenle pasar, y si dijere mentira, muera por ello ahorcado en la horca que allí se muestra". Ocurrió entonces que un hombre, que sin duda había leído a Russell, dijo que no iba a otra cosa que "a morir en aquella horca", con lo cual los encargados del cruce del puente quedaron desconcertados, pues si lo dejaban pasar libremente el hombre había mentido y debía morir en la horca, pero si era ahorcado había dicho la verdad y se debía dejar pasar libremente. Lo que sigue ya no es cuestión de lógica, pero vale la pena terminar el cuento. Consultado el buen Sancho, que no entiende de sutilezas lógicas, propone al principio una imposible solución salomónica:*
"que deste hombre aquella parte que juró verdad la dejen pasar y la que dijo mentira la ahorquen", mas luego, cediendo a razones no lógicas pero si humanitarias, resuelve que lo dejen pasar libremente "pues siempre es alabado más el hacer bien, que mal".
("Historia de la Matemática", vol 2. J. Rey Pastor y J. Babini)

SEGUNDA PARTE:

RELACIONES

Gráfica

***Definición*:** Sean A y B conjuntos, se denomina *gráfica en* $A\times B$ a cualquier subconjunto de $A\times B$.

Ejemplos:

1) $A = \{1, 2, 3, 5\}$, $B = \{a, b, c, d\}$
$G = \{(1, a), (1, b), (2, c), (2, d), (3, a), (5, b)\}$

2) $A = \mathbb{N}$ (conjunto de números naturales), $B = \mathbb{R}$ (conjunto de números reales)
$G = \{(x, y) / x = y^2\} \subset A\times B$

***Definiciones*:** Llamaremos *proyección*$_1$ *de* G y *proyección*$_2$ *de* G a los conjuntos:

$$Proy_1(G) = \{x \in A / \exists y \in B : (x, y) \in G\} \subset A$$
$$Proy_2(G) = \{y \in B / \exists x \in A : (x, y) \in G\} \subset B$$

Ejemplos:

1) Para los conjuntos A , B y G del ejemplo 1) anterior
$Proy_1(G) = \{1, 2, 3, 5\}$, $Proy_2(G) = \{a, b, c, d\}$

2) Para los conjuntos A , B y G del ejemplo 2) anterior
$Proy_1(G) = \mathbb{N}$ $Proy_2(G) = \{y \in \mathbb{R} / \exists x \in \mathbb{N} : y = \sqrt{x}\}$

Nota: $G \subset Proy_1(G) \times Proy_2(G) \subset A\times B$; las inclusiones recíprocas pueden no verificarse, como se observa en los ejemplos precedentes.

***Propiedades*:** Sean G_1 y G_2 dos gráficas en $A\times B$. Demostrar que:

1) $Proy_i(G_1 \cap G_2) \subset Proy_i(G_1) \cap Proy_i(G_2)$, $i = 1, 2$. ¿Se verifica siempre la igualdad?, ¿a veces?. Justificar.

2) $Proy_i(G_1 \cup G_2) = Proy_i(G_1) \cup Proy_i(G_2)$, $i = 1, 2$

***Demostración*:** Se deja como ejercicio.

***Definición*:** Sea G una gráfica en $A\times B$. Se denomina *gráfica inversa de* G a la gráfica en $B\times A$:

$$G^{-1} = \{(y, x) / (x, y) \in G\}$$

Ejemplos:

1) $A = \{1, 2, 3, 4, 5\}$, $B = \{a, b, c, d\}$

$G = \{(1, a), (1, b), (2, c), (2, d), (3, a), (5, b)\}$

$G^{-1} = \{(a, 1), (b, 1), (c, 2), (d, 2), (a, 3), (b, 5)\}$

2) $A = \mathbb{N}$ (conjunto de números naturales), $B = \mathbb{R}$ (conjunto de números reales)

$G = \{(x, y) / x = y^2\} \subset \mathbb{N} \times \mathbb{R}$

$G^{-1} = \{(x, y) / x \in \mathbb{R}, y \in \mathbb{N} \wedge y = x^2\} \subset \mathbb{R} \times \mathbb{N}$

***Propiedades*:**

1) $Proy_1(G) = Proy_2(G^{-1})$

2) $Proy_2(G) = Proy_1(G^{-1})$

***Demostración*:** Se deja como ejercicio.

***Definición*:** Sean G y H gráficas en $A \times B$ y $B \times C$ respectivamente. Llamaremos $H \circ G$ (G compuesto con H) a la gráfica en $A \times C$ definida por:

$$H \circ G = \{(x, y) \in A \times C / \exists z \in B : (x, z) \in G \wedge (z, y) \in H\}$$

Ejemplos:

1) $A=B=C=\mathbb{N}$, $G_1 = \{(2, 5), (3, 4), (6, 2), (3, 1), (2, 7)\}$,

$G_2 = \{(4, 8), (5, 3), (1, 9), (2, 2), (7, 4), (5, 10)\}$

$G_2 \circ G_1 = \{(2, 3), (3, 8), (6, 2), (2, 10), (3, 9), (2, 4)\}$

$G_1 \circ G_2 = \{(5, 4), (2, 5), (2, 7), (5,1)\}$

2) $A = \{1, 2, 3, 4, 5\}$, $B = \{a, b, c, d\}$, $C = \{7, 8, 9, 10\}$

$G_1 = \{(1, a), (1, b), (2, c), (2, d), (3, a), (5, b)\} \subset A \times B$

$G_2 = \{(a, 7), (a, 9), (b, 10), (c, 9), (c, 4)\} \subset B \times C$

$G_2 \circ G_1 = \{(1, 7), (1, 9), (1, 10), (2, 9), (2, 4), (3, 7), (3, 9), (5, 10)\} \subset A \times C$

Ejercicios:

i) Para los ejemplos *1)* y *2)* anteriores calcular:

$$G^{1-1}, \quad G^{2-1}, \quad (G^2 \circ G^1)^{-1}, \quad G_1^{-1} \circ G_2^{-1}$$

ii) Demostrar que siempre se verifica: $(G_2 \circ G_1)^{-1} = G_1^{-1} \circ G_2^{-1}$

Relaciones

***Definición*:** Una *relación* es una terna $\Re = (A, B, G)$ donde A y B son conjuntos cualesquiera y G es una gráfica en $A \times B$.

A se denomina *conjunto de partida*, y B *conjunto de llegada* o *codominio*.
Decimos que ***x** está relacionado con **y** por la relación* $\Re$, o que $x \Re y$, si $(x, y) \in G$. En este caso decimos que ***y** es un correspondiente de **x*** por la relación $\Re$.
Se puede definir una relación dando los conjuntos A, B y G o bien, en vez de explicitar el conjunto G, decir cuando un $x \in A$ está relacionado con un $y \in B$ por la relación en cuestión.

Ejemplos:

1) $\Re_1 = (A, B, G_1)$, donde $A = \{1, 2, 3, 4, 5\}$, $B = \{a, b, c, d\}$,
$G_1 = \{(1, a), (1, b), (2, c), (2, d), (3, a), (5, b)\}$.
Aquí tenemos que: $1 \Re_1 a$, $1 \Re_1 b$, $2 \Re_1 c$, $2 \Re_1 d$, $3 \Re_1 a$, $5 \Re_1 b$, $1 \not\Re_1 c$, $2 \not\Re_1 a$.

2) $A = B = \mathbb{N}$, $x \Re_2 y$ *si y sólo si* y es múltiplo de x.

En este caso la gráfica de la relación es un conjunto infinito, luego no puede definirse por extensión, pero dada la propiedad que define la relación, podemos afirmar que:

$1 \Re_2 3$, $1 \Re_2 4$, $3 \Re_2 6$, $6 \Re_2 6$
$2 \not\Re_2 3$, $4 \not\Re_2 6$, $3 \not\Re_2 5$, $6 \not\Re_2 8$

Si se quiere definir la gráfica, deberá hacerse por comprensión, y la propiedad que define a los pares ordenados que pertenecen a la gráfica es justamente la que establecimos como propiedad para definir la relación:

$$G = \{(x, y) \in \mathbb{N} \times \mathbb{N} \ / \ y \text{ es múltiplo de } x\}$$

3) $A = B = \mathbb{N}$, $x \Re_3 y$ *si y sólo si* $x.y = 1$

Para esta relación, con estos conjuntos de partida y de llegada respectivamente, tendremos un único par ordenado en la gráfica, el $(1, 1)$, pues $1 \Re_3 1$, y es el único par de números naturales relacionados.

Observación:
Si en vez de ser $A = B = \mathbb{N}$, fuese $A = B = \mathbb{Z}$ (conjunto de números enteros), en la gráfica habría dos pares ordenados: $(1, 1)$ y $(-1, -1)$, lo que muestra que las relaciones son diferentes, aunque la propiedad que define a los elementos que están relacionados sea la misma.
Si, en cambio, $A = B = \mathbb{Q}$ (conjunto de números racionales), la gráfica G_3 será

$G_3 = \left\{ (x, \frac{1}{x}) \ / \ x \in \mathbb{Q} \ \wedge \ x \neq 0 \right\}$, que es un conjunto infinito.

Nota: Estas consideraciones dejan bien en claro, que la relación es una terna en la cual los tres conjuntos A, B y G (o lo que es lo mismo, la propiedad que define a los elementos relacionados por ella) son igualmente importantes, cambiando cualquiera de ellos se modifica la relación.

***Definición*:** Sea $\Re$ = (*A, B, G*) una relación; llamamos *relación inversa de* $\Re$, a la relación $\Re^{-1} = (B, A, G^{-1})$, donde G^{-1} es la gráfica inversa de *G*.

Ejemplos:

1) $A = B = \mathbb{N}$, $x \ \Re_2^{-1} y$ *si y sólo si* x es múltiplo de y.

$3 \ \Re_2^{-1} 1$, $4 \Re_2^{-1} 2$, $9 \Re_2^{-1} 3$, $6 \ \Re_2^{-1} 6$

$3 \not\Re_2^{-1} 4$, $2 \not\Re_2^{-1} 4$, $6 \not\Re_2^{-1} 7$, $10 \not\Re_2^{-1} 8$

2) $A = B = \mathbb{N}$, $x \ \Re_3^{-1} \ y$ *si y sólo si* $x.y = 1$

En este caso $\Re_3 = \Re_3^{-1}$

En una relación $\Re$ = (*A, B, G*) puede ocurrir que $A = B$ o bien que $A \neq B$. Las relaciones del primer tipo, o sea en las que $A = B$, las llamaremos *relaciones en A*, y podremos notarlas como $\Re = (A,G)$

***Definición*:** Sea $\Re$ = (*A, B, G*) una relación, $E \subset A$, $D \subset B$, $H \subset G$ definido por $H = \{ (x, y) \in G \ / \ x \in E \wedge y \in D \}$, la relación $\Re' = (E, D, H)$ se denomina relación de *E* y *D* inducida por $\Re$.

Relaciones en un conjunto A

Sea $\Re = (A, G)$ una relación en un conjunto *A*.

***Definiciones*:** La relación $\Re$ se dice:

Reflexiva, si: $a \ \Re \ a \quad \forall a \in A$,
o lo que es equivalente, $(a, a) \in$ G, $\quad \forall a \in A$.

Simétrica, si: $a \ \Re \ b \Rightarrow b \ \Re \ a$, $a, b \in A$,
o sea $(a, b) \in G \Rightarrow (b, a) \in G$.

Antisimétrica , si: $a \ \Re \ b \wedge b \ \Re \ a \Rightarrow a = b$,
o equivalentemente $(a, b) \in G \wedge (b, a) \in G \Rightarrow a = b$.

Transitiva , si: $a \ \Re \ b \wedge b \ \Re \ c \Rightarrow a \ \Re \ c$, $\quad a, b, c \in A$,
o equivalentemente $\quad (a, b) \in G \wedge (b, c) \in G \Rightarrow (a, c) \in G$.

Entonces, tenemos que una relación $\Re$:

no es reflexiva si $\exists a \in A$ tal que $\quad a \not\Re a$, $((a, a) \notin G$, para algún $a \in A$)

no es simétrica si $\exists a, b \in A$ tales que $\quad a \Re \ b \wedge b \not\Re a$,
$(\exists a, b \in A : (a, b) \in G \wedge (b, a) \notin G)$.

no es antisimétrica si $\exists a, b \in A$ tales que $\quad a \neq b \wedge a \ \Re \ b \wedge b \ \Re \ a$,

$(\exists a, b \in A$ tales que $a \neq b \wedge (a, b) \in G \wedge (b, a) \in G)$.

no es transitiva si $\exists a, b, c \in A$ tales que $a \,\Re\, b \wedge b \,\Re\, c \wedge a \not\Re\, c$,
$(\exists a, b, c \in A : (a, b) \in G \wedge (b, c) \in G \wedge (a, c) \notin G)$.

Ejemplos:

1) $A = \mathbb{N}$, $x \,\mathfrak{L}_1\, y$ *si y sólo si* y es múltiplo de x.

Precisemos, primero, qué queremos decir cuando afirmamos que "*y es múltiplo de x*".

Definición*:** Sean $a, b \in \mathbb{N}$ **.** Decimos que ***b *es múltiplo de* ***a***, (o que ***a*** divide a ***b,*** o que ***a*** es factor de ***b,*** o que ***a*** es divisor de ***b,*** o que ***a*** es parte de ***b)*** si $\exists k \in \mathbb{N}$ tal que $b = k.a$.

De acuerdo con la definición dada, observamos que la relación $\mathfrak{L}_1$ es:

Reflexiva: pues $a \,\mathfrak{L}_1\, a \quad \forall a \in \mathbb{N}$, ya que $a = 1.a$, cualquiera sea el número natural a.

Antisimétrica: pues $a \,\mathfrak{L}_1\, b \wedge b \,\mathfrak{L}_1\, a \Rightarrow a = b$.

Vamos a demostrarlo:

Si b es múltiplo de a quiere decir que $\exists k \in \mathbb{N}$ tal que $b = k.a$, como a es múltiplo de b $\exists h \in \mathbb{N}$ tal que $a = h.b$

Reemplazando a por su expresión idéntica, tenemos que $b = k.h.b$, por lo tanto $k.h = 1$, siendo k y h números naturales, eso implica que $k = h = 1$, con lo cual vemos que $a = b$.

Transitiva: se verifica que $a \,\mathfrak{L}_1\, b \wedge b \,\mathfrak{L}_1\, c \Rightarrow a \,\mathfrak{L}_1\, c$
Demostrémoslo: si b es múltiplo de a entonces $\exists k \in \mathbb{N}$ tal que $b = k.a$;
si c es múltiplo de b entonces $\exists h \in \mathbb{N}$ tal que $c = h.b$
Reemplacemos b en esta última igualdad con lo cual obtenemos $c = h.k.a$, y como $h.k \in \mathbb{N}$ tenemos que c es múltiplo de a.

No es simétrica pues 4 es múltiplo de 2 y 2 no lo es de 4

2) $A = \mathbb{Z}$, $x \,\mathfrak{L}_2\, y$ *si y sólo si* x divide a y

Definición*:** Para $a \neq 0$ diremos que ***a *divide a* ***b*** si $\exists k \in \mathbb{Z}$ tal que $b = k.a$.

La definición para $\mathbb{Z}$ es completamente análoga a la de $\mathbb{N}$, con la excepción que para decir que a divide a b tenemos que suponer $a \neq 0$ (En $\mathbb{N}$ no es necesario, dado que $0 \notin \mathbb{N}$).
También en este caso se pueden utilizar todas las expresiones equivalentes que dimos anteriormente.

Nota: La exigencia de que $a \neq 0$ se impone porque cuando a divide a b , el $k \in \mathbb{Z}$ que según la definición existe, es además **único**, puesto que si $b = k.a = h.a$ entonces $k.a - h.a = 0$, y así $(k - h).a = 0$, siendo $a \neq 0$, debe ser $k - h = 0$, con lo cual $k = h$.
Si en cambio a pudiese ser igual 0, podríamos escribir $0 = 1.0 = 2.0 = 5.0$, y así sucesivamente; en otras palabras, podríamos decir que 0 divide a 0 pero con infinitos cocientes.

Volviendo a nuestra relación $\mathfrak{L}_2$, analicemos las propiedades que verifica y las que no.

No es reflexiva porque $0 \not\mathfrak{L}_2 0 \wedge 0 \in \mathbb{Z}$

No es antisimétrica porque $2\ \mathfrak{L}_2 -2 \wedge -2\ \mathfrak{L}_2 2 \wedge 2 \neq -2$ ($-2 = (-1).2$; $2 = (-1).(-2)$)

No es simétrica porque $3\ \mathfrak{L}_2\ 6 \wedge 6 \not\mathfrak{L}_2 3$ ($6 = 2.3$)

Es transitiva, la demostración es análoga a la realizada anteriormente.

Estos dos ejemplos muestran claramente la importancia de considerar en una relación, no sólo la propiedad o la gráfica, según cómo sea dada, sino el conjunto sobre el que se define la misma; sobre distintos conjuntos, vinculando los elementos con propiedades análogas, se obtienen dos relaciones con propiedades muy diferentes.

3) $A = \{1, 2, 3, 4, 5\}$, $G_3 = \{ (1, 1), (2, 2), (3, 3), (1, 2), (2, 1) \}$, $\mathfrak{L}_3 = (A, G_3)$

No es reflexiva porque $4 \not\mathfrak{L}_3 4$, pues $(4, 4) \notin G_3$

Es simétrica pues $1\ \mathfrak{L}_3 2 \wedge 2\ \mathfrak{L}_3 1$

Es transitiva pues $1\ \mathfrak{L}_3 2 \wedge 2\ \mathfrak{L}_3 1 \wedge 1\ \mathfrak{L}_3 1$

$2\ \mathfrak{L}_3 1 \wedge 1\ \mathfrak{L}_3 2 \wedge 2\ \mathfrak{L}_3 2$

No es antisimétrica porque $1\ \mathfrak{L}_3 2 \wedge 2\ \mathfrak{L}_3 1 \wedge 1 \neq 2$

4) $B = \{1, 2, 3\}$, $G_4 = \{ (1, 1), (2, 2), (3, 3), (1, 2), (2, 1) \}$, $\mathfrak{L}_4 = (B, G_4)$

Es reflexiva, simétrica y transitiva. No es antisimétrica.

5) $A = \{1, 2, 3, 4, 5\}$, $G_5 = \{ (1, 1), (2, 4), (3, 5) \}$, $\mathfrak{L}_5 = (A, G_5)$

No es reflexiva, ni simétrica.
Es antisimétrica y transitiva.

Nos concentraremos en el estudio de dos tipos particulares de relaciones en un conjunto *A*:
las ***relaciones de orden y las de equivalencia.***

Relaciones de Orden

Definición: Una relación $\mathfrak{R} = (A, G)$ se dice de *orden* si es reflexiva, antisimétrica y transitiva.

Cuando $\mathfrak{R}$ es una relación de orden decimos que $\mathfrak{R}$ define un *orden* en *A*, o también que $(A, \mathfrak{R})$ es un *conjunto ordenado.*

Ejemplos:

1) $(\mathbb{N}, \mathfrak{L}_1)$ del ejemplo 1) anterior, es un conjunto ordenado.

2) $(\mathbb{R}, \leq)$ donde $\leq$ es el orden usual de los números reales, es un conjunto ordenado.
Escribimos $x \leq y$, y se lee *x es menor o igual que y.*

3) $(\mathbb{R}, \geq)$, donde $x \geq y$ *sii* $y \leq x$, es también un conjunto ordenado.
$x \geq y$ se lee *x es mayor o igual que y.*

4) $(\mathbb{R}, <)$, donde $x < y$ *si y sólo si* (*sii*) $x \leq y \wedge x \neq y$.
$x < y$ se lee *x es menor que y.*

Esta **no** es una relación de orden aunque se denomine *orden estricto*, pues no es reflexiva, pero sí antisimétrica y transitiva.

5) $(\mathbb{R}, >)$, donde $x > y$ *sii* $y < x$ *sii* $x \geq y \wedge x \neq y$.
$x > y$ se lee *x es mayor que y.*
Tampoco es una relación de orden, por las mismas consideraciones que en la anterior, y también se denomina *orden estricto.*

6) $(\mathcal{P}(A), \subset)$, donde $\mathcal{P}(A)$ es el conjunto de partes de un conjunto A, $\subset$ es la relación de inclusión entre conjuntos, es un conjunto ordenado.

7) Definamos en $\mathbb{N} \times \mathbb{N}$ la siguiente relación $\Re_1$:

$$(a, b)\ \Re_1\ (c, d) \quad \textit{si y sólo si (sii)} \quad a \leq c \ \wedge \ b \leq d$$

¿Es una relación de orden?

¿Es reflexiva? Sí, pues $(a, b)\ \Re_1\ (a, b)$, $\forall (a, b) \in \mathbb{N} \times \mathbb{N}$.

¿Es antisimétrica?
Sí, pues si $(a, b)\ \Re_1\ (c, d) \wedge (c, d)\ \Re_1\ (a, b)$ entonces $a \leq c \wedge b \leq d$, y además
$c \leq a \wedge d \leq b$
$a \leq c \wedge c \leq a \Rightarrow a = c$
$d \leq b \wedge b \leq d \Rightarrow b = d$
Luego $(a, b) = (c, d)$.

¿Es transitiva?
Sí, pues si $(a, b)\ \Re_1\ (c, d) \ \wedge \ (c, d)\ \Re_1\ (e, f)$ entonces $a \leq c \ \wedge \ b \leq d$, y además
$c \leq e \ \wedge \ d \leq f$.
$a \leq c \ \wedge \ c \leq e \Rightarrow a \leq e$,
$b \leq d \ \wedge \ d \leq f \Rightarrow b \leq f$.
Luego $(a, b)\ \Re_1\ (e, f)$.

Así $\Re_1$ es una relación de orden sobre $\mathbb{N} \times \mathbb{N}$.

8) En $\mathbb{N} \times \mathbb{N}$ definamos la relación $\Re_2$:

$$(a, b)\ \Re_2\ (c, d) \Leftrightarrow a = c \ \wedge \ b \leq d.$$

Verificar que $(\mathbb{N} \times \mathbb{N}, \Re_2)$ es un conjunto ordenado.

9) En $\mathbb{N} \times \mathbb{N}$ definamos la relación $\Re_3$:

$$(a, b)\ \Re_3\ (c, d) \Leftrightarrow a \leq c \ \wedge \ b = d.$$

Verificar que $(\mathbb{N} \times \mathbb{N}, \Re_3)$ es un conjunto ordenado.

10) En $\mathbb{N} \times \mathbb{N}$ definamos la relación $\Re_4$:

$$(a, b)\ \Re_4\ (c, d) \Leftrightarrow a \leq c \ \wedge \ (\textit{si } a = c \Rightarrow b \leq d).$$

Verificar que $(\mathbb{N} \times \mathbb{N}, \mathfrak{R}_4)$ es un conjunto ordenado. Este orden se denomina *orden lexicográfico.*

Los ejemplos 7), 8), 9) y 10) nos muestran cuatro órdenes diferentes para $\mathbb{N} \times \mathbb{N}$,
(1, 2) $\wedge$ (3, 4) están relacionados por $\mathfrak{R}_1$ y $\mathfrak{R}_4$ pero no por $\mathfrak{R}_2$ ni por $\mathfrak{R}_3$.

(1, 2) $\mathfrak{R}_1$ (3, 4) $\wedge$ (1, 2) $\mathfrak{R}_4$ (3, 4)
(4, 3) $\mathfrak{R}_4$ (5, 2) , pero (4, 3) $\wedge$ (5, 2) no están relacionados por ninguno de los tres órdenes restantes.
En realidad podemos observar que todo par de elementos en $\mathbb{N} \times \mathbb{N}$ están relacionados en algún sentido por $\mathfrak{R}_4$, no así, necesariamente, por ninguno de los otros tres órdenes. Esta diferencia es sustancial, y nos lleva a precisar este concepto.

***Definición*:** Sea (A, $\mathfrak{R}$) un conjunto ordenado. Diremos que es *totalmente ordenado,* o que $\mathfrak{R}$ es *un orden total* para A, si $x \mathfrak{R} y \vee y \mathfrak{R} x \quad \forall x, y \in A$.

Cuando (A, $\mathfrak{R}$) no sea totalmente ordenado, o sea cuando $\exists x, y \in A$ tales que $x \not\mathfrak{R} y \wedge y \not\mathfrak{R} x$, diremos que es *parcialmente ordenado* o que $\mathfrak{R}$ es *un orden parcial* para A.

Ejemplos:

1) $(\mathbb{N} \times \mathbb{N}, \mathfrak{R}_4)$ es totalmente ordenado.
2) $(\mathbb{N} \times \mathbb{N}, \mathfrak{R}_1)$, $(\mathbb{N} \times \mathbb{N}, \mathfrak{R}_2)$, $(\mathbb{N} \times \mathbb{N}, \mathfrak{R}_3)$ son conjuntos parcialmente ordenados.
3) $(\mathbb{N}, \mathfrak{L}_1)$ del ejemplo anterior es parcialmente ordenado.
4) $(\mathbb{R}, \leq)$ del ejemplo precedente, es totalmente ordenado, al igual que $(\mathbb{R}, \geq)$.
5) $(\mathcal{P}(A), \subset)$ es parcialmente ordenado.

***Definiciones*:** Sea (A, $\mathfrak{R}$) un conjunto ordenado ; $B \subset A$, $B \neq \phi$, $a \in A$.
Diremos que a es *cota superior de* B si $x \mathfrak{R} a$, $\forall x \in B$.
Diremos que a es *cota inferior de* B si $a \mathfrak{R} x$, $\forall x \in B$.
Decimos que B *es acotado superiormente* si admite cotas superiores, *acotado inferiormente* si admite cotas inferiores, y *acotado* si lo es inferior y superiormente.

Decimos que a es *máximo* de B si:
i) a es cota superior de B
ii) $a \in B$
Notación: $a = máx\ B$

Decimos que a es *mínimo o primer elemento* de B si :
i) a es cota inferior de B
ii) $a \in B$.
Notación: $a = mín\ B$

Diremos que a es un *maximal* de B si:
i) $a \in B$.
ii) $a \mathfrak{R} x$, $x \in B \Rightarrow a = x$.

Diremos que *a* es un *minimal* de *B* si:

i) $a \in B$
ii) $x \,\Re\, a, \quad x \in B \Rightarrow a = x.$

Diremos que *a* es *supremo* de *B* si:

i) *a* es cota superior de *B*
ii) *b* es cota superior de $B \Rightarrow a \,\Re\, b$

Notación: $a = sup\ B$

Diremos que *a* es *ínfimo* de *B* si:

i) *a* es cota inferior de *B*
ii) *b* es cota inferior de $B \Rightarrow b \,\Re\, a$

Notación: $a = ínf\ B$

Observaciones:

Cuando un conjunto admite un máximo o un mínimo, éstos son ***únicos*** (en cada caso) pues si *a* y *a´* fueran dos máximos para *B* , como $a \in B$ y *a´* es cota superior de *B*, entonces $a \,\Re\, a'$, pero también $a' \in B$ y *a* es cota superior de *B*, entonces $a' \,\Re\, a$. Como $\Re$ es relación de orden, es antisimétrica, luego de $a \,\Re\, a' \ \wedge \ a' \,\Re\, a$, deducimos que $a = a'$
Análogamente si *a* y *a´* fueran mínimos de *B.*
Un conjunto puede no admitir máximo y/o mínimo, aun siendo acotado.
Las cotas, tanto inferiores como superiores, pudieran no existir para un conjunto, pero también podrían ser muchas, incluso infinitas. Idéntica observación puede hacerse respecto de maximales y minimales.

Nota: Para los casos de supremos e ínfimos, es condición necesaria para que éstos existan que el conjunto sea acotado superior o inferiormente, según el caso, pero si ésta fuera la situación, suponiendo que tuviéramos un conjunto acotado superiormente; la definición nos dice que el supremo es el mínimo en el conjunto de las cotas superiores (podemos decir que es *la menor* de las cotas superiores), y este mínimo podría no existir, pero si existiera, sería ***único***, como vimos anteriormente. Análogamente el ínfimo es el máximo en el conjunto de las cotas inferiores, o sea, *la mayor* de las cotas inferiores de *A*, y, como expresamos antes, podría no existir, pero si existiera, sería ***único***.

Ejemplos:

1) En $(\mathbb{R}\ , \leq)$, sea $B = \{\ x / 0 < x \leq 1\ \} = (\ 0,\ 1\ ]$ (intervalo semiabierto)

1, 2, $\frac{5}{2}$, 12 son cotas superiores de *B*, es más, el conjunto de cotas superiores de *B* es $\{\ x / x \geq 1\}$;
$1 = sup\ B = máx\ B.$

0, –1, $-\frac{3}{4}$, –16 son cotas inferiores de *B*; el conjunto de cotas inferiores de *B* es $\{\ x / x \leq 0\}$;
$0 = ínf\ B$; *B* no tiene mínimo.
Tiene un único elemento maximal, el 1, y ningún minimal.

2) Sea $A = \{1, 2, 3, 4, 5\}$, $(\mathcal{P}(A), \subset)$ o sea, $\mathcal{P}(A)$ ordenado por inclusión.

Llamemos $B = \mathcal{P}(A)$, $\phi = mín\ B = ínf\ B$, también es la única cota inferior y el único minimal.
$A = máx\ B = sup\ B$, además es el único maximal y la única cota superior.

Para el mismo conjunto ordenado sea

$\mathcal{F} = \{\{1, 2\}, \{1,2,3\}, \{1,3\}, \{1,3,5\}, \{4\}\}$

Cotas superiores de $\mathcal{F}$: A ; $A = sup\ \mathcal{F}$

Cotas inferiores de $\mathcal{F}$: ϕ ; $\phi = ínf.\ \mathcal{F}$

Maximales de $\mathcal{F}$: $\{1,2,3\}$, $\{1,3,5\}$, $\{4\}$

Minimales de $\mathcal{F}$: $\{1,2\}$, $\{1,3\}$, $\{4\}$

$\mathcal{F}$ no tiene máximo ni mínimo.

Ejercicios:

1) Sean $(A, \Re)$ un conjunto ordenado, $B \subset A$, $B \neq \phi$; demostrar que:

i) si B tiene mínimo b, entonces $b = ínf\ B$, y b es el único minimal de B.

ii) si B tiene máximo a, entonces $a = sup\ B$, y es el único maximal de B.

2) Sean $(A, \Re)$ un conjunto totalmente ordenado, $B \subset A$, $B \neq \phi$; demostrar:

i) a es mínimo de B *sii* a es minimal. En tal caso, hay un único minimal.

ii) b es máximo de B *sii* b es maximal. En tal caso, hay un único maximal.

Este ejercicio prueba que en un conjunto totalmente ordenado, los conceptos de minimal y maximal se funden en los de mínimo y máximo respectivamente.

3) Sean $A \neq \phi$, $(\mathcal{P}(A), \subset)$, o sea, $\mathcal{P}(A)$ ordenado por inclusión, $\mathcal{F} \subset \mathcal{P}(A)$, $\mathcal{F} \neq \phi$.

Demostrar que $\bigcup_{B \in \mathcal{F}} B = sup\ \mathcal{F} \wedge \bigcap_{B \in \mathcal{F}} B = ínf\ \mathcal{F}$. ¿Es verdadero o falso que se verifique siempre que $\bigcup_{B \in \mathcal{F}} B = máx\ \mathcal{F}$ y/o $\bigcap_{B \in \mathcal{F}} B = mín\ \mathcal{F}$? Justificar.

***Definición*:** Sea $(A, \Re)$ un conjunto ordenado, diremos que es *bien ordenado* (*b.o.*), o que $\Re$ es un *buen orden* para A, si todo subconjunto no vacío de A tiene mínimo.

Ejemplos:

1) En cualquier conjunto ordenado $(A, \Re)$, todo subconjunto es ordenado con el orden inducido y ϕ es bien ordenado, pues no admite subconjuntos no vacíos.

2) Los conjuntos unitarios $\{a\}$ son b.o. en cualquier conjunto ordenado $(A, \Re)$.

3) En $(\mathbb{R}, \leq)$, todo conjunto binario $\{a, b\}$ es b.o., también los conjuntos ternarios $\{a, b, c\}$ son b.o. (Esto vale en general para todo $(A, \Re)$ totalmente ordenado)

Ejercicios:

1) Sea $(A, \Re)$ un conjunto ordenado, demostrar que si es b.o. es totalmente ordenado. ¿Vale la recíproca?

2) Si $A \subset B \wedge B$ es b.o. $\Rightarrow A$ es b.o.

Relaciones de Equivalencia

***Definición*:** Sea *A* un conjunto no vacío, $\Re$ una relación en *A*.
$\Re$ *es una relación de equivalencia* si es *reflexiva, simétrica y transitiva.*
Ejemplos:

1) Sea *A* el conjunto de rectas del plano, $\Re$ la relación:

$$r \,\Re\, s \text{ sii } r \text{ es paralela a } s \ (r//s)$$

Esta relación es reflexiva, porque toda recta es paralela a sí misma; simétrica, porque si $r//s \Rightarrow s//r$; y transitiva, pues si $r//s \wedge s//t \Rightarrow r//t$, luego , es de equivalencia.

2) Sea *B* el conjunto de triángulos en el plano, $\equiv$ la relación:

$$\alpha \equiv \beta \Leftrightarrow \alpha \text{ es congruente a } \beta \text{, donde } \alpha, \beta \in B.$$

La congruencia de triángulos, también es una relación de equivalencia.

3) Sea *C* un conjunto no vacío, $\Re$ la relación de igualdad:

$$x, y \in C, \quad x \,\Re\, y \quad sii \quad x = y$$

Esta relación es reflexiva, simétrica y transitiva, pero además es también antisimétrica, luego es relación de equivalencia y de orden al mismo tiempo.

4) En $\mathbb{Z}$ (conjunto de números enteros), $n \in \mathbb{N}$, definamos la relación $\equiv$ (*mód n*)
(se lee *congruencia módulo n*):

$$a \equiv b \ (mód\ n) \quad si\ y\ sólo\ si \quad n \mid (a-b)$$

Esta relación se lee: ***a*** es congruente a ***b*** módulo n si y sólo si ***n*** divide a (***a – b***).

Veamos que es de equivalencia.
¿Es reflexiva? Sí, pues $n \mid (a-a) = 0$ (todo número natural divide a 0 pues $0 = 0.n$),
luego $a \equiv a \ (mód\ n) \quad \forall a \in \mathbb{Z}$.
¿Es simétrica? Sí, pues si $a \equiv b \ (mód\ n)$, entonces $n \mid (a-b)$, luego $\exists k \in \mathbb{Z}$ tal que $a - b = k.n$, de donde $b - a = (-k).n$, $-k \in \mathbb{Z}$, por lo tanto $n \mid (b-a)$,
y así $b \equiv a \ (mód\ n)$.
¿Es transitiva? Sí, pues si $a \equiv b \ (mód\ n) \wedge b \equiv c \ (mód\ n)$ entonces existen $k, h \in \mathbb{Z}$ tales que $a - b = k.n \wedge b - c = h.n$, sumando miembro a miembro (m.a.m) obtenemos que $a - c = (k + h).n$, con $k + h \in \mathbb{Z}$, luego $n \mid (a-c)$, entonces $a \equiv c \ (mód\ n)$.

Particiones

***Definición*:** Sea $(A_i)_{i \in I}$ una familia dada de subconjuntos de un conjunto *B*
(esto es $A_i \subset B \ \forall i \in I$). Se dice que la familia $(A_i)_{i \in I}$ es una *partición* de *B* si verifica:

1. $A_i \neq \phi \ \ \forall i \in I$
2. $\forall i, j \in I$, $i \neq j$ se verifica que $A_i \cap A_j = \phi$
3. $\bigcup_{i \in I} A_i = B$

Ejemplos:

1. La familia $\{\mathbb{P}, \mathbb{I}\}$, donde $\mathbb{P}$ designa al conjunto de enteros pares e $\mathbb{I}$ al conjunto de los enteros impares, constituye una partición de $\mathbb{Z}$.

2. La familia $(A_i)_{i\in\mathbb{Z}}$ donde $A_i = [i, i+1)\ \forall i \in \mathbb{Z}$ constituye una partición de $\mathbb{R}$

3. La familia $(C_i)_{i\in\mathbb{Z}}$ donde $C_i = [i, i+1]\ \forall i \in \mathbb{Z}$, no constituye una partición de $\mathbb{R}$ porque $C_i \cap C_{i+1} \neq \phi$.

Clases de equivalencia y Conjunto Cociente

***Definición*:** Sea $\approx$ una relación de equivalencia en el conjunto *A*, $a \in A$.
Se denomina *clase de equivalencia de a,* y se lo nota $\overline{a}$, al conjunto:

$$\overline{a} = \{ x / x \in A \ \wedge\ x \approx a \}$$

El conjunto de todas las clases de equivalencia en el conjunto *A*, se denomina *Conjunto Cociente de la relación* $\approx$, y se nota:

$$A/_{\approx} = \{\ \overline{a}\ / a \in A\ \}$$

La familia formada por las clases de equivalencia distintas del conjunto cociente determina una *partición* en *A* pues:

i) $\overline{a} \neq \phi$, $\forall a \in A$.

ii) para $a, b \in A$, se verifica una y sólo una de estas dos condiciones: $\overline{a} = \overline{b} \ \vee\ \overline{a} \cap \overline{b} = \phi$.

iii) $\bigcup_{a\in A} \overline{a} = A$.

Demostración:

i) Dado que la relación $\approx$, al ser de equivalencia, es reflexiva, tenemos que $a \approx a\ \ \forall a \in A$, y así $a \in \overline{a}$, $\forall a \in A$.

ii) Si $\overline{a} \cap \overline{b} \neq \phi$, entonces $\exists c \in A\ /\ c \in \overline{a} \wedge c \in \overline{b}$, luego $c \approx a \ \wedge\ c \approx b$, por ser simétrica y transitiva, implica que $a \approx b$ con lo cual $a \in \overline{b}$. Además si $x \in \overline{a}$, entonces $x \approx a$, y como $a \approx b$, por transitividad, $x \approx b$, con lo cual $x \in \overline{b}$, y así $\overline{a} \subset \overline{b}$.

Razonando en forma simétrica, tenemos que $\overline{b} \subset \overline{a}$, luego $\overline{a} = \overline{b}$.

iii) $\overline{a} \subset A\ \forall a \in A$, luego $\bigcup_{a\in A} \overline{a} \subset A$

Por otra parte si $x \in A$, como $x \in \overline{x} \ \wedge\ \overline{x} \subset \bigcup_{a\in A} \overline{a}$, entonces $x \in \bigcup_{a\in A} \overline{a}$, así $A \subset \bigcup_{a\in A} \overline{a}$.

Por lo tanto $\bigcup_{a\in A} \overline{a} = A$.

Recíprocamente, si la familia $(A_i)_{i\in I}$ es una partición del conjunto *B*, la relación

$$x \sim y \ \textit{si y sólo si}\ \exists i \in I \ \text{tal que}\ x, y \in A_i$$

es una relación de equivalencia en *B*

***Demostración*:**

- Es reflexiva, pues si $x \in B$, como $(A_i)_{i\in I}$ es una partición de *B*, se verifica que $\bigcup_{i\in I} A_i = B$, por lo tanto $\exists\, j \in I$ tal que $x \in A_j$; como por la relación definida todos los elementos de A_j están relacionados entre sí, en particular $x \sim x$.

- Es simétrica, pues si $x, y \in B$ son tales que $x \sim y$ entonces $\exists\, i \in I$ tal que $x , y \in A_i$, o sea que y , x ambos están en el mismo conjunto A_i , por lo tanto $y \sim x$.

- Es transitiva, pues si $x, y, z \in B$ son tales que $x \sim y \ \wedge\ y \sim z$, tenemos que
  $x \sim y \ \Leftrightarrow\ \exists\, i \in I$ tal que $x , y \in A_i$
  $y \sim z \ \Leftrightarrow\ \exists\, j \in I$ tal que $y , z \in A_j$
  como $(A_i)_{i\in I}$ es una partición en B , $\forall k, h \in I$, $k \neq h \ \Rightarrow\ A_k \cap A_h = \phi$,
  luego si $y \in A_i \cap A_j$ entonces $i = j \ \therefore\ A_i = A_j$
  Así $\exists\, i \in I$ tal que $x , y , z \in A_i$, en particular $x , z \in A_i$ por lo tanto $x \sim z$

Ejemplos:

1) Volvamos a la congruencia módulo *n* en $\mathbb{Z}$; para $n = 2$

$$a \equiv b\ (mód\ 2) \quad si\ y\ sólo\ si \quad 2 \,|\, (a-b) \quad sii \quad a-b \ \text{ es par.}$$

Sabemos que la suma y diferencia de dos números enteros es par si y sólo si ambos son pares o ambos son impares, esto es, si y sólo si tienen la misma paridad. Luego tendremos dos clases de equivalencia:

$\bar{0} = \{ x \in \mathbb{Z} \ / \ 2 \,|\, x \} = \{ \ x \in \ \mathbb{Z} \ / \ x \text{ es par } \} = \mathbb{P}$

$\bar{1} = \{ x \in \mathbb{Z} \ / \ 2 \,|\, (x-1) \} = \{ \ x \in \ \mathbb{Z} \ / \ x \text{ es impar } \} = \mathbb{I}$

Entonces, el conjunto cociente de la congruencia *mód.* 2 es finito, y tiene dos elementos:

$$\mathbb{Z} \big/ \equiv (mód\ 2) = \{ \bar{0}, \bar{1} \} = \{ \mathbb{P} , \mathbb{I} \}$$

2) En $\mathbb{Z}$, la congruencia módulo 3.

$$a \equiv b\ (mód\ 3) \quad si\ y\ sólo\ si \quad 3 \,|\, (a-b)$$

En este caso ya no es tan evidente, como lo es para 2, cuándo la diferencia de dos números es múltiplo de tres, así que veamos algunos ejemplos:

$0 \equiv 3 \equiv 6 \equiv -3 \equiv -9 \equiv 18 \equiv -15 \equiv 600 \equiv -1290\ (mód\ 3)$
$1 \equiv 4 \equiv 7 \equiv -2 \equiv -8 \equiv 13 \equiv -14 \equiv 1000 \equiv -599\ (mód\ 3)$
$2 \equiv 5 \equiv -1 \equiv 20 \equiv 998 \equiv -61 \equiv -1000 \equiv 800\ (mód\ 3)$
$0 \not\equiv 1$, $1 \not\equiv 2$, $2 \not\equiv 1\ (mód\ 3)$, luego ninguno de los números congruentes con 0 lo será con ninguno de los congruentes con 2, ni los congruentes con 1 lo serán con los que lo son con 2; pero eso igual no resuelve el problema de determinar las clases *mód* 3.

Supongamos que $x \equiv 0$ (*mód* 3) , entonces $x - 0$ es múltiplo de 3, luego x es múltiplo de 3; recíprocamente, si $x = 3k$, $k \in \mathbb{Z}$, claramente $3 \mid (x - 0)$ pues $x - 0 = x$ y $3 \mid x$.

Luego $\overline{0} = \{ x \ / \ 3 \mid x \} = \{ 3k \ / k \in \mathbb{Z} \} = 3\mathbb{Z}$ (esta notación designa al conjunto de los enteros múltiplos de 3).

Sea ahora $x \equiv 1$ (*mód* 3), luego $x - 1$ es múltiplo de 3, o sea, $x - 1 = 3k$ con $k \in \mathbb{Z}$, luego $x = 3k + 1$, lo que equivale a decir que x tiene resto 1 en la división por 3. Recíprocamente, sea x con resto 1 en la división por 3, luego $x = 3q + 1$, donde $q \in \mathbb{Z}$ y es el cociente en la división de x por 3; entonces $x - 1 = 3q$, y así $3 \mid (x - 1)$, con lo cual $x \equiv 1$ (*mód* 3).

Luego $\overline{1} = \{ x \ / \ 3 \mid (x-1) \} = \{ 3k + 1 \ / k \in \mathbb{Z} \}$.

En forma análoga se demuestra que $\overline{2}$ es el conjunto de los enteros con resto 2 en la división por 3, $\overline{2} = \{ x \ / \ 3 \mid (x-2) \} = \{ 3k + 2 \ / k \in \mathbb{Z} \}$.

Como todo número entero tiene uno y sólo uno de estos tres restos en la división por 3: 0, 1 o 2, tenemos sólo tres clases de equivalencia (*mód* 3):

$$\mathbb{Z} / \equiv (mód\ 3) = \{ \overline{0}, \overline{1}, \overline{2} \}$$

Comentario:

Si $\approx$ es una relación de equivalencia en el conjunto A, $a \in A$, y $\overline{a}$ es su clase de equivalencia, a se denomina *un representante de* $\overline{a}$. Como seguramente habrá otros $b \in \overline{a}$, también b es un representante de $\overline{a}$, en definitiva cualquier elemento que pertenezca a $\overline{a}$ podrá ser llamado *un representante* de esa clase de equivalencia. Cierto tipo de relaciones tienen, lo que podríamos llamar *representantes canónicos* para sus clases de equivalencia, por ejemplo, en las dos relaciones vistas anteriormente:

Congruencia mód 2 : 0 es el representante canónico de $\overline{0}$, aunque pueda uno designar muchos otros representantes de esta clase 2, –2, 4, –4, 6, –6, etc.
1 es el representante canónico de $\overline{1}$, pero hay muchos otros representantes –1, 3, –3, 5, –5, etc.

Congruencia mód 3: 0 es el representante canónico de $\overline{0}$, aunque pueda uno designar muchos otros representantes de esta clase 3, –3, 6, –6, 9, –9, etc.
1 es el representante canónico de $\overline{1}$, pero hay muchos otros representantes –2, 4, –5, 7, –8, etc.
2 es el representante canónico de $\overline{2}$, pero se pueden tomar otros representantes –1, 5, – 4, 8, – 7, etc.

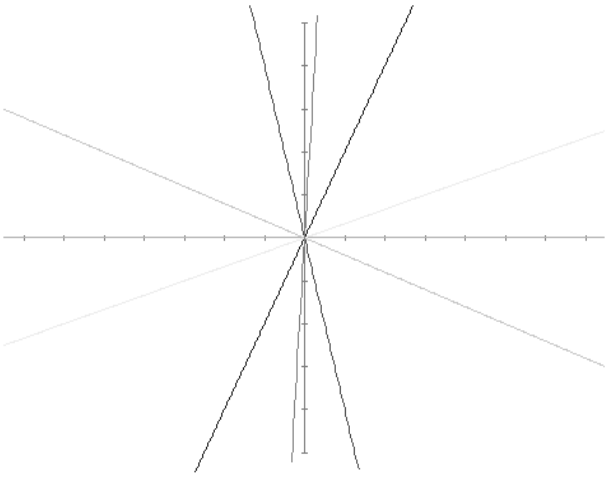
Nota: Obsérvese que las clases de equivalencia módulo n son notadas de la misma manera para distintos n ; eso no debe inducir a confusiones porque, para cada n, aunque la notación que usemos sea la misma, el símbolo $\overline{a}$ designa conjuntos diferentes, como puede observarse en los ejemplos precedentes.

Notación: Al conjunto cociente correspondiente a la relación de *congruencia mód n* lo designaremos $\mathbb{Z}_n$, o sea $\mathbb{Z}_n = \mathbb{Z} / \equiv (mód\ n)$

En el ejemplo de relación de equivalencia donde *A* es el conjunto de rectas del plano, $\Re$ la relación:

$$r \,\Re\, s \quad sii \quad r \text{ es paralela a } s \;(\, r//s)$$

Toda recta del plano *r* es paralela a una y sólo una de las rectas que pasan por el origen de coordenadas, y cada una de éstas, a su vez, determina una clase diferente de las demás, porque dos rectas que pasan por el origen son paralelas si y sólo si son iguales. En este caso, se pueden elegir las rectas que pasan por el origen como representantes canónicos en sus respectivas clases de equivalencia.



Ejercicio: Sea $\mathbb{R}$ el conjunto de números reales y $\prec$ la relación en $\mathbb{R}$ definida por:

$$x \prec y \quad sii \quad x - y \in \mathbb{Z}$$

i) Demostrar que $\prec$ es una relación de equivalencia en $\mathbb{R}$
ii) Determinar un subconjunto de $\mathbb{R}$ que pudiera ser considerado un conjunto de representantes canónicos de las clases de equivalencia, siguiendo la idea utilizada en el ejemplo de las rectas del plano.

***Aplicaciones de las relaciones de equivalencia*:**

Mostraremos con algunos ejemplos, de qué manera se usan las relaciones de equivalencia en Matemática.
Desde el punto de vista intuitivo, cada vez que se quieren "identificar" elementos de un determinado conjunto que satisfacen una misma propiedad, es decir, crear un conjunto en el que todos ellos *funcionen* como uno solo, se intenta definir una relación de equivalencia que cumpla con ese objetivo, o sea, tal que los elementos relacionados sean justamente los que queremos identificar.
Por ejemplo, en la relación de paralelismo de las rectas del plano, muchas de las propiedades sobre rectas basta demostrarlas para uno de los representantes de cada clase, y sin más, se extiende a las demás rectas de esa misma clase : por ej. si *t* es perpendicular a *r,* será perpendicular a *s*, para toda *s* tal que *r//s.*

Ejemplo 1: *Definir el conjunto* $\mathbb{Z}$ *de números enteros, conociendo* $\mathbb{N}_0$ (*conjunto de números naturales con el cero*) *con sus operaciones.*

En $\mathbb{N}_0 \times \mathbb{N}_0$ definimos la siguiente relación:

$$(a, b) \propto (c, d) \quad \textit{si y sólo si} \quad a + d = b + c$$

¿Es de equivalencia?

Reflexiva: ¿ $(a, b) \propto (a, b)$? . Sí pues $a + b = b + a$
Simétrica: ¿ $(a, b) \propto (c, d) \Rightarrow (c, d) \propto (a, b)$?. Sí puesto que si $(a, b) \propto (c, d)$ entonces $a + d = b + c$, luego $c + b = d + a$, de donde $(c, d) \propto (a, b)$.
Transitiva: ¿ $(a, b) \propto (c, d) \wedge (c, d) \propto (e, f) \Rightarrow (a, b) \propto (e, f)$? Veamos:
$(a, b) \propto (c, d)$ entonces $a + d = b + c$ (1)
$(c, d) \propto (e, f)$ entonces $c + f = d + e$ (2)
sumando f m.a.m. en (1), $a + d + f = b + c + f$
reemplazando la primera igualdad por (2), $a + d + f = b + d + e$
cancelando d en los dos miembros de esta última igualdad, obtenemos $a + f = b + e$
así tenemos que $(a, b) \propto (e, f)$.

Por lo tanto $\propto$ es una relación de equivalencia en $\mathbb{N}_0 \times \mathbb{N}_0$

Estudiemos las clases de equivalencia:

$$\overline{(0, 0)} = \{ (a, b) / (a, b) \propto (0,0) \} = \{ (a, b) / a + 0 = b + 0 \} = \{ (a, b) / a = b \} =$$
$$= \{ (a, a) / a \in \mathbb{N}_0 \}$$

$$\overline{(1, 0)} = \{ (a, b) / (a, b) \propto (1,0) \} = \{ (a, b) / a + 0 = b + 1 \} = \{ (a, b) / a = b + 1 \} =$$
$$= \{ (b + 1, b) / b \in \mathbb{N}_0 \}$$

$$\overline{(2, 0)} = \{ (a, b) / (a, b) \propto (2, 0) \} = \{ (a, b) / a + 0 = b + 2 \} = \{ (a, b) / a = b + 2 \} =$$
$$= \{ (b + 2, b) / b \in \mathbb{N}_0 \}$$

$$\overline{(3, 0)} = \{ (a, b) / (a, b) \propto (3, 0) \} = \{ (a, b) / a + 0 = b + 3 \} = \{ (a, b) / a = b + 3 \} =$$
$$= \{ (b + 2, b) / b \in \mathbb{N}_0 \}$$

En general, para $k \in \mathbb{N}_0$ tenemos

$$\overline{(k, 0)} = \{ (a, b) / (a, b) \propto (k, 0) \} = \{ (a, b) / a + 0 = b + k \} = \{ (a, b) / a = b + k \} =$$
$$= \{ (b + k, b) / b \in \mathbb{N}_0 \}$$

$$\overline{(0, 1)} = \{ (a, b) / (a, b) \propto (0, 1) \} = \{ (a, b) / a + 1 = b + 0 \} = \{ (a, b) / a + 1 = b \} =$$
$$= \{ (a, a + 1) / a \in \mathbb{N}_0 \}$$

$$\overline{(0, 2)} = \{ (a, b) / (a, b) \propto (0, 2) \} = \{ (a, b) / a + 2 = b + 0 \} = \{ (a, b) / a + 2 = b \} =$$
$$= \{ (a, a + 2) / a \in \mathbb{N}_0 \}$$

$$\overline{(0, 3)} = \{ (a, b) / (a, b) \propto (0, 3) \} = \{ (a, b) / a + 3 = b + 0 \} = \{ (a, b) / a + 3 = b \} =$$
$$= \{ (a, a + 3) / a \in \mathbb{N}_0 \}$$

En general, para $h \in \mathbb{N}_0$ tenemos

$$\overline{(0, h)} = \{ (a, b) / (a, b) \propto (0, h) \} = \{ (a, b) / a + h = b + 0 \} = \{ (a, b) / a + h = b \} =$$
$$= \{ (a, a + h) / a \in \mathbb{N}_0 \}$$

Claramente se ve que $(k, 0) \propto (0, h)$ si y sólo si $k + h = 0$, y como $k, h \in \mathbb{N}_0$, esto ocurre si y sólo si $k = h = 0$

Además $(k, 0) \propto (h, 0)$ si y sólo si $k = h$; análogamente $(0, k) \propto (0, h)$ si y sólo si $k = h$.

Por lo tanto las clases $\overline{(0, 0)}$; $\overline{(0, h)}$, $h \in \mathbb{N}$; $\overline{(k, 0)}$, $k \in \mathbb{N}$ son todas distintas. Veamos si hay otras clases además de éstas.

Sea $(a, b) \in \mathbb{N}_0 \times \mathbb{N}_0$; en $\mathbb{N}_0$ pueden ocurrir tres situaciones distintas, y sólo éstas:

$$a = b, \quad a < b \quad \vee \quad b < a$$

Si $a = b$, como ya vimos $(a, b) = (a, a) \propto (0, 0)$, entonces $\overline{(a, b)} = \overline{(0, 0)}$.

Si $a < b$, entonces $\exists h \in \mathbb{N}$ tal que $a + h = b$, entonces $(a, b) \propto (0, h)$,
luego $\overline{(a, b)} = \overline{(0, h)}$

Si $b < a$, entonces $\exists k \in \mathbb{N}$ tal que $a = b + k$, entonces $(a, b) \propto (k, 0)$,
luego $\overline{(a, b)} = \overline{(k, 0)}$

Ahora estamos en condiciones de definir completamente el conjunto cociente:

$$\mathbb{N}_0 \times \mathbb{N}_0 \Big/ \propto = \left\{ \overline{(k, 0)} \ / \ k \in \mathbb{N} \right\} \cup \left\{ \overline{(0, h)} \ / \ h \in \mathbb{N} \right\} \cup \left\{ \overline{(0, 0)} \right\}$$

Esta unión es disjunta dos a dos.

Ahora vamos a definir una *suma* y un *producto* en el conjunto cociente, valiéndonos de la suma y el producto de $\mathbb{N}_0$

Definimos: $\overline{(a, b)} + \overline{(c, d)} = \overline{(a + c, b + d)}$

$$\overline{(a, b)} \,.\, \overline{(c, d)} = \overline{(a.c + b.d, a.d + b.c)}$$

Para definir estas operaciones entre clases de equivalencia, en cada caso le hemos asignado la clase de un par ordenado que se obtiene operando las distintas coordenadas de los representantes elegidos en cada clase, lo que nos lleva a la inevitable pregunta: si eligiéramos otros representantes ¿obtendríamos el mismo resultado, o sea, la misma clase?, en otras palabras si:

$(a', b') \propto (a, b) \wedge (c', d') \propto (c, d) \Rightarrow (a + c, \ b + d) \propto (a' + c', \ b' + d') \wedge$

$(a'.c' + b'.d', a'.d' + b'.c') \propto (a.c + b.d, a.d + b.c)$

Veamos la primera, $(a', b') \propto (a, b) \Rightarrow a' + b = a + b'$

$(c', d') \propto (c, d) \Rightarrow c' + d = c + d'$

sumando m.a.m. tenemos $a' + c' + b + d = a + c + b' + d'$

entonces $(a' + c', b' + d') \propto (a + c, b + d)$.

Luego la suma no depende de los representantes elegidos para calcularla.

Para ver que el producto tampoco depende de los representantes, las cuentas no son tan sencillas, pero son realizables.

$(a', b') \propto (a, b) \Rightarrow a' + b = a + b'$ *(1)*

$(c', d') \propto (c, d) \Rightarrow c' + d = c + d'$ *(2)*

Debemos demostrar que $(a'.c' + b'.d', a'.d' + b'.c') \propto (a.c + b.d, a.d + b.c)$, o sea que

$a'.c' + b'.d' + a.d + b.c = a'.d' + b'.c' + a.c + b.d$

multipliquemos m.a.m. *(1)* por d' y *(2)* por a,

entonces $a.d' + b'.d' = a'.d' + b.d'$

$c'.a + d.a = c.a + d'.a$

multipliquemos m.a.m.*(1)* por c' y *(2)* por b,

entonces $a'.c' + b.c' = a.c' + b'.c'$

$c.b + b.d' = b.c' + d.b$

sumando m.a.m. tenemos:

$a.d' + b'.d' + c'.a + d.a + a'.c' + b.c' + c.b + b.d' = a'.d' + b.d' + c.a + d'.a + a.c' +$

$+ b'.c' + b.c' + d.b$

cancelando el término $b.d' + a.d' + c'.a + b.c'$ en ambos miembros de la igualdad, obtenemos la igualdad buscada $a'.c' + b'.d' + a.d + b.c = a'.d' + b'.c' + a.c + b.d$,

lo que significa que $(a'.c' + b'.d', a'.d' + b'.c') \propto (a.c + b.d, a.d + b.c)$.

Luego, las operaciones están *bien definidas.*

Veamos cómo se interpretan estas operaciones en las clases que constituyen el conjunto cociente $\mathbb{N}_0 \times \mathbb{N}_0 / \propto$.

$$\overline{(k,0)} + \overline{(h,0)} = \overline{(k+h,0)} \qquad \overline{(k,0)}.\overline{(h,0)} = \overline{(k.h,0)}$$
$$\overline{(k,0)} + \overline{(0,0)} = \overline{(k,0)}\ , \qquad \overline{(k,0)}.\overline{(0,0)} = \overline{(0,0)}$$
$$\overline{(k,0)} + \overline{(0,h)} = \overline{(k,h)} \qquad \overline{(k,0)}.\overline{(0,h)} = \overline{(0,k.h)}$$
$$\overline{(0,h)} + \overline{(0,0)} = \overline{(0,h)} \qquad \overline{(0,h)}.\overline{(0,0)} = \overline{(0,0)}$$
$$\overline{(0,k)} + \overline{(0,h)} = \overline{(0,k+h)} \qquad \overline{(0,k)}.\overline{(0,h)} = \overline{(k.h,0)}$$

Nótese que si sumamos o multiplicamos dos elementos del conjunto $\left\{\overline{(k,0)}, k \in \mathbb{N}\right\}$, obtenemos otro elemento de ese mismo conjunto; si sumamos dos elementos de $\left\{\overline{(0,h)}, h \in \mathbb{N}\right\}$ obtenemos otro elemento de ese conjunto, mientras que, si multiplicamos dos elementos de $\left\{\overline{(0,h)}, h \in \mathbb{N}\right\}$, obtenemos otro en $\left\{\overline{(k,0)}, k \in \mathbb{N}\right\}$. Multiplicar cualquier elemento por $\overline{(0,0)}$ nos da siempre $\overline{(0,0)}$.

La única situación no claramente definida es $\overline{(k,0)} + \overline{(0,h)} = \overline{(k,h)}$, o sea, sumar un elemento de $\left\{\overline{(k,0)}, k \in \mathbb{N}\right\}$ con uno de $\left\{\overline{(0,h)}, h \in \mathbb{N}\right\}$.

Ya vimos que $\overline{(k,h)} \in \left\{\overline{(k,0)}, k \in \mathbb{N}\right\}$ si y sólo si $k > h$

$\overline{(k,h)} \in \left\{\overline{(0,h)}, h \in \mathbb{N}\right\}$ si y sólo si $k < h$

y que $\overline{(k,h)} = \overline{(0,0)}$ si y sólo si $k = h$

Llamaremos *Conjunto de Números Enteros* al conjunto:

$$\mathbb{Z} = {}^{\mathbb{N}_0 \times \mathbb{N}_0}\!\!\diagup_{\propto} = \left\{ \overline{(k,\,0)} \;/\; k \in \mathbb{N} \right\} \cup \left\{ \overline{(0,\,h)} \;/\; h \in \mathbb{N} \right\} \cup \left\{ \overline{(0,\,0)} \right\}$$

Identificaremos cada $n \in \mathbb{N}_0$ con la clase $\overline{(n,\,0)}$

$$n \to \overline{(n,\,0)}$$

la identificación respeta las operaciones, puesto que $\forall\ n, m \in \mathbb{N}_0$

$$n + m \to \overline{(n+m,\,0)} = \overline{(n,\,0)} + \overline{(m,\,0)}$$
$$n.m \to \overline{(n.m,\,0)} = \overline{(n,\,0)}\,.\,\overline{(m,\,0)}$$

Esto permite *identificar* al conjunto de números naturales, con el subconjunto de $\mathbb{Z}$: $\left\{ \overline{(k,\,0)} \;/\; k \in \mathbb{N} \right\}$, por la cual cada elemento se identifica con un número natural, el 0 con $\left\{ \overline{(0,\,0)} \right\}$, y cada elemento de $\left\{ \overline{(0,\,h)} \;/\; h \in \mathbb{N} \right\}$ se puede pensar como el *inverso aditivo u opuesto de* uno de $\mathbb{N}$, puesto que $\overline{(n,\,0)} + \overline{(0,\,n)} = \overline{(0,\,0)}$.
Llamaremos $-n = \overline{(0,\,n)}$ (inverso aditivo u opuesto de *n*).

De esta manera, considerando que vía la identificación dada:
$\mathbb{N} \leftrightarrow \left\{ \overline{(k,\,0)} \;/\; k \in \mathbb{N} \right\}$, $\mathbb{N}^- \leftrightarrow \left\{ \overline{(0,\,h)} \;/\; h \in \mathbb{N} \right\}$, y $\overline{(0,\,0)} \leftrightarrow 0$
se tiene que:

$$\mathbb{Z} = \mathbb{N} \cup \mathbb{N}^- \cup \{\,0\,\} \text{ (unión disjunta dos a dos)}$$

Gracias a esta identificación $\mathbb{N} \subset \mathbb{Z}$, luego todo número natural *n* es también un número entero.

Ejemplo 2 : *Definir el conjunto* $\mathbb{Q}$ *de números racionales, a partir de* $\mathbb{Z}$ (*conjunto de números enteros*) *y sus operaciones.*

Vamos a definir una relación de equivalencia en $\mathbb{Z} \times \mathbb{Z}^*$, donde $\mathbb{Z}^* = \mathbb{Z} - \{\,0\,\}$.

$$(a,\,b) \prec (c,\,d) \quad \textit{si y sólo si} \quad a.d = b.c$$

Obsérvese que las primeras coordenadas están en $\mathbb{Z}$, luego son enteros cualesquiera, mientras que las segunda están en $\mathbb{Z}^*$, por lo tanto son enteros no nulos.

Ejercicio1: Demostrar que $\prec$ es una relación de equivalencia en $\mathbb{Z} \times \mathbb{Z}^*$.

Las clases de equivalencia $\overline{(a,\,b)}$ se notarán $\dfrac{a}{b}$, o sea $\dfrac{a}{b} = \overline{(a,\,b)}$,
por lo que, merced a la definición de la relación:

$$\frac{a}{b} = \frac{c}{d} \Leftrightarrow a.d = b.c$$

Tenemos, entonces que $\dfrac{a}{b} = \{\,(c,\,d) \;/\; a.d = b.c\,\}$

por lo que $\forall k \in \mathbb{Z}^*$ $(a.k, b.k) \in \frac{a}{b}$, y que si $h \mid a \wedge h \mid b$, $h \in \mathbb{Z}^*$, $\exists\, c, d \in \mathbb{Z}$ tales que

$a = h.c \wedge b = h.d$ entonces $(c, d) \in \frac{a}{b}$.

Por lo tanto en cada clase $\frac{a}{b}$ hay un representante (c, d) con la propiedad de que

$c \wedge d$ no admitan divisores comunes excepto el 1 y el – 1. Podemos además pedir que $d \in \mathbb{N}$ puesto que $(c, d) \prec (-c, -d)$. Este representante, así elegido es *único* pues si $(c, d) \prec (c', d')$, con $d, d' \in \mathbb{N}$, c, d sin divisores comunes excepto el 1 y el – 1, y c' y d' también sin divisores comunes excepto el 1 y el – 1, tendríamos que $c.d' = c'.d$ por lo que podríamos afirmar que $d = d'$ y por consiguiente que $c = c'$ (para una demostración rigurosa de este hecho, remitirse al capítulo de Números Enteros).

Llamaremos *Conjunto de Números Racionales* $\mathbb{Q}$ al conjunto cociente $\mathbb{Z} \times \mathbb{Z}^* \Big/ \prec$

O sea:

$$\mathbb{Q} = \left\{ \frac{a}{b} / a \in \mathbb{Z} \wedge\ b \in \mathbb{N}\ con\ \ a \wedge b\ \ sin\ divisores\ comunes\ excepto\ el\ 1\ y\ el\ -1 \right\}$$

Definiremos suma y producto en $\mathbb{Q}$

$$\frac{a}{b} + \frac{c}{d} = \frac{a.d + b.c}{b.d}$$
$$\frac{a}{b} \cdot \frac{c}{d} = \frac{a.c}{b.d}$$

Nótese que $b.d \neq 0$ pues $b \neq 0 \wedge c \neq 0$

Ejercicio 2: Demostrar que las operaciones están bien definidas (razone como en el ejemplo anterior)

Identificaremos cada $a \in \mathbb{Z}$ con el *número racional* $\frac{a}{1}$

$$a \to \frac{a}{1}$$

Es una identificación pues $(a, 1) \prec (b, 1)$ sii $a.1 = b.1$ sii $a = b$

Luego si $a \neq b$ entonces $(a, 1) \not\prec (b, 1)$ (no están relacionados), luego $\frac{a}{1} \neq \frac{b}{1}$

En particular $0 = \frac{0}{1} \wedge 1 = \frac{1}{1}$ (vía la identificación)

¿Cuándo $\frac{a}{b} = 1$?

$\frac{a}{b} = 1$ sii $\frac{a}{b} = \frac{1}{1}$ sii $(a, b) \prec (1, 1)$ sii $a.1 = b.1$ sii $a = b$

Entonces $\frac{1}{1} = \{ (a, b) / a = b \}$

Además $\frac{a}{b} = 0$ sii $\frac{a}{b} = \frac{0}{1}$ sii $a.1 = b.0$ sii $a.1 = 0$ sii $a = 0$

Entonces $\frac{0}{1} = \{ (0, b) \ / \ b \neq 0 \ \}$

Merced a la identificación efectuada consideramos al conjunto de los enteros $\mathbb{Z}$ como un subconjunto del conjunto de los números racionales $\mathbb{Q}$,

$$\mathbb{Z} \subset \mathbb{Q}$$

Por lo tanto cada número entero *a* es, además, un número racional, puesto que si sumamos o multiplicamos números enteros, pensándolos como racionales, obtenemos los mismos números que si hubiéramos realizado las operaciones en $\mathbb{Z}$.

***Ejercicios*:**

1.- Dados los conjuntos M y D, $G \subset M \times D$ gráfica. En cada uno de los casos siguientes, determinar $Proy_1\ G$ y $Proy_2\ G$:

a) $D = M = \mathbb{N}$; $G = \{ (m, n) \ / \ m+n \text{ es par} \}$

b) $D = M = \mathbb{Z}$; $G = \{ (m, n) \ / \ 2 \text{ divide a } m-n \}$

c) $D = M = \mathbb{N}$; $G = \{ (x, y) / x < y \}$

d) $D = M = \mathbb{R}$; $G = \{ (x, y) / x = y \}$

e) $D = M = \mathbb{Z}$; $G = \{ (x, y) / x \text{ divide a } y \}$

f) $D = M = \mathbb{Z}$; $G = \{ (x, y) / |x-y| \leq 2 \}$

g) $D = M = \mathbb{R}$; $G = \{ (x, y) \ / \ x-y \in \mathbb{Q} \}$

h) $D = M$ es el conjunto de las rectas del plano ; $G = \{ (s, l) \ / \ s \parallel l \}$

i) $M = \{ a, b, c, d \}$; $D = \{ 1, 2, 3, 4, 5 \}$; $G = \{ (a, 2), (a, 4), (b, 4), (d, 5) \}$

j) $M = \{ 1, 2, 3, 4, 5 \}$, $D = \{ 3, 4, 5 \}$; $G = \{ (x, y) \ / \ x+y \leq 5 \}$

2.- En los casos del ejercicio 1. hallar G^{-1}. En cada caso encontrar $Proy_1\ G^{-1}$ y $Proy_2\ G^{-1}$ y verificar que $Proy_1\ G^{-1} = Proy_2\ G \ \wedge \ Proy_1\ G = Proy_2\ G^{-1}$

3.- Dado M y G una gráfica en M, probar o refutar en cada uno de los casos las siguientes afirmaciones:

i) $G \cap G^{-1} = \phi$

ii) $G \cup G^{-1} = M \times M$

iii) $(G^{-1})^{-1} = G$

iv) $G = Proy_1 G \times Proy_2 G$

v) $Proy_i (G_1 \cap G_2) = Proy_i G_1 \cap Proy_i G_2 \quad i = 1,2$

vi) $Proy_i (G_1 \cup G_2) = Proy_i G_1 \cup Proy_i G_2$

4.- Enunciar una condición necesaria y suficiente sobre los $(x, y) \in G \subset M \times M$, para que se verifiquen las siguientes propiedades:

i) $G = G^{-1}$ ii) $Proy_1 G = M$ iii) $Proy_2 G = M$

5.- Dado un conjunto M , G gráfica en M ($G \subset M \times M$). Decir en los siguientes casos si la relación $\Re = (M, G)$ es reflexiva, simétrica , transitiva y/o antisimétrica :

k) $M = \mathbb{N}$; $G = \{ (m, n) \ / \ m+n \text{ es par} \}$

l) $M = \mathbb{Z}$; $G = \{ (m, n) \ / \ 2 \text{ divide a } m-n \}$

m) $M = \mathbb{R}$; $G = \{ (x, y) / x < y \}$

n) $M = \mathbb{R}$; $G = \{ (x, y) / x = y \}$

o) $M = \mathbb{Z}$; $G = \{ (x, y) / x \text{ divide a } y \}$

p) $M = \mathbb{Z}$; $G = \{ (x, y) / |x-y| \leq 2 \}$

q) $M = \mathbb{R}$; $G = \{ (x, y) \ / \ x-y \in \mathbb{Q} \}$

r) $M = D$ el conjunto de las rectas del plano ; $G = \{ (s, l) \ / \ s \parallel l \}$

6.- En cada uno de los casos del ejercicio 5. encontrar $\Re^{-1}$ y decir qué propiedades verifica.

7.- Sea $\Re = (M, G)$, $G \subset M \times M$, una relación; probar o refutar las siguientes afirmaciones:

i) $\Re$ es reflexiva $\Rightarrow$ $\Re^{-1}$ es reflexiva
ii) $\Re$ es simétrica $\Rightarrow$ $\Re^{-1}$ es simétrica
iii) $\Re$ es antisimétrica $\Rightarrow$ $\Re^{-1}$ es antisimétrica
iv) $\Re$ es transitiva $\Rightarrow$ $\Re^{-1}$ es transitiva
v) $\Re$ es simétrica $\Rightarrow$ $\Re$ no es antisimétrica
vi) $\Re$ es simétrica y antisimétrica $\Rightarrow$ $\Re$ es la relación de igualdad
vii) $\Re$ es simétrica y antisimétrica $\Rightarrow$ $G = \phi$
viii) $\Re$ simétrica y antisimétrica $\Leftrightarrow$ $G = \phi \vee \Re$ es la igualdad

8.- Dados los siguientes conjuntos M y las relaciones $\approx$, probar que $\approx$ es relación de equivalencia; para cada $a \in M$ describir $\overline{a}$, la clase de equivalencia de a, y hallar un conjunto de representantes (es decir describir el conjunto cociente de $M/_{\approx}$).

a) $M = \mathbb{Z}$; $n \approx m \Leftrightarrow m - n$ es par
b) $M = \mathbb{R}$; $x \approx y \Leftrightarrow x = y$
c) $M = \mathbb{R}$; $x \approx y \Leftrightarrow |x| = |y|$
d) $M = \mathbb{R}^2$; $(x, y) \approx (z, t) \Leftrightarrow x = z$
e) $M = \mathbb{R}$; $x \approx y \Leftrightarrow (\exists\, \lambda \neq 0$ tal que $y = \lambda x)$
f) $n \in \mathbb{N}$, $M = \mathbb{Z}$, $a \approx b\ (mód\ n) \Leftrightarrow a - b = kn$ para algún $k \in \mathbb{Z}$
g) $M = \mathbb{N} \times \mathbb{N}$, $(a, b) \approx (c, d) \Leftrightarrow a + d = b + c$
h) $M = \mathbb{Z} \times \mathbb{Z}^*$, $\mathbb{Z}^* = \mathbb{Z} - \{0\}$, $(a, b), (c, d) \in \mathbb{Z} \times \mathbb{Z}^*$, $(a, b) \approx (c, d) \Leftrightarrow a \cdot d = b \cdot c$
i) $M = \mathbb{R}$; $x \approx y \Leftrightarrow x - y \in \mathbb{Z}$

9.- Demostrar que las siguientes relaciones en el conjunto dado son de orden e indicar cuáles son órdenes totales y cuáles parciales:
i) $U \neq \phi$, $R = \mathcal{P}(U)$, $A \leq B \Leftrightarrow A \subset B$
ii) $R = \mathbb{N}$, $x \leq y \Leftrightarrow x$ divide a y
iii) $R = \mathbb{N} \times \mathbb{N}$, $(a, b) \leq (c, d) \Leftrightarrow a < c \vee (si\ a = c \Rightarrow b \leq d)$
iv) $R = \mathbb{Z} \times \mathbb{Z}$, $(a, b) \leq (c, d) \Leftrightarrow a \leq c \wedge b \leq d$
v) $R = \mathbb{N} \times \mathbb{N}$, $(a, b) \leq (c, d) \Leftrightarrow a = c \wedge b \leq d$.
vi) $R = \{1, 2\}$, $G = \{(1, 1), (1, 2), (2, 2)\}$
vii) $R = \{a, b, c\}$, $G = \{(a, a), (b, b), (c, c), (a, b), (a, c), (b, c)\}$
viii) $R = \{2, 3, 6, 9, 12, 36\}$, $a \leq b \Leftrightarrow a$ divide a b
ix) $R = \{\phi, \{a\}, \{a, b\}, \{a, b, c\}\}$, $X \prec Y \Leftrightarrow X \subset Y$

10.- Sea $X = \{ a , b \}$

i) $G_1 = \{ (a, a), (b, b) \}$
Verificar que G_1 es la gráfica de una relación de orden. Hallar elementos maximales y minimales en X.

ii) Idem i) con $G_2 = \{(a, a), (b, b), (a, b)\}$.

11.- Sean $A = (0, 2)$, $B = (-3, ½)$, $C = \left\{ \frac{1}{n} \ / \quad n \in \mathbb{N} \right\}$, subconjuntos del conjunto ordenado $(\mathbb{R}, \leq)$

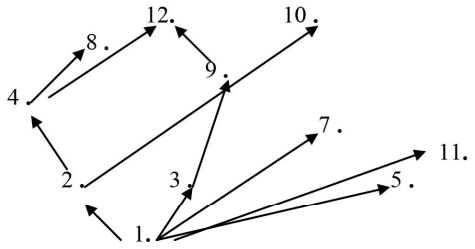
i) Hallar cotas superiores e inferiores, si las hubiere de A, B y C
ii) Hallar elementos maximales y minimales de A, B y C
iii) Hallar supremos e ínfimos, máximos y mínimos de los conjuntos dados si los hubiere.

12.- Sea $A = \{1, 2, 3, ….., 20\}$, y la relación : $a \leq b \Leftrightarrow a$ divide a b

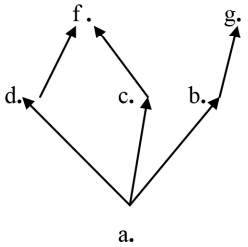
i) Encontrar cotas superiores e inferiores, máximos y mínimos, ínfimos y supremos, cuando los hubiere, para los subconjuntos:
$B = \{ 2, 4, 6, 8, 10, 12, 14, 16, 18, 20 \}$
$C = \{1, 3, 5, 6, 7, 8, 10, 11, 12 \}$
$D = \{ 2, 3, 4, 6, 8, 9, 15, 16, 18, 19, 20 \}$
ii) Encontrar los elementos maximales y minimales de A ¿Tiene máximo y/o mínimo?

13.- Dadas las relaciones de órdenes representadas en los diagramas (Aclaración: en todos los diagramas, cada elemento está relacionado con sí mismo. No se dibujaron los lazos para no sobrecargar el dibujo).

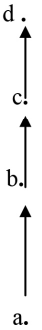
a)



b)



c)



i) Encontrar maximales y minimales, máximos y mínimos, si los hubiere, del conjunto total.

ii) Hallar cuando corresponda, maximales, minimales, cotas inferiores y superiores, supremos, ínfimos, máximos y mínimos de:

ii-1) {1, 2, 3, 7, 11}
ii-2) {*a, b*}
ii-3) {2, 4, 8, 9, 10}
ii-4) {*a, c, d, e*}
ii-5) {5, 7, 8, 10, 11, 12}
ii-6) {*a, c, d, f* }

14.-

i) Sea E un conjunto, $(\mathcal{P}(E), \subset)$. Encontrar máximos y/o mínimos si los hubiere.

ii) Sea $A \subset \mathcal{P}(E)$, $A \neq \phi$. Describir las cotas superiores e inferiores de A si las tuviere. Encontrar el ínfimo y el supremo. ¿Tiene A máximo y/o mínimo?

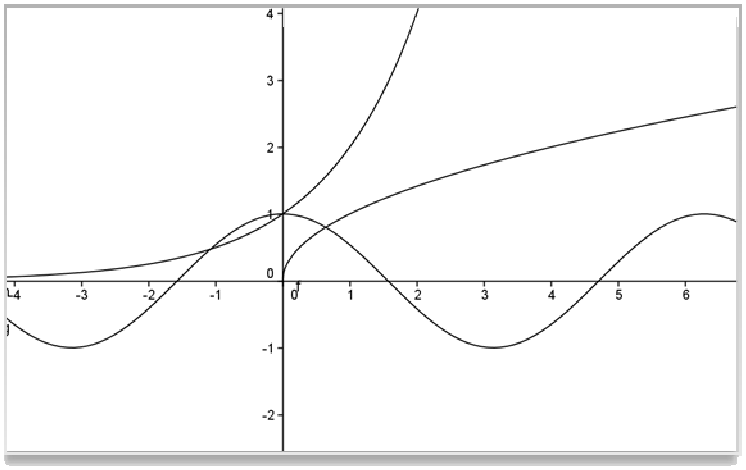
15.- Demostrar que si $(A, \leq)$ es un conjunto bien ordenado, $A \neq \phi$, entonces $(A, \leq)$ es totalmente ordenado.

TERCERA PARTE:

FUNCIONES

Los escolásticos del siglo XIV no conocieron la noción de función en el sentido de la matemática moderna, pero estaban familiarizados con la idea de la dependencia funcional.
Tomás Bradwardine (1290-1349) investigó en su Tractatus proportiorum, de 1328 la regla matemática (o ecuación funcional) que determina la dependencia entre la fuerza de resistencia y la velocidad de un cuerpo en movimiento. Nicole Oresme (1323-1382), a quien se le atribuye la primera aproximación al concepto de función al describir las leyes de la naturaleza como relaciones de dependencia entre dos magnitudes, fue el primero en hacer uso sistemático de diagramas para representar magnitudes variables en un plano.
Podemos, pues, concluir que durante el siglo XIV tuvieron lugar en este respecto investigaciones que en muchos casos no prosiguieron, detenidas por la retórica renacentista.
En la revolución científica iniciada en el siglo XVI los científicos centraron su atención en los fenómenos de la naturaleza, poniendo énfasis en las relaciones entre las variables que determinaban dichos fenómenos y que podían ser expresadas en términos matemáticos. Era necesario comparar las variables, relacionarlas, expresarlas mediante números y representarlas en algún sistema geométrico adecuado.
Los estudios de Galileo Galilei (1564-1642) sobre el movimiento contienen la clara comprensión de una relación entre variables.
La noción propiamente moderna de función (matemática) comienza en el siglo XVII a finales del cual aparece por primera vez el término función. En 1693 y en 1694 Jacob Bernoulli (1654-1705) y Leibniz aplicaron explícitamente la noción de función a expresiones matemáticas; Leibniz parece haber sido, además, el primero que usó el vocablo 'función' en tales contextos. En palabras de Johann Bernoulli, una función es "una cantidad formada de alguna manera a partir de cantidades indeterminadas y constantes".
La notación 'f (x)' fue usada por Leonhard Euler en 1734 quien en su libro "Introducción al análisis infinito" definió función como:

> *"Una función de una cantidad variable es una expresión analítica compuesta de cualquier manera a partir de la cantidad variable y de números o cantidades constantes."*



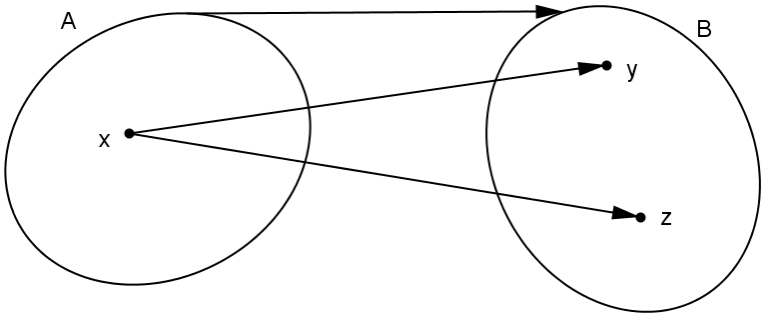
Estudiaremos un tipo particular de relaciones $\Re = (A, B, G)$, en las cuales *A* puede ser distinto de *B* o no, pero *G* es una gráfica con propiedades especiales.

***Definición*:** Sea *G* una gráfica en $A \times B$, diremos que *G es una gráfica funcional* si:

$$(x, y) \in G \wedge (x, y') \in G \Rightarrow y = y'$$

Esto es equivalente a: $(x, y) \in G \wedge (x', y') \in G, \quad y \neq y' \Rightarrow x \neq x'$

Si entendemos que $x \Re y$, o sea $(x, y) \in G$, se representa en el diagrama de Venn con la flecha $x \rightarrow y$, lo que dice la definición de gráfica funcional es que **no** puede ocurrir que algún *x* esté relacionado con dos elementos distintos, o sea, *que salgan dos flechas de un x,* como se muestra en el siguiente dibujo:



Ejemplos: En $\mathbb{R} \times \mathbb{R}$

1) $G = \{(x, y) / \ y = x^2 \ \}$ es una gráfica funcional
2) $F = \{(x, y) / \ y^2 = x \}$ **no** es una gráfica funcional pues $(1, 1) \in F$, $(1, -1) \in F$, y $1 \neq -1$
3) $H = \{(x, y) / \ x \cdot y = 1 \}$ es una gráfica funcional
4) $T = \{(x, y) / \ x = \cos y \}$ **no** es una gráfica funcional pues $\cos 0 = \cos 2\pi = 1$
   luego $(1, 0), \ (1, \ 2\pi) \in T$

***Definición*:** Una relación $\mathcal{F} = (A, B, F)$ se denomina *función o aplicación de A en B* si:

i) $Dom\mathcal{F} = Proy_1 F = A$ (*Dom*$\mathcal{F}$ se lee *dominio de* $\mathcal{F}$)
ii) F es gráfica funcional

Ejemplos: en los ejemplos anteriores

1) $\mathcal{G} = (\mathbb{R} , \mathbb{R} , G)$ es función puesto que *G* es gráfica funcional y $Dom\mathcal{G} = \mathbb{R}$

2) $\mathcal{F} = (\mathbb{R} , \mathbb{R} , F)$ **no** es función porque *F* no es gráfica funcional y $Dom\mathcal{F} = \mathbb{R}_{\geq 0}$, donde $\mathbb{R}_{\geq 0} = \{ x \in \mathbb{R} \ / \ x \geq 0 \} \neq \mathbb{R}$.

3) $\mathcal{H} = (\mathbb{R} , \mathbb{R} , H)$ **no** es función puesto que $Dom\mathcal{H} = \mathbb{R} - \{ 0 \} \neq \mathbb{R}$.

4) $\mathcal{T} = (\mathbb{R} , \mathbb{R} , T)$ **no** es función pues la gráfica no es funcional y $Dom\mathcal{T} = [-1, \ 1] \neq \mathbb{R}$

5) $\mathcal{H}_1 = (\mathbb{R}-\{0\},\ \mathbb{R},\ H)$ es función.

6) $\mathcal{F}_1 = (\mathbb{R}_{\geq 0},\ \mathbb{R}_{\geq 0},\ F_1)$ es función , donde $F_1 = F \cap (\mathbb{R}_{\geq 0} \times \mathbb{R}_{\geq 0})$

7) $\mathcal{T}_1 = ([-1,\ 1],\ [0,\ \pi],\ T_1)$ es función , donde $T_1 = T \cap \times \left([-1,1]\times[0,\ \pi]\right)$

Notación: Si tenemos una función $\mathcal{F} = (A, B, F)$, llamaremos *correspondiente o imagen de* $x \in A$ por la función $\mathcal{F}$ al elemento $y \in B$ tal que $(x, y) \in F$, y lo notaremos $y = \mathcal{F}(x)$.
Nótese que la expresión no genera ambigüedades dado que cada $x \in A$ admite un **único** correspondiente $y \in B$.

Notaremos a las funciones, en general, con letras minúsculas: *f, g, h, j, t,* etc., en vez de mayúsculas como las otras relaciones, y como todos los elementos del conjunto de partida tienen su correspondiente *imagen*, y ésta es única, la forma de definir una función será explicitando su dominio, su codominio o conjunto de llegada, y la imagen por la función de cada uno de los elementos del dominio.

Ejemplos:

1) $g : \mathbb{R} \to \mathbb{R}$
$g(x) = x^2$

2) $h_1 : \mathbb{R}-\{0\} \to \mathbb{R}$

$$h_1(x) = \frac{1}{x}$$

3) $f_1 : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$
$f_1(x) = \sqrt{x}$

4) $t_1 : [-1,\ 1] \to [0,\ \pi]$
$t_1(x) = arc.cos.(x)$

***Igualdad de funciones*:** Sean $f = (A, B, F)$, $g = (C, D, G)$ dos funciones
$f = g$ si y sólo si $(A, B, F) = (C, D, G)$ si y sólo si $A = C$, $B = D \wedge F = G$; luego dos funciones son *iguales* si y sólo si tienen el mismo dominio, el mismo codominio y valen igual en cada uno de los elementos del dominio, o sea:

$f : A \to B$, $g : A \to B$,

$$f = g \quad \textit{si y sólo si} \quad f(x) = g(x)\ \forall x \in A$$

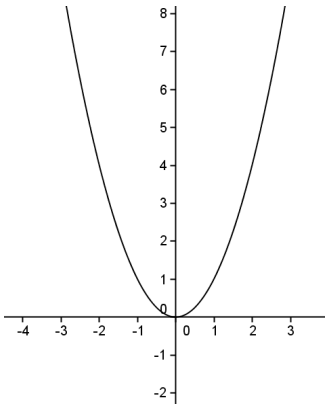
Por lo tanto $f \neq g$ *si y sólo si* $\exists x \in A$ tal que $f(x) \neq g(x)$

Representación Gráfica

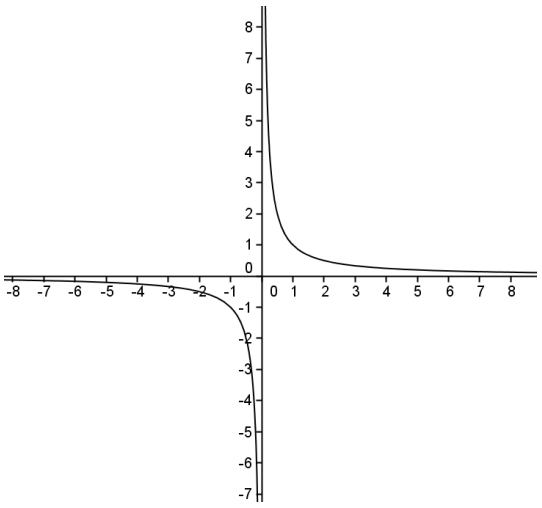
Las funciones suelen representarse gráficamente en un sistema de ejes cartesianos, especialmente cuando tienen dominio y codominio en $\mathbb{R}$ (funciones *reales*) o en algún subconjunto de $\mathbb{R}$. El dominio se representa en el eje horizontal o de las *abscisas*, y el codominio en el eje vertical o de las *ordenadas.*

Ejemplos: En los ejemplos anteriores

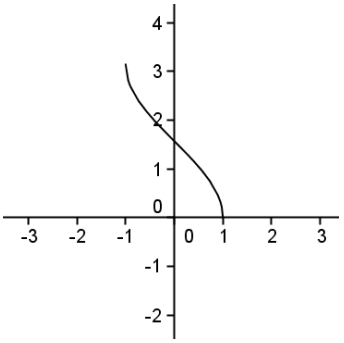
1) $g: \mathbb{R} \rightarrow \mathbb{R}$
$g(x) = x^2$



2) $h_1 : \mathbb{R} - \{0\} \rightarrow \mathbb{R}$
$h_1(x) = \frac{1}{x}$



3) $t_1 : [-1,\ 1] \rightarrow [0,\ \pi]$
$t_1(x) = arc.cos\ (x)$



También pueden representarse en Diagramas de Venn, pero sólo se los utiliza para funciones sobre conjuntos finitos, y de pocos elementos, o bien funciones genéricas, en las cuales se desee resaltar alguna propiedad en especial, como lo hicimos cuando dimos la definición.

Daremos otros ejemplos importantes de funciones:

Ejemplos:

1) Para A conjunto cualquiera, la aplicación *identidad en A* ,

$$id._A : A \to A, \text{ tal que } id_A(x) = x \ \forall x \in A.$$

2) Si $A' \subset A$, la aplicación *inclusión*, $i : A' \to A$, $i(x) = x$, $\forall x \in A'$.

3) $\varphi : \mathbb{Z} \to \mathbb{Z}_n$, tal que $\varphi(a) = \overline{a}$, $\forall a \in \mathbb{Z}$, donde $\overline{a}$ es la clase de equivalencia de a (*mód n*). φ se denomina *proyección canónica al cociente* $\mathbb{Z}_n$.

4) En general, si A es un conjunto, $\approx$ una relación de equivalencia en A, y $A/_{\approx}$ su conjunto cociente, la aplicación $\varphi : A \to A/_{\approx}$, tal que $\varphi(a) = \overline{a}$, $\forall a \in A$, también se denomina *proyección canónica al cociente.*

5) En $\mathbb{N}_0 \times \mathbb{N}_0$ **,** como aplicación de la relación de equivalencia en el capítulo anterior, definimos la relación $\propto$. La aplicación :

$$j : \mathbb{N}_0 \to \mathbb{N}_0 \times \mathbb{N}_0 /_{\propto}, \quad \text{tal que} \quad j(n) = \overline{(n, 0)}$$

Es una *inmersión* de $\mathbb{N}_0$ en el cociente $\mathbb{N}_0 \times \mathbb{N}_0 /_{\propto}$, pues

$j(n + m) = j(n) + j(m)$
y $j(n.m) = j(n) \,.\, j(m)$

6) Análogamente para la relación $\prec$ definida en las aplicaciones del capítulo anterior en $\mathbb{Z} \times \mathbb{Z}^* /_{\prec}$ la aplicación $h : \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}^* /_{\prec}$ tal que $h(a) = \frac{a}{1}$ es una *inmersión* de $\mathbb{Z}$ en $\mathbb{Z} \times \mathbb{Z}^* /_{\prec}$ dado que

$$h(a + b) = h(a) + h(b)$$
$$h(a.b) = h(a) \,.\, h(b)$$

Imagen y preimagen de conjuntos por una función

***Definiciones*:** Sean $f : A \to B$ una función , $A' \subset A$ y $B' \subset B$.

Llamaremos *imagen por f de A´* , al conjunto: $f(A') = \{ f(x) / x \in A' \}$
Llamaremos *preimagen por f de B´* , al conjunto:

$$f^{-1}(B') = \{ x \in A / \exists y \in B' \text{ tal que } y = f(x) \}$$

En particular, *la imagen* de f es $Im(f) = f(A)$, o sea

$$Im(f) = \{ f(x)) / x \in A \} = \{ y \in B / \exists x \in A \text{ tal que } y = f(x) \}$$

***Definición*:** Sean $f : A \to B$ una función, $b \in B$. Llamamos *preimagen de* b *por* f al ***subconjunto de A*:** $f^{-1}(b) = \{ x \in A / f(x) = b \}$

Nótese que $f^{-1}(b) = f^{-1}(\{b\})$, y a diferencia de la imagen de un $x \in A$ que siempre es un elemento, por definición de función, la preimagen de un elemento en general **no** es un elemento, es un conjunto, que puede tener uno, varios o ningún elemento.

Ejemplos:

1) $g: \mathbb{R} \to \mathbb{R}$, $g(x) = x^2$

$A_1 = [-1, 1]$, $B_1 = [-1, 2]$, $A_2 = [0, 1]$, $B_2 = [1, 4]$

$C = \left[\frac{1}{2}, 5\right]$, $D = [-3, 0]$, $E = (-4, -1)$

En este caso todos los conjuntos son subconjuntos tanto del dominio cuanto del codominio, así que podremos calcular imagen y preimagen de todos ellos.

Imágenes:

$g([-1, 1]) = [0, 1]$, $g([-1, 2]) = [0, 4]$, $g([0, 1]) = [0, 1]$,

$g([1, 4]) = [1, 16]$, $g\left(\left[\frac{1}{2}, 5\right]\right) = \left[\frac{1}{4}, 25\right]$, $g([-3, 0]) = [0, 9]$, $g((-4, -1)) = (1, 16)$

$Im(g) = \mathbb{R}_{\geq 0}$

Preimágenes:

$g^{-1}([-1, 1]) = [-1, 1]$, $g^{-1}([-1, 2]) = \left[-\sqrt{2}, \sqrt{2}\right]$,

$g^{-1}([0, 1]) = [-1, 1]$, $g^{-1}([1, 4]) = [-2, -1] \cup [1, 2]$,

$g^{-1}\left(\left[\frac{1}{2}, 5\right]\right) = \left[-\sqrt{5}, -\frac{\sqrt{2}}{2}\right] \cup \left[\frac{\sqrt{2}}{2}, \sqrt{5}\right]$

Las imágenes de conjuntos no vacíos son siempre conjuntos no vacíos, porque el dominio de la función es todo el conjunto de partida, luego todo elemento tiene su correspondiente imagen; no así la preimagen, conjuntos no vacíos pueden tener preimágenes vacías.
Conjuntos distintos pueden tener la misma imagen:
$g([0, 1]) = [0, 1]$, $g([-1, 1]) = [0, 1]$

Para pensar: ¿Pueden dos conjuntos distintos tener la misma preimagen?

2) $h_1: \mathbb{R} - \{0\} \to \mathbb{R}$

$h_1(x) = \frac{1}{x}$

$$A = [-2, 0)\ , A_1 = (0, 1]\ , A_2 = \left(-\frac{1}{3},\ \frac{5}{4}\right) - \{0\}\ , A_3 = [-6,\ -1]$$

$$h_1([-2, 0)) = \left(-\infty,\ -\frac{1}{2}\right] = \{x \in \mathbb{R}\ / x \le -\frac{1}{2}\ \}$$

$$h_1((0,\ 1]) = [1,\ \infty) = \{x \in \mathbb{R}\ / x \ge 1\ \}$$

$$h_1\left(\left(-\frac{1}{3},\ \frac{5}{4}\right) - \{0\}\right) = (-\infty, -3) \cup \left(\frac{4}{5},\ \infty\right)$$

$$h_1([-6,\ -1]) = \left[-1,\ -\frac{1}{6}\right] \qquad h_1^{-1}([-2, 0)) = \left(-\infty,\ -\frac{1}{2}\right]$$

$$h_1^{-1}((0,\ 1]) = [1,\ \infty) \qquad h_1^{-1}([-6,\ -1]) = \left[-1,\ -\frac{1}{6}\right]$$

$$h_1^{-1}\left(\left(-\frac{1}{3},\ \frac{5}{4}\right) - \{0\}\right) = (-\infty, -3) \cup \left(\frac{4}{5},\ \infty\right)$$

$$Im(h_1) = \mathbb{R} - \{0\}$$

Ejemplo: Para la función *g* dada antes,
$g^{-1}(0) = \{0\}$, $g^{-1}(1) = \{-1,\ 1\}$, $g^{-1}(-1) = \phi$.

En los casos en que la preimagen de un elemento sea un conjunto unitario, como en este primer ejemplo, puede usarse la notación: $g^{-1}(0) = 0$

***Proposición*:** Sea $f : A \to B$ una función; X, X' subconjuntos de A ; Y, Y' subconjuntos de B. Entonces:

i) $X \subset X' \Rightarrow f(X) \subset f(X')$. En particular $f(X) \subset Im(f),\ \forall X \subset A$

ii) $Y \subset Y' \Rightarrow f^{-1}(Y) \subset f^{-1}(Y')$. En particular $f^{-1}(b) \subset f^{-1}(Y),\ \forall b \in Y$

***Demostración*:**

i) Sea $y \in f(X)$, entonces $\exists x \in X$ tal que $f(x) = y$.
Como $X \subset X', x \in X \Rightarrow x \in X'$, luego $f(x) = y \in f(X')$,
Y así $f(X) \subset f(X')$.
Claramente si $X \subset A$, entonces $f(X) \subset f(A) = Im(f)$.

ii) Sea $x \in f^{-1}(Y)$, entonces $f(x) \in Y$.
Como $Y \subset Y'$, $f(x) \in Y \Rightarrow f(x) \in Y'$,
luego $x \in f^{-1}(Y')$, y así $f^{-1}(Y) \subset f^{-1}(Y')$.
Es inmediato ver que si $b \in Y$ entonces $\{b\} \subset Y$,

luego $f^{-1}(b) \subset f^{-1}(Y)$.

Ejercicio: Demostrar que $f^{-1}(b) \neq \phi$ *sii* $b \in Im(f)$.

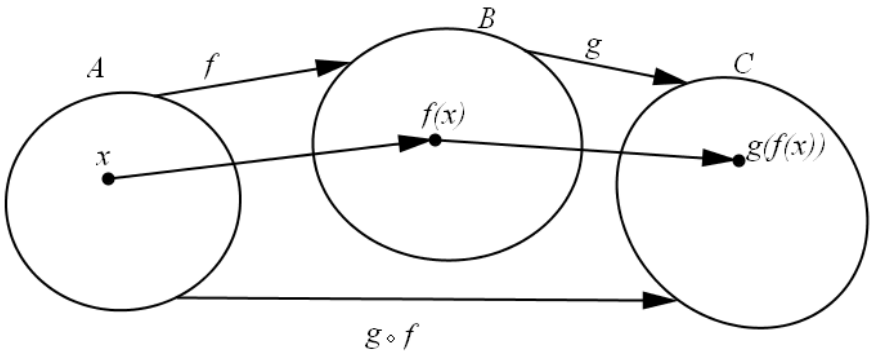
***Para pensar*:** ¿Es posible establecer, en general, una relación de inclusión entre estos dos conjuntos: X y $f^{-1}(f(X))$?

¿Y entre estos dos: Y y $f(f^{-1}(Y))$? Justificar.

Composición de funciones

***Definición*:** Sean $f: A \to B$, $g: B \to C$ dos funciones.
Llamamos *f compuesta con g* a la función:

$g \circ f: A \to C$, definida por $(g \circ f)(x) = g(f(x))$



El orden en que se escribe $g \circ f$ (f compuesta con g) es de derecha a izquierda, a la inversa de nuestra escritura corriente, y es para facilitar la interpretación de que primero se aplica f y luego g: $g(f(x))$
Esta "operación" entre funciones en general no es tal porque para poder definirla es *necesario y suficiente* que el codominio de la primera coincida con el dominio de la segunda, lo que significa que pudiendo definir $g \circ f$ podría no poder hacerlo con $f \circ g$, lo que descarta la idea de *conmutatividad* en la composición de funciones.
Aun en los casos en que podamos realizar ambas composiciones, $g \circ f$ y $f \circ g$, en general no coinciden. Por ejemplo:

$$f: \mathbb{R} \to \mathbb{R}\ , f(x) = x^2 + 1\ , g: \mathbb{R} \to \mathbb{R}\ , g(x) = 3x - 4$$

$$g \circ f: \mathbb{R} \to \mathbb{R}\ , (g \circ f)(x) = 3(x^2 + 1) - 4 = 3x^2 - 1$$

$$f \circ g: \mathbb{R} \to \mathbb{R}\ , (f \circ g)(x) = (3x - 4)^2 + 1 = 9x^2 - 24x + 17$$

$$f \circ g \neq g \circ f \quad \text{pues} \quad 17 = (f \circ g)(0) \neq (g \circ f)(0) = -1$$

Propiedades de la composición

Ya vimos que la composición no es conmutativa.

1) Pero sí es **asociativa** (para aquellos casos que pueda definirse)**:**

$h \circ (g \circ f) = (h \circ g) \circ f$, donde $f: A \to B$, $g: B \to C$, $h: C \to D$

Nótese que $g \circ f : A \to C$ por lo que se puede componer con h , y que $h \circ g : B \to D$, luego f se puede componer con ella, con lo cual no tenemos contradicciones en nuestro enunciado; sólo resta demostrar la igualdad entre esas dos funciones.

***Demostración*:** $h \circ (g \circ f) = (h \circ g) \circ f \Leftrightarrow (h \circ (g \circ f))(x) = ((h \circ g) \circ f)(x) \quad \forall x \in A$

Sea $x \in A \quad (h \circ (g \circ f))(x) = h((g \circ f)(x))$, $\quad (g \circ f)(x) = g(f(x))$

entonces $\quad h((g \circ f)(x)) = h(g(f(x)))$

por definición de composición $\quad ((h \circ g) \circ f)(x) = (h \circ g)(f(x)) = h(g(f(x)))$

luego $\quad (h \circ (g \circ f))(x) = ((h \circ g) \circ f)(x)$, y esto es $\forall x \in A$

entonces $\quad h \circ (g \circ f) = (h \circ g) \circ f$

2) Sea $f : A \to B$ una función. Entonces:

i) $id_B \circ f = f$

ii) $f \circ id_A = f$

***Demostración*:**

i) $id_B \circ f = f \Leftrightarrow (id_B \circ f)(x) = f(x) \ \forall x \in A$

Sea $x \in A$, $(id_B \circ f)(x) = id_B (f(x)) = f(x)$ pues $id_B : B \to B$, $id_B (y) = y \ \forall y \in B \wedge f(x) \in B$.

Luego $(id_B \circ f)(x) = f(x) \ \forall x \in A$, por lo tanto $\quad id_B \circ f = f$

ii) $f \circ id_A = f \Leftrightarrow (f \circ id_A)(x) = f(x) \ \forall x \in A$

Dejamos esta demostración al lector.

Nota: La propiedad nos dice que una función compuesta a izquierda o a derecha por la *función identidad* no altera la función dada, pero hay que observar que, de acuerdo a que sea en un sentido o en el otro, las funciones identidad deben ser las adecuadas para que la composición pueda efectuarse, y por más que a ambas las llamemos *función identidad*, en general no son la misma función porque no coinciden ni dominio, ni codominio, ni gráfica.
Si $f : A \to A$, entonces tendremos que:

$$id_A \circ f = f \circ id_A = f, \quad \text{y esto es} \quad \forall f, \quad \text{tal que} \quad f : A \to A$$

En este caso diremos que id_A es un *elemento neutro* para la composición de funciones de A en A

Funciones inyectivas, suryectivas y biyectivas

***Definiciones*:** Sea $f : A \to B$ una función.

- Diremos que f es *inyectiva* si dos elementos distintos del dominio tienen imágenes distintas: $x \neq x' \Rightarrow f(x) \neq f(x')$, donde $x, x' \in A$

o lo que es equivalente, si las imágenes de dos elementos coinciden, es porque los elementos son iguales: $f(x) = f(x') \Rightarrow x = x'$

Luego f **no** es inyectiva si $\exists\, x, x' \in A$, $x \neq x'$ tales que $f(x) = f(x')$

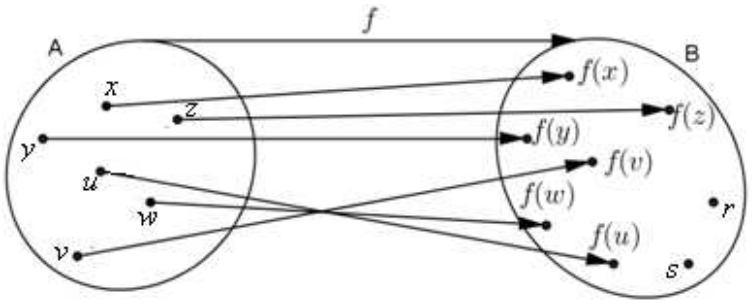
- Diremos que f es *suryectiva o sobreyectiva*, si $Im(f) = B$, o sea, si todos los elementos de B admiten una preimagen: $\forall\, y \in B\ \exists\, x \in A$ tal que $f(x) = y$

Luego f **no** es suryectiva si $Im(f) \neq B$, o sea si $\exists\ y \in B$ tal que $y \notin Im(f)$

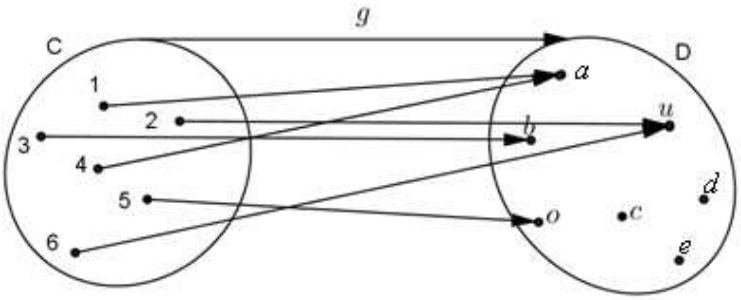
Nota: siempre $Im(f) \subset B$

- Diremos que f es biyectiva si es inyectiva y suryectiva, o sea: $\forall\ y \in B\ \ \exists!\, x \in A$ (*existe un único x perteneciente a A*), tal que $f(x) = y$

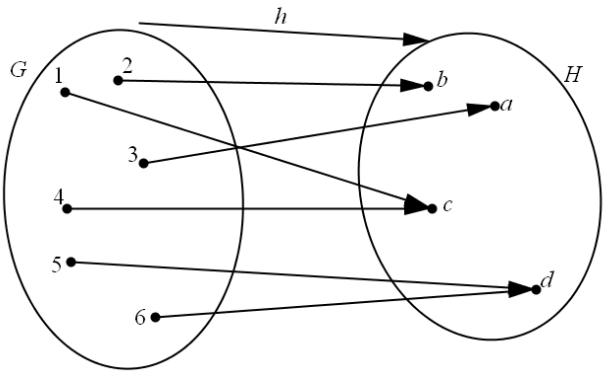
Representaremos en Diagramas de Venn estas definiciones:



El diagrama representa una función **inyectiva**, pero no suryectiva, ya que $s \notin Im(f)$ y $r \notin Im(f)$.

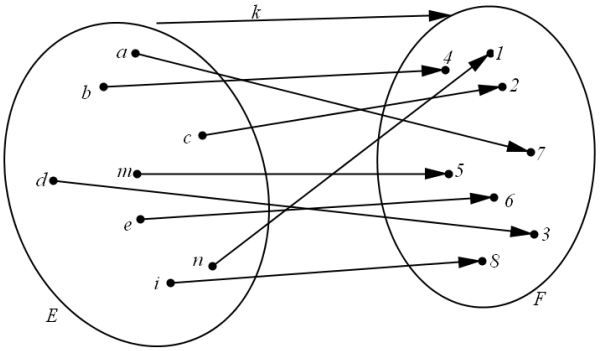


Este otro diagrama representa una función *g* que no es inyectiva, pues
$g(1) = g(4) = a$, $g(2) = g(6) = u$, ni tampoco suryectiva pues $e, c, d \notin Im(g)$



La función *h* aquí representada es **suryectiva**, pero no inyectiva, ya que

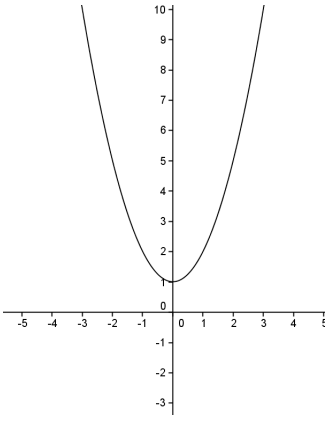
$h(1) = h(4) = c \wedge h(5) = h(6) = d$



En este diagrama *k* representa una función **biyectiva.**
El diagrama de Venn "grafica" de una manera bastante clara los conceptos de funciones inyectivas, suryectivas y biyectivas: cuando la función es *inyectiva* a cada uno de los elementos del codominio le llega, ***cuanto más***, una flecha; cuando es *suryectiva* le llega ***al menos*** una flecha, y cuando es *biyectiva*, a cada uno de los elementos del codominio le llega ***exactamente*** una flecha.

Ejemplos:

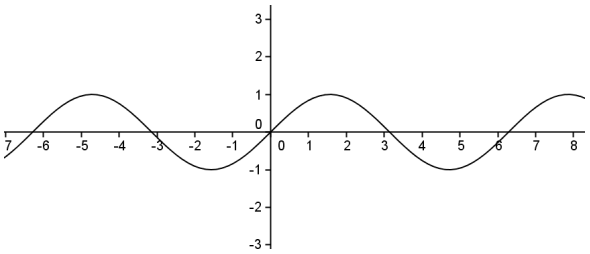
1) $f : \mathbb{R} \rightarrow \mathbb{R}$
$f(x) = x^2 + 1$



f no es inyectiva pues $f(1) = f(-1) = 2$

f no es suryectiva pues $0 \notin Im(f)$
$Im(f) = [1, \infty) \subsetneq \mathbb{R}$

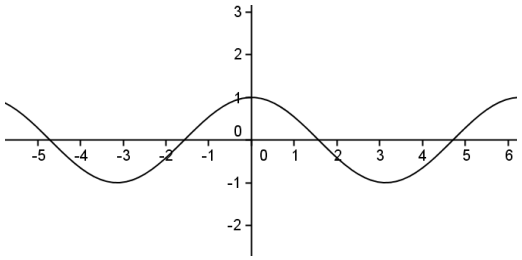
2) $g : \mathbb{R} \rightarrow \mathbb{R}$
$g(x) = sen\,(x)$



g tampoco es inyectiva pues
$g(0) = g(\pi)$,
ni suryectiva pues $2 \notin Im(g)$.

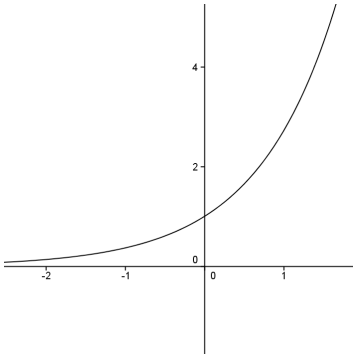
$Im(g) = [-1,\ 1] \subsetneq \mathbb{R}$

3) $h : \mathbb{R} \rightarrow [-1,\ 1]$
$h(x) = cos(x)$



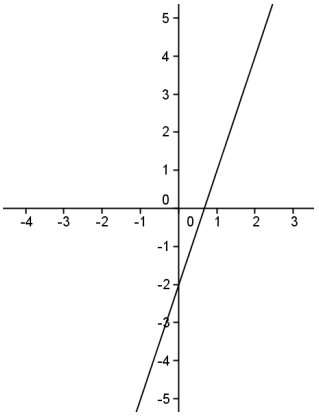
h es suryectiva, pero no inyectiva :
$h(0) = h(2\pi)$.

4) $t : \mathbb{R} \rightarrow \mathbb{R}$
$t(x) = e^x$



t es inyectiva y no suryectiva pues
$Im(t) = \mathbb{R}_{>0} \subsetneq \mathbb{R}$

5) $j : \mathbb{R} \rightarrow \mathbb{R}$
$j(x) = 3x - 2$



j es biyectiva. Vamos a demostrarlo:

Para ver que es inyectiva, debemos probar que:
$x \neq x' \Rightarrow j(x) \neq j(x')$
o lo que es equivalente:
$j(x) = j(x') \Rightarrow x = x'$.

Si $j(x) = j(x')$ entonces $3x - 2 = 3x' - 2$,
sumando 2 m.a.m. obtenemos $3x = 3x'$
multiplicando por $\frac{1}{3}$ m.a.m. tenemos que $x = x'$, que es lo que queríamos demostrar. Luego *j* es inyectiva.

Veamos que es suryectiva. Para demostrarlo debemos ver que cualquiera sea el elemento *y* en el codominio, en este caso $\mathbb{R}$, hay un elemento en el dominio, también en este caso $\mathbb{R}$, cuya imagen por *j* es *y*.

Sea $x = \frac{y+2}{3}$, $j(x) = j(\frac{y+2}{3}) = 3(\frac{y+2}{3}) - 2 = (y+2) - 2 = y$,

entonces $y \in Im(j)$, y esto es $\forall y \in \mathbb{R}$, luego j es suryectiva.

Por ser j suryectiva e inyectiva es **biyectiva.**

6) Para A conjunto cualquiera, la aplicación *identidad en A*, $id_A : A \to A$, tal que $id_A(x) = x$ $\forall x \in A$, *es biyectiva.*

7) Si $A' \subset A$, la aplicación *inclusión*, $i : A' \to A$, $i(x) = x$ $\forall x \in A'$, *es inyectiva.*

8) En general, si A es un conjunto, $\approx$ una relación de equivalencia en A, y $A/\approx$ su conjunto cociente, la aplicación $\varphi : A \to A/\approx$, tal que $\varphi(a) = \overline{a}$, $\forall a \in A$, (se denomina *proyección canónica al cociente*). Esta función es *siempre* suryectiva.
En particular $\varphi : \mathbb{Z} \to \mathbb{Z}_n$, tal que $\varphi(a) = \overline{a}$, $\forall a \in \mathbb{Z}$, donde $\overline{a}$ es la clase de equivalencia de a (*mód n*) (φ es la *proyección canónica al cociente* $\mathbb{Z}_n$).

***Propiedades*:** Sean $f : A \to B$, $g : B \to C$ funciones.

1) Si f y g son inyectivas entonces $g \circ f$ es inyectiva
2) Si $g \circ f$ es inyectiva entonces f es inyectiva. ¿También lo es siempre g ?
3) Si f y g son suryectivas entonces $g \circ f$ es suryectiva
4) Si $g \circ f$ es suryectiva entonces g es suryectiva. ¿También lo es siempre f ?
5) Si f y g son biyectivas entonces $g \circ f$ es biyectiva.
6) Si $g \circ f$ es biyectiva, ¿qué podemos decir de f y de g ?

***Demostración*:** Demostraremos 2) a modo de ejemplo; los demás quedan como ejercicios.

2) Si $g \circ f$ es inyectiva entonces $\forall x, x' \in A$, $x \neq x' \Rightarrow (g \circ f)(x) \neq (g \circ f)(x')$
para ver que f es inyectiva debemos demostrar que $f(x) = f(x') \Rightarrow x = x'$.
Si $f(x) = f(x')$, como es un elemento del dominio de g, y g es función, cada elemento del dominio tiene una única imagen, luego $g(f(x)) = g(f(x'))$ entonces $(g \circ f)(x) = (g \circ f)(x')$
y por ser $g \circ f$ inyectiva, tenemos que $x = x'$.
Luego f es inyectiva.
La pregunta la dejamos para que la analice el lector.

Ejercicio: ¿Qué relación de inclusión verifican los conjuntos $Im(g) \wedge Im(g \circ f)$, si es que verifican alguna?

Teorema: Sea $f : A \to B$ una función. Entonces:

i) f es inyectiva si y sólo si $\exists\, g : B \to A$ función tal que $g \circ f = id_A$. ¿Es g única?

ii) f es suryectiva si y sólo si $\exists\, h : B \to A$ función tal que $f \circ h = id_B$. ¿Es h única?

iii) f es biyectiva si y sólo si $\exists\, t : B \to A$ función tal que $t \circ f = id_A \wedge f \circ t = id_B$. ¿Es t única?

***Demostración*:**

i) Debemos demostrar dos implicaciones:

$\Rightarrow$) Sea f inyectiva; queremos definir una función $g : B \to A$, que satisfaga $g \circ f = id_A$. ; para ello debemos asignarle por g a cada elemento del dominio B una imagen en A .

Supondremos que f no es suryectiva, pues el caso f biyectiva será considerado por separado. Por lo tanto $Im(f) \subsetneq B$

Sea $y \in B$, entonces $y \in Im(f) \vee y \notin Im(f)$.

Si $y \in Im(f)$, , $\exists\, x \in A$ tal que $y = f(x)$, como f es inyectiva, este x es único, luego definimos: $g(y) = x$.

Si $y \notin Im(f)$ entonces elegimos un $x_0 \in A$ y definimos $g(y) = x_0$

Queda definida así: $g : B \to A$, tal que $g(y) = \begin{cases} x & si \quad y = f(x) \\ x_0 & si \quad y \notin \mathrm{Im}(f) \end{cases}$

Calculemos $g \circ f$. Para $x \in A$ $(g \circ f)(x) = g(f(x)) = x = id_A(x)$, pues si $y = f(x)$, se verifica que $g(y) = x$, por definición de g . Luego $g \circ f = id_A$.

Si $Im(f) \neq B$, g **no es única** pues si definimos $g' : B \to A$ tal que

$g'(y) = \begin{cases} x & si \quad y = f(x) \\ x_1 & si \quad y \notin \mathrm{Im}(f) \end{cases}$

para algún $x_1 \neq x_0$; luego tenemos que $g \neq g'$.

$\Leftarrow$) Supongamos que $\exists\, g : B \to A$ función tal que $g \circ f = id_A$, queremos ver que f es inyectiva:

Sean $x, x' \in A$ tales que $f(x) = f(x')$, entonces $g(f(x)) = g(f(x'))$ pues g es función.

Como $g \circ f = id_A$, será $x = g(f(x)) = g(f(x')) = x'$, luego $x = x'$, y f es inyectiva.

ii) $\Rightarrow$) Sea f suryectiva, queremos ver que $\exists\, h : B \to A$ función tal que $f \circ h = id_B$

Para definir h , sea $y \in B$; por ser f suryectiva, $Im(f) = B$, así $f^{-1}(y) \neq \phi$, $\forall\, y \in B$.

Elegimos en cada $f^{-1}(y)$ un x_y , y definimos $h(y) = x_y$ (como $x_y \in f^{-1}(y)$, entonces $f(x_y) = y$).

h está definido en cada elemento de B, y la imagen de cada elemento es única pues elegimos sólo uno en cada uno de los $f^{-1}(y)$, luego h es función.

¿ $f \circ h = id_B$? . Para $y \in B$ $(f \circ h)(y) = f(h(y)) = f(x_y) = y = id_B(y)$, luego $f \circ h = id_B$.

h en general **no es única** pues si f no es inyectiva $\exists y_0 \in B$ tal que en $f^{-1}(y_0)$ podemos elegir un $x'_{y_0} \neq x_{y_0}$, y así se puede definir una función *h'*, en forma análoga a *h* , tal que *h'* (*y*) = x_y $\forall y \in B$, $y \neq y_0$, $h'(y_0) = x'_{y_0}$; h' tiene las mismas propiedades que *h*, pero es distinta.

$\Leftarrow$) Supongamos que $\exists h : B \to A$ función tal que $f \circ h = id_B$, queremos ver que f es suryectiva.

Sea $y \in B$, como $f \circ h = id_B$, $y = f(h(y))$, luego $y \in Im(f)$, por lo tanto, f es suryectiva.

iii) Este ítem lo dejamos como ejercicio; sólo haremos mención al tema de la unicidad:
t **es única** . Para demostrarlo supongamos que hubiera otra función $t' : B \to A$ tal que

$$t' \circ f = id_A \wedge f \circ t' = id_B$$

$$t = id_A \circ t = (t' \circ f) \circ t = t' \circ (f \circ t) = t' \circ id_B = t'$$

Definición*:** La función *t* del ítem iii) se denomina ***función inversa de f , y se la nota f^{-1}.

Luego , *f es biyectiva sii admite una función inversa* $f^{-1} : B \to A$, (se dice que *f es inversible*) y la inversa , que es única, verifica:

$$f^{-1} \circ f = id_A \quad \wedge \quad f \circ f^{-1} = id_B$$

Ejercicios:

1) Si f es biyectiva entonces f^{-1} es biyectiva, y la inversa de f^{-1} es f, o sea $\left(f^{-1}\right)^{-1} = f$

2) Si $f : A \to B$, $g : B \to C$ son inversibles, entonces $g \circ f$ es inversible, y su inversa es:
$(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

3) Mostrar con sendos ejemplos concretos que las funciones g y h que mencionan los ítems i) e ii) del teorema, no son únicas.

Restricción y extensión de funciones

***Definición*:** Sean $f : A \to B$ una función , $A' \subset A$, $B' \subset B$ tales que $f(A') \subset B'$.
Podemos definir una función $g : A' \to B'$, asignando a cada $x \in A'$ la misma imagen por *g* que por *f* , o sea : $g(x) = f(x)$ $\forall x \in A'$.
g se denomina *restricción de f a A' y a B'*

Notación: $g = f\big/_{A',B'}$ y se lee g *es* f *restringida a* A' *y a* B'.

$f\big/_{A',B'} : A' \to B'$, $f\big/_{A',B'}(x) = f(x)$

Observación: Cualquiera sea A' subconjunto del dominio, podemos definir la restricción $f\big/_{A',B}$ (que se puede notar directamente $f\big/_{A'}$ porque no se introdujo ninguna modificación en el codominio); diferente es la situación cuando queremos restringir el codominio, en este caso es **imprescindible que $f(A') \subset B'$**, pues si esto no ocurriera la restricción no sería función.

Ejemplo: Sea $g : \mathbb{R} \to \mathbb{R}$, $g(x) = sen(x)$

$g\big/_{[0,\pi]} : [0, \pi] \to \mathbb{R}$, $g\big/_{[0,\pi]}(x) = sen(x)$, es una función mientras que

$g\big/_{[0,2\pi],[0,1]} : [0, 2\pi] \to [0, 1]$, $g\big/_{[0,2\pi],[0,1]}(x) = sen(x)$

no es función puesto que $\frac{3\pi}{2}$ no tiene imagen en la restricción, luego no está en el dominio, pero

$\frac{3\pi}{2} \in [0, 2\pi]$, lo que contradice la definición de función.

***Definición*:** Sea $f : A \to B$ una función, $A \subset C$, $B \subset D$. Llamamos *extensión de f a C y a D* a una función $h : C \to D$ tal que $h\big/_{A,B} = f$.

Observación: Claramente puede observarse que para definir restricciones tenemos la limitación antes mencionada que $f(A') \subset B'$, pero si esto se verifica, se puede definir la restricción de f a A' y a B' y ésta es **única,** pues ya están determinadas las imágenes de cada uno de los elementos de A' para la restricción, por ser las mismas que las de f. No ocurre lo mismo con las extensiones; si $C \neq A$, tenemos, en general, muchas opciones para definir la nueva función en los puntos de $C - A$, aun cuando $B = D$, pero **siempre existen extensiones de f a C y a D**:

Resumen: *la restricción de f a A' y a B' no siempre existe, pero si existe es única.*
La extensión de f a C y a D existe siempre, pero no necesariamente es única.

Ejercicios:

1) Sea $f : A \to B$ una función, $A' \subset A$, $B' \subset B$ tales que $f(A') \subset B'$:
i) Demostrar que si f es inyectiva entonces $f\big/_{A',B'}$ es inyectiva.
ii) Si f es suryectiva, ¿es $f\big/_{A',B'}$ suryectiva ?

2) Si $A \subset C$, $B \subset D$ y h es una extensión de f a C y a D, ¿se verifica que:
i) f es inyectiva $\Rightarrow$ h es inyectiva ?
ii) f es suryectiva $\Rightarrow$ h es suryectiva ?

3) Demostrar que si $f : A \to B$ es una función inyectiva, la restricción
$f\big/_{A,f(A)} : A \to f(A)$ es biyectiva

Aplicaciones de relaciones de equivalencia a funciones

- Sea $\mathcal{F}$ un conjunto de conjuntos (conjunto cuyos elementos son, a su vez, conjuntos). Vamos a definir en $\mathcal{F}$ una relación de equivalencia:

$$A \approx B \Leftrightarrow \exists f : A \to B \text{ función biyectiva}$$

Se lee: *A es coordinable con B si y sólo si existe una función biyectiva de A sobre B.*

Ejercicio: Demostrar que $\approx$ es una relación de equivalencia en $\mathcal{F}$.

La clase de equivalencia de un conjunto *A* se denomina *cardinal de A,*

Notación: clase de A = card(A) ; dos conjuntos *A* y *B* tienen el mismo cardinal si y sólo si son coordinables.

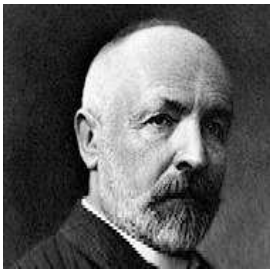
***Definición*:** Sean $n \in \mathbb{N}$, *A* un conjunto. *A* se dice *finito de cardinal n* si *A* es coordinable con $[\![1,n]\!] = [1,n] \cap \mathbb{N}$ (intervalo natural 1, *n*).
Se lo nota *card*(*A*) = *n*, intuitivamente esto dice que *A* "tiene *n* elementos".

Nota: El cardinal del conjunto ϕ se define igual a 0 : *card*(ϕ) = 0

***Definición*:** Diremos que un conjunto *A* es *finito,* si es finito de cardinal *n* , para algún número $n \in \mathbb{N}_0$

***Definición*:** Un conjunto *A* se dice *numerable* si es coordinable con el conjunto de números naturales $\mathbb{N}$.

El cardinal de $\mathbb{N}$, y por tanto de los conjuntos numerables, se denomina *aleph* 0 : $\aleph_0$;
card($\mathbb{N}$) = $\aleph_0$



א (Aleph) es la primera letra del alfabeto hebreo y fue Cantor quien decidió utilizar el símbolo compuesto aleph-cero $\aleph_0$ *para nombrar el cardinal de los conjuntos numerables.*

*Georg Cantor (*1845-1918*)*

Ejemplos:

1) El conjunto $\mathbb{P}$ de los números naturales pares es numerable:
La aplicación $f : \mathbb{N} \to \mathbb{P}$, $f(n) = 2n$ es biyectiva (demostrarlo)

2) El conjunto $\mathbb{I}$ de los números naturales impares es numerable:
La aplicación $g : \mathbb{N} \to \mathbb{I}$, $g(n) = 2n - 1$ es biyectiva (demostrarlo).

3) El conjunto $\mathbb{N}_0$ de los naturales con el cero, es numerable
La aplicación $h : \mathbb{N} \to \mathbb{N}_0$, $h(n) = n - 1$ es biyectiva (demostrarlo)

4) El conjunto $\mathbb{Z}$ de los números enteros es numerable.
La aplicación $j : \mathbb{Z} \to \mathbb{N}_0$,

$$j(x) = \begin{cases} 2x & si\ x \geq 0 \\ -2x-1 & si\ x < 0 \end{cases}$$

es biyectiva (demostrarlo)

Ejercicios:

Sea A un conjunto finito. Demostrar:

1) Si $card(A) = n \in \mathbb{N}$, $a \in A$, entonces $card(A - \{a\}) = n - 1$
2) Si $card(A) = n \in \mathbb{N}_0$, $b \notin A$, entonces $card(A \cup \{b\}) = n + 1$

- Sea $f : A \to B$ una función. Definimos en A la siguiente relación:

$$a \propto b \quad si\ y\ sólo\ si \quad f(a) = f(b)$$

Demostrar que es una relación de equivalencia en A.

¿Cuál es la clase de equivalencia de cada $a \in A$?

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

¿y el conjunto cociente?

$$A/_{\propto} = \{ \quad f^{-1}(t) / t \in Im(f) \quad \}$$

***Ejercicios*:**

1.- i) Dados los conjuntos $A = \{1, 2, 3\}$ y $B = \{0, 1, 2, 3, 8\}$. ¿Es posible definir una función $f : A \to B$ que asigne a cada elemento del dominio su cuadrado disminuido en 1?. Representar en gráfico cartesiano y por diagrama de Venn.
ii) Idem i) para los conjuntos $A = \{-1, 1, 2, 3, 5, -7\}$, $B = \{-3, 0, 1, 2, 3, 5, 6, 8, 9\}$.

2.- Siendo $A = \{-2, -1, 1, 3\}$ representar la función $f : A \to \mathbb{Z}$ tal que la imagen de cada elemento de A sea el resto que tiene ese número en la división por 3.

3.- Sea $A = \{1, 2, 3, 4, 5, 6\}$ y consideremos las siguientes gráficas en $A \times A$.
¿Cuáles de ellas sirven para definir funciones de A en A ? Hacer los diagramas en $A \times A$ y las tablas correspondientes.

$G_1 = \{(x, y) \in A \times A \ / \ y = 2x\}$

$G_2 = \{(x, y) \in A \times A \ / \ y = 5\}$

$G_3 = \{(x, y) \in A \times A \ / \ y = x \vee y = 5\}$

$G_4 = \{(x, y) \in A \times A \ / \ y = x \wedge y = 5\}$

$G_5 = \{(x, y) \in A \times A \ / \ y.x = 6\}$

4.- Cada una de las siguientes expresiones define una función de $\mathbb{R}$ en $\mathbb{R}$. Determinar la imagen de cada una de ellas:

a) $f(x) = x^3$ b) $h(x) = x^2 + 1$ c) $g(x) = sen\ x$ d) $t(x) = (sen\ x)^2$

e) $f(x) = 1 + sen\ x$ f) $g(x) = |sen\ x|$

5.- Demostrar las siguientes propiedades de la imagen de subconjuntos del dominio:
a) Sean $f : X \to Y, A \subset X, B \subset X$, $A \subset B$ entonces $f(A) \subset f(B)$;
en particular $\forall A \subset X$, $f(A) \subset \text{Im}(f)$
b) Sean $f : X \to Y, A \subset X, B \subset X$ entonces $f(A \cup B) = f(A) \cup f(B)$
c) Sean $f : X \to Y, A \subset X, B \subset X$ entonces $f(A \cap B) \subset f(A) \cap f(B)$. Mostrar un ejemplo en el cual no se verifique la igualdad.

6.- Proponer conjuntos $X, Y, A \subset X$ y una función $f : X \to Y$ para los cuales :
a) $f(X - A) \subset Y - f(A)$
b) $Y - f(A) \subset f(X - A)$
c) $f(X - A) \cap (Y - f(A)) = \phi$

7.- Indicar el mayor subconjunto de $\mathbb{R}$, si existe, que puede considerarse para que las siguientes relaciones sean funciones:

a) $y = 2x^2 + 1$ b) $y = \dfrac{1}{x}$ c) $y = \dfrac{1}{x^2 + 1}$ d) $y = \dfrac{1}{(x+1)^2}$

8 - Determinar las imágenes y preimágenes de los siguientes subconjuntos del dominio y del codominio, respectivamente, para la función dada en cada caso:
a) $f : \mathbb{R} \to \mathbb{R}$ definida por $f(x) = x^2 + 1$

Dominios: [–3 , 3] ; (0, 5) ; $(-\infty, \frac{3}{4})$

Codominios: [–1, 1) ; (– ∞, ½] ; [1, 10]

b) $f: \mathbb{R} \to \mathbb{R}$ definida por $f(x) = sen\, x$

Dominios: [0 , 2π) ; $\left(-\frac{\pi}{2}, \frac{\pi}{2}\right)$; $\left[-\pi, \frac{\pi}{2}\right)$

Codominios: [–3, 2] ; (0 , 2] ; (–1 , ½)

9.- Demostrar las siguientes propiedades de la preimagen:

a) $A \subset B \Rightarrow f^{-1}(A) \subset f^{-1}(B)$

b) $f^{-1}(A \cup B) = f^{-1}(A) \cup f^{-1}(B)$

c) $f^{-1}(A \cap B) = f^{-1}(A) \cap f^{-1}(B)$

d) $f^{-1}(\overline{A}) = \overline{f^{-1}(A)}$

10.- Determinar si son verdaderas o falsas las siguientes proposiciones. Justificar.
Sea $f: A \to B$ función:

i) $A' \subset A\,, \quad A' \neq \phi \Rightarrow f(A') \neq \phi$

ii) $B' \subset B\,, \quad B' \neq \phi \Rightarrow f^{-1}(B') \neq \phi$

iii) $A_1 \subset A_2 \subset A \Rightarrow f(A_1) \subset f(A_2)$

iv) $B_1 \subset B_2 \subset B \Rightarrow f^{-1}(B_1) \subset f^{-1}(B_2)$

v) $A' \subset A \Rightarrow f^{-1}(f(A')) \subset A'$

vi) $A' \subset A \Rightarrow A' \subset f^{-1}(f(A'))$

vii) $B' \subset B \Rightarrow f\ (f^{-1}(B')) \subset B'$

viii) $B' \subset B \Rightarrow B' \subset f\ (f^{-1}(B'))$

11.- i) Determinar dominios y codominios adecuados para que la expresión funcional $f(x) = x^2$ represente una función que sea:

a) inyectiva y no suryectiva
b) suryectiva y no inyectiva
c) no suryectiva y no inyectiva
d) biyectiva

11.- ii) Idem 11-i) para la función $f: \mathbb{R} \to \mathbb{R}$, con $f(x) = |x - 1|$

12.- Analizar si las siguientes funciones son inyectivas, suryectivas y/o biyectivas:

a) $f: \mathbb{R} \to \mathbb{R}\,, \quad f(x) = \sqrt[3]{x-1}$

b) $[\,.\,]: \mathbb{R} \to \mathbb{R}\,, \quad [\,x\,] = máx\{n \in \mathbb{Z} \ / \ \ n \leq x\}$ (parte entera de x)

c) $(\,.\,): \mathbb{R} \to \mathbb{R}\,, \quad (\,x\,) = x - [\,x\,]$ (parte decimal de x)

d) $f: \mathcal{P}(A) \to \mathcal{P}(B)\,, \quad f(X) = X \cap B,$ siendo $A = \{1, 2, 3\}\,, \quad B = \{1, 2\}$

e) $f: \mathbb{R} - \{0\} \to \mathbb{R}\,, \quad f(x) = \frac{x+1}{x}$

13.- Sean $f: \mathbb{R} \to \mathbb{R}\,, \ f(x) = 1 - x^2\,, \ g: \mathbb{R}^+ \to \mathbb{R}\,, \ g(x) = \sqrt{x}$ y $h: \mathbb{R} \to \mathbb{R}\,, \ h(x) = 2x$

Hallar: a) $f \circ g$ b) $h \circ g$ c) $f \circ (h \circ g)$ d) $h \circ (f \circ g)$

14.- Sean $f: A \to B$, $g: B \to C$, $h: C \to D$ funciones.
i) Demostrar que:
a) $id_B \circ f = f \wedge f \circ id_A = f$ b) $h \circ (g \circ f) = (h \circ g) \circ f$

ii) Si $C = A$ ¿es verdadero o falso que $g \circ f = f \circ g$? Justificar.

15. Sea $f: A \to B$ función . Demostrar que:
i) f es inyectiva sii existe $g: B \to A$ tal que $g \circ f = id_A$. ¿Es g única? Justificar.
ii) f es suryectiva sii existe $g: B \to A$ tal que $f \circ g = id_B$. ¿Es g única? Justificar.
iii) f es biyectiva sii existe $g: B \to A$ tal que $g \circ f = id_A \wedge f \circ g = id_B$. ¿Es g única? Justificar.
En este caso g se denomina la *función inversa* de f y se la denota $g = f^{-1}$

16.- Sea f una función biyectiva de A en B , y sea g una función biyectiva de B en C. Probar que $g \circ f$ es biyectiva y que $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$

17.- Sean f_1 una aplicación de A en B y f_2 una aplicación de B en C ; sea $f = f_2 \circ f_1$
Probar:
a) Si $f_1 \wedge f_2$ son inyectivas entonces f es inyectiva
b) Si $f_1 \wedge f_2$ son suryectivas entonces f es suryectiva
c) Si f es inyectiva entonces f_1 también lo es
d) Si f es suryectiva entonces f_2 también lo es
e) ¿es verdadero o falso que f biyectiva implica $f_1 \wedge f_2$ son biyectivas?
f) ¿es verdadero o falso que f biyectiva implica $f_1 \vee f_2$ es biyectivas?

18.- Sea $f: A \to B$ función, $A' \subset A$, $B' \subset B$. En los siguientes casos decir cuándo es posible definir la restricción $f|_{A'}$, $f|_{A,B'}$, $f|_{A',B'}$
a) $f(x) = |x| + 2$, $A' = \mathbb{R}_{\geq 0}$, $B' = \mathbb{R}_{>2}$, $A = \mathbb{R}$, $B = \mathbb{R}$
b) $f(x) = x - 1$, $A' = \mathbb{N}$, $B' = \mathbb{N}$, $A = \mathbb{R}$, $B = \mathbb{R}$
c) $f(x) = [x]$, $A' = \mathbb{Z}$, $B' = \mathbb{Z}$, $A = \mathbb{R}$, $B = \mathbb{R}$

19) Sean $f: A' \to B'$ función, $A' \subset A$, $B' \subset B$.
En los siguientes casos definir, si es posible, una extensión de f con dominio A, y otra con dominio A y codominio B

a) $f(x) = \begin{cases} -x^2 - 2 & si \quad x \leq \dfrac{1}{2} \\ |x - 1| & si \quad x > \dfrac{1}{2} \end{cases}$, $A' = \mathbb{R} - (0, 1)$, $B' = \mathbb{R} - (-2, 0)$, $A = \mathbb{R}$, $B = \mathbb{R}$

b) $f(x) = \begin{cases} \dfrac{1}{x-1} & si \quad x < 1 \\ 2x & si \quad x > 1 \end{cases}$, $A' = \mathbb{R} - \{1\}$, $B' = \mathbb{R} - [0, 2]$, $A = \mathbb{R}$, $B = \mathbb{R}$

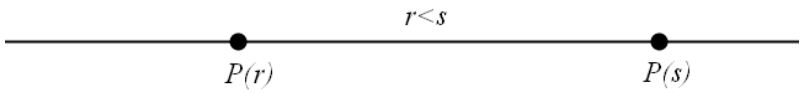
20.- Sean $f: A \to B$ función, $A' \subset A$, $B' \subset B$ tales que $f(A') \subset B$.
¿Es verdadero o falso que:
i) f inyectiva $\Rightarrow f|_{A',B'}$ es inyectiva? ii) f suryectiva $\Rightarrow f|_{A',B'}$ es suryectiva?

CAPÍTULO III

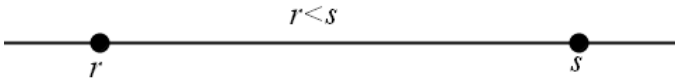
NÚMEROS REALES

Demostraremos propiedades de los números reales que son quizás "verdades evidentes" para muchas personas que han manipulado algebraicamente números y ecuaciones y, al hacerlo, las han utilizado con frecuencia, sin plantearse si eran verdaderas y por qué.

En este Capítulo definiremos al conjunto de números reales $\mathbb{R}$, que lo pensamos como puntos de una recta, es decir que a todo número real r, le corresponde uno y sólo un punto $P(r)$ de la recta. De tal modo, si r y s son números reales tales que $r < s$, en su representación sobre la recta real se ubicará $P(r)$ a la izquierda de $P(s)$:



Nota: en general, por abuso de notación, indicaremos simplemente con r al punto $P(r)$:



Consideraremos a $\mathbb{R}$ como un conjunto provisto de dos operaciones, *suma* y *producto*, y de un *orden*. Más aun, veremos que definiendo *axiomáticamente* un conjunto dotado de dos operaciones y un orden, con propiedades que especificaremos, obtendremos el conjunto de números reales que *conocemos*, o algo similar a él.

> *"Un significado originario del término "**axioma**" es dignidad. Por derivación "axioma" significa lo que es digno de ser estimado, creído o valorado....En los An.post(I,2,72 a 19 ss), de Aristóteles, el término "axioma" tiene todavía este significado: Los axiomas son para el Estagirita principios evidentes que constituyen el fundamento de toda ciencia. (Ferrater Mora, J. T I, p.167).*
> *La matemática y la lógica contemporáneas distinguen entre axiomas y teoremas, los primeros son enunciados primitivos, aceptados como verdaderos, sin probar su validez, mientras que la validez de los teoremas debe ser sometida a prueba.*

Definición axiomática

Sea $\mathbb{R}$ un conjunto no vacío, provisto de dos operaciones: *suma* **+** , *y producto* **. ,** esto es, dos funciones:

$+ : \mathbb{R}\times\mathbb{R} \rightarrow \mathbb{R}$, $\quad . : \mathbb{R}\times\mathbb{R} \rightarrow \mathbb{R}$, que verifican las siguientes propiedades:

$$\text{suma} : + : \mathbb{R}\times\mathbb{R} \rightarrow \mathbb{R}$$
$$(a, b) \rightarrow a + b$$

($a + b$ debe interpretarse aquí como la imagen del par (a, b) por la función + , olvidándonos por el momento del significado que le tenemos asignado a esta expresión).

Esta operación verifica las propiedades que pasamos a enunciar:

S1) *asociativa*: $a + (b + c) = (a + b) + c \ \forall a, b, c \in \mathbb{R}$

(esto debe interpretarse así: la imagen del par $(a, b + c)$ coincide con la del par $(a + b, c)$)

S2) *conmutativa*: $a + b = b + a \ \forall a, b \in \mathbb{R}$

(la imagen del par (a, b) coincide con la del par (b, a))

S3) *Existencia de elemento neutro*: $\exists\, e \in \mathbb{R}$ tal que $e + a = a + e = a$, $\forall\, a \in \mathbb{R}$

(las imágenes de (e, a) y de (a, e) coinciden y son iguales a a)

S4) *Existencia del elemento inverso*: $\forall\, a \in \mathbb{R}\ \ \exists\, a' \in \mathbb{R}$ tal que $a + a' = a' + a = e$.

Cuando tenemos un conjunto no vacío, como lo es en este caso $\mathbb{R}$, con una operación, como + , que verifica las cuatro propiedades anteriores, se denomina *grupo abeliano*: ($\mathbb{R}$, +) es un grupo abeliano

Nótese que lo que llamamos grupo abeliano es el par ordenado, pues interesa no sólo el conjunto sino también la operación; todo ello es lo que constituye el grupo.

Antes de continuar explicitando las propiedades que verifica la otra operación, demostraremos algunas otras que resultan de los axiomas dados.

Teorema: El neutro e es ***único.***

***Demostración*:** Generalmente, cuando deseamos demostrar que algo es único, suponemos que hay más de uno, y vemos que coinciden, o bien que esa suposición nos lleva a alguna contradicción que muestre que es imposible que eso ocurriere.

Supongamos que $\exists\, e, e' \in \mathbb{R}$ tales que $a + e = e + a = a$ y $a + e' = e' + a = a\ \ \forall\, a \in \mathbb{R}$
entonces, $e + e' = e$ porque e' es neutro
pero $e + e' = e'$ porque e es neutro
luego $e = e'$

Notación: al elemento neutro de la suma que existe y es único por lo que demostramos arriba, lo llamaremos *cero***:** 0

La propiedad S3) se escribirá así: $\exists\, 0 \in \mathbb{R}$ tal que $0 + a = a + 0 = a$, $\forall\, a \in \mathbb{R}$.

***Teorema*:** $\forall\, a, b \in \mathbb{R}\ \ \exists!\, x \in \mathbb{R}$ (existe un único $x \in \mathbb{R}$) tal que $a + x = b$.

***Demostración*:**

Existencia de x: Para ver que x existe debemos definirlo, y luego verificar que cumple con la propiedad pedida.

Sean $a, b \in \mathbb{R}$, por S4) $\exists\, a' \in \mathbb{R}$ tal que $a + a' = a' + a = 0$

Definimos: $x = a' + b$

Veamos si este x verifica la ecuación: $a + x = a + (a' + b) =$

por asociatividad de + : $= (a + a') + b = 0 + b = b$

pues 0 es neutro para +.

Luego $a + x = b$, para el x definido, y así la ecuación dada **siempre** tiene solución.

Unicidad de x:

Supongamos que $\exists\, x, x' \in \mathbb{R}$ tales que $a + x = b \wedge a + x' = b$,

entonces $a + x = a + x'$

sumando a' m.a.m. (miembro a miembro) $a' + (a + x) = a' + (a + x')$

asociando $(a' + a) + x = (a' + a) + x'$

$a' + a = 0$, reemplazando $0 + x = 0 + x'$

0 es neutro para + , entonces $x = x'$

Entonces la solución x **es única**.

Corolario*:** El inverso de cada $a \in \mathbb{R}$ es ***único.

***Demostración*:**

Este es un caso particular del teorema; para $a \in \mathbb{R}$, como $0 \in \mathbb{R}$ $\exists! x \in \mathbb{R}$ tal que $a + x = 0$,

Este *x es el inverso aditivo u opuesto de a,* y lo notaremos $-a$ (el número que sumado a izquierda y a derecha con a da 0).

Propiedades de la operación producto: $\mathbb{R} \times \mathbb{R} \to \mathbb{R}$

$$(a,b) \to a \cdot b$$

P1) *asociativa*: $a.(b.c) = (a.b).c$ $\forall a, b, c \in \mathbb{R}$

P2) *conmutativa*: $a.b = b.a$ $\forall a, b \in \mathbb{R}$

P3) *existencia de elemento neutro*:
$\exists e' \in \mathbb{R}$, $e' \neq 0$, tal que $e'.a = a.e' = a$, $\forall a \in \mathbb{R}$

P4) *existencia del elemento inverso*:
$\forall a \in \mathbb{R}$, $a \neq 0$, $\exists a'' \in \mathbb{R}$ tal que $a.a'' = a''.a = e'$.

Enunciaremos para el producto teoremas semejantes a los dados para la suma; las demostraciones se dejan como ejercicios pues se razonan en forma totalmente análoga a las ya vistas.

Teorema*:** El neutro e' es ***único.

Notación: al elemento neutro del producto que existe y es único por el teorema, lo llamaremos **uno: 1**
En el axioma de existencia se pide que $1 \neq 0$, lo que garantiza que las dos operaciones + y **.** sean distintas.

La propiedad P3) se escribirá así:
$\exists 1 \in \mathbb{R}$, $1 \neq 0$, tal que $1.a = a.1 = a$, $\forall a \in \mathbb{R}$

***Teorema*:** $\forall a, b \in \mathbb{R}$, $a \neq 0$, $\exists!$ $x \in \mathbb{R}$ (existe un único $x \in \mathbb{R}$) tal que $a.x = b$.

Corolario*:** El inverso de cada $a \in \mathbb{R}$, $a \neq 0$, es ***único.

Notación: al inverso de cada $a \neq 0$, lo notaremos a^{-1}, y significa eso, *el número que multiplicado a derecha e izquierda por a, da* 1.

Quizás, a primera vista, parezca que las dos operaciones cumplen propiedades idénticas, mas no es así, porque para la suma **todos** los elementos tienen inverso, mientras que para el producto, el

axioma dice que **los elementos no nulos** tienen inverso, y no dice nada sobre el 0, pero ya veremos que el 0 no admite inverso multiplicativo; ésta es una diferencia considerable.

Además, tenemos una propiedad que vincula ambas operaciones, la *distributividad*:

D) El producto es distributivo respecto de la suma:

$$a.(b + c) = a.b + a.c \quad \forall a, b, c \in \mathbb{R}$$

Cuando tenemos un conjunto no vacío, como lo es en este caso $\mathbb{R}$, con dos operaciones, como + y . , que verifican todas las propiedades anteriores, lo llamamos *cuerpo*: $(\mathbb{R}, +, .)$ es un cuerpo.

Como antes, lo que llamamos cuerpo es la terna ordenada, pues interesan no sólo el conjunto sino también las operaciones, todo ello es lo que constituye el cuerpo.
De este conjunto más las propiedades dadas en forma axiomática (quiere decir que se asume su veracidad sin necesidad de demostrarlas), podemos deducir otras muchas que pueden demostrarse a partir de los axiomas.

Comentario: Las propiedades que enunciaremos y deberemos demostrar son quizás "verdades evidentes" para muchas personas que han manipulado algebraicamente números y ecuaciones y, al hacerlo, las han utilizado con frecuencia, sin plantearse si eran verdaderas y por qué; ahora veremos que son verdaderas y cómo demostrarlo.

Propiedades deducibles a partir de los axiomas de suma y producto:

Para $a, b, c \in \mathbb{R}$

1) Si $a + a = a$ *entonces* $a = 0$

2) $-0 = 0$ (el inverso aditivo u opuesto de 0 es 0)

3) $-(-a) = a$ (el inverso aditivo del inverso aditivo de a es a)

4) $a = b \Leftrightarrow -a = -b$

Notación: escribiremos $a - b$ al número $a + (-b)$

5) $-(a + b) = (-a) + (-b) = -a - b$

6) $a + b = a - (-b)$

7) $a \neq 0 \Rightarrow -a \neq 0$ (un número no nulo tiene opuesto no nulo)

8) $a.0 = 0$ (esta propiedad implica que 0 no puede tener inverso multiplicativo)

9) $(-1).a = -a$ (el opuesto de a es igual a multiplicar el opuesto de 1 por a)

10) $(-a).b = a.(-b) = -(a.b)$ (esto se lee el opuesto de $a.b$)

11) $(-a).(-b) = a.b$ (regla de los signos)

12) $(-a).(-b).(-c) = -(a.b.c)$

13) $a.(b - c) = a.b - a.c$

14) $(a + b).(c + d) = a.c + a.d + b.c + b.d$

15) Si $a \neq 0$ *entonces* $a^{-1} \neq 0 \wedge (a^{-1})^{-1} = a$

16) $a.b = 0 \Leftrightarrow a = 0 \vee b = 0$

17) $a \neq 0 \wedge b \neq 0 \Rightarrow a.b \neq 0 \wedge (a.b)^{-1} = a^{-1}.b^{-1}$

18) $1^{-1} = 1 \wedge (-1)^{-1} = -1$

19) $a^2 = 1 \Leftrightarrow a = 1 \vee a = -1$

Demostraremos algunas de ellas a modo de ejemplo. Recordemos que estas propiedades deben deducirse a partir de los axiomas; debemos dejar de lado todo preconcepto que tengamos al respecto, y utilizar sólo las hipótesis, que son los axiomas, los teoremas y las propiedades ya demostradas.

> *A lo largo de la historia, las demostraciones han sido, en cada época, reflejo estructural de las concepciones matemáticas de ese entonces.*
> *La demostración es una actividad característica de la matemática; pero no es algo que se haya hecho siempre de la misma manera. De hecho, la actividad demostrativa ha evolucionado con la matemática misma, dejando, en cada momento, el testimonio de la íntima relación entre los métodos de demostración y la naturaleza de los objetos matemáticos en cuestión.*
> *La demostración no es sólo una actividad sintáctica, un mero juego deductivo; por el contrario, en la actividad demostrativa, la cognición se dirige a la construcción de un universo donde los objetos construidos son los que intervienen en el discurso demostrativo. La matemática se caracteriza por ser una ciencia que no toma su objeto de la realidad sino que lo construye en la cognición del sujeto. De ahí que sean inseparables construcción del objeto y demostración.*

***Demostración*:**

1) Si $a + a = a$ entonces $a = 0$

Aquí debemos demostrar una implicación, así que partiendo de la hipótesis:
$a + a = a$ debemos obtener que $a = 0$.

Si $a + a = a$

sumando $-a$ m.a.m.	$-a + (a + a) = -a + a = 0$
asociando	$(-a + a) + a = 0$
reemplazando por 0	$a = 0 + a = 0$
luego	$a = 0$

3) $-(-a) = a$

Aquí debemos demostrar una igualdad: que el opuesto del opuesto de a es a .

Podemos elegir dos caminos diferentes para demostrar esta igualdad.

1ra. forma:

la ecuación $x + (-a) = 0$ admite solución y ésta es única

tenemos que $a + (-a) = 0$ porque $-a$ es el opuesto de a

y también que $-(-a) + (-a) = 0$ porque $-(-a)$ es el opuesto de $-a$

luego encontramos dos soluciones para la misma ecuación, por lo tanto coinciden, y así $-(-a) = a$

2da. forma:

$-(-a) = -(-a) + 0 = -(-a) + (-a + a) = (-(-a) + (-a)) + a = 0 + a = a$

***Comentario*:** En este caso usamos dos caminos diferentes, e igualmente válidos, para demostrar la propiedad ; esto no es excepcional, generalmente no existe un único camino para comprobar la veracidad de una afirmación, si es que es verdadera, y todas son aceptables en la medida que se utilicen correctamente las leyes lógicas, los axiomas y los teoremas ya demostrados.

5) $-(a + b) = (-a) + (-b) = -a - b$

La primera igualdad nos dice que el opuesto de $a + b$ es el opuesto de a más el opuesto de b . Para ver que un número es opuesto de otro, debemos sumarlos y ver si suman 0.

$(a + b) + [(-a) + (-b)] = (b + a) + [(-a) + (-b)] = b + \{a + [(-a) + (-b)]\} =$

$= b + \{ [a + (-a)] + (-b)\} = b + [0 + (-b)] = b + (-b) = 0$

Aplicamos la asociatividad, la conmutatividad, las propiedades del inverso y del neutro para la suma.
Como $(a + b) + [(-a) + (-b)] = 0$ entonces $(-a) + (-b)$ es el opuesto de $a + b$,
y así $-(a + b) = (-a) + (-b)$

8) $a.0 = 0$

La propiedad a demostrar es una igualdad, que obviamente no sabemos si es verdadera hasta demostrarla, por lo tanto **no podemos usarla como hipótesis;** luego partiremos de uno de los miembros de la igualdad y trataremos de llegar al otro.

$a.0 = a.(0 + 0) = a.0 + a.0$

Hasta aquí utilizamos que el cero es neutro, por lo tanto $0 + 0 = 0$, y la distributividad del producto respecto de la suma.
Aplicando la propiedad demostrada en *1)* tenemos que $a.0 = 0$.

Nota: Esta propiedad excluye la posibilidad de que 0 pudiera tener inverso multiplicativo dado que $\nexists\, a \in \mathbb{R}$ tal que $a.0 = 1$ (Nótese que por axioma $1 \neq 0$)

9) $(-1).a = -a$

Aquí hay que demostrar que el opuesto de a es igual al opuesto de 1 por a
Nuevamente, para demostrar que un número es opuesto de otro hay que sumarlos y ver si da 0.

$(-1).a + a = (-1).a + 1.a = (-1 + 1).a = 0.a = 0$

Aplicamos la propiedad del neutro del producto, la distributividad y la *8)*

Luego $(-1).a = -a$

10) $(-a).b = a.(-b) = -(a.b)$

Vamos a demostrar $(-a).b = -(a.b)$, la demostración de la otra igualdad es análoga.

Tenemos que probar que el opuesto de $a.b$ es b por el opuesto de a. Sumemos:

$a.b + (-a).b = (a - a).b = 0.b = 0$

Entonces $-(a.b) = (-a).b$

Comentario: Como tenemos las igualdades $(-a).b = a.(-b) = -(a.b)$, lo escribiremos directamente : $-a.b$

16) $a.b = 0 \Leftrightarrow a = 0 \vee b = 0$ (el producto de dos números es 0 si y sólo si uno de ellos es 0)

Aquí debemos probar dos implicaciones:

$\Leftarrow$) Ésta ya ha sido demostrada en *8)*.

$\Rightarrow$) Supongamos que $a.b = 0$, entonces $a = 0 \vee a \neq 0$.

Si $a = 0$ no hay nada que demostrar.
Si $a \neq 0$, entonces $\exists\, a^{-1}$; multiplicamos m.a.m. la igualdad $a.b = 0$ por a^{-1}: $a^{-1}.a.b = a^{-1}.0 = 0$

como $a^{-1}.a = 1$, entonces $1.b = 0$, de donde $b = 0$

Hasta aquí nos hemos ocupado de los axiomas relativos a las operaciones en $\mathbb{R}$, pero nos falta incorporar los axiomas de *orden.*

En $\mathbb{R}$ definimos un orden total $\leq$ con propiedades que vinculen la relación de orden con las operaciones:
$(\mathbb{R}, \leq)$ es un conjunto totalmente ordenado por lo tanto la relación $\leq$ verifica:

O1) reflexiva: $x \leq x \ \forall\ x \in \mathbb{R}$

O2) antisimétrica: $x \leq y \wedge y \leq x \Rightarrow x = y$

O3) transitiva: $x \leq y \wedge y \leq z \Rightarrow x \leq z$

O4) orden total: $x \leq y \vee y \leq x \ \forall\, x, y \in \mathbb{R}$

que además satisface:

O5) *consistencia del orden respecto de la suma*:
$x \leq y \Rightarrow x + z \leq y + z\,,\ \forall z \in \mathbb{R}$

O6*) consistencia del orden respecto del producto*:
$x \leq y \wedge 0 \leq z \Rightarrow x.z \leq y.z$

Nótese que la consistencia del orden respecto de la suma se verifica cualquiera sea el número real z, mientras que la del producto sólo dice qué ocurre con una desigualdad cuando se multiplica a ambos miembros por un z tal que $0 \leq z$, pero no afirma nada cuando $z \leq 0$.

Cuando un conjunto, como en este caso $\mathbb{R}$, está provisto de dos operaciones y un orden total que verifican **todas** las propiedades que enunciamos (de S1 a S4, de P1 a P4, D, de O1 a O6) se dice que $(\mathbb{R}, +, ., \leq)$ **es un cuerpo ordenado.**

***Notaciones*:** A partir del orden $\leq$ definiremos otras relaciones en $\mathbb{R}$:

I) $x \geq y$ si y sólo si $y \leq x$ ($x \geq y$ se lee *x es mayor o igual que y*)

II) $x < y$ si y sólo si $x \leq y \wedge x \neq y$ ($x < y$ se lee *x menor que y*)

III) $x > y$ si y sólo si $y < x$ sii $x \geq y \wedge x \neq y$ ($x > y$ se lee *x mayor que y*)

Ejercicio: Demostrar que I) es una relación de orden total y que II) e III) son antisimétricas y transitivas pero no reflexivas, luego **no** son órdenes, aunque se denominen *orden estricto.*

***Definiciones*:** Un número real *a* se dice:

positivo si $a > 0$

negativo si $a < 0$

no positivo si $a \leq 0$

no negativo si $a \geq 0$

$\mathbb{R}_{>0} = \{ x / x \in \mathbb{R} \wedge x > 0 \}$ conjunto de reales positivos

$\mathbb{R}_{\geq 0} = \{ x / x \in \mathbb{R} \wedge x \geq 0 \}$ conjunto de reales no negativos

$\mathbb{R}_{<0} = \{ x / x \in \mathbb{R} \wedge x < 0 \}$ conjunto de reales negativos

$\mathbb{R}_{\leq 0} = \{ x / x \in \mathbb{R} \wedge x \leq 0 \}$ conjunto de reales no positivos

Propiedades de los cuerpos ordenados:

20) tricotomía: $\forall a, b \in \mathbb{R}$ se verifica una y sólo una de estas tres condiciones:

$$a < b \vee b < a \vee a = b$$

En particular, todo número real *a* verifica una y sólo una de estas tres condiciones:

$$a > 0 \vee a < 0 \vee a = 0$$

21) consistencia del orden estricto respecto de la suma:

$$x < y \, , z \in \mathbb{R} \Rightarrow x + z < y + z$$

22) $a < b \Rightarrow -b < -a$

23) consistencia del orden estricto respecto del producto:

$$x < y \wedge z > 0 \Rightarrow x.z < y.z$$

24) $a < 0 \Leftrightarrow -a > 0$ (obsérvese que $-a$ indica el opuesto de a , no dice si es positivo o negativo, eso dependerá de cómo sea a)

25) $x < y \wedge z < 0 \Rightarrow x.z > y.z$. ¿Qué sucede con la desigualdad si $z = 0$?

26) $0 < 1$

27) $a > 0 \Leftrightarrow a^{-1} > 0$. ¿Y si $a < 0$?

28) $a < b \wedge c < d \Rightarrow a + c < b + d$

29) $a.b > 0 \Leftrightarrow (a > 0 \wedge b > 0) \vee (a < 0 \wedge b < 0)$

Expresar la equivalencia de $a.b < 0$

30) $a^2 > 0$, $\forall a \neq 0$, ¿ y si $a = 0$?

31) Si $a > 0, b > 0$, entonces $a < b \Leftrightarrow b^{-1} < a^{-1}$

¿ Y si $a < 0 \wedge b < 0$?, ¿ y si $a < 0 \wedge b > 0$?

32) $a^2 + b^2 = 0 \Leftrightarrow a = b = 0$.

Además si $a \neq b$ entonces $a^2 + b^2 > 0$

33) $\nexists x \in \mathbb{R}$, tal que $x^2 + 1 = 0$

34) $\nexists z \in \mathbb{R}$ tal que $x \leq z$, $\forall x \in \mathbb{R}$ ($\mathbb{R}$ no admite cotas superiores)

35) Sean $a > 0$, $b > 0$. Entonces: $a^2 < b^2 \Leftrightarrow a < b$, ¿ y si $a \not> 0 \vee b \not> 0$?

36) Sean $x, y \in \mathbb{R}$, $x < y \Rightarrow x < \dfrac{x+y}{2} < y$

***Demostraciones*:**

21) $x < y$, $z \in \mathbb{R} \Rightarrow x + z < y + z$

Si $x < y \Rightarrow x \leq y \wedge x \neq y$

Por el axioma de consistencia del orden respecto de la suma,

$x \leq y \Rightarrow x + z \leq y + z$, $\forall z \in \mathbb{R}$

como $x + z \leq y + z \Rightarrow x + z < y + z \vee x + z = y + z$

Si $x + z = y + z$

sumando $-z$ a ambos miembros de la igualdad

$x + z - z = y + z - z$

$x + 0 = y + 0$

$x = y$!! (¡absurdo!) pues $x < y$, por lo tanto $x \neq y$

entonces $x + z \neq y + z$

así $x + z < y + z$

24) $\Rightarrow$) Sea $a < 0$

sumando $-a$ m.a.m.:

$-a + a < -a + 0$ (consistencia del orden respecto de la suma)

$-a + a = 0$, $-a + 0 = -a$, luego $0 < -a$.

$\Leftarrow$) la demostración es análoga a la anterior.

25) $x < y \wedge z < 0 \Rightarrow x.z > y.z$ ¿Qué sucede con la desigualdad si $z = 0$?

Sean $x < y \wedge z < 0$

entonces $x < y \wedge -z > 0$

multiplicando por $-z$ a ambos miembros de la desigualdad, por consistencia del orden respecto del producto por números positivos: $x.(-z) < y.(-z)$

por *10)* $-x.z < -y.z$

por *22)* $y.z < x.z$

Cuando $z = 0$, $x.z = y.z = 0$, luego $x.z \not< y.z \wedge x.z \not> y.z$.

26) $0 < 1$

Sabemos de la existencia y unicidad de ambos neutros, y sabemos por el axioma P3 que $0 \neq 1$; por la tricotomía tenemos dos posibilidades mutuamente excluyentes:

$0 < 1 \vee 1 < 0$

Como queremos demostrar que $0 < 1$ debemos ver que es *imposible* que $1 < 0$.

Razonaremos *por el absurdo*, suponiendo que $1 < 0$ y veremos como esta suposición nos lleva a alguna contradicción, por lo cual es imposible que sea verdadera.

Supongamos que $1 < 0$, entonces , por *24)*, tenemos que $-1 > 0$
como -1 es positivo, podemos multiplicar ambos miembros de la desigualdad $1 < 0$ por -1 y ella no varía por *23)*

$(-1).1 < (-1).0$

$(-1).1 = -1$ por ser 1 neutro para el producto

$(-1).0 = 0$ por *8)*

luego $-1 < 0$!! (absurdo!)

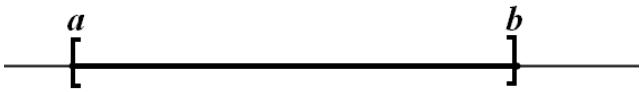
(Obtuvimos la contradicción: $-1 < 0 \wedge -1 > 0$).

Por lo tanto no es posible que sea $1 < 0$, y como $0 \neq 1$, la única alternativa que queda es que $0 < 1$.

Intervalos acotados en $\mathbb{R}$

***Definiciones*:** Sean $a, b \in \mathbb{R}$. Llamaremos:
Intervalo cerrado a, b, y lo notaremos $[a, b]$, al subconjunto de $\mathbb{R}$:

$$[a, b] = \{ x / \ a \leq x \leq b \}$$



Notación: $a \leq x \leq b$ simboliza $a \leq x \wedge x \leq b$

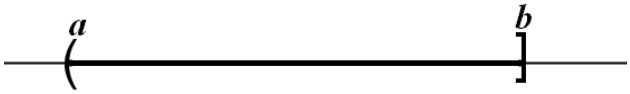
Intervalo abierto a, b, y lo notaremos (a, b) , al subconjunto de $\mathbb{R}$:

$$(a, b) = \{ x / \ a < x < b \}$$

Intervalos semiabiertos a, b , y los notaremos $[a, b)$ y $(a, b]$, a los subconjuntos de $\mathbb{R}$:

$$[a, b) = \{ x / \ a \leq x < b \}$$

$$(a, b] = \{ x / \ a < x \leq b \}$$



Nótese que si $b < a$ **todos** estos subconjuntos son **vacíos,** por lo tanto carece de interés considerarlos, luego siempre pensaremos que $a \leq b$.

No obstante, cuando $a = b$, $[a, b] = \{a\}$, y los demás son vacíos.

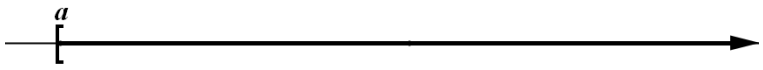
Sólo cuando $a < b$ tenemos que todos estos subconjuntos son **no vacíos**, y más aun, infinitos (en el sentido que no tienen una cantidad finita de elementos)

La denominación de *intervalos acotados* proviene del hecho que son conjuntos acotados para el orden $\leq$, pues si $a < b$, en todos los casos a es cota inferior y b cota superior.

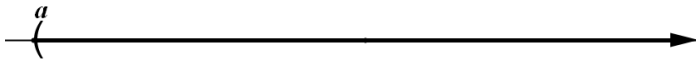
Intervalos no acotados en $\mathbb{R}$

***Definiciones*:** Sea $a \in \mathbb{R}$. Llamaremos:

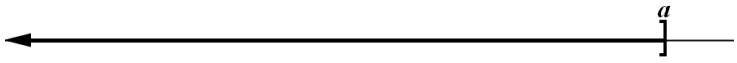
Intervalo cerrado con origen en a, y lo notaremos $[a, \infty)$, al subconjunto de $\mathbb{R}$

$[a, \infty) = \{ x / \ x \geq a \}$ 

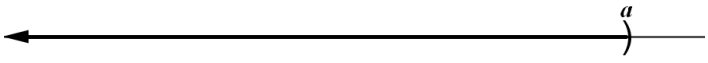
Intervalo abierto con origen en a, y lo notaremos (a, ∞) , al subconjunto de $\mathbb{R}$

$(a, \infty) = \{ x / \ x > a \}$ 

Intervalo cerrado con extremo en a, y lo notaremos $(-\infty, a]$, al subconjunto de $\mathbb{R}$

$(-\infty, a] = \{ x / \ x \leq a \}$ 

Intervalo abierto con extremo en a, y lo notaremos $(-\infty, a)$, al subconjunto de $\mathbb{R}$

$(-\infty, a) = \{ x / \ x < a \}$ 

Ejercicio de aplicación: Demostraremos que 0 = *ínf A*, y 1 = *supA* , cuando $A = (0, 1)$.

***Demostración*:** $(0, 1) = \{ x / \ 0 < x < 1 \}$

Por definición $0 < x$, $\forall x \in A$, luego 0 es cota inferior de *A*.

Para ver que 0 = *ínf A*, hay que ver que 0 es *la mayor* de las cotas inferiores de *A*, o lo que es equivalente, que ningún $z > 0$ puede ser cota inferior de *A*.

Sea $z > 0$; si $z > 1$ claramente no es cota inferior de *A* pues $\frac{1}{2} < 1 < z \wedge \frac{1}{2} \in A$.

Si $0 < z \leq 1$, entonces $0 < \frac{z}{2} < z \leq 1$, luego $\frac{z}{2} \in (0, 1) = A$, por lo tanto z no es cota inferior de *A*. Así $0 = ínf\, A$.

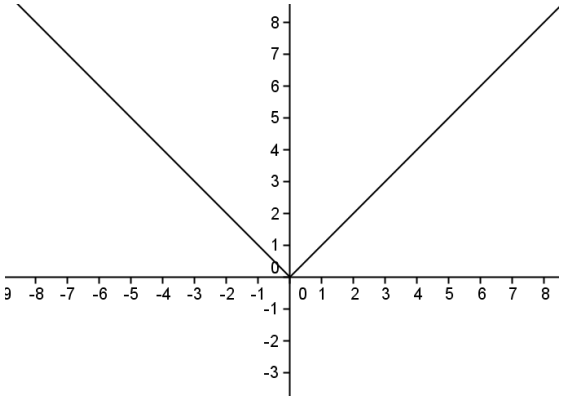
Para demostrar que 1 = *sup A* se razona en forma análoga.

Valor absoluto

Vamos a definir una función de $\mathbb{R} \to \mathbb{R}$, llamada *valor absoluto,* que a cada $x \in \mathbb{R}$ le asigna el número real $|x|$ (valor absoluto de *x*) definido por:

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

La gráfica de la función valor absoluto es:



Propiedades:

1) $|x| \geq 0$, $\forall x \in \mathbb{R}$. Además $|x| = 0$ si y sólo si $x = 0$ (O lo que es equivalente: $|x| > 0$ $\forall x \neq 0$)

2) $|x| = |-x|$, $\forall x \in \mathbb{R}$

3) $|x.y| = |x|.|y|$, $\forall x, y \in \mathbb{R}$

4) $|x^2| = x^2$, $\forall x \in \mathbb{R}$

5) $-|x| \leq x \leq |x|$, $\forall x \in \mathbb{R}$

6) Para $r > 0$, $|x| \leq r \Leftrightarrow -r \leq x \leq r$

7) $|x + y| \leq |x| + |y|$, $\forall x, y \in \mathbb{R}$ (*Desigualdad Triangular*)

Establecer condiciones necesarias y suficientes sobre x e y para que se verifique la igualdad.

8) $|x - y| \geq ||x| - |y||$, $\forall x, y \in \mathbb{R}$.

Establecer condiciones necesarias y suficientes sobre *x* e *y* para que se verifique la igualdad.

Demostraremos algunas propiedades, a modo de ejemplo, y las demás quedan como ejercicios.

***Demostración*:**

1) $|x| \geq 0$, $\forall x \in \mathbb{R}$

Como la definición de $|x|$ depende de cómo sea x en relación con el cero, debemos analizar ambas situaciones, para demostrar que se verifica lo postulado.

Si $x \geq 0$, entonces $|x| = x$, por definición, entonces $|x| \geq 0$.
Si $x < 0$, entonces $|x| = -x$, por definición. Si $x < 0 \Rightarrow -x > 0$,

luego $|x| > 0$, y por lo tanto $|x| \geq 0$.
Así $|x| \geq 0 \ \forall x \in \mathbb{R}$
Ahora hay que demostrar que: $|x| = 0$ si y sólo si $x = 0$, o lo que es equivalente : $|x| > 0 \ \forall x \neq 0$ (pues por definición $|0| = 0$).

Si $x \neq 0$ entonces $x > 0 \vee x < 0$;
si $x > 0$, $|x| = x > 0$, luego $|x| > 0$
si $x < 0$, $|x| = -x > 0$, luego $|x| > 0$
$\therefore |x| > 0 \ \forall x \neq 0$

5) $-|x| \leq x \leq |x|$, $\forall x \in \mathbb{R}$
Si $x \geq 0$, entonces $|x| = x$, luego $x \leq |x|$.
Además $|x| \geq 0$ entonces $-|x| \leq 0$, luego $-|x| \leq 0 \leq x \leq |x|$, como queríamos demostrar.

Si $x < 0$, entonces $|x| = -x$, entonces $-|x| = x$, y así $-|x| \leq x$.
Además $x < 0 < |x|$, por lo tanto $-|x| \leq x \leq |x|$, como queríamos demostrar.

6) Para $r > 0$, $|x| \leq r \Leftrightarrow -r \leq x \leq r$
Aquí debemos probar dos implicaciones.

$\Rightarrow) \ |x| \leq r \Rightarrow -r \leq x \leq r$

Si $x \geq 0$, entonces $|x| = x$, y como $|x| \leq r$, entonces $x \leq r$.
Además $r > 0 \Rightarrow -r < 0$, entonces $-r < 0 \leq x \leq r$.

Si $x < 0$, entonces $|x| = -x \leq r$, entonces $-r \leq x < 0 < r$.
Así si $|x| \leq r$ entonces $-r \leq x \leq r$.

$\Leftarrow) \ -r \leq x \leq r \Rightarrow |x| \leq r$
Para ver que $|x| \leq r$ con la hipótesis dada, debemos analizar qué sucede con los x negativos y no negativos.

Si $x \geq 0$, entonces $|x| = x \leq r$, por hipótesis , entonces $|x| \leq r$.
Si $x < 0$, entonces $|x| = -x$, como $-r \leq x$ por hipótesis, tenemos que $-x \leq r$,
luego $|x| \leq r$.

7) $|x+y| \leq |x| + |y|$, $\forall\, x, y \in \mathbb{R}$ (*Desigualdad Triangular*)

Por *5)* $-|x| \leq x \leq |x|$

y $-|y| \leq y \leq |y|$

sumando m.a.m. $-|x| - |y| \leq x + y \leq |x| + |y|$

$-(|x| + |y|) \leq x + y \leq |x| + |y|$

como $|x| + |y| \geq 0$, aplicando *6)* tenemos que $|x+y| \leq |x| + |y|$.

Nota: De las propiedades *1)* y *2)* se desprende que la $Im(|\cdot|) = \mathbb{R}_{\geq 0}$ y que la función **no** es inyectiva.

Función Distancia:

Queremos definir una función que cumpla todas las propiedades que intuitivamente le asignamos al concepto de distancia:

- la distancia entre dos puntos es un valor no negativo, y sólo es nula cuando los puntos coinciden.
- la distancia entre *a* y *b* es la misma que entre *b* y *a*.
- la distancia entre dos puntos *a* y *b* siempre es menor o igual que la distancia de *a* a cualquier otro punto *c* más la distancia de ese punto *c* al *b*.

Para cumplir nuestro cometido en $\mathbb{R}$ haremos uso de la función **valor absoluto.**

***Definición*:** Llamamos *función distancia* en $\mathbb{R}$ a la función:

$$d : \mathbb{R} \times \mathbb{R} \to \mathbb{R}_{\geq 0}$$
$$(a, b) \to |a - b|$$

***Propiedades*:**

i) $d(a, b) \geq 0 \;\; \forall\, a, b \in \mathbb{R}$; y $d(a, b) = 0$ sii $a = b$

ii) $d(a, b) = d(b, a) \;\; \forall\, a, b \in \mathbb{R}$

iii) $d(a, b) \leq d(a, c) + d(c, b) \;\; \forall\, a, b, c \in \mathbb{R}$

***Demostración*:** Se deja como ejercicio.

***Para pensar*:** Dados *a* y *b* en $\mathbb{R}$, ¿ para qué valores $c \in \mathbb{R}$ se verifica la igualdad en iii)? ¿Puede establecer las condiciones necesarias y suficientes que deben cumplir esos números?

***Ejercicios*:**

1) Sea $r > 0$, obsérvese que, por propiedades de la función valor absoluto
$[-r, r] = \{ x \ / \ d(x,0) \leq r \}$

Para $a \leq b$, ¿puede encontrar un c y un s en $\mathbb{R}$ tales que $[a, b] = \{ x \ / \ d(x,c) \leq s \}$?

2) Para el c y el s encontrados en 1) ¿cómo escribiría el conjunto de los x tales que $d(x, c) \geq s$?

Ejercicios: En lo que sigue, $a, b, c, d \in \mathbb{R}$

1.) Si $b \neq 0$ entonces $\frac{0}{b} = 0$

2.) Si $b \neq 0 \wedge d \neq 0$ entonces $\frac{a}{b} = \frac{c}{d}$ si y sólo si $a \,.\, d = b \,.\, c$

3.) Si $b \neq 0 \wedge c \neq 0$ entonces $\frac{a}{b/c} = \frac{a \cdot c}{b}$

4.) Si $b \neq 0 \wedge d \neq 0$ entonces $\left(\frac{b}{d}\right)^{-1} = \frac{d}{b}$

5.) Si $b \neq 0$, $-\left(\frac{a}{b}\right) = \frac{(-a)}{b} = \frac{a}{(-b)} \wedge \frac{(-a)}{(-b)} = \frac{a}{b}$

6.) Si $b \neq 0 \wedge d \neq 0$ entonces $\frac{a}{b} \cdot \frac{c}{d} = \frac{a \cdot c}{b \cdot d}$

7.) Si $b \neq 0$, $d \neq 0 \wedge \frac{a}{b} = \frac{c}{d}$

entonces $\frac{a+b}{b} = \frac{c+d}{d} \wedge \frac{a-b}{b} = \frac{c-d}{d}$

Si además $a - b \neq 0 \wedge c - d \neq 0$ entonces $\frac{a+b}{a-b} = \frac{c+d}{c-d}$

Si además $b + d \neq 0$ entonces $\frac{a}{b} = \frac{a+c}{b+d}$

8.) Si $b \neq 0 \wedge d \neq 0$ entonces $\frac{a}{b} \pm \frac{c}{d} = \frac{a \cdot d \pm b \cdot c}{b \cdot d}$

9.) Si $a < b$, para todo $c \in \mathbb{R}$, $a - c < b - c$

10.) Si $a + a = 0$ entonces $a = 0$

11.) Si $a + a + a = 0$ entonces $a = 0$

12.) Demostrar las siguientes propiedades:

12.1) $a \leq b \ \wedge \ -a \leq b \ \Rightarrow \ |a| \leq b$

12.2) $|a + b + c| \leq |a| + |b| + |c|$

12.3) $|a| - |b| \leq |a - b|$

12.4) Si $a \neq 0$ entonces $|a|^{-1} = |a^{-1}|$

12.5) Si $b \neq 0$ entonces $\left|\frac{a}{b}\right| = \frac{|a|}{|b|}$

12.6) $2 \cdot |a \cdot b| \leq a^2 + b^2$

12.7) $2 \cdot |a \cdot b| = a^2 + b^2$ *si y sólo si* $|a| = |b|$

13.) Determinar todos los $a \in \mathbb{R}$, tales que $|a^2 + a + 1| = a^2 + a + 1$

14.) i) Demostrar que para $a \in \mathbb{R}$, $a^3 = 1 \Leftrightarrow a = 1$

ii.) Demostrar que en general $a^3 = b^3 \Leftrightarrow a = b$

15.) Sean $x, y \in \mathbb{R}$ tales que $0 < y < x$. Probar que $y < \frac{2xy}{x+y} < x$

16.) Demostrar que $\forall a > 0$, $a + \frac{1}{a} \geq 2$

17.) Sean $x, y \in \mathbb{R}_{>0}$, demostrar que:

i. Si $x < 1 < y \Rightarrow x.y + 1 \leq x + y$

ii. Si $x.y.z = 1 \Rightarrow x + y + z \geq 3$

18.) Demostrar que $\forall x, y, z \in \mathbb{R}_{>0}$ $(x + y + z)(\frac{1}{x} + \frac{1}{y} + \frac{1}{z}) \geq 9$

19.) Demostrar que si $a, b, c \in \mathbb{R}_{>0}$ son tales que $a + b + c = 1$ entonces

$$\left(\frac{1}{a} - 1\right)\left(\frac{1}{b} - 1\right)\left(\frac{1}{c} - 1\right) \geq 8$$

20.) ¿Existe $a \in \mathbb{R}$ tal que:

i. $1 - \frac{1}{1 + \frac{1}{a}} = \frac{1}{a}$?

ii. $1 - \frac{1}{1 + \frac{1}{a}} = -\frac{1}{a}$? Justificar.

21.) ¿Existen $a, b \in \mathbb{R}$ tales que $\frac{1}{a+b} = \frac{1}{a} + \frac{1}{b}$? Justificar.

22.) Probar que $|x| \geq y \Leftrightarrow x \geq y \vee -x \geq y$

(o sea $|x| \geq y \Leftrightarrow y \leq x \vee x \leq -y$)

23.) Probar que $x^2 < y^2$ si y sólo si $|x| < |y|$

24.) Determinar todos los $x \in \mathbb{R}$ tales que:

a) $\dfrac{1}{x^2+2}<3$ b) $\dfrac{1}{x+3}\le 6$ c) $|2-6x|+|3x-1|>4$

d) $\dfrac{|x+3|}{|2x-1|}<1$ e) $\dfrac{|4x-8|}{1-|x-2|}<2$ f) $|x-3|>1+|x+1|$

g) $\dfrac{x-3}{|x|+x}<2$ h) $|x+x^{-1}|\le 2$ i) $\dfrac{x}{|x+1|}\le 2$

25.) Demostrar:

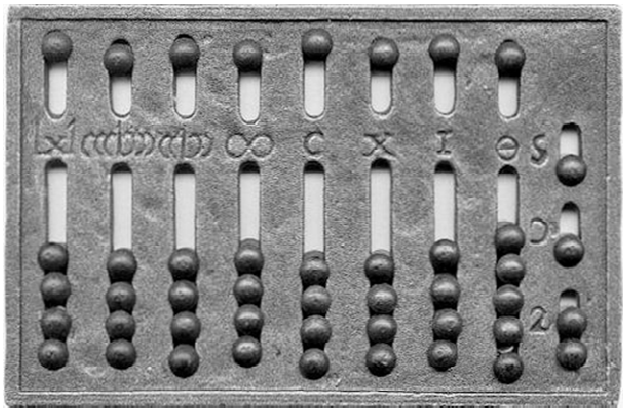
i. $x^3>1 \Leftrightarrow x>1$ ii. $x^3<-1 \Leftrightarrow x<-1$

iii. $0<x<1 \Leftrightarrow 0<x^3<1$ iv. $-1<x<0 \Leftrightarrow -1<x^3<0$

CAPÍTULO IV

NÚMEROS NATURALES

"*Dios creó los números naturales, el resto es obra del hombre*"
(Leopoldo Kronecker)



Cuando definimos axiomáticamente el conjunto $\mathbb{R}$ de números reales, con sus operaciones y su orden, observamos que teníamos dos puntos distinguidos: los neutros de la suma y del producto, 0 y 1 respectivamente, impusimos que fueran distintos, y demostramos que $0 < 1$. La consistencia del orden respecto de la suma nos lleva a que $0 + 1 < 1 + 1$, y si llamamos $2 = 1 + 1$, esto es que $1 < 2$. También se verifica que $1 + 1 < 2 + 1$, llamando $3 = 2 + 1$, tenemos que $2 < 3$, y así siguiendo, llamando $4 = 3 + 1$, tenemos que $3 < 4$, que $4 < 5$, para $5 = 4 + 1$, y así sucesivamente.

Así comprobamos que podemos obtener números cada vez más grandes, lo que muestra que el conjunto $\mathbb{R}$ es infinito, y que, además, por este mecanismo obtenemos los números que conocemos como *naturales*. La descripción que acabamos de hacer sirve para darnos una idea intuitiva del *Conjunto de Números Naturales*, pero no puede ser considerada una definición, por lo que debemos encontrar la manera de definir dicho conjunto.

LA IDEA DE GIUSEPPE PEANO (1858-1932)

Lentamente, con el avance de la civilización, la humanidad se apoderó de ese modelo abstracto de contar (uno, dos, tres,...) que son los números naturales, conjunto al que denominamos con la letra ***N****. La esencia de su caracterización reside en la palabra* ***sucesor****. Intuitivamente, decimos que un número natural m es sucesor de otro número natural n, si m sigue inmediatamente a n no habiendo entre ellos ningún otro número natural. Del mismo modo, y ante esta situación, decimos también que n es* ***antecesor*** *de m.*

El uso y propiedades del término ***sucesor****, al que nos referimos, están regidos por las reglas conocidas como* ***Axiomas de Peano*** *que enunciamos a continuación:*

- ***1)*** 1 *es un número*
- ***2)*** *Si a es un número, su sucesor (a+*1*) es un número*
- ***3)*** *Si dos números son iguales, entonces sus sucesores también lo son*
- ***4)*** 1 *no es sucesor de ningún número*
- ***5)*** *Toda propiedad que pertenece al número* 1*, si al pertenecer al número x, pertenece también al sucesor, es un propiedad de todos los números*

Definición**:** Un subconjunto $A \subset \mathbb{R}$ se dice *inductivo* si:
i) $1 \in A$
ii) $x \in A \Rightarrow x + 1 \in A$

Ejemplos**:**

1) $A_0 = [0, \infty) = \{ x / \ x \geq 0 \}$ **es** inductivo, porque:

i) $1 \in A_0$ pues $1 \geq 0$

ii) $x \in A_0 \Rightarrow x + 1 \in A_0$. Vamos a demostrarlo.

Si $x \in A_0$ entonces $x \geq 0$,

Luego $x + 1 \geq x \geq 0$,

así $x + 1 \in A_0$

2) $A_1 = [1, \infty) = \{ x / \ x \geq 1 \}$ **es** inductivo. Demostrémoslo.

i) $1 \in A_1$ pues $1 \geq 1$

ii) $x \in A_1 \Rightarrow x + 1 \in A_1$?

Si $x \in A_1$ entonces $x \geq 1$,

luego $x + 1 \geq x \geq 1$,

así $x + 1 \in A_1$

3) $B_0 = (0, \infty)$ **es** inductivo, y la demostración es análoga a la de 1)

4) $B_1 = (1, \infty) = \{ x / \ x > 1 \}$ **no** es inductivo pues $1 \notin B_1$

5) $B_2 = [2, \infty)$ **no** es inductivo pues $1 \notin B_2$

6) $A_2 = \{1\} \cup [2, \infty)$ **es** inductivo pues:

i) $1 \in A_2$

ii) $x \in A_2 \Rightarrow x + 1 \in A_2$?

Si $x \in A_2 \Rightarrow x = 1 \vee x \geq 2$

Si $x = 1$, entonces $x + 1 = 2 \geq 2$, luego $x + 1 \in A_2$

Si $x \geq 2$, entonces $x + 1 \geq x \geq 2$, luego $x + 1 \in A_2$

Así si $x \in A_2 \Rightarrow x + 1 \in A_2$

7) $B_3 = \{1\} \cup (2, \infty)$ **no** es inductivo pues $1 \in B_3 \ \wedge \ 1 + 1 = 2 \notin B_3$

8) $A_3 = \{1, 2\} \cup [3, \infty)$ **es** inductivo, y la demostración es análoga a la de 6).

9) Igual que antes, podemos ver que los conjuntos $\{1, 2, 3\} \cup [4, \infty)$,
$\{1, 2, 3, 4\} \cup [5, \infty)$, $\{1, 2, 3, 4, 5\} \cup [6, \infty)$,….. son todos inductivos.

Si llamamos $\Gamma = \{ A \ / \ A \subset R$ inductivo $\}$ (el conjunto de todos los subconjuntos inductivos de $\mathbb{R}$) y lo ordenamos por inclusión, podemos definir:

***Definición*:** Llamamos *conjunto de Números Naturales*, y lo simbolizamos con $\mathbb{N}$, al "menor" subconjunto inductivo de $\mathbb{R}$.

Esto es, en el conjunto ordenado $(\Gamma, \subset)$, se define $\mathbb{N} = mín\, \Gamma$.
Por lo tanto $\mathbb{N}$ verifica:
i) $\mathbb{N}$ es inductivo
ii) si $A \subset \mathbb{R}$ es inductivo, entonces $\mathbb{N} \subset A$.

Sabemos que en un conjunto ordenado el mínimo puede no existir, así que debemos demostrar que un tal mínimo existe, para garantizar que esta definición tenga sentido.

***Proposición*:** El conjunto ordenado $(\Gamma, \subset)$ tiene mínimo.

***Demostración*:** Sea $H = \bigcap_{A \in \Gamma} A = \{ x / \ x \in A, \ \forall A \in \Gamma \}$.
Vamos a demostrar que H es inductivo.
i) $1 \in H$ pues $1 \in A$, $\forall A \in \Gamma$ (dado que todos los A son inductivos, por definición de Γ).
ii) $x \in \mathrm{H} \Rightarrow x + 1 \in H$?
Si $x \in H$ entonces $x \in A$, $\forall A \in \Gamma$ (por definición de H),
como A es inductivo $\forall A \in \Gamma$, entonces $x + 1 \in A$, $\forall A \in \Gamma$, luego $x + 1 \in H$.
Por lo tanto H es inductivo.

Además, por definición de *H*, tenemos que $H \subset A \ \forall A \in \Gamma$, luego $H = mín\ \Gamma$.

Hemos demostrado que el mínimo en $(\Gamma, \subset)$ existe, con lo cual la definición dada tiene sentido, y naturalmente el conjunto $\mathbb{N} = H$.

Veremos que esta definición de $\mathbb{N}$ es compatible con la idea intuitiva que tenemos de los números naturales.

***Propiedad 1*:** Todo número natural *n* es positivo.

***Demostración*:** Si $n \in \mathbb{N}$, como $\mathbb{N} \subset B_0 = (0, \infty)$, por ser B_0 inductivo, entonces $n \in (0, \infty)$, luego $n > 0$.

***Propiedad 2*:** Si $n \in \mathbb{N}$, entonces $n \geq 1$.

***Demostración*:** Si $n \in \mathbb{N}$, como $\mathbb{N} \subset A_1 = [1, \infty) = \{ x / \ x \geq 1 \}$, por ser A_1 inductivo, entonces $n \in [1, \infty)$, luego $n \geq 1$.

***Propiedad 3*:** Si $n \in \mathbb{N} \ \wedge \ n \neq 1 \Rightarrow n \geq 2$ ($\nexists\ n \in \mathbb{N}$, tal que $1 < n < 2$).

***Demostración*:** Si $n \in \mathbb{N}$, como $\mathbb{N} \subset A_2 = \{ 1 \} \cup [2, \infty)$, por ser A_2 inductivo, entonces
$n = 1 \vee n \geq 2$
Luego, si $n \neq 1 \Rightarrow n \geq 2$.

De la misma forma podríamos demostrar que si $n \in \mathbb{N} \ \wedge \ n \neq 1 \ \wedge \ n \neq 2 \Rightarrow n \geq 3$, o sea que $\nexists\ n \in \mathbb{N}$, tal que $1 < n < 2$, y $\nexists\ n \in \mathbb{N}$, tal que $2 < n < 3$, y así sucesivamente; lo que aun no podemos demostrar, pero ya lo haremos, es que si $n \in \mathbb{N}$, $\nexists\ m \in \mathbb{N}$, tal que $n < m < n + 1$, cualquiera sea *n* .
Para demostrar ésta y otras propiedades del conjunto $\mathbb{N}$, enunciaremos el *Principio de Inducción Completa,* que se desprende directamente de la definición del conjunto de Números Naturales, y brinda una herramienta eficaz para ese propósito.

Principio de inducción completa:

> *..."La **inducción** es un modo de razonar que conduce al descubrimiento de leyes generales a partir de la observación de casos particulares y de sus combinaciones. Se emplea en todas las ciencias, aún en matemáticas. En cuanto a la **inducción matemática** no se emplea más que en matemáticas a fin de demostrar un cierto tipo de teoremas. Es bastante molesto que las dos expresiones estén ligadas, ya que entre los dos procedimientos no existe más que un lazo lógico, extremadamente sutil. Existe, sin embargo, un cierto lazo práctico, puesto que a menudo se emplean los dos métodos al mismo tiempo"... (George Polya: "Cómo plantear y resolver problemas).*

La minimalidad de $\mathbb{N}$ como subconjunto inductivo de $\mathbb{R}$, tiene como consecuencia otra propiedad:

- si $A \subset \mathbb{R}$ es inductivo, entonces $\mathbb{N} \subset A$.

implica que :

- si $H \subset \mathbb{N}$ es inductivo, entonces $H = \mathbb{N}$.

A esta formulación la denominamos: *Principio de Inducción Completa.*

***Principio de Inducción Completa*:** Si $H \subset \mathbb{N}$ es inductivo, entonces $H = \mathbb{N}$.

Utilizaremos el Principio de Inducción Completa para demostrar propiedades sobre el conjunto de Números Naturales.

***Teorema*:** Si $n, m \in \mathbb{N} \Rightarrow n + m \in \mathbb{N} \wedge n.m \in \mathbb{N}$.

***Demostración*:** Nos valdremos del Principio de Inducción Completa para demostrarlo.

Sea $m \in \mathbb{N}$ fijo. Definimos el conjunto H_m de la siguiente manera:

$H_m = \{n \in \mathbb{N} / n + m \in \mathbb{N}\}$

Por definición $H_m \subset \mathbb{N}$. Veamos que H_m es inductivo:

i) $1 \in H_m$ pues si $m \in \mathbb{N}$, entonces $m + 1 \in \mathbb{N}$, por ser $\mathbb{N}$ inductivo.

ii) $n \in H_m \Rightarrow n + 1 \in H_m$?

Si $n \in H_m$, por definición de H_m, $n + m \in \mathbb{N}$,

como $\mathbb{N}$ es inductivo, $n + m \in \mathbb{N} \Rightarrow (n + m) + 1 \in \mathbb{N}$, $(n + m) + 1 = (n + 1) + m$

por asociatividad y conmutatividad de la suma de números reales luego $(n + 1) + m \in \mathbb{N}$,

entonces $n + 1 \in H_m$

Por lo tanto H_m es inductivo, entonces $\mathbb{N} \subset H_m$, pero $H_m \subset \mathbb{N}$, por lo tanto $H_m = \mathbb{N}$.

Luego $\forall\, n \in \mathbb{N}\ n + m \in \mathbb{N}$, y esto es $\forall\, m \in \mathbb{N}$, entonces $n + m \in \mathbb{N}$, $\forall\, n, m \in \mathbb{N}$

Establecida la veracidad de que $n + m \in \mathbb{N}$, $\forall\, n, m \in \mathbb{N}$, demostraremos que

$n.m \in \mathbb{N}\ \forall\, n, m \in \mathbb{N}$. Lo haremos nuevamente usando el Principio de Inducción Completa.

Sea $m \in \mathbb{N}$ fijo, definimos el conjunto G_m como sigue: $G_m = \{n \in \mathbb{N} / m.n \in \mathbb{N}\}$

Por definición $G_m \subset \mathbb{N}$. Veamos que G_m es inductivo:

i) $1 \in G_m$ pues como $m \in \mathbb{N}$, entonces $m.1 = m \in \mathbb{N}$.

ii) $n \in G_m \Rightarrow n + 1 \in G_m$?

Si $n \in G_m$, por definición de G_m, $n.m \in \mathbb{N}$,

por lo visto anteriormente , como $m \in \mathbb{N}$, $n.m + m \in \mathbb{N} \Rightarrow (n + 1).m \in \mathbb{N}$,

pues $(n + 1).m = n.m + m$ por la distributividad del producto respecto de la suma de los números reales, luego $(n + 1).m \in \mathbb{N}$, entonces $n + 1 \in G_m$

Por lo tanto G_m es inductivo, entonces $\mathbb{N} \subset G_m$, pero $G_m \subset \mathbb{N}$, por lo tanto $G_m = \mathbb{N}$.

Luego $\forall\, n \in \mathbb{N}\ n.m \in \mathbb{N}$, y esto es $\forall\, m \in \mathbb{N}$, entonces $n.m \in \mathbb{N}$, $\forall\, n, m \in \mathbb{N}$

El teorema establece que la suma y el producto de números naturales es un número natural, o lo que es equivalente, que la suma y el producto son *dos operaciones* en $\mathbb{N}$:

$+: \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ $\qquad$ $.: \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$

$(n, m) \rightarrow n + m$ $\qquad$ $(n, m) \rightarrow n.m$

son dos funciones, que verifican las siguientes propiedades:

Suma:

- ✓ asociativa
- ✓ conmutativa

Producto:

- ✓ asociativa
- ✓ conmutativa
- ✓ tiene elemento neutro
- ✓ distributividad del producto respecto de la suma.

Nota: Todas estas propiedades, excepto la existencia del neutro para el producto, se verifican porque los naturales son números reales.
El neutro de la suma, el 0, no es número natural, por la propiedad 1; de igual forma, si $n \in \mathbb{N}$, por la misma propiedad, $n > 0$, entonces $-n < 0$, luego $-n \notin \mathbb{N}$, de aquí que, no solamente no se cumple que todo número natural tenga un inverso aditivo en $\mathbb{N}$, sino que **ningún** número natural tiene inverso aditivo en $\mathbb{N}$.

Con respecto al inverso multiplicativo, si $n \in \mathbb{N}$ y $n \neq 1 \Rightarrow n > 1$, con lo cual $n^{-1} = \frac{1}{n} < 1$, luego $n^{-1} \notin \mathbb{N}$, por propiedad 2. Por lo tanto, el único natural con inverso en $\mathbb{N}$ es el 1, y $1^{-1} = 1$ pues 1.1=1.

***Comentarios*:** Si $n, m \in \mathbb{N}$ debemos preguntarnos si $n - m \in \mathbb{N}$ y si $n \,.\, m^{-1} = \frac{n}{m} \in \mathbb{N}$.
Algunas respuestas estamos en condiciones de dar, por ejemplo si $n < m$, se verifica que $n - m < 0$, y $\frac{n}{m} < 1$ entonces $n - m \notin \mathbb{N}$ y $\frac{n}{m} \notin \mathbb{N}$. Para $n = m$, $n - m = 0 \notin \mathbb{N}$ y $\frac{n}{m} = 1 \in \mathbb{N}$. Cuando $n > m$ tenemos que $n - m > 0$ y que $\frac{n}{m} > 1$ pero esas propiedades no dicen que sean números naturales, sólo dicen que podrían serlo. Veamos si podemos precisar algo más.

Criterio de Inducción Completa:

A partir del Principio de Inducción Completa estamos en condiciones de formular una herramienta para demostrar *por inducción* propiedades sobre el conjunto de Números Naturales: *el Criterio de Inducción Completa* .

***Criterio*:** Sea P(n) una función proposicional con dominio en $\mathbb{N}$ (esto es P es una función que a cada $n \in \mathbb{N}$ le asigna una *proposición* P(n) que, como tal, tiene un valor de verdad : verdadera "V", o falsa "F")
Supongamos que P verifica:

i. P(1) es V

ii. $P(n)\ V \Rightarrow P(n+1)\ V$

Entonces, podemos afirmar que $P(n)$ es V $\forall n \in \mathbb{N}$

"Si tuviéramos las 28 fichas de un dominó y las pusiéramos todas de pie, en fila india, de manera que si cae una, cae con seguridad la siguiente, ocurriría sin lugar a dudas que si alguien tirara la primera hacia la segunda ¡caerían todas!"

Miguel de Guzmán: "Aventuras Matemáticas"

***Demostración*:** Usaremos el Principio de Inducción para demostrarlo.

Sea $H = \{ n \in \mathbb{N} \ / \ P(n) \text{ es V} \} \subset \mathbb{N}$

Veamos que H es inductivo.

a) $1 \in H$ pues P(1) es V por i.

b) $n \in H \Rightarrow n+1 \in H$?

Si $n \in H \Rightarrow P(n)$ es V ,

por ii. $P(n)\ V \Rightarrow P(n+1)\ V$

Luego $n+1 \in H$

Por lo tanto H es inductivo, con lo cual $\mathbb{N} \subset H$, y así $\mathbb{N} = H$.

Por lo tanto $P(n)$ es V $\forall n \in \mathbb{N}$.

***Teorema*:** Sean $n , m \in \mathbb{N}$. Si $m < n$ entonces $n - m \in \mathbb{N}$.

***Demostración*:** Probaremos primero un Lema auxiliar.

***Lema*:** Si $n \in \mathbb{N} \ \wedge \ n \neq 1$ entonces $\exists m \in \mathbb{N}$ tal que $m + 1 = n$ (Esto es equivalente a decir que si $n \in \mathbb{N} \ \wedge \ n > 1 \Rightarrow n - 1 \in \mathbb{N}$).

***Demostración del Lema*:** Sea $H = \{ 1 \} \cup \{ n+1 \ / \ n \in \mathbb{N} \} \subset \mathbb{N}$,

H es inductivo (la demostración queda como ejercicio), entonces $\mathbb{N} = H$.

Luego si $k \in \mathbb{N} \ \wedge \ k \neq 1 \Rightarrow k \in \{ n+1 \ / \ n \in \mathbb{N} \}$, así $\exists m \in \mathbb{N}$ tal que $m + 1 = k$.

***Demostración del Teorema*:**

Sea $P(n)$ la función proposicional:

$P(n)$: si $m \in \mathbb{N} \ \wedge \ m > n \Rightarrow m - n \in \mathbb{N}$.

Veamos si cumple las condiciones i. e ii. del Criterio.

i. P(1) es V ?

Si $m \in \mathbb{N} \ \wedge \ m > 1$, por el Lema $\exists h \in \mathbb{N}$ tal que $h + 1 = m$, entonces $m - 1 = h \in \mathbb{N}$.

Por lo tanto P(1) es V.

ii. P(n) V $\Rightarrow$ P($n+1$) V?

Si P(n) es V , $\forall\, m \in \mathbb{N}$ tal que $m > n$ se verifica que $m - n \in \mathbb{N}$ (*Hipótesis Inductiva*).

Para ver que P($n+1$) es verdadera debemos ver que si $k \in \mathbb{N} \wedge k > n+1$, entonces $k-(n+1) \in \mathbb{N}$.

Sea $k \in \mathbb{N}$ tal que $k > n+1 > 1$, entonces $k-1 > n$ y por el Lema $k-1 \in \mathbb{N}$.

Por *Hipótesis Inductiva* si $k-1 \in \mathbb{N} \wedge k-1 > n$ entonces $(k-1)-n \in \mathbb{N}$.

Pero $(k-1)-n = k-(n+1)$, luego $k-(n+1) \in \mathbb{N}$, y así P($n+1$) es V.

Luego P(n) es V $\forall\, n \in \mathbb{N}$, por lo tanto, cualquiera sea $n \in \mathbb{N}$, si $m \in \mathbb{N} \wedge m > n$ entonces $m - n \in \mathbb{N}$.

***Corolario*:** Sea $n \in \mathbb{N}$, si $m \in \mathbb{N} \wedge n < m$ entonces $n+1 \leq m$ (Esto equivale a decir que si $n \in \mathbb{N}$ $\nexists\, k \in \mathbb{N}$ tal que $n < k < n+1$, o sea " entre dos números naturales consecutivos no existe ningún número natural").

***Demostración*:** Si $n, m \in \mathbb{N} \wedge n < m$, por el teorema $m - n \in \mathbb{N}$, entonces $m - n \geq 1$, luego $n+1 \leq m$.

Definiciones inductivas:

Usaremos el razonamiento por inducción para definir objetos matemáticos.

Sea $a_1, a_2, a_3, a_4, ..., a_n, ...$ una sucesión de números reales. Queremos definir la suma de los n primeros términos de esa sucesión, para cualquier $n \in \mathbb{N}$.

La notación que indica esa suma es $\sum_{i=1}^{n} a_i$, y debemos definirla de manera tal que obtengamos lo que pretendemos: que sume los $a_1, a_2, a_3, a_4, ...$, hasta a_n .

***Definición*:** Se llama *sumatoria* de los n primeros términos de la sucesión $a_1, a_2, a_3, a_4, ..., a_n, ...$, y se la simboliza con $\sum_{i=1}^{n} a_i$, a la suma definida por :

$$\sum_{i=1}^{n} a_i =: \begin{cases} \sum_{i=1}^{1} a_i = a_1 \\ \sum_{i=1}^{n+1} a_i = \sum_{i=1}^{n} a_i + a_{n+1} \end{cases}$$

Veamos que esta definición satisface nuestras expectativas:

$\sum_{i=1}^{2} a_i = \sum_{i=}^{1+1} a_i = \sum_{i=1}^{1} a_i + a_2 = a_1 + a_2$, usando la definición.

$\sum_{i=1}^{3} a_i = \sum_{i=1}^{2+1} a_i = \sum_{i=1}^{2} a_i + a_3 = a_1 + a_2 + a_3$, por definición y lo visto antes.

$\sum_{i=1}^{4} a_i = \sum_{i=1}^{3+1} a_i = \sum_{i=1}^{3} a_i + a_4 = a_1 + a_2 + a_3 + a_4$, por definición y lo ya demostrado.

Y así siguiendo…..

Ejercicios: Demostrar que si $a_0, a_1, a_2, a_3, a_4, ..., a_n, ...$ es una sucesión de números reales:

1. $\sum_{i=1}^{n} a_i = \sum_{i=0}^{n-1} a_{i+1}$
2. $\sum_{i=0}^{n} a_i + \sum_{i=0}^{n} b_i = \sum_{i=0}^{n} (a_i + b_i)$
3. $\sum_{i=0}^{n} c.a_i = c.\sum_{i=0}^{n} a_i \ , \ \forall c \in \mathbb{R}$.

Lo que hicimos para la suma podemos reproducirlo para el producto.

***Definición*:** Se llama *productoria* de los *n* primeros términos de la sucesión $a_0, a_1, a_2, a_3, ..., a_n, ...$ y se la simboliza con $\prod_{i=1}^{n} a_i$, al producto definido por:

$$\prod_{i=1}^{n} a_i =: \begin{cases} \prod_{i=1}^{1} a_i = a_1 \\ \prod_{i=1}^{n+1} a_i = \prod_{i=1}^{n} a_i \cdot a_{n+1} \end{cases}$$

De la misma manera que para la suma, podemos ver que esta definición nos proporciona lo que estábamos buscando: el producto de los *n* primeros términos de la sucesión, sea cual fuere *n.*

Estas definiciones resultan útiles en el momento de demostrar fórmulas que involucran sumas o productos de términos de una sucesión.

Ejemplo: Demostrar que $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$, $\forall n \in \mathbb{N}$.

En este caso la sucesión dada es $a_i = i \ \ \forall i \in \mathbb{N}$.

Vamos a demostrarlo usando el Criterio de Inducción Completa.

Sea P(n) : $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$

Debemos ver si P(n) cumple con las hipótesis del criterio:

i. P(1) : $\sum_{i=1}^{1} i = \frac{1.(1+1)}{2}$ es V ?

$\sum_{i=1}^{1} i = 1$ pues $a_1 = 1$

$\frac{1 \cdot (1+1)}{2} = \frac{1 \cdot 2}{2} = 1$

Luego P(1) es V

ii. $P(n)\ V \Rightarrow P(n+1)\ V$?

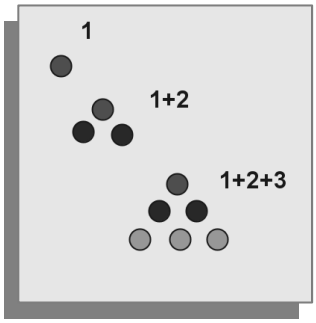
Debemos ver si a partir de suponer $P(n): \sum_{i=1}^{n} i = \frac{n(n+1)}{2}$ verdadera (Hipótesis inductiva : HI) podemos demostrar que $P(n+1): \sum_{i=1}^{n+1} i = \frac{(n+1)\cdot(n+2)}{2}$ es verdadera.

Comencemos con uno de los miembros de la igualdad que hay que probar.

$$\sum_{i=1}^{n+1} i = \sum_{i=1}^{n} i + (n+1) = (\text{ por HI }) \frac{n\cdot(n+1)}{2} + (n+1) =$$
$$= \frac{n\cdot(n+1)+2(n+1)}{2} = \frac{(n+1)\cdot(n+2)}{2}$$

que es lo que queríamos demostrar; luego $P(n+1)$ es V , y entonces $P(n)$ es V $\forall n \in \mathbb{N}$.

Hemos demostrado que $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$, $\forall n \in \mathbb{N}$.



*Carl Friedrich Gauss (*1777-1855*) fue un verdadero niño prodigio. Su padre era un obrero en Brunswick obstinado en sus puntos de vista, que intentó evitar que su hijo recibiera una educación adecuada, pero en cambio su madre, que tampoco había recibido ningún tipo de educación, animó siempre a su hijo en sus estudios.*
El maestro de la clase a la que asistía Gauss, con objeto de mantener a la clase atareada y en silencio durante un buen rato, tuvo la idea de hacer sumar a sus alumnos todos los números del 1 *al* 100*, ordenándoles además que, según fuera terminando cada uno esta tarea, deberían colocar su pizarra sobre la mesa del maestro. Casi inmediatamente coloco Carl su pizarra sobre la mesa diciendo: "ya está". Cuando todos hubieron terminado y el maestro revisó al fin los resultados obtenidos se encontró con la sorpresa de que en la única pizarra que aparecía la respuesta correcta,* 5050*, sin ningún cálculo accesorio era la de Gauss. El muchachito de* 10 *años había hecho evidentemente el cálculo mental de sumar la progresión aritmética* 1+2+3+4…….+100 *asociando parejas de términos igualmente alejados de los extremos:*

$$1 + 2 + 3 + \ldots\ldots + 49 + 50 + \ldots\ldots + 98 + 99 + 100 =$$
$$= (1 + 100) + (2 + 99) + (3 + 98) + \ldots.. + (50 + 51) = 50\ .\ 101 = \frac{100.101}{2}$$

es decir, esencialmente utilizando la fórmula $\frac{n\,(n+1)}{2}$.

Destacaremos dos casos particulares de productoria:

Caso 1: ***Potencia natural de un número real***

Sean $a \in \mathbb{R}$, $n \in \mathbb{N}$. Definiremos inductivamente a^n como sigue:

$$a^n =: \begin{cases} a^1 = a \\ a^{n+1} = a^n \cdot a \end{cases}$$

***Propiedades de la potencia*:**

Para $a, b \in \mathbb{R}$, $n, m \in \mathbb{N}$.

a) $a^n . b^n = (a.b)^n$
b) $a^n . a^m = a^{n+m}$
c) $(a^n)^m = a^{n.m}$

***Demostración*:** Demostraremos *a)* y las demás quedan como ejercicio.

a) $a^n . b^n = (a.b)^n$

Sea P(n) : $a^n . b^n = (a.b)^n$

i. P(1) es V? , o sea ¿ $a^1 . b^1 = (a.b)^1$?
$a^1 . b^1 = a.b = (a.b)^1$

ii. P(n) V $\Rightarrow$ P($n+1$) V ?
$a^n . b^n = (a.b)^n \Rightarrow a^{n+1} . b^{n+1} = (a.b)^{n+1}$?
$a^{n+1} . b^{n+1} = a^n . a . b^n . b = a^n . b^n . a . b = (a.b)^n . (a.b)$ (por HI) $= (a.b)^{n+1}$.

Luego P(n) es V $\forall n \in \mathbb{N}$, o sea $a^n . b^n = (a.b)^n \quad \forall n \in \mathbb{N}$.

Ejercicios: Demostrar por inducción sobre $n \in \mathbb{N}$:

1) $0^n = 0 \ \forall n \in \mathbb{N}$.
2) $1^n = 1 \ \forall n \in \mathbb{N}$.
3) $a \neq 0$ entonces $a^n \neq 0$, $\forall n \in \mathbb{N}$.

Extenderemos la definición de potencia de números reales a los exponentes 0 y $-n$, con $n \in \mathbb{N}$.

***Definición*:** Sean $a \in \mathbb{R}$, $a \neq 0$, $n \in \mathbb{N}$.

Definimos: $a^0 =: 1 \qquad a^{-n} =: (a^{-1})^n$

***Propiedades*:** Para $a, b \in \mathbb{R}$, $a \neq 0$, $b \neq 0$, $n, m \in \mathbb{N}_0$.

i. $a^{-n} = (a^n)^{-1}$
ii. $(a.b)^{-n} = a^{-n} . b^{-n}$
iii. $a^{-n} . a^{-m} = a^{-(n+m)}$
iv. $a^n . a^{-m} = a^{n-m}$
v. $(a^{-n})^{-m} = a^{n.m}$
vi. $(a^{-n})^m = (a^n)^{-m} = a^{-n.m}$

***Demostración*:** Demostraremos i. y iv. , y los demás quedan como ejercicios.

Para la demostración de estas propiedades podría utilizarse la inducción matemática, pero ello no será necesario, si se recurre a las definiciones y a las propiedades ya demostradas.

i. Sea $a \neq 0$, si $n = 0$ entonces $-n = 0$, luego $a^{-n} = a^0 = 1$; $a^n = a^0 = 1$, $\wedge \ 1^{-1} = 1$, entonces , para $n = 0$ se verifica que $a^{-n} = (a^n)^{-1}$.
Sea ahora, $n \in \mathbb{N}$. Para demostrar que $a^{-n} = (a^n)^{-1}$, o sea, que el inverso multiplicativos de a^n es a^{-n} , debemos multiplicar ambos números y ver si el producto es 1, utilizando la definición de a^{-n}.
$a^n . a^{-n} = a^n . (a^{-1})^n = (a.a^{-1})^n = 1^n = 1$

Luego $a^{-n} = (a^n)^{-1} \ \forall n \in \mathbb{N}_0$.

iv. Sean n , $m \in \mathbb{N}_0$, $a \neq 0$. Queremos ver que $a^n.a^{-m} = a^{n-m}$
Si $n = 0$, $a^n.a^{-m} = a^0.a^{-m} = 1.\ a^{-m} = a^{-m} = a^{0-m} = a^{n-m}$

Si $m = 0$, $a^n.a^{-m} = a^n.a^0 = a^n.1 = a^n = a^{n-0} = a^{n-m}$

Sean $n \neq 0$, $m \neq 0$. Tenemos que $n < m \vee m < n \vee n = m$

- Si $n = m$ $a^n.a^{-m} = a^n.a^{-n} = 1$ (por i.) $= a^0 = a^{n-n} = a^{n-m}$
- Si $n < m$ entonces $\exists k \in \mathbb{N}$ tal que $n + k = m$.
  Reemplazando m tenemos:
  $a^n.a^{-m} = a^n.a^{-(n+k)} = a^n.\ (a^{n+k})^{-1} = a^n.\ (a^n.a^k)^{-1} = a^n.(a^n)^{-1}.(a^k)^{-1} = a^{-k} = a^{n-m}$.
- Si $m < n$ entonces $\exists h \in \mathbb{N}$ tal que $m + h = n$.
  Reemplazando n tenemos:
  $a^n.a^{-m} = a^{m+h}.a^{-m} = a^m.a^h.a^{-m} = a^m.a^{-m}.a^h = a^h = a^{n-m}$.

Luego, cualesquiera sean $n, m \in \mathbb{N}_0$, $a \neq 0$, tenemos que $a^n.a^{-m} = a^{n-m}$.

Caso 2: *Factorial de n* , ($n \in \mathbb{N}_0$):

Sea $n \in \mathbb{N}$, definimos el *factorial de n,* y lo simbolizamos $n!$, al número tal que:

$$n! =: \begin{cases} 1! = 1 \\ (n+1)! = n!.(n+1) \end{cases}$$

También definimos: 0! =: 1

Ejemplos:

1) 2! = (1 + 1)! = 1!.2 = 1.2 = 2
2) 3! = (2 + 1)! = 2!.3 = 2.3 = 6
3) 10! = (9 + 1)! = 9!.10 = (8 + 1)!.10 = 8!.9.10 = (7 + 1)!.9.10 = 7!.8.9.10 =
= (6 + 1)!.8.9.10 = 6!.7.8.9.10 = 5!.6.7.8.9.10 = 4!.5.6.7.8.9.10 =
= 3!.4.5.6.7.8.9.10 = 2.3.4.5.6.7.8.9.10 = 3.628.800

Ejercicio: Demostrar que $\forall n \in \mathbb{N}$, $\prod_{i=1}^{n} i = n!$ (también en este caso $a_i = i$).

***Progresiones aritméticas y geométricas*:**

Sea $a_0, a_1, a_2, a_3, a_4, ..., a_n, ...$ una sucesión de números reales.

***Definición*:** Dicha sucesión es una *progresión aritmética* si $\exists d \in \mathbb{R}$, tal que $a_{i+1} = a_i + d$ $\forall i \in \mathbb{N}_0$.

Ejercicio: Demostrar por inducción sobre *n* que en una progresión aritmética $a_n = a_0 + nd$ $\forall n \in \mathbb{N}$.

Calcularemos la suma de los *n* primeros términos de una progresión aritmética.

Sea $a_0, a_1, a_2, a_3, a_4, ..., a_n, ...$ una progresión aritmética; luego $\exists d \in \mathbb{R}$, tal que $a_{i+1} = a_i + d \quad \forall i \in \mathbb{N}_0$.

$$\sum_{i=0}^{n} a_i = \sum_{i=0}^{n} (a_0 + i.d) = \sum_{i=0}^{n} a_0 + \sum_{i=0}^{n} i.d = a_0 . \sum_{i=0}^{n} 1 + d. \sum_{i=0}^{n} i = a_0 (n+1) + \frac{d.n.(n+1)}{2} = (n+1). \frac{(2a_0 + d.n)}{2}$$

Definiremos, ahora, *progresión geométrica*:

Sea $a_0, a_1, a_2, a_3, a_4, ..., a_n, ...$ una sucesión de números reales.

***Definición*:** Dicha sucesión es una *progresión geométrica* si $\exists d \in \mathbb{R} - \{0\}$, tal que $a_{i+1} = d a_i$ $\forall i \in \mathbb{N}_0$.

Ejercicio: Demostrar por inducción sobre *n* que en una progresión geométrica $a_n = d^n a_0$ $\forall n \in \mathbb{N}$.

Calcularemos la suma de los *n* primeros términos de una progresión geométrica.

Sea $a_0, a_1, a_2, a_3, a_4, ..., a_n, ...$ una progresión geométrica; luego $\exists d \in \mathbb{R} - \{0\}$, tal que $a_n = d^n a_0$, $\forall n \in \mathbb{N}_0$. Si llamamos $S_n = \sum_{i=0}^{n} a_i$, tenemos que

$$S_n = \sum_{i=0}^{n} d^i \cdot a_0 = a_0 \cdot \sum_{i=0}^{n} d^i$$

$$d.S_n = a_0 \, . \, d \, . \sum_{i=0}^{n} d^i = a_0 \, . \sum_{i=0}^{n} d^{i+1} = a_0 \, . \sum_{i=1}^{n+1} d^i$$

$$S_n - d.S_n = a_0 \, . \sum_{i=0}^{n} d^i - a_0 \, . \sum_{i=1}^{n+1} d^i = a_0 \, (\sum_{i=0}^{n} d^i - \sum_{i=1}^{n+1} d^i) =$$

$$= a_0 \, (d^0 + \sum_{i=1}^{n} d^i - \sum_{i=1}^{n} d^i - d^{n+1}) = a_0 \, . \, (1 - d^{n+1})$$

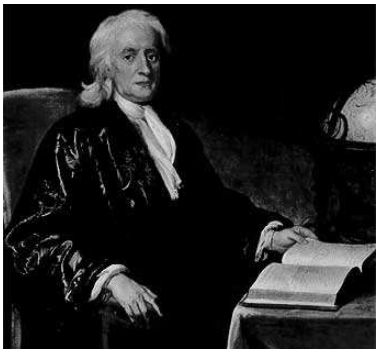
Además $S_n - d.S_n = (1 - d) \, . \, S_n$

luego $(1 - d) \, . \, S_n = a_0 \, . \, (1 - d^{n+1})$

de donde $S_n = \dfrac{a_0 (1 - d^{n+1})}{1 - d}$ siempre que $d \neq 1$.

Si $d = 1$ $S_n = a_0 \, . \sum_{i=0}^{n} d^i = a_0 \, . \sum_{i=0}^{n} 1 = a_0 \, .(n + 1)$.

Binomio de Newton:



Isaac Newton (*1642-1727*)

El teorema del Binomio, descubierto hacia 1664-1665*, fue comunicado por primera vez en dos cartas dirigidas en* 1676 *a Henry Oldenburg (hacia* 1619-1677*), secretario de la Royal Society que favorecía los intercambios de correspondencia entre los científicos de su época. En la primera carta, fechada el* 13 *de junio de* 1676*, en respuesta a una petición de Leibintz que quería conocer los trabajos de matemáticos ingleses sobre series infinitas, Newton presenta el enunciado de su teorema y un ejemplo que lo ilustra, y menciona ejemplos conocidos en los cuales se aplica el teorema.*
Newton no publicó nunca el teorema del Binomio, lo hizo Wallis por primera vez en 1685 *en su Algebra, atribuyendo a Newton este descubrimiento.*

http://thales.cica.es/rd/Recursos/rd97/Biografias/03-1-b-newton.html

Sabemos que la potenciación no es distributiva respecto de la suma, porque, por ejemplo:
$(2 + 3)^2 = 5^2 = 25$, mientras que $2^2 + 3^2 = 4 + 9 = 13$; luego , claramente $(2 + 3)^2 \neq 2^2 + 3^2$

Nos interesa, entonces, buscar una manera, una fórmula de ser posible, que nos permita calcular la potencia *n*-ésima de un binomio, sin necesidad de multiplicar *n* veces dicho binomio por sí mismo, y esto cualquiera sea $n \in \mathbb{N}$.

Comencemos por el caso más simple, $n = 2$:

$(a + b)^2 = (a + b).(a + b) = a.a + a.b + b.a + b.b$, como $a.b = b.a$ porque el producto es conmutativo, luego $(a + b)^2 = a^2 + 2a.b + b^2$

$(a + b)^3 = (a + b).(a + b).(a + b) = (a + b).(a^2 + 2a.b + b^2) = a . (a^2 + 2a.b + b^2) +$
$+ b . (a^2 + 2a.b + b^2) = a^3 + 2a^2.b + a.b^2 + b.a^2 + 2a.b^2 + b^3 =$
$= a^3 + 3a^2.b + 3a.b^2 + b^3$

$(a + b)^4 = (a + b).(a + b).(a + b).(a + b) = (a + b).(a + b)^3 = (a + b) . (a^3 + 3a^2.b +$
$+ 3a.b^2 + b^3) = a^4 + 3\,a^3 . b + 3\,a^2.b^2 + a.b^3 + a^3 .b + 3a^2.b^2 + 3a.b^3 + b^4 =$
$= a^4 + 4\,a^3 . b + 6\,a^2.b^2 + 4\,a.b^3 + b^4$

$(a + b)^5 = (a + b).(a + b).(a + b).(a + b).(a + b) = (a + b) .(a + b)^4 = (a + b) . (a^4 +$
$+ 4\,a^3 . b + 6\,a^2.b^2 + 4\,a.b^3 + b^4) = a^5 + 4\,a^4. b + 6\,a^3.b^2 + 4\,a^2.b^3 + a.b^4 + a^4.b +$
$+ 4\,a^3 .b^2 + 6\,a^2.b^3 + 4\,a.b^4 + b^5 = a^5 + 5a^4. b + 10a^3.b^2 + 10a^2.b^3 + 5a.b^4 + b^5$

A partir del ejemplo precedente, podemos observar que para calcular todos los términos del desarrollo de $(a + b)^5$ debemos determinar lo que podríamos llamar la *parte literal* de esos términos, que en este caso son productos de potencias de *a* y *b* respectivamente, y por otro, los *coeficientes* que multiplican a cada uno de esos productos de potencias.
Cuando efectuamos el producto: $(a + b)^5 = (a + b)\,(a + b).(a + b).\,(a + b).(a + b)$
aplicando la propiedad distributiva las veces que sean necesarias, elegimos de cada factor un término, que en este caso puede ser *a* o *b* para todos ellos. Por ejemplo, para obtener el coeficiente de a^4b debemos calcular *de cuántas maneras distintas podemos elegir en cuatro factores a y en el otro b* . En este caso se ve fácilmente que son 5. Si queremos saber, sin efectuar la propiedad distributiva como lo hicimos más arriba, *de cuántas maneras distintas podemos elegir en tres factores a y en los dos restantes b* , eso ya no es tan sencillo. Lo que se ve es que no resulta obvio

encontrar los *coeficientes binomiales* a simple vista cuando $n = 5$, y menos aun si $n = 10$ o $n = 100$, por ejemplo.
Si este procedimiento, aplicar propiedad distributiva, lo queremos hacer para calcular $(a + b)^{10}$ claramente se complica, ¡ y ni hablar si queremos desarrollar $(a + b)^{100}$!

Por ejemplo, para hallar el desarrollo de $(a + b)^{100}$, como esto es el producto de $(a + b).(a + b).(a + b).(a + b)\ldots\ldots(a + b)$ cien veces, así como hicimos para $(a + b)^5$, sabemos que tenemos una única manera de obtener a^{100} , que es multiplicando las a de cada uno de los cien factores (igual que para obtener b^{100}) ; es fácil darse cuenta que tenemos 100 maneras distintas de elegir en 99 factores a y en el restante b, porque elegimos la b en cada uno de los cien factores, luego será $100.a^{99}.b$ (de igual manera obtenemos $100.a.b^{99}$) . Ahora, calcular cuántas maneras distintas tenemos para elegir a en noventa y ocho factores, y en los dos restantes b, sin un método, ya no es tan sencillo.
Sabemos que cada término es de la forma ¿?$a^i.b^j$ con $i + j = 100$, para $0 \leq i, j \leq 100$, donde ¿? representa el coeficiente que desconocemos; sabemos que ese número desconocido es la cantidad de maneras distintas con las que podemos elegir i veces a y j veces b. Ese número se denomina *el número combinatorio n, m* , y corresponde a *las combinaciones de n elementos tomados de a m* (en nuestro caso $n = 100$).

***Definición*:** Sean $n, m \in \mathbb{N}_0$, $m \leq n$. Llamamos *Número Combinatorio n, m ,* o *Combinaciones de n tomadas de a m* , y lo notamos $C_{n,m} = \binom{n}{m}$, al número:

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

Ejemplos: $C_{0,0} = \binom{0}{0} = \frac{0!}{0!.0!} = \frac{1}{1.1} = \frac{1}{1} = 1$ $\quad C_{3,0} = \binom{3}{0} = \frac{3!}{3!.0!} = \frac{3!}{3!.1} = 1$

$C_{1,0} = \binom{1}{0} = \frac{1!}{1!.0!} = \frac{1}{1.1} = \frac{1}{1} = 1$ $\quad C_{3,1} = \binom{3}{1} = \frac{3!}{2!.1!} = \frac{3.2!}{2!.1} = \frac{3}{1} = 3$

$C_{1,1} = \binom{1}{1} = \frac{1!}{1!.0!} = 1$ $\quad C_{3,2} = \binom{3}{2} = \frac{3!}{2!.1!} = \frac{3.2!}{2!.1} = \frac{3}{1} = 3$

$C_{2,0} = \binom{2}{0} = \frac{2!}{2!.0!} = \frac{2}{2} = 1$ $\quad C_{3,3} = \binom{3}{3} = \frac{3!}{3!.0!} = \frac{3!}{3!.1} = 1$

$C_{2,1} = \binom{2}{1} = \frac{2!}{1!.1!} = \frac{2}{1} = 2$ $\quad C_{2,2} = \binom{2}{2} = \frac{2!}{0!.2!} = 1$

$$C_{10,7} = \binom{10}{7} = \frac{10!}{7!.3!} = \frac{10.9.8.7!}{7!.3!} = \frac{10.9.8}{6} = 10.3.4 = 120$$

***Propiedades*:**

i. $\binom{n}{m} = \binom{n}{n-m}$ $\forall\ n, m \in \mathbb{N}_0, m \leq n$

ii. $\binom{n}{0} = \binom{n}{n} = 1$ $\forall\ n \in \mathbb{N}_0$

iii. $\binom{n}{1} = \binom{n}{n-1} = n \quad \forall\ n \in \mathbb{N}$

iv. $\binom{n}{2} = \binom{n}{n-2} = \frac{n(n-1)}{2} \quad \forall\ n \in \mathbb{N},\ n \geq 2$

Las demostraciones se dejan como ejercicio.

En el ejemplo $C_{10,7}$ pudimos observar que el cálculo del número $C_{n,m}$ puede resultar muy dificultoso si *n* y *m* son muy grandes, y más aun si están distanciados uno de otro; por otra parte, si bien en los ejemplos **siempre** obtuvimos un número natural, ello no parece tan evidente a la luz de la definición, y si $C_{n,m}$ no fuera un número natural para ciertos n y m, con $m \leq n$, querría decir que ese número no se correspondería con la idea : *"de cuántas maneras distintas puedo elegir m elementos en un total de n"*, cuya respuesta **debe ser** un número natural. Por lo tanto tenemos que demostrar que $C_{n,m} \in \mathbb{N}$, $\forall\ n, m \in \mathbb{N}_0$, $m \leq n$, pero antes demostraremos una ley que nos permitirá calcular $C_{n,m}$ por recurrencia.

Ley de Recurrencia de Pascal:

$$\binom{n+1}{m} = \binom{n}{m} + \binom{n}{m-1} \quad \forall\ n, m \in \mathbb{N},\ m \leq n$$

***Demostración*:**

Por definición: $\binom{n+1}{m} = \frac{(n+1)!}{(n+1-m)!.m!}$, $\binom{n}{m} = \frac{n!}{m!(n-m)!}$,

$$\binom{n}{m-1} = \frac{n!}{(m-1)!.[\,n-(m-1)\,]!}$$

Calculemos:

$$\binom{n}{m} + \binom{n}{m-1} = \frac{n!}{m!(n-m)!} + \frac{n!}{(m-1)!.[\,n-(m-1)\,]!} =$$

$$m! = m.(m-1)!\ ; \quad [\,n-(m-1)\,]! = (n-m+1)! = (n-m+1).(n-m)!$$

$$= \frac{n!}{m.(m-1)!.(n-m)!} + \frac{n!}{(m-1)!.(n-m+1).(n-m)!} = \frac{n!.(n-m+1)+n!.m}{m.(m-1)!.(n-m+1).(n-m)!} =$$

$$= \frac{n!.(n+1)-n!.m+n!.m}{m!.(n+1-m)!} = \frac{(n+1)!}{(n+1-m)!.m!} = \binom{n+1}{m}$$

***Teorema*:** $\binom{n}{m} \in \mathbb{N}$, $\forall\ n, m \in \mathbb{N}_0$, con $m \leq n$.

***Demostración*:** Si $n = 0$, como $m \leq n \Rightarrow m = 0$.

Entonces $\binom{n}{m} = \binom{0}{0} = 1 \in \mathbb{N}$,

Si $n \in \mathbb{N}$, y $m = 0 \ \vee \ m = n$, como $\binom{n}{0} = \binom{n}{n} = 1 \in \mathbb{N}$,

Falta demostrarlo para $n \in \mathbb{N}$, y $0 < m \leq n$, y lo haremos por inducción sobre n.

Sea P(n): Si $m \in \mathbb{N} \ \wedge\ 0 \leq m \leq n \Rightarrow \binom{n}{m} \in \mathbb{N}$,

i. P(1) es V ?

Sí, pues si $n = 1 \Rightarrow m = 0 \ \vee\ m = 1$, y $\binom{1}{0} = \binom{1}{1} = 1 \in \mathbb{N}$,

ii. P(n) V $\Rightarrow$ P($n + 1$) V ?

Por HI, si $m \in \mathbb{N} \ \wedge\ 0 \leq m \leq n \Rightarrow \binom{n}{m} \in \mathbb{N}$,

Queremos demostrar que si $k \in \mathbb{N} \ \wedge\ 0 \leq k \leq n + 1 \Rightarrow \binom{n+1}{k} \in \mathbb{N}$,

Para $k = 0 \ \vee\ k = n + 1$ ya está.

Si $0 < k < n + 1$, por la Ley de Recurrencia de Pascal:

$$\binom{n+1}{m} = \binom{n}{m} + \binom{n}{m-1} \quad \forall\ n, m \in \mathbb{N}, m \leq n$$

como $0 < k < n + 1 \Rightarrow k \in \mathbb{N} \ \wedge\ k \leq n$, luego tenemos que:

$$\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}$$

por HI $\binom{n}{k} \in \mathbb{N} \ \wedge\ \binom{n}{k-1} \in \mathbb{N}$

y, como la suma de números naturales es un número natural $\binom{n+1}{k} \in \mathbb{N}$.

Luego P(n) es V $\forall n \in \mathbb{N}$, y por lo tanto $\binom{n}{m} \in \mathbb{N}$, $\forall\ n, m \in \mathbb{N}_0$, con $m \leq n$.

A partir de la Ley de Recurrencia de Pascal, se puede construir en forma iterativa, el llamado *Triángulo de Pascal,* que nos permite calcular los números combinatorios con mucha economía de operaciones, dado que requiere sólo efectuar sumas, y no productos como lo establece la definición.

TRIÁNGULO DE PASCAL (1623-1662) (Fig.1)

$$\binom{0}{0}$$

$$\binom{1}{0}\ \binom{1}{1}$$

$$\binom{2}{0}\ \binom{2}{1}\ \binom{2}{2}$$

$$\binom{3}{0}\ \binom{3}{1}\ \binom{3}{2}\ \binom{3}{3}$$

$$\binom{4}{0}\ \binom{4}{1}\ \binom{4}{2}\ \binom{4}{3}\ \binom{4}{4}$$

$$\binom{5}{0}\ \binom{5}{1}\ \binom{5}{2}\ \binom{5}{3}\ \binom{5}{4}\ \binom{5}{5}$$

.....

TRIÁNGULO DE TARTAGLIA (1500-1557) (Fig.2)

1

1 1

1 2 1

1 3 3 1

1 4 6 4 1

1 5 10 10 5 1

.....

*La tabla de la Fig.*2*, es conocida como Triángulo de Tartaglia (Niccolò Fontana (*1499-1557*), apodado Tartaglia debido a su tartamudez). Sin embargo, fue Blaise Pascal (*1623-1662*) quien relacionó los coeficientes del desarrollo de la potencia de un binomio con los números combinatorios, por lo cual, expresado en la forma de la Fig.*1 *se conoce también como Triángulo de Pascal.*

Por ejemplo: $\binom{3}{1} = \binom{2}{0} + \binom{2}{1}$, $\binom{4}{2} = \binom{3}{1} + \binom{3}{2}$, $\binom{5}{2} = \binom{4}{1} + \binom{4}{2}$

$\binom{5}{3} = \binom{4}{2} + \binom{4}{3}$, y así , sumando los elementos adecuados de una fila se construye la siguiente.

Fórmula del Binomio de Newton:

Para $a, b \in \mathbb{R}$

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} \cdot a^k \cdot b^{n-k} \quad \forall n \in \mathbb{N}.$$

***Demostración*:** La haremos por inducción sobre *n*.

Para $n = 1$ $(a+b)^1 = a + b$; $\sum_{k=0}^{1} \binom{1}{k} a^k b^{1-k} = \binom{1}{0} a^0 b^1 + \binom{1}{1} a^1 b^0 = b + a$

y como $a + b = b + a$, la proposición es verdadera para $n = 1$.

Supongamos, como Hipótesis Inductiva, que la proposición sea verdadera para *n*, o sea que:

$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} \cdot a^k \cdot b^{n-k}$. Queremos ver si lo es para $n+1$. Para ello debemos probar que

$(a+b)^{n+1} = \sum_{k=0}^{n+1} \binom{n+1}{k} a^k b^{n+1-k}$.

Comencemos por el primer miembro de la igualdad:

$$(a+b)^{n+1} = (a+b).(a+b)^n = a.(a+b)^n + b.(a+b)^n =$$

$$= a.\sum_{k=0}^{n} \binom{n}{k} \cdot a^k \cdot b^{n-k} + b.\sum_{k=0}^{n} \binom{n}{k} \cdot a^k \cdot b^{n-k} = \sum_{k=0}^{n} \binom{n}{k} a^{k+1} \cdot b^{n-k} + \sum_{k=0}^{n} \binom{n}{k} a^k \cdot b^{(n-k)+1} =$$

$$= a^{n+1} + b^{n+1} + \sum_{k=0}^{n-1} \binom{n}{k} a^{k+1} \cdot b^{n-k} + \sum_{k=1}^{n} \binom{n}{k} a^k \cdot b^{n+1-k} =$$

$$= a^{n+1} + b^{n+1} + \sum_{k=1}^{n} \binom{n}{k-1} a^k \cdot b^{n-(k-1)} + \sum_{k=1}^{n} \binom{n}{k} a^k \cdot b^{n+1-k} =$$

$$= a^{n+1} + b^{n+1} + \sum_{k=1}^{n} \left[\binom{n}{k-1} + \binom{n}{k} \right] a^k \cdot b^{n+1-k} =$$

Por la Ley de Recurrencia de Pascal $\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}$

$$= a^{n+1} + b^{n+1} + \sum_{k=1}^{n} \binom{n+1}{k} a^k \cdot b^{n+1-k} = \sum_{k=0}^{n+1} \binom{n+1}{k} a^k b^{n+1-k}$$

dado que $a^{n+1} = \binom{n+1}{n+1} a^{n+1} \cdot b^{n+1-(n+1)}$ y $b^{n+1} = \binom{n+1}{0} a^0 \cdot b^{n+1-0}$.

Así, la proposición es verdadera para $n+1$; luego se verifica $\forall n \in \mathbb{N}$.

Inducción Generalizada:

Existen propiedades o fórmulas que se verifican para números naturales, pero quizás no para todos, sino a partir de cierto número natural, y así como está formulado, no podríamos utilizar el poderoso recurso de la Inducción Completa para demostrarlas, por ello enunciaremos y demostraremos un nuevo criterio que resolverá estos inconvenientes: el *Criterio de Inducción Generalizada.*

Criterio de Inducción Generalizada:

Sea P(n) una función proposicional con dominio en $\mathbb{N}$; sea $n_0 \in \mathbb{N}$.

Supongamos que P(n) verifique estas dos propiedades:

i. P(n_0) es V

ii. P(n) V $\Rightarrow$ P($n+1$) V

Entonces P(n) es V $\forall n \in \mathbb{N}$, con $n \geq n_0$.

***Demostración*:** Sea Q(n) la función proposicional definida por: Q(n) = P(n+ n_0 – 1);
veremos que Q(n) verifica las hipótesis del criterio de Inducción Completa.

Q(1) es V ?
Q(1) = P(1+ n_0 – 1) = P(n_0) que por i. es V.

Q(n) V $\Rightarrow$ Q(n + 1) V ?
por H.I. Q(n) = P(n + n_0 – 1) es V, como P verifica ii., P(n + n_0 – 1 + 1) es V,
y P(n + n_0 – 1 + 1) = Q(n + 1) , luego Q(n + 1) es V.

Por el criterio de Inducción Completa Q(n) es V $\forall n \in \mathbb{N}$.
Entonces P(n) es V $\forall n \in \mathbb{N}$, con $n \geq n_0$.

Ejemplo: Queremos comparar los números naturales 2^n y $n!$

$2^0 = 1 = 0!$
$2^1 = 2 > 1 = 1!$
$2^2 = 4 > 2 = 2!$
$2^3 = 8 > 6 = 3!$
$2^4 = 16 < 24 = 4!$
$2^5 = 32 < 120 = 5!$

Pareciera que esta desigualdad se mantendrá para los siguientes números naturales, dado que para obtener 2^6 debemos multiplicar a 2^5 por 2 , que es menor que 6, y 6! = 5!.6.

Vamos a demostrar esta propiedad :

$$2^n < n! \ \forall n \in \mathbb{N}, \text{ con } n \geq 4$$

Para $n = 4$ ya lo vimos: $2^4 = 16 < 24 = 4!$.

Supongámosla verdadera para n, o sea $2^n < n!$,
y queremos demostrarla para $n + 1$: $2^{n+1} < (n + 1)!$?

$$2^{n+1} = 2 \cdot 2^n < 2 \cdot n! < (n + 1) \cdot n! = (n + 1)! ,$$

pues como $n \geq 4$, entonces $n + 1 > 2$.

Luego $2^n < n! \ \forall n \in \mathbb{N}$, con $n \geq 4$.

Principio de Buena Ordenación:

Recordaremos la definición de conjunto *bien ordenado*, pero en esta oportunidad nos referiremos siempre a subconjuntos del conjunto ordenado $\mathbb{R}$ de números reales con su orden usual $\leq$.

***Definición*:** Sea $A \subset \mathbb{R}$, decimos que está *bien ordenado* si todos sus subconjuntos no vacíos tienen mínimo, o sea :

$$A \text{ es b.o. sii } \forall B \subset A \ \wedge \ B \neq \phi \ \Rightarrow B \text{ tiene mínimo}$$

Ejemplos:

1) ϕ es b.o. , pues no admite subconjuntos no vacíos.
2) $\{a\}$ es b.o. pues el único subconjunto no vacío que admite es el propio $\{a\}$ y tiene mínimo *a.*
3) $\{a,b\}$ es b.o. . Sus subconjuntos no vacíos son : $\{a\}$, $\{b\}$ y $\{a,b\}$. Los dos primeros tienen mínimo por lo visto en 2), en el caso de $\{a,b\}$, si tiene dos elementos, debe ser $a \neq b$, entonces será $a < b \vee b < a$.
   Si $a < b$, $a = mín\ \{a,b\}$, y si $b < a$, $b = mín\{a,b\}$, en cualquier caso $\{a,b\}$ tiene mínimo . Si $a = b$ estamos en el caso 2).
4) $\{a,b,c\}$ es b.o.. Sea $\{a,b,c\}$ con *a, b, c* distintos dos a dos (si no fuera así, estaríamos en alguno de los casos anteriores, que ya vimos que son b.o.).
   Los subconjuntos no vacíos de este conjunto son: $\{a\}$, $\{b\}$, $\{c\}$, $\{a,b\}$, $\{a,c\}$, $\{b,c\}$ y el propio $\{a,b,c\}$. En los casos anteriores vimos que los seis primeros son b.o., y como son no vacíos, tienen mínimo. Para ver que $\{a,b,c\}$ tiene mínimo debemos comparar, por ejemplo, *c* con el $mín\{a,b\}$, y como son distintos, uno de ellos es el menor, luego ese número será el $mín\{a,b,c\}$

Podríamos seguir ejemplificando con conjuntos finitos de cinco, seis, siete,.. elementos, pero no podemos, de esta forma, demostrarlo para todo subconjunto finito de $\mathbb{R}$, sí lo podremos hacer por inducción.

Recordaremos algunas definiciones y propiedades dadas en el CAP II, Parte 3, que nos serán útiles.

***Definición*:** Sea $n \in \mathbb{N}$, *A* un conjunto. *A* se dice *finito de cardinal n* si es coordinable con $[\![1,\ n]\!] = [1,\ n] \cap \mathbb{N}$ (intervalo natural 1, *n*), o sea, si $\exists\ f$ función biyectiva,

$$f : [\![1,\ n]\!] \to A$$

Se lo nota *card*(*A*) = *n*, intuitivamente esto dice que *A* "tiene *n* elementos".

***Definición*:** Diremos que un conjunto *A* es *finito,* si es finito de cardinal *n* , para cierto número natural *n* .

Nota: Al conjunto ϕ se lo considera finito de cardinal 0 : *card*(ϕ) = 0.

***Propiedades*:** Sea *A* un conjunto finito.

1) Si *card*(*A*) = $n \in \mathbb{N}$, $a \in A$, entonces *card*($A - \{a\}$) = $n - 1$.
2) Si *card*(*A*) = $n \in \mathbb{N}_0$, $b \notin A$, entonces *card*($A \cup \{b\}$) = $n + 1$.

***Demostración* :** es un ejercicio del capítulo correspondiente a funciones.

***Teorema*:** Todo subconjunto finito de $\mathbb{R}$ es b.o.

***Demostración*:** Sea $A \subset \mathbb{R}$, tal que *card*(*A*) = $n \in \mathbb{N}_0$.
Si $n = 0 \Rightarrow A = \phi$, luego *A* es b.o.
Para $n \in \mathbb{N}$ lo demostraremos por inducción sobre *n* .

Si $card(A) = 1$, A es un conjunto unitario, y ya vimos que es b.o.

Supongamos que todo subconjunto de $\mathbb{R}$, de cardinal n, sea b.o. (HI).

Queremos demostrar que todo subconjunto de $\mathbb{R}$, de cardinal $n + 1$ es b.o..
Sea $A \subset \mathbb{R}$, tal que $card(A) = n + 1$ y sea $a \in A$. Para demostrar que A es b.o. debemos probar que todo subconjunto no vacío de A tiene mínimo.
Sea entonces $B \subset A$, tal que $B \neq \phi$. Pueden ocurrir dos situaciones: $a \in B \vee a \notin B$.

- Si $a \in B$ entonces $B - \{a\} \subset A - \{a\}$, y como $card(A) = n + 1 \Rightarrow card(A - \{a\}) = n$;
  - si $B - \{a\} \neq \phi$, por HI $B - \{a\}$ tiene mínimo b;

luego si $b = mín\ B - \{a\}$, entonces $b \in B - \{a\}$, con lo cual $b \in B \wedge b \neq a$; además $b \leq x$ $\forall x \in B - \{a\}$. Como $b \neq a \Rightarrow b < a \vee a < b$.
Si $b < a$, entonces $b = mín\ B$, ya que $b \in B \wedge b \leq x\ \forall x \in B$
Si $a < b$, entonces $a = mín\ B$, pues $a \in B \wedge a < b \leq x\ \forall x \in B - \{a\}$, luego $a \leq x\ \forall x \in B$.
  - si $B - \{a\} = \phi \Rightarrow B = \{a\}$, luego B tiene mínimo.

- Si $a \notin B$, entonces $B \subset A - \{a\}$, y como $card(A - \{a\}) = n$, por HI B tiene mínimo.

Luego, todo conjunto de cardinal $n + 1$ es b.o., com lo cual todo conjunto finito es b.o.

***Teorema*:** $\mathbb{N}$ es un conjunto bien ordenado.

***Demostración*:** Queremos ver que todo subconjunto no vacío de $\mathbb{N}$ tiene mínimo, y para ello recurriremos al criterio de inducción completa.

Sea P(n) : si $A \subset \mathbb{N} \wedge n \in A \Rightarrow A$ tiene mínimo

I. P(1) es V ? ; P(1): si $A \subset \mathbb{N} \wedge 1 \in A \Rightarrow A$ tiene mínimo?
   Si $A \subset \mathbb{N} \wedge 1 \in A \Rightarrow 1 = mín\ A$, pues si $x \in \mathbb{N}$, $x \geq 1$; en particular si $x \in A$, $x \geq 1$.

II. P(n) V $\Rightarrow$ P($n + 1$) V ?
   Para ver que P($n + 1$) es V a partir de la suposición de que P(n) lo sea, debemos probar que todo subconjunto que contenga a $n + 1$ debe tener mínimo.

Sea $A \subset \mathbb{N}$ tal que $n + 1 \in A$; puede ocurrir que $n \in A \vee n \notin A$.

- Si $n \in A$, por HI , A tiene mínimo.

- Si $n \notin A$, sea $B = A \cup \{n\}$. Como $A \subset B \wedge n + 1 \in A \Rightarrow n + 1 \in B$,
  y como $n \in B$, por HI, B tiene mínimo m.
  $m \in B \wedge m \leq x\ \forall x \in B$, en particular $m \leq n\ \therefore\ m = n \vee m < n$
  - Si $m < n \Rightarrow m = mín\ A$, pues si $m \leq x\ \forall x \in B \wedge A \subset B$, entonces $m \leq x\ \forall x \in A$. Además como $m \neq n \wedge m \in B \Rightarrow m \in A$.
  - Si $m = n$, $n + 1 = mín\ A$, pues si $n \leq x\ \forall x \in B \wedge n \notin A$ entonces $n < x$, $\forall x \in A$, luego $n + 1 \leq x\ \forall x \in A$.

En todos los casos A tiene mínimo.

Luego P(n) es V $\forall n \in \mathbb{N}$, lo que equivale a decir que cualquier subconjunto que contenga un número natural tiene mínimo, o sea, todo subconjunto no vacío de $\mathbb{N}$ tiene mínimo, luego $\mathbb{N}$ es b.o.

***Teorema*:** Todo subconjunto no vacío de $\mathbb{N}$, acotado superiormente en $\mathbb{N}$, tiene máximo.

***Demostración*:** Sea $A \subset \mathbb{N}$, y $A \neq \phi$ y acotado superiomente en $\mathbb{N}$.
Sea $L = \{ x \in \mathbb{N} / x$ es cota superior de $A \}$; $L \subset \mathbb{N}$, y $L \neq \phi$, por ser $\mathbb{N}$ b.o., L tiene mínimo m .
Luego $m \in L$, o sea m es una cota superior de A, y $m \leq y \quad \forall y \in L$.
Decimos que $m = máx\ A$; para ver que esto es cierto, debemos probar que $m \in A$, pues ya sabemos que es cota superior.
Si $m \notin A$, como m es cota superior de A, tendríamos que $x < m \quad \forall x \in A$, entonces $x \leq m - 1 \quad \forall x \in A$, por ser x y m números naturales; con lo cual $m - 1$ sería una cota superior de A, y $m - 1 < m$!! , porque $m = mín\ L$.
Luego $m \in A$, y $m = máx\ A$.

Otro Criterio de Inducción:

Existen propiedades o teoremas relativos a los números naturales, para cuya demostración resultaría muy útil poder valerse del principio de Inducción Completa, pero aparecen dificultades para utilizar la hipótesis inductiva, o sea, cómo demostrar que la proposición si es verdadera para n, lo es también para $n + 1$. Para estas situaciones tenemos un criterio, que usando el mismo principio, tiene una formulación diferente que resuelve estas dificultades.

***Criterio*:** Sea P(n) una función proposicional con dominio en $\mathbb{N}$ (esto es P es una función que a cada $n \in \mathbb{N}$ le asigna una *proposición* P(n) , que como tal, tiene un valor de verdad: verdadera "V", o falsa "F").
Supongamos que P verifica:

i. P(1) es V
ii. Si $n > 1$, y P(k) es V $\forall k \quad 1 \leq k < n \Rightarrow$ P(n) es V.

Entonces, podemos afirmar que P(n) es V $\forall n \in \mathbb{N}$.

***Demostración*:** Sea H = $\{ n \in \mathbb{N}$ / P(n) es V $\} \subset \mathbb{N}$.
Si H $\neq \mathbb{N}$ entonces $\mathbb{N} - H \neq \phi$, y $\mathbb{N} - H \subset \mathbb{N}$, tiene mínimo.
Sea $m = mín(\mathbb{N} - H)$, luego $m \in \mathbb{N} - H$, con lo cual $m \notin H$, y así P(m) es F, y $m \leq x \quad \forall x \in \mathbb{N} - H$, o lo que es equivalente: si $k < m \Rightarrow k \notin \mathbb{N} - H$, o bien , si $k < m \Rightarrow k \in H$.
Luego si $k < m$ se verifica que P(k) es V , por ii. eso implica que P(m) es V !! .
Luego $\mathbb{N} - H = \phi$ y así $\mathbb{N} = H$, con lo cual P(n) es V , $\forall n \in \mathbb{N}$.

***Ejercicios*:**

1. Demostrar las propiedades de la potencia natural de números reales enunciadas en el texto.

2. Demostrar las propiedades de las potencias 0 y opuestas de números naturales enunciadas anteriormente.

3. Demostrar las siguientes propiedades válidas para todo $n, m \in \mathbb{N}$, para todo $a, b \in \mathbb{R}$:

   3.1. Si $b \neq 0$ $\left(\frac{a}{b}\right)^n = \frac{a^n}{b^n}$

   3.2. $a^n = 0$ sií $a = 0$

   3.3. Si $1 < a$ entonces $1 < a^n$

4. Si $a \geq 0$ entonces $(1 + a)^n \geq 1 + n.a$. ¿Para qué $a \in \mathbb{R}$ vale la igualdad para todo $n > 1$?

5. Demostrar las siguientes fórmulas usando el principio de inducción:

a) $\sum_{i=1}^{n}(2i-1) = n^2$ b) $\sum_{i=1}^{n} 2^i = 2^{n+1} - 2$

c) $\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$ d) $\sum_{i=1}^{n} i(i+1) = \frac{n(n+1)(n+2)}{3}$

e) $\sum_{i=1}^{n}(6i^2 - 1) = n^2(2n+3)$ f) $\sum_{i=1}^{n}(n+2i) = 2n^2 + n$

6. Sea $a \in \mathbb{R}$, $a \neq 1$. Demostrar que para todo $n \in \mathbb{N}$.

   6.1. $\sum_{j=1}^{n} a^{j-1} = \frac{1-a^n}{1-a}$. ¿Cuánto vale la suma $\sum_{j=1}^{n} a^{j-1}$ si $a = 1$?

   6.2. Calcular $\sum_{i=1}^{8} 3^{i+2}$

   6.3. Calcular $\frac{3}{10} + \frac{3}{100} + \frac{3}{1000} + ... + \frac{3}{1000000}$

7. a) Sea $a \in \mathbb{R}$; probar que $a > 0 \Rightarrow a + a^{-1} \geq 2$.

b) Sean $a_1, a_2, a_3, a_4, ..., a_n$ números reales positivos; probar que:

$$\left[\sum_{i=1}^{n} a_i\right] \cdot \left[\sum_{i=1}^{n} a_i^{-1}\right] \geq n^2$$

8. Sea $a \in \mathbb{R}$, $a \neq 1$. Demostrar que para todo $n \in \mathbb{N}$, $\prod_{i=1}^{n}\left(1 + a^{2^{i-1}}\right) = \frac{1-a^{2^n}}{1-a}$.

¿Está definido el producto para $a = 1$? ¿Cuál es su valor?

9. Sean $a_1, a_2, a_3, a_4, ..., a_n \in \mathbb{R}$, $a_i \geq 0$, probar que $\prod_{i=1}^{n}(1 + a_i) \geq 1 + \sum_{i=1}^{n} a_i$

Deducir, como caso particular, que si $a \in \mathbb{R}$, $a \geq 0$, $(1 + a)^n \geq 1 + na$.

10. Usando el principio de inducción generalizada, demostrar:

    10.1 Para todo $n \in \mathbb{N}$, $n \geq 2$, es $(1 + a)^n > 1 + na$ si $a > 0$.

10.2. Para todo $n \in \mathbb{N}$, $n > 3$, es $4n + 2 < n.(n + 1)$.

10.3. Para todo $n \in \mathbb{N}$, $n \geq 2$, es $\sum_{i=1}^{n} (n + 2i) > n(n+1)$

10.4. Para todo $n \in \mathbb{N}$, $n \geq 3$ es $2n + 1 < 2^n$

10.5. Para todo $n \geq 2$ $\sum_{i=1}^{2n} \frac{i}{i+1} \leq 2n - 1$.

10.6. Para todo $n \geq 3$ $\sum_{i=1}^{n} \frac{2^i}{i} \leq n! + 1$

11. Calcular: $\binom{0}{0}, \binom{1}{0}, \binom{1}{1}, \binom{k}{0}, \binom{8}{7}, \binom{8}{8}, \binom{3}{2}, \binom{8}{5}, \binom{6}{3}$

12. Demostrar que para $n \in \mathbb{N}$, $0 \leq k \leq n$ $\binom{n}{k} = \binom{n}{n-k}$

13. Demostrar que para todo $n \in \mathbb{N}$, $\sum_{i=1}^{n} i.i! = (n+1)! - 1$

14. Mediante el Teorema del Binomio, deducir una fórmula para $(a - b)^n$.

15. Usando el Binomio de Newton, demostrar:

i. $\sum_{i=0}^{n} \binom{n}{i} = 2^n$ ii. $\sum_{i=0}^{n} (-1)^i \binom{n}{i} = 0$

16. Calcular el coeficiente de x^{20} en el desarrollo del binomio $(2x^2 + y^2)^{12}$.

17. Probar que para todo $n \in \mathbb{N}$ $\binom{n}{1} + 2\binom{n}{2} + ... + n\binom{n}{n} = n.2^{n-1}$

18. Demostrar que $2^n n! < (n+1)^n \quad \forall n > 1$

19. i. Sea $n \in \mathbb{N}$. Determinar si $\exists\, x \in \mathbb{N}$ tal que $3^n + x = 3^{n+1}$.

ii. Sean $n, m \in \mathbb{N}$, demostrar que $2^n \leq 2^m \Leftrightarrow n \leq m$

iii. Sean $n, m \in \mathbb{N}$, demostrar que $\exists s \in \mathbb{N}$ tal que $2^n + 2^m = 2^s$.
si y sólo si $n = m$.

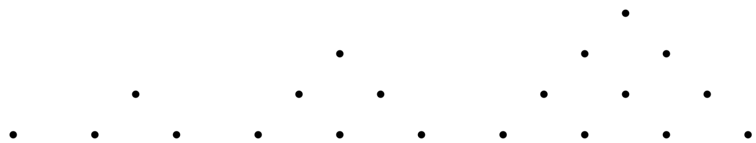
20. Demostrar que para $z, y \in \mathbb{R}$, $n \in \mathbb{N}$, $z^n - y^n = (z - y).\sum_{i=0}^{n-1} z^i y^{n-1-i}$

Algo más…

*Fermat (*1601-1665*) esperaba conseguir interesar a Pascal (*1623-1662*) en la teoría de números, y en* 1654 *le envió el enunciado de uno de sus más bellos teoremas (que no fue demostrado hasta el siglo XIX):*

> *Todo número entero se compone de uno, dos o tres números triangulares; de uno, dos, tres o cuatro cuadrados; de uno, dos, tres, cuatro o cinco pentagonales; de uno, dos, tres, cuatro, cinco o seis hexagonales, y así hasta el infinito.*

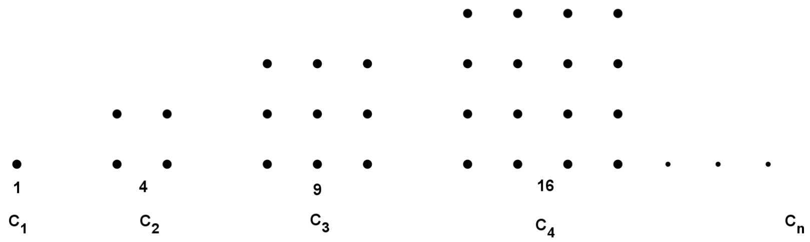
Los números 1, 1+2, 1+2+3, 1+2+3+4, 1+2+3+4+5, ... *que se pueden representar, por ejemplo, como muestra la ilustración, se llaman **números triangulares** :*



- *¿qué número representa el vigésimo término?, el centésimo? el n-ésimo término?.*

*Los números representados en la ilustración, se denominan **números cuadrados**:*

- *¿Qué número cuadrado ocupa el décimo lugar?, el centésimo ?, y el n-ésimo lugar?*

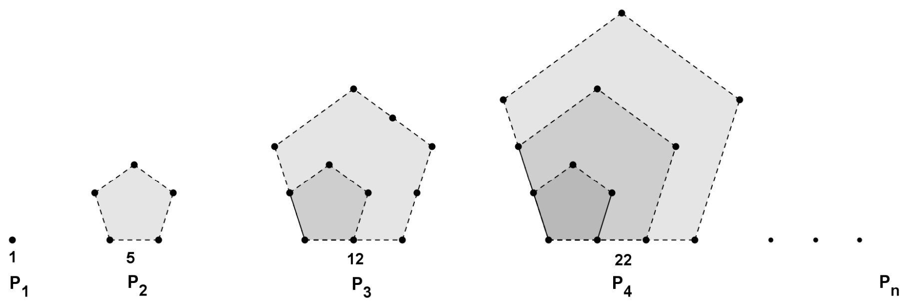


Observando el esquema podemos notar que

C_1=1, C_2 = 1+3, C_3 = 1+3+5 ,

C_4 =……,………..., C_9 =……..……………….., C_n =……………..

*La siguiente ilustración muestra los **números pentagonales**:*



¿Cuál es el octavo número pentagonal?,¿cuál es el vigésimo?,

¿el centésimo?....¿qué expresión puede representar el n-ésimo número pentagonal?

- *Compruebe el teorema que Fermat le enviara a Pascal para el caso de los números:* 17; 38; 126*;* …

- *Observando la siguiente lista, elabore a partir de ella una conjetura y demuéstrela:*

$1^2 - 0^2 = 1$
$2^2 - 1^2 = 3$
$3^2 - 2^2 = 5$
$4^2 - 3^2 = 7$

- *La observación de las siguientes igualdades de la derecha sugiere que la expresión* $n^2 - n + 41$*, siendo n un número natural, sirve para generar números primos (se dice que un número natural es primo si admite exacatamente dos divisore positivos) ,*
Pero, ¿qué ocurre cuando n = 41*?*

$1^2 - 1 + 41 = 41$
$2^2 - 2 + 41 = 43$
$3^2 - 3 + 41 = 47$
$4^2 - 4 + 41 = 53$
$5^2 - 5 + 41 = 61$

El razonamiento inductivo, *que fuimos aplicando supone la observación de cierta cantidad de casos que siguen alguna regularidad y que permiten elaborar una conjetura, pero* ***la formulación de una conjetura no garantiza de ningún modo la veracidad de la misma.***
Para probar la falsedad de una conjetura, recurrimos a la utilización del contraejemplo: es decir, buscamos un caso en el que la misma no se verifique.

CAPÍTULO V

NÚMEROS ENTEROS

Grabado de la "Aritmética" de Magnitski (editada en el año 1703). El dibujo representa el Templo de la Sabiduría. La Sabiduría está sentada en el trono de la Aritmética y en los escalones están los nombres de las operaciones aritméticas (división, multiplicación, sustracción, adición, cálculo). Las columnas son las ciencias en que la aritmética encuentra aplicación: geometría, estereometría, astronomía, óptica (conocimientos adquiridos por "vanidad"), mercatoria (es decir cartografía), geografía, fortificación, arquitectura (conocimientos adquiridos por "estudio"). Bajo las columnas dice, también en eslavo antiguo: "La Aritmética que se apoya en las columnas, lo abarca todo"

Definimos en $\mathbb{R}$ el conjunto de números naturales, demostramos que la suma y el producto de números naturales son, en cada caso, números naturales; vimos las propiedades que verificaban estas operaciones en $\mathbb{N}$, y aquéllas que no, como por ejemplo, que no siempre es posible resolver la ecuación lineal:

$$a + x = b$$

pero que, cuando la solución existe, es única.

Para subsanar este inconveniente extendemos el conjunto $\mathbb{N}$ a un conjunto más amplio, que contenga al neutro de la suma: 0 , y a los opuestos de los números naturales.
Para ello definimos el conjunto de números enteros $\mathbb{Z}$ (del alemán ***zahl***: número) como sigue:

$$\mathbb{Z} = \mathbb{N} \cup \mathbb{N}^- \cup \{0\} \text{ donde } \mathbb{N}^- = \{-n / n \in \mathbb{N}\}$$

Un poco de historia…

Los chinos utilizaban bastoncillos de bambú negros o rojos para representar cantidades positivas o negativas respectivamente. De este modo podían tratar cuestiones relacionadas con los aumentos y disminuciones de magnitudes, con distancias recorridas en sentidos opuestos y con cáculos comerciales.

La incorporación del cero es atribuída a la cultura India hacia el 650 DC . Los matemáticos hindúes diferenciaban entre números positivos y negativos, interpretando a éstos como créditos y débitos respectivamente. El matemático hindú Brahmagupta fue quien presentó en su obra soluciones negativas para ecuaciones cuadráticas.

Los antiguos griegos, sin embargo, rechazaron la existencia de los números negativos.

En la Europa medieval, fueron los árabes quienes introdujeron los números negativos de los hindúes.

Durante el Renacimiento y gracias a su utilización en la contabilidad, estos números fueron introduciéndose lentamente en las Matemáticas.

Recién en el siglo XV, el matemático alemán Michael Stifel (1487-1567), monje agustino convertido al protestantismo y amigo personal de Lutero, popularizó la notación para los números positivos y negativos, mediante los símbolos germánicos (+) *y* (-). *Antes de esto se utilizaba la letra* ***p*** *para simbolizar a los números positivos y la letra* ***m*** *para los negativos.*

Recién hacia el siglo XVIII, cuando los números negativos comenzaron a ser entendidos como opuestos de los números positivos, alcanzó aceptación general la consideración de las cantidades negativas como correspondientes a números matemáticamente legítimos.

***Proposición*:** Si $a, b \in \mathbb{Z}$, entonces $a + b \in \mathbb{Z}$ y $a.b \in \mathbb{Z}$.

***Demostración*:** Queda como ejercicio.

Por la proposición, la suma y el producto son operaciones en $\mathbb{Z}$, o sea

$+ : \mathbb{Z}\times\mathbb{Z} \to \mathbb{Z}$ $\quad$ $. : \mathbb{Z}\times\mathbb{Z} \to \mathbb{Z}$

$(a, b) \to a + b$ $\quad$ $(a, b) \to a.b$

son funciones, restricciones de las correspondientes en $\mathbb{R}$.

Las operaciones en $\mathbb{Z}$ satisfacen las siguientes propiedades:
La suma:

- asociativa
- conmutativa
- tiene elemento neutro: 0
- todo elemento tiene inverso u opuesto.

Por verificar todas estas propiedades, se dice que ($\mathbb{Z}$, +) es un *grupo abeliano.*

Ejercicio: Demostrar que en $\mathbb{Z}$ se verifica que la ecuación $a + x = b$ admite solución, y ésta es única.

El producto:

- asociativo
- conmutativo
- tiene elemento neutro: 1

- Además se verifica la distributividad del producto respecto de la suma.

Por tener en $\mathbb{Z}$ dos operaciones: **+** y **.** , que verifican todas las propiedades enunciadas, decimos que ($\mathbb{Z}$, + , **.**) es un *anillo conmutativo con identidad.*

No hemos hecho mención a la existencia de inversos para enteros no nulos, pero podemos demostrar que:

***Proposición*:** Si $a, b \in \mathbb{Z}$ son tales que $a.b = 1$ entonces $a = b = 1 \ \vee \ a = b = -1$

***Demostración*:** Queda como ejercicio.

Nota: Por la proposición, tenemos que los ***únicos*** elementos inversibles de $\mathbb{Z}$ son 1 y –1.

Divisibilidad en $\mathbb{Z}$ *:*

Definición*:** Sean $a, b \in \mathbb{Z}$, $a \neq 0$, decimos que ***a *divide a* ***b*** (o que *a es factor de b,* o que *a es parte de b*, o que *a es divisor de b,* o que *b es múltiplo de a*) si $\exists c \in \mathbb{Z}$ tal que $b = c.a$

Notación: $a \mid b$;
para indicar que ***a*** *no divide a* ***b*** *,* escribimos $a \nmid b$.

Ejemplos: $3 \mid 12$ pues $12 = 4.3$, $1 \mid 5$ pues $5 = 1.5$, $2 \mid 14 \ \wedge \ 7 \mid 14$ pues $14 = 2.7$

$3 \nmid 10$ pues $3.3 = 9 < 10 \ \wedge \ 3.4 = 12 > 10 \ \therefore \ 3.k \geq 12 > 10$, $\forall k \geq 4$

$1 \mid a \wedge -1 \mid a;\ \forall a \in \mathbb{Z}$, pues $a = 1.a = (-1).(-a)$.

Si $a \neq 0$, $a \mid a$; $a \mid -a$; $-a \mid a$ pues $-a = (-1).a$.

***Propiedades*:** Sean $a, b, c \in \mathbb{Z}$, $a \neq 0 \wedge b \neq 0$.

i. $a \mid b \wedge b \mid c \Rightarrow a \mid c$ (transitiva)
ii. $a \mid b \wedge b \mid a \Rightarrow |a| = |b|$
iii. $a \mid b \wedge a \mid c \Rightarrow a \mid (b + c)$. ¿Vale la recíproca?
iv. $a \mid (b + c) \wedge a \mid b \Rightarrow a \mid c$
v. $a \mid b \Rightarrow a \mid b.c \ \forall\, c \in \mathbb{Z}$; ¿es verdadero que si $a \mid b.c \Rightarrow a \mid b \vee a \mid c$?
vi. $a \mid b \Rightarrow -a \mid b \wedge a \mid -b$
vii. $a \mid 1 \vee a \mid -1 \Rightarrow a = 1 \vee a = -1$
viii. $a \mid 0$, $\forall\, a \in \mathbb{Z}$, $a \neq 0$.

***Proposición*:** Si $m, n \in \mathbb{N}$ son tales que $m \mid n$ entonces $m \leq n$.

***Demostración*:** Si $m \mid n$ entonces $\exists k \in \mathbb{Z}$ tal que $n = m \,.\, k$,
Como $n > 0 \wedge m > 0$ se tiene $k > 0 \ \therefore\ k \in \mathbb{N}$, y por consiguiente $k \geq 1$, así, multiplicando m.a.m. la desigualdad por m , tenemos que: $n = m \,.\, k \geq m \,.\, 1 = m$ como queríamos demostrar.

La proposición que demostramos nos dice que el conjunto de divisores naturales de un número natural está acotado superiormente por dicho número, por lo tanto es finito. Pero además, hemos visto que $a \mid b \Rightarrow -a \mid b \wedge a \mid -b$, lo que nos indica que los divisores de un número natural son los mismos que los de su opuesto, y que si un número divide a otro, también lo hace su opuesto, vale decir que para calcular los divisores de un número entero no nulo, podemos referirnos a su valor absoluto, que es natural, y ocuparnos sólo de los divisores naturales de éste, pues con ellos podemos determinarlos todos . Así, si $a \neq 0$, $a \in \mathbb{Z}$, el conjunto de divisores de a es finito, y tiene un número par de elementos.

Sea, para $b \in \mathbb{Z}$, el conjunto $D(b) = \{\, a \in \mathbb{Z} \ / \ a \mid b \,\}$

$D(0) = \mathbb{Z} - \{0\}$; $D(1) = D(-1) = \{1, -1\}$

Para $b \in \mathbb{Z} - \{0, 1, -1\}$, $4 \leq card\ D(b) < \infty$, pues $\{1, -1, b, -b\} \subset D(b)$.

***Definición*:** Sea $p \in \mathbb{Z}$, p se llama *número primo* si $card\ D(p) = 4$, o sea $D(p) = \{1, -1, p, -p\}$ y son todos distintos.

Ejemplo:

- 2 es primo,
  pues si $n \in \mathbb{N}$, $n \mid 2 \Rightarrow n \leq 2$, $\therefore\ n = 1 \vee n = 2$, y como $1 \mid 2 \wedge 2 \mid 2$ entonces
  $D(2) \cap \mathbb{N} = \{1, 2\}$ $\therefore$ $D(2) = \{1, -1, 2, -2\}$.

- 3 es primo,
  pues si $n \in \mathbb{N}$, $n \mid 3 \Rightarrow n \leq 3$, $\therefore\ n = 1 \vee n = 2 \vee n = 3$,
  como $1 \mid 3 \wedge 3 \mid 3$, falta ver que $2 \nmid 3$.
  $2.1 = 2 < 3$; $2.2 = 4 > 3$, $\therefore\ 2.k \geq 4 > 3$, $\forall k \geq 2$, luego $2 \nmid 3$.

- 5 es primo. Demostrarlo.

Nota:

- p es primo sii $-p$ es primo .
- $n \in \mathbb{N} - \{1\}$ no es primo sii $\exists k \in \mathbb{N}$ tal que $k \mid n \wedge 1 < k < n$.

Los números enteros pueden clasificarse en cuatro conjuntos disjuntos dos a dos, según el cardinal del conjunto de sus divisores:

$$\mathbb{Z} = \boldsymbol{P} \cup \boldsymbol{C} \cup \{1, -1\} \cup \{0\}$$

P conjunto de números primos (tienen exactamente cuatro divisores)
C conjunto de números *compuestos* (los que tienen finitos divisores y más de cuatro)
$\{1, -1\}$ las unidades, o elementos inversibles de $\mathbb{Z}$ (tienen exactamente dos divisores)
$\{0\}$ el neutro de la suma (tiene infinitos divisores)

***Teorema*:** Todo entero, distinto de 1 y –1 , es divisible por un número primo.

***Demostración*:** 0 es divisible por todo entero no nulo, en particular por los primos.
Demostraremos que todo $n \in \mathbb{N}$, $n > 1$, es divisible por un número primo, y lo haremos por inducción generalizada sobre *n.* Luego lo extenderemos a los demás enteros.

Sea la función proposicional " P(n) : $\exists p \in \mathbb{N}$ primo tal que $p \mid n$ "

P(2) es V pues 2 | 2 y 2 es primo

HI : sea $n > 2$, $\forall\ k \in \mathbb{N}$ tal que $2 \leq k < n$, $\exists p \in \mathbb{N}$ primo tal que $p \mid k$

¿Es verdadero que $\exists p \in \mathbb{N}$ primo tal que $p \mid n$?
Como $n \in \mathbb{N}$ y $n > 1 \Rightarrow n$ es primo $\vee$ n es compuesto

- Si n es primo como $n \mid n$ entonces P(n) es V.
- Si n es compuesto, entonces $\exists k \in \mathbb{N}$ tal que $k \mid n \wedge 1 < k < n$; k es tal que $2 \leq k < n$,
por HI $\exists p \in \mathbb{N}$ primo tal que $p \mid k$, y como $k \mid n \Rightarrow p \mid n$.

Luego P(n) es V, y todo número natural $n \geq 2$ es divisible por un número primo.
Sea ahora $-n$, con $n \in \mathbb{N}$, $n \neq 1$.

Por lo visto anteriormente, $\exists p \in \mathbb{N}$ primo tal que $p \mid n \Rightarrow p \mid -n$.
Entonces $\forall\ n \in \mathbb{Z} - \{1, -1\}$, $\exists p \in \mathbb{N}$ primo tal que $p \mid n$.

***Teorema* (*Euclides, –300*):** Hay infinitos números primos en $\mathbb{Z}$.

***Demostración*:** Basta con demostrar que los naturales primos son infinitos.

Supongamos que el conjunto ***P*** de naturales primos sea finito.

$$\boldsymbol{P} = \{p_1, p_2, p_3, ..., p_n\}$$

Sea $a = \prod_{i=1}^{n} p_i + 1$; $a \in \mathbb{N} \ \wedge a > 1 \Rightarrow \exists p \in \mathbb{N}$ primo tal que $p \mid a$

Como todos los naturales primos pertenecen a $\boldsymbol{P} \Rightarrow \exists j$, con $1 \leq j \leq n$ tal que $p = p_j$

$\therefore p \mid a \wedge p \mid \prod_{i=1}^{n} p_i \Rightarrow p \mid 1$!! (absurdo!)

Luego no todos los primos pueden estar en ***P***, o sea, ningún conjunto finito puede contener todos los naturales primos, por lo tanto ***P*** es un conjunto infinito.

Algoritmo de la División en $\mathbb{Z}$ **(*Euclides, –300*)**:

A pesar de ser el matemático más famoso de la antigüedad, poco se conoce de su biografía. Es probable que se educara en Atenas. Trabajó en la escuela de Alejandría alrededor de 300 AC. En su obra más importante "Los Elementos"(en griego Στοιχεια), que consta de trece libros, Euclides incluye toda la matemática desarrollada hasta esa época constituyendo un modelo de rigor matemático, por tratarse un desarrollo sistemático de proposiciones a partir de definiciones y axiomas.
Si bien de los trece libros, la mayor parte está dedicada a temas de geometría, los libros VII, VIII y IX desarrollan la teoría de números.

Sean $a, b \in \mathbb{Z}$, $a \neq 0$. $\exists! q, r \in \mathbb{Z}$ tales que $b = q.a + r$ con $0 \leq r < |a|$.

***Demostración*:** Demostraremos, primero, la *existencia* de q y r.

Supongamos, en primer término, que $a \in \mathbb{N}$.
Sea $B = \{b - k.a / k \in \mathbb{Z}\}$
Por ejemplo, en B están: b ; $b - a$; $b + a$; $b - 2a$; $b + 2a$; $b - 5a$; $b + 9a$;….

$0 \in B \Leftrightarrow a \mid b \Leftrightarrow \exists q \in \mathbb{N}$ tal que $b = q.a = q.a + 0$.
Luego, cuando $0 \in B$, $\exists! q, r \in \mathbb{Z}$ tales que $b = q.a + r$ con $0 \leq r < |a|$.

Sea, ahora, $0 \notin B$. Afirmamos que $B \cap \mathbb{N} \neq \phi$, dado que:

- si $b \in \mathbb{N}$ entonces $b \in B \cap \mathbb{N}$
- si $b \notin \mathbb{N}$ entonces $b = 0 \vee b \in \mathbb{N}^-$

$b \neq 0$ pues $0 \notin B \therefore b \in \mathbb{N}^-$.
Para $b \in \mathbb{N}^-$, $b - (b-1).a \in B \wedge b - (b-1).a = b.(1-a) + a$,
como $b < 0 \wedge (1-a) \leq 0 \Rightarrow b.(1-a) + a > 0 \therefore b.(1-a) + a \in B \cap \mathbb{N}$.

$B \cap \mathbb{N} \subset \mathbb{N} \ \wedge B \cap \mathbb{N} \neq \phi$, entonces tiene mínimo. Sea $r = mín\, B \cap \mathbb{N}$.
$r \in B \cap \mathbb{N} \ \therefore r = b - q.a$ para cierto $q \in \mathbb{Z} \ \therefore b = q.a + r$; falta ver que $r < a = |a|$.
Supongamos que $r \geq a$, en ese caso $\exists k \in \mathbb{N}_0$ tal que $r = a + k \therefore$
$k = r - a = b - q.a - a = b - (q+1).a \in B \cap \mathbb{N}_0$, pero $k \neq 0$ pues $k \in B$ y $0 \notin B$, entonces
$k \in B \cap \mathbb{N} \ \wedge k < r$!! (absurdo!) , pues $r = mín\, B \cap \mathbb{N}$

$\therefore\ r \not\geq a \Rightarrow r < a.$
Por lo tanto, cuando $a \in \mathbb{N}\ \exists q, r \in \mathbb{Z}$ tales que $b = q.a + r$ con $0 \leq r < |a| = a.$

Sea, ahora, $a \in \mathbb{N}^- \Rightarrow -a \in \mathbb{N}\ \therefore \exists q, r \in \mathbb{Z}$ tales que $b = q.(-a) + r$ con $0 \leq r < -a = |a|$. Por lo tanto $b = (-q).a + r$ con $0 \leq r < -a = |a|$.

Hemos demostrado la existencia de q y r cualquiera sea $a \in \mathbb{Z} - \{0\}$.

Unicidad de q *y* r :

Supongamos que existan $q, q', r, r' \in \mathbb{Z}$ tales que $b = q.a + r = q'.a + r'$, con
$0 \leq r < |a| \wedge 0 \leq r' < |a|$. Entonces $(q - q').a = r' - r \Rightarrow |q - q'| \cdot |a| = |r' - r|$
$\therefore |a| \mid |r' - r|, |a| \in \mathbb{N} \wedge |r' - r| \geq 0 \Rightarrow |a| \leq |r' - r| \vee |r' - r| = 0$
Si $|r' - r| \in \mathbb{N}$, es $|r' - r| \leq máx\{r, r'\} < |a| \leq |r' - r|$!! (absurdo!)
Luego $|r' - r| \notin \mathbb{N} \Rightarrow |r' - r| = 0\ \therefore r' - r = 0$, y así $r = r'$.
Entonces $(q - q').a = 0$, y como $a \neq 0$ es $q - q' = 0\ \therefore q = q'$.
Luego q y r son únicos tales que $b = q.a + r$, con $0 \leq r < |a|$.

Máximo Común Divisor (MCD):

Sean $a, b \in \mathbb{Z}$, no simultáneamente nulos.

Sea $D = D(a) \cap D(b) \cap \mathbb{N}$, $1 \in D\ \therefore D \neq \phi$.
D está acotado superiormente en $\mathbb{N}$, pues $|a| \in \mathbb{N} \vee |b| \in \mathbb{N}$, con lo cual el $máx\{|a|, |b|\}$ es cota superior de D, por lo tanto D tiene máximo d.
$d = máx\ D \Leftrightarrow d \in \mathbb{N} \wedge$ (si $s \in \mathbb{N}$ es tal que $s \mid a \wedge s \mid b$ entonces $s \leq d$)

Nota: d es *único* pues es el máximo en un conjunto no vacío.

***Definición*:** d se denomina *máximo común divisor de* a *y* b ; y se lo denota : $d = (a, b)$

***Definición*:** a y b se dicen *coprimos,* o *primos entre sí* si $(a, b) = 1$
.
Observación: a y b son coprimos sii los únicos divisores comunes son 1 y –1.

***Teorema*:** Sean $a, b \in \mathbb{Z}$, no simultáneamente nulos, $d \in \mathbb{N}$ tal que $d \mid a \wedge d \mid b$.
Entonces, son equivalentes:

i. $d = (a, b)$
ii. $\exists u, v \in \mathbb{Z}$ tales que $d = u.a + v.b$
iii. si $s \in \mathbb{Z}$ es tal que $s \mid a \wedge s \mid b$ entonces $s \mid d$.

***Demostración*:** Para demostrar la equivalencia de estas tres propiedades, bastará con demostrar que: i. $\Rightarrow$ ii. , ii. $\Rightarrow$ iii. , y que iii. $\Rightarrow$ i. , y por la transitividad de la implicación se establecen las implicaciones que restan.

i. $\Rightarrow$ ii.) Nuestra hipótesis es que $d = (a, b)$; debemos probar que $\exists u, v \in \mathbb{Z}$ tales que:
$d = u.a + v.b$

Sea $K = \{k.a + h.b \ / \ k,h \in \mathbb{Z}\}$; por ejemplo están en *K*: *a, b, – a, – b, a + b, a – b,* 0, $a + 2b$, $2a - b$, *etc.*

Como $\{a, -a, b, -b\} \cap \mathbb{N} \neq \phi \Rightarrow K \cap \mathbb{N} \neq \phi$, luego $K \cap \mathbb{N}$ tiene mínimo d'.

$d' \in \mathbb{N} \ \wedge \ d' \in K \ \therefore \ \exists u,v \in \mathbb{Z}$ tales que $d' = u.a + v.b$.
Como $d \mid a \ \wedge \ d \mid b \Rightarrow d \mid u.a \ \wedge \ d \mid v.b \ \therefore \ d \mid (u.a + v.b) = d'$, y como $d, d' \in \mathbb{N} \Rightarrow d \leq d'$.

Para ver que $d' \leq d$ usaremos la maximalidad de d en *D.*
Veamos si $d' \mid a$:
Por el Algoritmo de la División, $\exists!\ q, r \in \mathbb{Z}$ tales que $a = q.d' + r$ con $0 \leq r < d'$;
reemplazando d' tenemos que $a = q.(u.a + v.b) + r$, de donde $r = (1 - q.u).a - q.v.b \in K$.
Como $d' = mín\ K \cap \mathbb{N} \ \wedge \ r < d' \Rightarrow r \notin \mathbb{N} \ \therefore \ r = 0$ luego $d' \mid a$.
En forma análoga demostramos que $d' \mid b$.
Por lo tanto $d' \mid a \ \wedge \ d' \mid b \ \wedge \ d' \in \mathbb{N} \Rightarrow d' \leq d$, por definición de *d.*
Luego $d = d'$ y entonces $\exists u, v \in \mathbb{Z}$ tales que $d = u.a + v.b$.

ii. $\Rightarrow$ iii.) Ahora nuestra hipótesis es que $\exists u, v \in \mathbb{Z}$ tales que $d = u.a + v.b$, debemos probar que si $s \in \mathbb{Z}$ es tal que $s \mid a \ \wedge \ s \mid b \Rightarrow s \mid d$.

Sea, entonces, $s \in \mathbb{Z}$ tal que $s \mid a \ \wedge \ s \mid b$, se verifica que $s \mid u.a \ \wedge \ s \mid v.b \ \therefore \ s \mid (u.a + v.b) = d$.

iii. $\Rightarrow$ i.) La hipótesis es " si $s \in \mathbb{Z}$ es tal que $s \mid a \ \wedge \ s \mid b$ entonces $s \mid d$ ", y con ella debemos probar que $d = (a , b)$.

Sabemos que $d \in \mathbb{N} \ \wedge \ d \mid a \ \wedge \ d \mid b$, sólo nos queda ver que es el mayor natural con esa propiedad.
Sea $k \in \mathbb{N}$ tal que $k \mid a \ \wedge \ k \mid b$; $k \in \mathbb{Z}$ pues $\mathbb{N} \subset \mathbb{Z}$, luego, por hipótesis $k \mid d$, como ambos son naturales, eso implica que $k \leq d$, y así $d = máx\ D$, $\therefore \ d = (a , b)$.

Nota: En virtud de las definiciones, y de las propiedades de divisibilidad, se verifica que
$(a , b) = (a , –b) = (–a , –b) \quad \forall a, b \in \mathbb{Z}$ no simultáneamente nulos.

***Corolario (Teorema de Bezout)*:** Sean $a, b \in \mathbb{Z}$, no simultáneamente nulos. Entonces
a y b son coprimos si y sólo si $\exists u, v \in \mathbb{Z}$ tales que $u.a + v.b = 1$.

***Demostración*:** Es un caso particular del teorema.

***Propiedades*:** Sean $a, b, c \in \mathbb{Z}$, no simultáneamente nulos, $d \in \mathbb{N}$ tal que $d \mid a \ \wedge \ d \mid b$

Demostrar:

i. Si $d = (a , b)$ entonces $dc = (ac , bc) \quad \forall c \in \mathbb{N}$
ii. $d = (a , b) \Leftrightarrow \left(\frac{a}{d} , \frac{b}{d}\right) = 1$
iii. Para $a \neq 0$, $(a , b) = |a| \Leftrightarrow a \mid b$
iv. Si $b = q.a + r$ entonces $(a , b) = (a , r)$. En particular $(a - b , a) = (a , b) = (a + b , a)$
v. Para $c \neq 0, c \mid a.b \ \wedge \ (a , c) = 1 \Rightarrow c \mid b$
vi. Para $a \neq 0, b \neq 0, a \mid c \ \wedge \ b \mid c \ \wedge \ (a , b) = 1 \Rightarrow a.b \mid c$
vii. Generalización: si $a_i \neq 0$, $a_i \mid c \ \forall i$, $i = 1,2,..n$, y $(a_i , a_j) = 1$, para $i \neq j$, entonces $\prod_{i=1}^{n} a_i \mid c$

viii. $p, q \in \mathbb{N}$ primos , $(p , q) = 1 \Leftrightarrow p \neq q$
ix. $(a , c) = (b , c) = 1 \Rightarrow (ab , c) = 1$

***Demostración*:** Queda como ejercicio.

Ejemplo: Vamos a encontrar (a , b) usando la propiedad : $(a – b , a) = (a , b) = (a + b , a)$.

$(1347 , 784) = (1347 – 784 , 784) = (563 , 784) = (563 , 221) = (342 , 221) =$
$= (121 , 221) = (100 , 121) = (100 , 21) = (21 , 79) = (21 , 58) = (21 , 37) =$
$= (21 , 16) = (5 , 16) = (5 , 11) = (5 , 6) = (5 , 1) = 1$.

***Teorema*:** Sea $p \in \mathbb{N}$, $p > 1$. Son equivalentes:
i. p es primo.
ii. $\forall a \in \mathbb{Z}$ se verifica una y sólo una de estas propiedades: $p \mid a \vee (p , a) = 1$.
iii. Si $p \mid a.b$, para ciertos $a,b \in \mathbb{Z}$, entonces $p \mid a \vee p \mid b$.

***Demostración*:** En este caso es conveniente demostrar las equivalencias: i. $\Leftrightarrow$ii., e i. $\Leftrightarrow$iii.

i. $\Rightarrow$ ii.) Sea p primo; para $a \in \mathbb{Z}$ $\Rightarrow p \mid a \vee p \nmid a$.
Si $p \mid a$ no hay nada que demostrar .
Si $p \nmid a$, sea $d = (a , p)$. Si $d > 1$, $\exists q \in \mathbb{N}$ primo tal que $q \mid d$
como $d \mid a \wedge d \mid p$ entonces $q \mid a \wedge q \mid p$
pero p y q son naturales primos $\therefore p = q$, o sea $p \mid a$!! (absurdo!)
Luego $d = 1$ y $(a , p) = 1$.

ii. $\Rightarrow$ i.) Supongamos que p fuera compuesto, $\exists k, h \in \mathbb{N}$ tales que $p = k.h$ con
$1 < k < p \wedge 1 < h < p \therefore p \nmid k \wedge p \nmid h$, pues $k, h < p$, y $(p , k) \neq 1 \wedge (p , h) \neq 1$.

i $\Rightarrow$ iii.) Sean p primo, $a , b \in \mathbb{Z}$ tales que $p \mid a.b$.
Puede ocurrir que $p \mid a \vee p \nmid a$.
Si $p \mid a$ no hay nada que demostrar pues $p \mid a \vee p \mid b$.
Si $p \nmid a$ $\Rightarrow (a , p) = 1$, pues p es primo. Por el Teorema de Bezout $\exists u, v \in \mathbb{Z}$ tales que

$1 = u.a + v.p$

multiplicando m.a.m. por b, $b = u.a.b + v.p.b$

como $p \mid a.b \Rightarrow p \mid a.b.u$, además $p \mid v.p.b \therefore p \mid (a.b.u + v.b.p) = b$, que es lo que queríamos probar.

iii. $\Rightarrow$ i.) Supongamos que p fuera compuesto, $\exists k, h \in \mathbb{N}$ tales que $p = k.h$ con

$1 < k < p \wedge 1 < h < p \therefore p \mid k.h \wedge p \nmid k \wedge p \nmid h$, pues $k, h < p$.

Ejercicios:

1) Sea p primo, tal que $p \mid \prod_{i=1}^{n} a_i$, con los $a_i \in \mathbb{Z}$, entonces $\exists j$, $1 \leq j \leq n$, tal que $p \mid a_j$.

2) Sea $p \in \mathbb{N}$, $p > 1$; p es primo $\Leftrightarrow (p , k) = 1$ $\forall k$, $1 \leq k < p$.

Algoritmo de Euclides para hallar el MCD:

Veremos como, usando el Algoritmo de la División, podemos encontrar el MCD de dos números enteros.

Si $a, b \in \mathbb{Z}$, no simultáneamente nulos, $(a , b) = (|a| , |b|)$, donde $|a| \vee |b| \in \mathbb{N}$.

Además, si $b = q.a + r$ entonces $(a , b) = (a , r)$ y para $a \neq 0$, $(a , b) = |a| \Leftrightarrow a \mid b$.

Por lo tanto, $b = 0 \Rightarrow (a , b) = |a|$.

Sean entonces $a, b \in \mathbb{N}$, con $a < b$, pues cuando $a = b$, tenemos que $(a , b) = a$.

Aplicando el Algoritmo de la División (AD), tenemos que

$$b = q.a + r \text{ con } 0 \leq r < a$$

Si $r = 0$ entonces $(a , b) = (a , 0) = a$,

si $r \neq 0$ entonces $0 < r < a$, apliquemos AD, dividiendo a por r :

$$a = q_1 .r + r_1 \text{ con } 0 \leq r_1 < r < a.$$

Si $r_1 = 0$ entonces $(a , b) = (a , r) = r$,

si $r_1 \neq 0$ entonces $0 < r_1 < r < a$, dividiendo r por r_1

$$r = q_2 . r_1 + r_2 \text{ con } 0 \leq r_2 < r_1 < r < a$$

Si $r_2 = 0$ entonces $(a , b) = (a , r) = (r , r_1) = r_1$,

si $r_2 \neq 0$ entonces $0 < r_2 < r_1 < r < a$, dividiendo r_1 por r_2

$$r_1 = q_3 .r_2 + r_3 \quad \text{con} \quad 0 \leq r_3 < r_2 < r_1 < r < a$$

Continuando con este proceso, llegamos a

$r_k = q_{k+2} .r_{k+1} + r_{k+2}$, $0 \leq r_{k+2} < r_{k+1} < r_k < \ldots < r < a$, para algún k,

con $r_{k+2} = 0$, pues la sucesión $(r_i)_i$ con $0 < r_i < r_{i-1}$ no puede tener infinitos términos, porque no hay más que finitos números naturales menores que a.

Luego, si $r_{k+2} = 0$, como $r_{k-1} = q_{k+1} .r_k + r_{k+1}$ con $0 < r_{k+1} < r_k < r_{k-1} < \ldots < r < a$

tenemos que

$(a , b) = (a , r) = (r , r_1) = (r_1, r_2) = (r_2, r_3) = \ldots\ldots = (r_{k-1}, r_k) = (r_k , r_{k+1}) = r_{k+1}$.

Por lo tanto, el MCD de a y b es el *último resto no nulo* en este proceso.

Ejemplo: $a = 348$, $b = 1346$

$$1346 = 3.348 + 302$$
$$348 = 1.302 + 46$$
$$302 = 6.46 + 26$$
$$46 = 1.26 + 20$$
$$26 = 1.20 + 6$$
$$20 = 3.6 + 2$$
$$6 = 3.2 + 0$$

Luego 2 = (348 , 1346).

Además de poder calcular el MCD de a y b, podemos encontrar u y v tales que $d = u.a + v.b$. Veámoslo más claro volviendo al ejemplo anterior :

2 = 20 – 3.6 = (46 – 1.26) – 3.(26 – 1.20) = 46 – 4.26 + 3.20 =
= 46 – 4.(302 – 6.46) + 3.(46 – 1.26) = 28.46 – 4.302 – 3.26 =
= 28.46 – 4.302 – 3.(302 – 6.46) = 46.46 – 7.302 =
= 46. (348 – 1.302) – 7.302 = 46.348 – 53.302 = 46.348 – 53.(1346 – 3.348) =
= 205.348 – 53.1346.

Así tenemos que $u = 205$, $v = -53$ verifican que $u.a + v.b = 2$

u y v ***no*** son únicos , como se ve en el ejemplo:

2 = 205.348 – 53.1346 = 205.348 – 53.1346 + 348.1346 – 348.1346 =
= (205 + 1346).348 – (53 + 348).1346 = 1551.348 – 401.1346

y así obtuvimos u' y v' , *distintos de* u *y* v , tales que $u'.a + v'.b = 2$.

Generalización del Máximo Común Divisor:

Sean $a_1, a_2, a_3, \ldots, a_n \in \mathbb{Z}$, no simultáneamente nulos;
Sea $D = \{ t \in \mathbb{N} \ / \ t \mid a_i \ \ \forall i = 1,2,....,n \}$; $D \neq \phi$ y acotado superiormente, luego tiene máximo d , que se denomina *máximo común divisor de* $a_1, a_2, a_3, \ldots, a_n$.

Notación : $(a_1, a_2, a_3, \ldots, a_n) = d$

***Definición*:** Sean $a_1, a_2, a_3, \ldots, a_n \in \mathbb{Z}$, no simultáneamente nulos, se dicen *coprimos* si $(a_1, a_2, a_3, \ldots, a_n) = 1$.

Nota: no es lo mismo decir que $a_1, a_2, a_3, \ldots, a_n$ son *coprimos*, que decir que *son coprimos dos a dos* , o sea $(a_i , a_j) = 1$ para $i \neq j$, pues si $a_1, a_2, a_3, \ldots, a_n$ son coprimos dos a dos entonces $a_1, a_2, a_3, \ldots, a_n$ son coprimos , pero la recíproca no es cierta (demostrarlo).

Ejercicio: Sean $a_1, a_2, a_3, \ldots, a_n \in \mathbb{Z}$, no nulos, $n > 2$, $d \in \mathbb{N}$ tal que $d \mid a_i \ \ \forall i = 1,2,...,n$; demostrar que $d = (a_1, a_2, a_3, \ldots, a_n) \Leftrightarrow d = (d_1 , a_n)$, con $d_1 = (a_1, a_2, a_3, \ldots, a_{n-1})$.

***Teorema*:** Sean $a_1, a_2, a_3, \ldots, a_n \in \mathbb{Z}$, no simultáneamente nulos, $n \geq 2$, $d \in \mathbb{N}$ tal que $d \mid a_i \ \ \forall i = 1,2,...,n$. Demostrar que son equivalentes:

i. $d = (a_1, a_2, a_3, \ldots, a_n)$

ii. $\exists u_i \in \mathbb{Z} \ \ i = 1,2,....,n$, tales que $d = \sum_{i=1}^{n} u_i a_i$

iii. Si $t \in \mathbb{Z}$ es tal que $t \mid a_i \ \ \forall i = 1,2,...,n$ entonces $t \mid d$

***Demostración*:** Queda como ejercicio.

Pista: usar inducción para demostrar alguna implicación.

***Corolario*:** Sean $a_1, a_2, a_3, \ldots, a_n \in \mathbb{Z}$, no simultáneamente nulos, $n \geq 2$,

$(a_1, a_2, a_3, \ldots, a_n) = 1$ si y sólo si $\exists u_i \in \mathbb{Z} \quad i = 1, 2, \ldots, n$, tales que $1 = \sum_{i=1}^{n} u_i a_i$.

Mínimo Común Múltiplo (MCM):

Sea $a \in \mathbb{Z}$, escribiremos $a\mathbb{Z} = \{ ak \ / \ k \in \mathbb{Z} \}$.

Sean $a, b \in \mathbb{Z} - \{0\}$.

Sea $M = a\mathbb{Z} \cap b\mathbb{Z} \cap \mathbb{N} = \{ x \in \mathbb{N} / \ a \mid x \wedge b \mid x \}$; $M \neq \phi$ pues $|a \cdot b| \in M$,
luego tiene mínimo m, que por ser tal verifica:

i. $m \in \mathbb{N}$
ii. $a \mid m \wedge b \mid m$
iii. si $c \in \mathbb{N}$ es tal que $a \mid c \wedge b \mid c$ entonces $m \leq c$.

.

***Definición*:** Al número m que cumple las condiciones *i.,ii.,iii.,* se lo denomina el *mínimo común múltiplo de* a *y* b, y se lo denota $m = [a, b]$.

Nota: m es *único* porque es el mínimo en un conjunto no vacío.

***Teorema*:** Sean $a, b \in \mathbb{Z} - \{0\}$, $m \in \mathbb{N}$ tales que $a \mid m \wedge b \mid m$.
Entonces, son equivalentes :

i. $m = [a, b]$
ii. si $c \in \mathbb{Z}$ es tal que $a \mid c \wedge b \mid c$ entonces $m \mid c$.

***Demostración*:** i. $\Rightarrow$ ii.)

Sea $m = [a, b]$ y sea $c \in \mathbb{Z}$ tal que $a \mid c \wedge b \mid c$.
Queremos ver que $m \mid c$:
Aplicando el Algoritmo de la División: $c = m.q + r$ con $0 \leq r < m$
Si $r > 0$ entonces $r \in \mathbb{N} \wedge r < m$
$a \mid m \Rightarrow a \mid m.q$, además $a \mid c \therefore a \mid r$
$b \mid m \Rightarrow b \mid m.q$, además $b \mid c \therefore b \mid r$
Por lo tanto $r \in M$, pero $r < m \wedge m = mín\, M$!! (absurdo!).
Entonces $r = 0$, luego $m \mid c$.

ii. $\Rightarrow$ i.) Sea $c \in \mathbb{N}$ tal que $a \mid c \wedge b \mid c$; queremos ver que $m \leq c$.
Por ii., como $c \in \mathbb{Z} \wedge a \mid c \wedge b \mid c \Rightarrow m \mid c \therefore m \leq c$, porque ambos son naturales.
Luego $m = [a, b]$.

Ejercicios:

1) $[a, b]=[|a|, |b|]$, $\forall a,b\in \mathbb{Z}-\{0\}$.

2) $[a, b]=|b| \Leftrightarrow a \mid b$.

3) Sean $a, b\in \mathbb{Z}$, $m\in \mathbb{N}$, tales que $a \mid m \wedge b \mid m$. Entonces:

$$m=[a, b] \Leftrightarrow \left(\frac{m}{a}, \frac{m}{b}\right)=1 .$$

***Teorema*:** Sean $a, b\in \mathbb{Z}-\{0\}$, $m=[a, b]$, $d=(a, b)$. Entonces $|a\cdot b|=m.d$.

***Demostración*:** Supongamos, primero, que $a, b\in \mathbb{N}$.

Si $m=[a, b]$, entonces $m=a.a'=b.b'$, con $(a', b')=1$, $a', b'\in \mathbb{N}$,

si $d=(a, b)$, tenemos que $a=d.k$, $b=d.h$, con $(k, h)=1$, $k, h\in \mathbb{N}$.

$m=a.a'=d.k.a'=b.b'=d.h.b'$.

De la igualdad $dk.a'=d.h.b'$ obtenemos que $k.a'=h.b'$.

Por lo tanto $k \mid h.b' \wedge (k, h)=1 \Rightarrow k \mid b'$, $\therefore b'=k.b''$

igualmente $h \mid k.a' \wedge (k, h)=1 \Rightarrow h \mid a' \therefore a'=h.a''$

reemplazando a' y b' en la igualdad: $k.a'=h.b'$

$k.h.a''=h.k.b'' \Rightarrow a''=b''$

pero $a''=b'' \mid b' \wedge b''=a'' \mid a' \wedge (a', b')=1 \Rightarrow a''=b''=1$

$\therefore a'=h \wedge b'=k$.

Luego $m=a.a'=d.k.h \Rightarrow m.d=d.k.h.d=a.b$.

Sean, ahora, $a, b\in \mathbb{Z}-\{0\}$, $m=[a, b]=[|a|, |b|]$, $d=(a, b)=(|a|, |b|)$,

con $|a|, |b|\in \mathbb{N}$, por lo tanto $m.d=|a|.|b|=|a\cdot b|$.

***Corolario*:** Para $a, b\in \mathbb{N}$, $[a, b]=a.b \Leftrightarrow (a, b)=1$.

Teorema Fundamental de la Aritmética (TFA):

$\forall a\in \mathbb{Z}-\{0, 1,-1\}$, $\exists p_1, p_2, ..., p_k\in \mathbb{N}$ primos, con $p_1\le p_2\le .....\le p_k$, tales que

$a=sg(a)\prod_{i=1}^{k} p_i$, donde $sg(a)=\begin{cases} 1 & si \quad a>0 \\ -1 & si \quad a<0 \end{cases}$

Los primos p_i *son únicos* en el sentido siguiente:

Si $p_1\cdot p_2\cdot p_3\cdot .....\cdot p_k=q_1\cdot q_2\cdot q_3\cdot .....\cdot q_h$, con $k, h\in \mathbb{N}$, $p_i, q_j\in \mathbb{N}$, p_i, q_j primos,

$\forall\, i, i=1,2,3,\ldots,k$; $\forall\, j, j=1,2,3\ldots,h$, $p_1\le p_2\le .....\le p_k$; $q_1\le q_2\le q_3\le ....\le q_h$

Entonces $k=h \wedge p_i=q_i \ \forall\, i=1,2,\ldots..,k.$

***Demostración*:** *Existencia de la factorización en primos.*

Sea $n\in \mathbb{N}$, $n>1$. Demostraremos por inducción sobre n, que se puede factorizar como producto de primos.

Sea P la función proposicional:

$P(n)$: $\exists\, p_1, p_2, ..., p_k \in \mathbb{N}$ primos, con $p_1 \le p_2 \le ..... \le p_k$, tales que $n = \prod_{i=1}^{k} p_i$.

i. $P(2)$ es V pues 2 es primo y $2 = 2$, con $k = 1$

ii. sea $n > 2$, supongamos, como hipótesis inductiva, que $P(k)$ es V , $\forall\, k, 2 \le k < n$.

Queremos demostrar que eso implica que $P(n)$ es V.

Por ser $n > 1$ se verifica que n es primo ó n es compuesto

- si n es primo, entonces $P(n)$ es V pues $n = n$, con $k = 1$
- si n es compuesto, $\exists p \in \mathbb{N}$, p primo, tal que $p \mid n$ y $1 < p \le n$, por ser p natural y primo; además $p \ne n$, pues n es compuesto, luego $1 < p < n$.

  Sea $p_1 = mín\{\, q \in \mathbb{N} \ / \ q \text{ es primo} \wedge q \mid n \,\}$.

  p_1 existe pues $\{\, q \in \mathbb{N} / \ q \text{ es primo} \wedge q \mid n \,\} \subset \mathbb{N}$, es no vacío, y $\mathbb{N}$ es b.o.

Entonces $n = p_1.m$, donde $1 < m < n$; por HI $P(m)$ es V , por lo tanto

$\exists\, p_2, ..., p_k \in \mathbb{N}$ primos tales que $m = p_2 \cdot p_3 \cdot ..... \cdot p_k$ con $p_2 \le p_3 \le ..... \le p_k$

reemplazando m , tenemos $n = p_1 \cdot m = p_1 \cdot p_2 \cdot p_3 \cdot ..... \cdot p_k$, luego $P(n)$ es V.

Por lo tanto $P(n)$ es V $\forall\, n \in \mathbb{N}$.

Supongamos ahora $a \in \mathbb{N}^-$, entonces $\exists n \in \mathbb{N}$ tal que $a = -n$.

Por ser $n \in \mathbb{N}$, $\exists\, p_1, p_2, ..., p_k \in \mathbb{N}$ primos, con $p_1 \le p_2 \le ..... \le p_k$, tales que

$n = \prod_{i=1}^{k} p_i$ entonces $a = -n = -\prod_{i=1}^{k} p_i = sg(a) \cdot \prod_{i=1}^{k} p_i$.

Unicidad de la factorización:

Si $p_1 \cdot p_2 \cdot p_3 \cdot ..... \cdot p_k = q_1 \cdot q_2 \cdot q_3 \cdot ..... \cdot q_h$, con $k, h \in \mathbb{N}$, p_i , $q_j \in \mathbb{N}$, p_i , q_j primos,

$\forall\, i, i = 1,2,3,\ldots,k$; $\forall\, j, j = 1,2,3\ldots,h$, $p_1 \le p_2 \le ..... \le p_k$; $q_1 \le q_2 \le q_3 \le .... \le q_h$,

debemos probar que $k = h \wedge p_i = q_i \ \ \forall i = 1, 2, 3, ..., k$.

Lo haremos por inducción sobre k.

Si $k = 1$, $p_1 = q_1 \cdot q_2 \cdot q_3 \cdot ..... \cdot q_h$.

Si $h > 1$, $q_1 \mid p_1 \wedge q_1.q_2 \mid p_1 \wedge 1 \mid p_1$!! (absurdo!) pues p_1 es primo $\Rightarrow h = 1 \wedge p_1 = q_1$.

Supongamos que todo producto de k primos se factorice de manera única.

Sea un producto de $k + 1$ primos, y supongamos que:

$$p_1.p_2 \cdot p_3 \cdot \ldots \cdot p_k \cdot p_{k+1} = q_1 \cdot q_2 \cdot q_3 \cdot ..... \cdot q_h \quad \text{(I)}$$

p_i , $q_j \in \mathbb{N}$, primos, $p_1 \le p_2 \le ..... \le p_k \le p_{k+1}$, $q_1 \le q_2 \le q_3 \le .... \le q_h$.

$p_1 \mid q_1 \cdot q_2 \cdot q_3 \cdot ..... \cdot q_h$, como p_1 es primo $\Rightarrow \exists\, j_1$, $1 \le j_1 \le h$ tal que $p_1 \mid q_{j_1}$,

y como q_{j_1} también es primo, se verifica que $p_1 = q_{j_1} \geq q_1$.

Recíprocamente $q_1 \mid p_1.p_2.p_3.....p_k.p_{k+1}$ como q_1 es primo ,

$\exists i_1$, $1 \leq i_1 \leq k+1$ tal que $q_1 \mid p_{i_1}$, y como también p_{i_1} es primo, $q_1 = p_{i_1} \geq p_1$.

Luego $p_1 = q_1$. De esta igualdad y de la (I) tenemos que

$$p_2.p_3.....p_k.p_{k+1} = q_2 \cdot q_3 \cdot .....\cdot q_h \ .$$

En el primer miembro de la igualdad tenemos un producto de *k* primos, por HI se factoriza de manera única, entonces $k = h - 1$ (el segundo miembro de la igualdad tiene $h - 1$ primos) $\Rightarrow k + 1 = h$, además, por HI , $p_i = q_i \ \ \forall\, i = 2,....,k+1$,

pero como $p_1 = q_1$, tenemos que $p_i = q_i \ \ \forall\, i = 1,2,....,k+1$.

Entonces, la proposición se verifica $\forall\, k \in \mathbb{N}$, y la factorización es única, sea cual fuere la cantidad de primos que en ella intervinieren.

Aplicaciones del TFA:

- ***Caracterizar los divisores naturales de un número natural, y calcular el cardinal del conjunto que constituyen.***

Sea $a \in \mathbb{N}$, $a > 1$, y sea $D = \{ x \in \mathbb{N} / \quad x \mid a \}$.

- Supongamos, primero, que $a = p$, con $p \in \mathbb{N}$, p primo.
  Sea $b \in \mathbb{N}$ tal que $b \mid a$ entonces $b = 1 \vee b = p \ \therefore \ card\, D = 2$.

- Sea $a = p^2$; $D = \{ 1,\ p,\ p^2 \}$ pues si $b \in \mathbb{N}$ es tal que $b \mid a$, con $b > 1$

$\exists q \in \mathbb{N}$, q primo, tal que $q \mid b \Rightarrow q \mid a \ \therefore \ q \mid p$, y como ambos son primos $q = p$.
Está claro que 1 , p y p^2 dividen a a .
Veamos que una potencia mayor que 2 de p no divide a a.
Si $p^k \mid a$, con $k > 2$, $a = p^k.s$, $s \in \mathbb{N}$ $\therefore\ p^2 = p^k.s \Rightarrow p^{k-2}.s = 1$; como $k - 2 \in \mathbb{N}$,
eso significa que $p \mid p^{k-2} \Rightarrow p \mid 1$!! (absurdo!) $\therefore\ p^k \nmid a \ \ \forall\, k \geq 3$.

$\therefore\ D = \{ 1,\ p,\ p^2 \}$, y $card\, D = 3$.

Además podemos afirmar que para $b \in \mathbb{N}$, $b \mid a \Leftrightarrow b = p^i$, con $0 \leq i \leq 2$.

- Sea en general $a = p^k$, $k \in \mathbb{N}$.

Veamos que para $b \in \mathbb{N}$, $b \mid a \Leftrightarrow b = p^i$, con $0 \leq i \leq k$.

$\Leftarrow$) Si $b = p^i$, con $0 \leq i \leq k$, $a = p^k = p^{k-i}\ .\ p^i = p^{k-i}.\ b$, donde $k - i \geq 0 \ \therefore\ p^{k-i} \in \mathbb{N}$,
por lo tanto $b \mid a$.

$\Rightarrow$) Si $b \mid a \wedge b > 1 \Rightarrow \exists q \in \mathbb{N}$, q primo, tal que $q \mid b \ \therefore\ q \mid a$, como $a = p^k$ y q es primo, entonces $q \mid p$, al ser p también primo , tenemos que $q = p$.
$\therefore$ en la factorización de b aparece un único primo que es p.
Sea entonces, $b = p^i$, con $i \in \mathbb{N}$. Si $i > k$, $a = p^k = b.c = p^i.c \Rightarrow p^{i-k}.c = 1$.
Como $i - k > 0$, $p \mid p^{i-k} \ \therefore\ p \mid 1$!! (absurdo!) , entonces $i \leq k$.

Para saber cuántos números hay en D , debemos contar los enteros i tales que $0 \le i \le k$, y éstos son $k + 1$.

$$D = \left\{ p^i \,/\, 0 \le i \le k \right\} = \left\{ p^0 = 1,\ p^1 = p,\ p^2,\ p^3, \ldots\ldots,\ p^k = a \right\}.$$

- Sea, ahora, $a = p_1^{r_1} \cdot p_2^{r_2}$, $p_i \in \mathbb{N}$, p_i primos, $r_i \in \mathbb{N}$, $i = 1, 2$, $p_1 \neq p_2$

Para $b \in \mathbb{N}$, $b \mid a \Leftrightarrow b = p_1^{s_1} \cdot p_2^{s_2}$, con $0 \le s_i \le r_i$, $i = 1, 2$.

$\Leftarrow$) Si $b = p_1^{s_1} \cdot p_2^{s_2}$, con $0 \le s_i \le r_i$, $i = 1, 2$.

$a = p_1^{r_1} \cdot p_2^{r_2} = (p_1^{s_1} \cdot p_2^{s_2}) \cdot (p_1^{r_1 - s_1} \cdot p_2^{r_2 - s_2}) = b.c$,

donde $c = p_1^{r_1 - s_1} \cdot p_2^{r_2 - s_2}$, $c \in \mathbb{N}$ pues $r_i - s_i \ge 0$, para $i = 1, 2 \therefore b \mid a$.

$\Rightarrow$) Sea $b \in \mathbb{N}$, $b \neq 1$, tal que $b \mid a$.

Si $q \in \mathbb{N}$, q primo, tal que $q \mid b \Rightarrow q \mid a \therefore \exists i$, $1 \le i \le 2$, tal que $q = p_i$,

por lo tanto los únicos primos que podrían dividir a b son p_1 o p_2 , de allí que la factorización de b en producto de primos debe ser de la forma: $b = p_1^{s_1} \cdot p_2^{s_2}$ con $s_i \ge 0$, $1 \le i \le 2$.

Falta ver que $s_i \le r_i$ para $i = 1, 2$.

Supongamos que $s_1 > r_1$.

$p_1^{s_1} \mid b \wedge b \mid a \Rightarrow p_1^{s_1} \mid a \therefore a = k \,.\, p_1^{s_1}$ con $k \in \mathbb{N}$;

como $a = p_1^{r_1} \cdot p_2^{r_2}$ tenemos que $p_1^{r_1} \cdot p_2^{r_2} = k.\, p_1^{s_1} \therefore p_2^{r_2} = k \,.\, p_1^{s_1 - r_1}$;

como $s_1 - r_1 > 0$, $p_1 \mid p_1^{s_1 - r_1}$, con lo cual $p_1 \mid p_2^{r_2} \Rightarrow p_1 = p_2$!! (absurdo!)

Análogamente si suponemos que $s_2 > r_2$, entonces $0 \le s_i \le r_i$, $i = 1, 2$.

Esta caracterización de los divisores de a nos permite determinar de qué forma son los elementos de D : $D = \left\{ p_1^{s_1} \cdot p_2^{s_2} \,/\, 0 \le s_i \le r_i ,\ i = 1, 2 \right\}$.

Para calcular cuántos elementos hay en D tenemos que contar cuántos pares ordenados (s_1 , s_2) podemos encontrar con $0 \le s_i \le r_i$, $i = 1, 2$. Escribamos la matriz formada por los pares (s_1 , s_2) indicados más arriba:

$$\begin{array}{ccccc}
(0, 0) & (1, 0) & (2, 0)..... & (r_1 - 1, 0) & (r_1, 0) \\
(0, 1) & (1, 1) & (2, 1)..... & (r_1 - 1, 1) & (r_1, 1) \\
(0, 2) & (1, 2) & (2, 2)..... & (r_1 - 1, 2) & (r_1, 2) \\
\vdots & \vdots & \vdots & \vdots & \vdots \\
(0, r_2) & (1, r_2) & (2, r_2)..... & (r_1 - 1, r_2) & (r_1, r_2)
\end{array}$$

Por lo tanto hay $(r_1 + 1).(r_2 + 1)$ divisores positivos de a.

Ejercicios:

Sea $a = p_1^{r_1} \cdot p_2^{r_2} \cdot p_3^{r_3} \ldots . p_k^{r_k}$, $p_i \in \mathbb{N}$, p_i primos $\forall i$, $i = 1,2\ldots,k$, $p_i \neq p_j$ para $i \neq j$, $r_i \in \mathbb{N}$.

i) Demostrar que para $b \in \mathbb{N}$, $b \mid a \Leftrightarrow b = \prod_{i=1}^{k} p_i^{s_i}$ con $0 \leq s_i \leq r_i$, $i = 1,2,\ldots,k$.

ii) Demostrar, por inducción sobre k , que la cantidad de divisores positivos de a es

$$(r_1 + 1).(r_2 + 1) \ldots\ldots.(r_k + 1).$$

Ejemplos:

1) *Determinar el menor número natural que posee* 15 *divisores positivos*.

Un tal número a es : $a = \prod_{i=1}^{k} p_i^{r_i}$, $p_i \in \mathbb{N}$, p_i primos, $r_i \in \mathbb{N}$.

Primero trataremos de determinar los posibles valores de k.

$(r_1 + 1).(r_2 + 1) \ldots\ldots.(r_k + 1) = 15$

las posibles factorizaciones de 15 son: 15 ($k = 1$) , 3.5 ($k = 2$) .

Si $k = 1$, hay un solo primo, y al tener que buscar el menor natural con 15 divisores, debe elegirse al primo 2, pues es el menor entre los naturales primos.

El exponente, en este caso, es r_1, y como $r_1 + 1 = 15 \Rightarrow r_1 = 14$.

Si $k = 2$, se eligen los dos primos menores : 2, 3 , y los exponentes satisfacen

$r_1 + 1 = 3 \wedge r_2 + 1 = 5 \Rightarrow r_1 = 2 \wedge r_2 = 4$.

Luego hay que comparar a los números: 2^{14} , $2^2 . 3^4$, $2^4 . 3^2$ y elegir el menor.

Comparemos $2^2 . 3^4$ y $2^4 . 3^2$: $2^2 . 3^4 = 2^2 . 3^2 . 3^2$ y $2^4 . 3^2 = 2^2 . 2^2 . 3^2$.

Como $2^2 < 3^2 \Rightarrow 2^2 . 2^2 . 3^2 < 2^2 . 3^2 . 3^2$ $\therefore$ $2^4 . 3^2 < 2^2 . 3^4$.

Comparemos 2^{14} y $2^4 . 3^2$: $2^{14} = 2^4 . 2^{10}$; $3^2 < 2^{10} \Rightarrow 3^2 . 2^4 < 2^{10} . 2^4$ $\therefore$ $2^4 . 3^2 < 2^{14}$.

Luego, el menor natural con 15 divisores positivos es $2^4 . 3^2$.

2) *Determinar el menor natural impar con* 13 *divisores positivos.*

Un tal número a es : $a = \prod_{i=1}^{k} p_i^{r_i}$, $p_i \in \mathbb{N}$, p_i primos , $r_i \in \mathbb{N}$.

Como $(r_1 + 1).(r_2 + 1).....(r_k + 1) = 13 \Rightarrow k = 1$ (pues 13 es primo)

$\therefore$ $r_1 + 1 = 13 \Rightarrow r_1 = 12$; además hay que elegir el menor primo impar, con lo cual $p_1 = 3$ $\therefore$ el número pedido es 3^{12} .

- ***Demostrar que*** $\nexists m, n \in \mathbb{Z} - \{0\}$ ***tales que*** $\mathbf{m^2 = 2n^2}$.

Como $m^2 = (-m)^2 \ \forall m \in \mathbb{Z}$,

$\exists m, n \in \mathbb{Z} - \{0\}$ tales que $m^2 = 2n^2 \Leftrightarrow \exists m, n \in \mathbb{N}$ tales que $m^2 = 2n^2$

Supongamos, entonces, que $\exists m, n \in \mathbb{N}$ tales que $m^2 = 2n^2$

$m > 1$, pues $n \geq 1$, entonces $n^2 \geq 1 \therefore 2n^2 \geq 2 \Rightarrow m^2 \neq 1 \therefore m \neq 1$.

Por el TFA $\exists\, p_1, p_2, ..., p_k \in \mathbb{N}$ primos tales que $m = p_1 \cdot p_2 \cdot p_3 \cdot ..... \cdot p_k$
con $p_1 \leq p_2 \leq ..... \leq p_k$.

- Si $n = 1$, entonces $m^2 = 2$, pero la factorización en producto de primos de m^2 es:
  $m^2 = p_1 \cdot p_1 \cdot p_2 \cdot p_2 ..... \cdot p_k \cdot p_k = 2$!! (absurdo!)

pues en el primer miembro de la igualdad, 2 aparece un número par de veces (pudiendo ser 0), y en el segundo, 2 aparece una sola vez, o sea un número impar de veces.
Por lo tanto $n > 1$.

- Si $n > 1$, por el TFA $\exists q_1, q_2, ..., q_h \in \mathbb{N}$, q_j primos, tales que
  $n = q_1 \cdot q_2 \cdot q_3 \cdot ..... \cdot q_h$ con $q_1 \leq q_2 \leq q_3 \leq .... \leq q_h$.

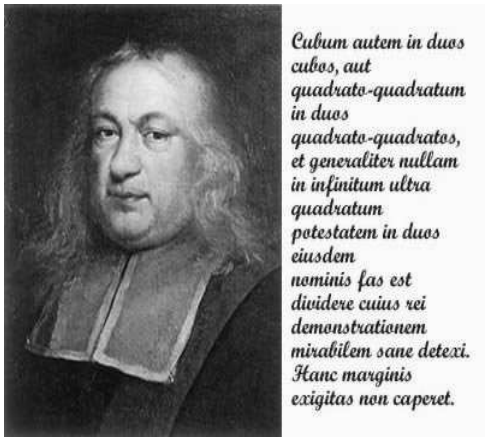
La factorización de $n^2 = q_1 \cdot q_1 \cdot q_2 \cdot q_2 ..... \cdot q_h \cdot q_h$, y de la igualdad $m^2 = 2n^2$ tenemos que

$p_1 \cdot p_1 \cdot p_2 \cdot p_2 ..... \cdot p_k \cdot p_k = 2.\ q_1 \cdot q_1 \cdot q_2 \cdot q_2 ..... \cdot q_h \cdot q_h$!! (absurdo!)

pues en el primer miembro de la igualdad, el 2 aparece un número par de veces, mientras que en el segundo 2 aparece un número impar de veces.
Por lo tanto $\nexists\, m, n \in \mathbb{N}$ tales que $m^2 = 2n^2 \Rightarrow \nexists\, m, n \in \mathbb{Z} - \{0\}$ tales que $m^2 = 2n^2$

Ecuaciones diofantinas (Diofanto de Alejandría, 200).

Poco se conoce de la vida de Diofanto, uno de los matemáticos de la llamada segunda escuela de Alejandría. Su nacimiento se ubica alrededor del año 200. Su obra más importante fue Aritmética, la primera en que se trata esta materia de forma sistemática.
Se supone que vivió 84 años, gracias al problema que un discípulo suyo escribió en su tumba a modo de epitafio: "Transeúnte, aquí yace Diofanto. Es él quien con esta sorprendente distribución te confiesa el número de años que vivió. Su niñez ocupó la sexta parte de su vida. Después, durante la doceava parte su mejilla se cubrió con el primer bozo. Pasó aún una séptima parte de su vida antes de tomar esposa y, cinco años después, tuvo un precioso niño que, una vez alcanzada la mitad de la edad de su padre, pereció de una muerte desgraciada. Su padre tuvo que sobrevivirle, llorándole, durante cuatro años. De todo esto se deduce su edad"
Diofanto se consagró al Álgebra y ha legado a la posteridad el término" ecuaciones difantinas" que se refiere a las soluciones enteras de ecuaciones polinomiales con coeficientes enteros.



Se denominan *ecuaciones diofantinas* a aquellas ecuaciones polinomiales con coeficientes en $\mathbb{Z}$ para las que se buscan soluciones enteras.
Nos ocuparemos de estudiar la resolubilidad de las ecuaciones diofantinas del tipo

$$ax + by = c \quad a, b, c \in \mathbb{Z} .$$

***Teorema*:**

i) La ecuación diofantina lineal en dos variables $ax + by = c$, con $a, b, c \in \mathbb{Z}$, admite solución en $\mathbb{Z}\times\mathbb{Z}$ si y sólo si $(a , b) \mid c$.

ii) Sean $d = (a , b) \mid c$, $(x_0 , y_0) \in \mathbb{Z}\times\mathbb{Z}$; (x_0 , y_0) es solución de la ecuación

$ax + by = c$ sii (x_0 , y_0) es solución de la ecuación $\frac{a}{d}x + \frac{b}{d}y = \frac{c}{d}$.

***Demostración*:**
i) $\Rightarrow$) Sean $d = (a , b)$ y $(x_0 , y_0) \in \mathbb{Z}\times\mathbb{Z}$ solución de la ecuación $ax + by = c$.
Entonces $a x_0 + b y_0 = c$; como $d \mid a \wedge d \mid b \Rightarrow d \mid a x_0 \wedge d \mid b y_0$
$\therefore d \mid (a x_0 + b y_0) = c$, como se quería demostrar.

$\Leftarrow$) Sea $d = (a , b) \mid c$. Por ser $d = (a , b)$ $\exists u, v \in \mathbb{Z}$ tales que $au + bv = d$,
y como $d \mid c$ $\exists k \in \mathbb{Z}$ tal que $c = kd$.
Luego $c = kd = auk + bvk$; llamando $x_0 = uk \wedge y_0 = vk$, obtenemos que (x_0 , y_0) es solución de la ecuación $ax + by = c$.

ii) $\Rightarrow$) Sean $d = (a , b) \mid c \wedge (x_0 , y_0) \in \mathbb{Z}\times\mathbb{Z}$ solución de la ecuación $ax + by = c$.
Entonces $a x_0 + b y_0 = c$ (I) ; como $d \mid a \wedge d \mid b \wedge d \mid c$, dividiendo la igualdad (I) por d se obtiene $\frac{a}{d} x_0 + \frac{b}{d} y_0 = \frac{c}{d}$, donde $\frac{a}{d}, \frac{b}{d}, \frac{c}{d} \in \mathbb{Z}$.
Por lo tanto (x_0 , y_0) es solución de la ecuación $\frac{a}{d}x + \frac{b}{d}y = \frac{c}{d}$.

$\Leftarrow$) Recíprocamente, si $(x_0 , y_0) \in \mathbb{Z}\times\mathbb{Z}$ es solución de la ecuación $\frac{a}{d}x + \frac{b}{d}y = \frac{c}{d}$,
se tiene la igualdad en $\mathbb{Z}$: $\frac{a}{d} x_0 + \frac{b}{d} y_0 = \frac{c}{d}$,

multiplicándo m.a.m la igualdad por d, se obtiene $a x_0 + b y_0 = c$,
luego (x_0 , y_0) es solución de la ecuación $ax + by = c$.

***Teorema*:** Si $d = (a , b) \mid c$, $(x_0 , y_0) \in \mathbb{Z}\times\mathbb{Z}$, solución particular de la ecuación $ax + by = c$. Entonces todas las soluciones de dicha ecuación son:

$$x_k = x_0 + \frac{b}{d}k \quad ; \qquad y_k = y_0 - \frac{a}{d}k, \quad k \in \mathbb{Z}.$$

***Demostración*:**

Sea (x_0, y_0) solución de la ecuación $ax + by = c$, veamos que los enteros de la forma $x_k = x_0 + \frac{b}{d}k$; $y_k = y_0 - \frac{a}{d}k$, $k \in \mathbb{Z}$ son también solución de la ecuación.

Reemplazando se obtiene:

$$a(x_0 + \frac{b}{d}k) + b(y_0 - \frac{a}{d}k) = a\,x_0 + a\,\frac{b}{d}k + b\,y_0 - b\,\frac{a}{d}k = a\,x_0 + b\,y_0 = c.$$

Sea ahora $(x', y') \in \mathbb{Z}\times\mathbb{Z}$ otra solución de la ecuación.

Entonces $a\,x_0 + b\,y_0 = ax' + by' = c.$

Por lo tanto $a(x' - x_0) = b(y_0 - y').$

Dividiendo m.a.m. por d: $\frac{a}{d}(x' - x_0) = \frac{b}{d}(y_0 - y')$ (II)

$$d = (a, b) \Rightarrow (\frac{a}{d}, \frac{b}{d}) = 1 \wedge \frac{a}{d} \mid \frac{b}{d}(y_0 - y') \Rightarrow \frac{a}{d} \mid (y_0 - y')$$

$\therefore \quad (y_0 - y') = \frac{a}{d}k$ para cierto $k \in \mathbb{Z}$.

Análogamente $\frac{b}{d} \mid \frac{a}{d}(x' - x_0) \Rightarrow \frac{b}{d} \mid (x' - x_0)$

$\therefore \quad (x' - x_0) = \frac{b}{d}h$ para cierto $h \in \mathbb{Z}$.

Reemplazando en (II) $\frac{a}{d} \cdot \frac{b}{d} \cdot h = \frac{b}{d} \cdot \frac{a}{d} \cdot k \Rightarrow k = h.$

Así $x' = x_0 + \frac{b}{d}k \quad \wedge \quad y' = y_0 - \frac{a}{d}k$ con $k \in \mathbb{Z}$.

Ejemplos : Determinar si la siguiente ecuación diofantina en dos variables admite solución, y en caso afirmativo, resolverla.

$30x + 63y = 621$

$(30, 63) = 3 \mid 621 \ \therefore$ admite solución

1ra. forma:

$621 = 207.3$, $3 = 63 - 2.30 \Rightarrow 621 = 207.63 - 414.30$

tomando $x_0 = -414$, $y_0 = 207$ como soluciones particulares, obtenemos que las soluciones de la ecuación son todos los pares ordenados (x_k, y_k) donde

$$\begin{cases} x_k = -414 + k.21 \\ y_k = 207 - k.10 \end{cases} \quad \text{pues} \quad 21.3 = 63 \quad \wedge \quad 10.3 = 30\,, \quad k \in \mathbb{Z}$$

2da. forma:

$21.3 = 63 \wedge 10.3 = 30 \therefore$ resolveremos la ecuación equivalente:
$10x + 21y = 207$ con $(10\,,\,21) = 1$

$21 = 2.10 + 1 \Rightarrow 1 = 21 - 2.10 \therefore 207 = 207.21 - 414.10$

tomando $x_0 = -414$, $y_0 = 207$ como soluciones particulares, obtenemos que las soluciones de la ecuación son todos los pares ordenados $(x_k\,,y_k)$ donde

$$\begin{cases} x_k = -414 + k.21 \\ y_k = 207 - k.10 \end{cases}, \; k \in \mathbb{Z}$$

***Congruencia mód n*:**

> *"Dos años solamente después de la pubicación de su tesis (1801), publicó Gauss su libro más conocido, un tratado de Teoría de Números en latín, titulado "Disquisitiones arithmeticae", dedicado a su protector el duque de Brunswick. Esta famosísima obra es la principal responsable del desarrollo del lenguaje y de las notaciones de la rama de la teoría de números conocida como el álgebra de las congruencias, ejemplo primitivo de trabajo con clases de equivalencia. La exposición se abre con la definición siguiente:*
>
> > *"Si un número **a** divide a la diferencia entre dos números **b** y **c**, entonces **b** y **c** se llaman congruentes, y en caso contrario incongruentes, y el número **a** se llama módulo. Cada uno de los dos números se llama un residuo del otro, en el primer caso, un no residuo en el segundo caso".*
>
> *La notación que adoptó Gauss es la misma que seguimos usando hoy,* $b \equiv c \,(\text{mod}\, a)$ *"*
>
> Boyer, C. "Historia de la Matemática" (pág 633)

En el capítulo II, Segunda Parte, definimos en $\mathbb{Z}$ la relación de equivalencia llamada *congruencia módulo n*, o también, *de restos módulo n* , de la siguiente manera:

Para $n \in \mathbb{N}$, $a, b \in \mathbb{Z}$, $a \equiv b\ (mód\ n)$ si y sólo si $n \mid (a-b)$

Es una relación de equivalencia porque es reflexiva, simétrica y transitiva.
Las *clases de equivalencia* son:
Para $a \in \mathbb{Z}$, $\overline{a} = \{\, b \in \mathbb{Z} \;/\; b \equiv a (mód\, n) \,\}$

Estas clases de equivalencia establecen una *partición* en $\mathbb{Z}$,y el conjunto que forman, el *conjunto cociente*, es $\mathbb{Z}_n = \mathbb{Z} \big/ \equiv (mód\, n) = \{\, \overline{a} \;/\; a \in \mathbb{Z} \,\}$

También en ese capítulo brindamos ejemplos concretos para $n = 2$ y $n = 3$, se recomienda su relectura para comprender mejor lo que se dará a continuación.

Allí mostramos que $\mathbb{Z}_2 = \{\bar{0}, \bar{1}\}$ y $\mathbb{Z}_3 = \{\bar{0}, \bar{1}, \bar{2}\}$, pero aun no podemos determinar para todo $n \in \mathbb{N}$ que $\mathbb{Z}_n$ es finito, y menos aun que tiene n elementos.

El siguiente teorema nos brinda esa respuesta.

***Teorema*:**

Para $a, b \in \mathbb{Z}$, $a \equiv b \ (mód\ n) \Leftrightarrow a$ y b tienen el mismo resto en la división por n.

***Demostración*:**

$\Rightarrow$) Sean $a, b \in \mathbb{Z}$, tales que $a \equiv b \ (mód\ n)$.

Apliquemos el AD:

$a = q.n + r$, con $0 \le r < n$
$b = h.n + s$, con $0 \le s < n$.

Sin pérdida de generalidad, supongamos que $s \le r$,
$a - b = (q - h).n + r - s$, donde $0 \le r - s \le r < n$.
Como $n \mid (a - b) \ \wedge \ n \mid (q - h).n \Rightarrow n \mid (r - s)$, y $0 \le r - s < n \Rightarrow r - s \notin \mathbb{N}$
$\therefore \ r - s = 0$, con lo cual $r = s$, como queríamos probar.

$\Leftarrow$) Si a y b tienen el mismo resto en la división por n
$a = q.n + r$, $b = h.n + r$, con $0 \le r < n$
restando $a - b = (q - h).n \Rightarrow n \mid (a - b) \ \therefore \ a \equiv b \ (mód\ n)$.

***Corolario*:** $\mathbb{Z}_n$ es finito y tiene exactamente n elementos, a saber:

$$\mathbb{Z}_n = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, ..., \overline{n-2}, \overline{n-1}\}$$

donde las clases corresponden a los posibles restos de cualquier entero en la división por n.

Nota: esta caracterización de la congruencia módulo n es la que le da el nombre de *clase de restos módulo n.*

Vamos a definir en $\mathbb{Z}_n$ una suma y un producto:

$a, b \in \mathbb{Z}$

$$\bar{a} + \bar{b} =: \overline{a+b}$$
$$\bar{a} \,.\, \bar{b} =: \overline{a \cdot b}$$

Para saber que las operaciones están bien definidas, debemos probar que éstas no dependen de los representantes elegidos en cada clase.

***Teorema*:** Sean $a, a', b, b' \in \mathbb{Z}$ tales que $a \equiv a' \ \wedge \ b \equiv b' \ (mód\ n)$

Entonces $a + b \equiv a' + b' \ \wedge \ a.b \equiv a'.b' \ (mód\ n)$

***Demostración*:** Como $a \equiv a' \wedge b \equiv b' \ (mód\ n)$, $\exists k, h \in \mathbb{Z}$ tales que $a - a' = k.n \wedge b - b' = h.n$.

Sumando ambas igualdades, tenemos que $(a - a') + (b - b') = (k + h).n$

Asociando $(a + b) - (a' + b') = (k + h).n$

Entonces $n \mid \left[(a+b) - (a'+b') \right] \therefore a + b \equiv a' + b' \ (mód\ n)$.

Para demostrar la congruencia correspondiente al producto, volvamos a las igualdades:

$a - a' = k.n \quad \wedge \quad b - b' = h.n$

Multiplicando la primera por b y la segunda por a' , tenemos:

$a.b - a'.b = k.b.n \quad \wedge \quad b.a' - a'b' = h.a'.n$

Sumándolas obtenemos: $a.b - a'.b' = (k.b + h.a').n$

$\Rightarrow n \mid (a.b - a'.b') \therefore a.b \equiv a'.b' \ (mód\ n)$.

Algo sobre criptografia…

Desde la Antigüedad surgió para el hombre la necesidad del intercambio de mensajes en forma confidencial y eso dio origen a la Criptografía, pero era utilizada principalmente por militares y diplomáticos.

Actualmente es utilizada por todos aunque no lo hayamos advertido. Preguntémonos, si no: ¿qué estamos utilizando en el momento de ingresar la clave para averiguar el saldo de nuestra cuenta bancaria en un cajero automático o por Internet?

Sin la Criptografía no funcionaría la banca electrónica y tampoco podría existir el comercio electrónico que nos permite efectuar compras por medio de INTERNET y nuestra tarjeta de crédito.

Entre los diversos sistemas criptográficos inventados a lo largo de los tiempos encontramos la idea del emperador romano Julio César que consistía en efectuar una sustitución de las letras del alfabeto utilizando a una de ellas como ***clave.***

Analicemos el sistema de Julio César asignando un número natural a cada letra de nuestro alfabeto y uno al espacio en blanco, según la siguiente tabla, en la que (–) simboliza el espacio en blanco:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14

P	Q	R	S	T	U	V	W	X	Y	Z	-
15	16	17	18	19	20	21	22	23	24	25	26

Tomemos, por ejemplo, como clave la letra T, *es decir que la* T *estará representada por la A y tratemos de descifrar el mensaje:* FMEXJGKSHJAEGK *Para ello tendremos que reemplazar cada letra por la que le corresponda según la tabla siguiente*:

Texto cifrado	T	U	V	W	X	Y	Z	-	A	B	C	D	E	F	G
Texto llano	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O

Texto cifrado	H	I	J	K	L	M	N	O	P	Q	R	S
Texto llano	P	Q	R	S	T	U	V	W	X	Y	Z	-

Texto cifrado: **F M E X J G K S H J A E G K**

Texto llano **: N U M E R O S _ P R I M O S**

Si bien parecía muy difícil descifrar este mensaje, este sistema ya era totalmente transparente para los "criptoanalistas" árabes del Siglo IX expertos en desencriptar mensajes. Vigenère en el Siglo XVI, construyó un sistema donde la clave tenía varias letras, por ejemplo MODULO*, que se repite tantas veces cuanto sea necesario.*

Consiste en tomar la primera letra del mensaje original y modificarla con la M, a la segunda con la O*, a la tercera con la* D*, etc. De esta forma, una misma letra en el mensaje original tendrá distintas representaciones en el mensaje cifrado.*

Utilizando esta clave (MODULO), *cifremos el mismo mensaje*

Texto llano: **N U M E R O S _ P R I M O S**
13 20 12 4 17 14 18 26 15 17 8 12 14 18

Clave: M O D U L O M O D U L O M O
12 14 3 20 11 14 12 14 3 20 11 14 12 14

Texto llano	N	U	M	E	R	O	S		P	R	I	M	O	S
	13	20	12	4	17	14	18	26	15	17	8	12	14	18
CLAVE	M	O	D	U	L	O	M	O	D	U	L	O	M	O
	12	14	3	20	11	14	12	14	3	20	11	14	12	14
Suma mod 27	25	7	15	24	1	1	3	13	18	10	19	26	26	5
Texto cifrado	Z	H	P	Y	B	B	D	N	S	K	T	_	_	F

Si el trabajo que hicimos es correcto al descifrar el mensaje ZHPYBBDNSKT_ _F *deberíamos obtener el mensaje original:* NUMEROS_ PRIMOS. *Comprobémoslo:*

Texto cifrado	Z	H	P	Y	B	B	D	N	S	K	T	_	_	F
	25	7	15	24	1	1	3	13	18	10	19	26	26	5
Clave	M	O	D	U	L	O	M	O	D	U	L	O	M	O
	12	14	3	20	11	14	12	14	3	20	11	14	12	14
Resta mod 27	13	20	12	4	17	14	18	26	15	17	8	12	14	18
Texto llano	N	U	M	E	R	O	S		P	R	I	M	O	S

Ejercicio 1: Ponga en juego sus habilidades de criptoanalista y cifre el siguiente mensaje eligiendo Ud. mismo su clave: TEOREMA DE FERMAT

Ejercicio 2: Descifre el siguiente mensaje, utilizando la clave MODULO: SEDWTODNIYB_MG .

Aritmética en $\mathbb{Z}_n$

Hemos definido dos operaciones en $\mathbb{Z}_n$, suma y producto:

$+ : \mathbb{Z}_n \times \mathbb{Z}_n \rightarrow \mathbb{Z}_n$ $\qquad$ $. : \mathbb{Z}_n \times \mathbb{Z}_n \rightarrow \mathbb{Z}_n$

$(\overline{a}, \overline{b}) \rightarrow \overline{a+b}$ $\qquad$ $(\overline{a}, \overline{b}) \rightarrow \overline{a \cdot b}$

que verifican las siguientes propiedades:

Suma:

- asociativa : $(\overline{a} + \overline{b}) + \overline{c} = \overline{a} + (\overline{b} + \overline{c})$
- conmutativa: $\overline{a} + \overline{b} = \overline{b} + \overline{a}$
- existencia de elemento neutro: $\overline{0}$, $\quad \overline{a} + \overline{0} = \overline{a}$, $\quad \forall\ \overline{a} \in \mathbb{Z}_n$
- todo elemento tiene inverso u opuesto: $- \overline{a} = \overline{-a}$

Por verificar la suma esas propiedades, $(\mathbb{Z}_n, +)$ es un *grupo abeliano,* y además sabemos que es finito.

Producto:

- asociativa: $(\overline{a} . \overline{b}) . \overline{c} = \overline{a} . (\overline{b} . \overline{c})$
- conmutativa: $\overline{a} . \overline{b} = \overline{b} . \overline{a}$
- existencia de elemento neutro: $\overline{1}$, $\quad \overline{a} . \overline{1} = \overline{a}$, $\quad \forall\ \overline{a} \in \mathbb{Z}_n$

- Distributividad del producto respecto de la suma

Por tener dos operaciones que verifican todas las propiedades precedentes más la distributividad del producto respecto de la suma, tenemos que

$$(\mathbb{Z}_n, +, .)$$

es un *anillo conmutativo con identidad.*

Ejemplos: Veremos las tablas de sumar y multiplicar para algunos $n \in \mathbb{N}$.

1) $n = 2$, tablas de sumas y productos en $\mathbb{Z}_2$

+	$\bar{0}$	$\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{1}$
$\bar{1}$	$\bar{1}$	$\bar{0}$

·	$\bar{0}$	$\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$

2) $n = 3$, tablas de sumas y productos en $\mathbb{Z}_3$

+	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{0}$	$\bar{1}$

·	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{1}$

3) $n = 4$, tablas de sumas y productos en $\mathbb{Z}_4$

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$

·	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{0}$	$\bar{2}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

4) $n = 5$, tablas de sumas y productos en $\mathbb{Z}_5$

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$

·	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{1}$	$\bar{3}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{1}$	$\bar{4}$	$\bar{2}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

5) $n = 9$, tablas de suma y producto en $\mathbb{Z}_9$

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	$\bar{8}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	$\bar{8}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	$\bar{8}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	$\bar{8}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	$\bar{8}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	$\bar{8}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{5}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	$\bar{8}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{6}$	$\bar{6}$	$\bar{7}$	$\bar{8}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{7}$	$\bar{7}$	$\bar{8}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
$\bar{8}$	$\bar{8}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$

·	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	$\bar{8}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	$\bar{8}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{6}$	$\bar{8}$	$\bar{1}$	$\bar{3}$	$\bar{5}$	$\bar{7}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{6}$	$\bar{0}$	$\bar{3}$	$\bar{6}$	$\bar{0}$	$\bar{3}$	$\bar{6}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{8}$	$\bar{3}$	$\bar{7}$	$\bar{2}$	$\bar{6}$	$\bar{1}$	$\bar{5}$
$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{1}$	$\bar{6}$	$\bar{2}$	$\bar{7}$	$\bar{3}$	$\bar{8}$	$\bar{4}$
$\bar{6}$	$\bar{0}$	$\bar{6}$	$\bar{3}$	$\bar{0}$	$\bar{6}$	$\bar{3}$	$\bar{0}$	$\bar{6}$	$\bar{3}$
$\bar{7}$	$\bar{0}$	$\bar{7}$	$\bar{5}$	$\bar{3}$	$\bar{1}$	$\bar{8}$	$\bar{6}$	$\bar{4}$	$\bar{2}$
$\bar{8}$	$\bar{0}$	$\bar{8}$	$\bar{7}$	$\bar{6}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Un dato: La aritmética en el ISBN

En todos los libros que llegan a nuestras manos junto a los datos de editorial, edición, autor, etc., aparece un número identificado con la sigla ISBN (International Standard Book Number). Es el número que se utiliza universalmente para catalogar publicaciones y contiene información que identifica a la editorial y al título en cuestión.
El ISBN está constituido por nueve dígitos, que aparecen en grupos separados por guiones, seguidos de un número de control (al que llamaremos d_{10}) para la suma de verificación. Este número puede tomar valores entre 0 y 10, usándose la letra X para representar el valor 10.
Es muy sencillo calcular el d_{10} mediante la congruencia módulo 11 representando los 9 dígitos como $d_1\, d_2\, d_3 ....d_9$ y calculando $\boxed{d_{10} \equiv 1.d_1 + 2.d_2 + 3.d_3 + ... + 9.d_9 \quad (mód\ 11)}$

A partir del año 2007 el ISBN se rige por la norma EAN13 (European Article Number), la misma que se utiliza en la mayoría de los productos de consumo. Este número consta de 13 dígitos (12 más uno de control). En algunos libros se encuentran los dos ISBN.
El dígito de control del EAN13 (al que llamaremos d_{13}) se añade a los otros 12 de forma que la expresión $\sum_{i\ impar} d_i + 3.\sum_{j\ par} d_j + d_{13}$ sea siempre múltiplo de 10 (es decir que d_{13} es el resto del opuesto de $\sum_{i\ impar} d_i + 3.\sum_{j\ par} d_j$ módulo 10).
A modo de poner en práctica esta curiosidad, se propone la siguiente actividad:

a) Verificar el número de control en el ISBN de este libro.
b) Calcular el número de control de los siguientes textos:
   b-1) Larson-Edwards- *Introducción al Algebra Lineal*:
   ISBN: 968-18-4886-1
   b-2) Juan Ignacio Fuxman Bass- *Resolviendo Problemas de Matemáticas*:
   ISBN: 978-987-9072-66-….
   b-3) Becker-Pietrocola-Sanchez- *Aritmética*: ISBN: 987-9072-35-….

Elementos inversibles en $\mathbb{Z}_n$

***Definición*:** Sea $\overline{u} \in \mathbb{Z}_n$, $\overline{u}$ se dice *inversible* en $\mathbb{Z}_n$, o *unidad* de $\mathbb{Z}_n$, si $\exists\, \overline{v} \in \mathbb{Z}_n$ tal que $\overline{u}\,.\,\overline{v} = \overline{1}$; $\overline{v}$ se denomina el *inverso* de $\overline{u}$, y se nota $\overline{v} = \overline{u}^{-1}$.

Llamaremos $\mathbb{Z}_n^* = \{\, \overline{u} \in \mathbb{Z}_n \,/\ \overline{u}\ es\ inversible \,\}$.

Ejemplos: 1) En $\mathbb{Z}_2$ hay un único elemento no nulo, el $\overline{1}$, y es inversible, pues $\overline{1} \cdot \overline{1} = \overline{1}$, luego $\overline{1}^{-1} = \overline{1}$.

2) En $\mathbb{Z}_3$ hay dos elementos no nulos, el $\overline{1}$ y el $\overline{2}$, y ambos son inversibles, pues $\overline{1}^2 = \overline{1} \ \wedge\ \overline{2}^2 = \overline{1}$.

3) En $\mathbb{Z}_4$, hay dos elementos no nulos e inversibles: el $\overline{1}$ y el $\overline{3}$.

El $\overline{2}$ no sólo no es inversible, sino que $\overline{2} \cdot \overline{2} = \overline{0}$ siendo $\overline{2} \neq \overline{0}$ (esta es una situación novedosa, porque no ocurre en $\mathbb{Z}$).

4) En $\mathbb{Z}_5$, todo elemento no nulo es inversible: $\overline{1} \cdot \overline{1} = \overline{1}$; $\overline{2} \cdot \overline{3} = \overline{1} \ \wedge \ \overline{4} \cdot \overline{4} = \overline{1}$.

5) En $\mathbb{Z}_9$, los elementos inversibles, de acuerdo con lo que se desprende de la tabla, son: $\overline{1}$, $\overline{2}$, $\overline{4}$, $\overline{5}$, $\overline{7}$, $\overline{8}$.

***Propiedades*:**

1) $\overline{u}, \overline{v} \in \mathbb{Z}_n^* \Rightarrow \overline{u} \,.\, \overline{v} \in \mathbb{Z}_n^* \ \wedge \ (\overline{u} \,.\, \overline{v})^{-1} = \overline{v}^{-1} . \ \overline{u}^{-1}$.
2) $\overline{1} \in \mathbb{Z}_n^* \ \wedge \ \overline{1}^{-1} = \overline{1}$.
3) Si $\overline{u} \in \mathbb{Z}_n^*$ entonces $\overline{u}^{-1} \in \mathbb{Z}_n^* \ \wedge \ (\overline{u}^{-1})^{-1} = \overline{u}$.

***Demostración*:** Se deja como ejercicio.

Por verificar esas propiedades, tenemos que $(\mathbb{Z}_n^*, .)$ es un grupo abeliano, llamado *el grupo de unidades de* $\mathbb{Z}_n$.

Queremos caracterizar las unidades de $\mathbb{Z}_n$, para cada $n \in \mathbb{N}$.

***Teorema*:** Sean $n \in \mathbb{N}$, $a \in \mathbb{Z}$, entonces:
$\exists b \in \mathbb{Z}$ tal que $a.b \equiv 1$ (*mód n*) si y sólo si $(a\,,\,n) = 1$.

***Demostración*:** $\exists b \in \mathbb{Z}$ tal que $a.b \equiv 1$ (*mód n*) $\Leftrightarrow$ $\exists b \in \mathbb{Z}$ tal que $ab - 1 = k.n$, para algún $k \in \mathbb{Z}$ $\Leftrightarrow$ $\exists b, k \in \mathbb{Z}$ tales que $a.b - k.n = 1$ $\Leftrightarrow$ $(a\,,\,n) = 1$ (T. de Bezout).

***Corolario*:** Sea $n \in \mathbb{N}$, $\overline{a}$ es inversible en $\mathbb{Z}_n$ $\Leftrightarrow (a\,,\,n) = 1$.

***Demostración*:** $\overline{a}$ es inversible en $\mathbb{Z}_n$ $\Leftrightarrow$ $\exists\, \overline{b} \in \mathbb{Z}_n$ tal que $\overline{a} \cdot \overline{b} = \overline{1}$
$\Leftrightarrow$ $\exists b \in \mathbb{Z}$ tal que $a.b \equiv 1$ (*mód n*) $\Leftrightarrow$ $(a\,,\,n) = 1$.

Por lo tanto $\mathbb{Z}_n^* = \left\{ \overline{u} \in \mathbb{Z}_n \,/ \quad (u\,,\,n) = 1 \right\}$.

Ejemplos:

$$\mathbb{Z}_2^* = \left\{\overline{1}\right\} \ ; \ \mathbb{Z}_3^* = \left\{\overline{1}, \overline{2}\right\} \ ; \ \mathbb{Z}_4^* = \left\{\overline{1}, \overline{3}\right\} \ ; \ \mathbb{Z}_5^* = \left\{\overline{1}, \overline{2}, \overline{3}, \overline{4}\right\} \ ; \quad \mathbb{Z}_9^* = \left\{\overline{1}, \overline{2}, \overline{4}, \overline{5}, \overline{7}, \overline{8}\right\}$$

Nota: En todo $\mathbb{Z}_n$, con $n > 2$, hay, al menos, dos elementos inversibles :
$\overline{1} \ \wedge \ \overline{-1} = \overline{n-1}$ pues $(\overline{-1})^2 = \overline{-1} \,.\, \overline{-1} = \overline{(-1)\cdot(-1)} = \overline{(-1)^2} = \overline{1}$.
Cuando $n = 2$, $\overline{1} = \overline{-1}$.

En los ejemplos precedentes, vimos que hay anillos $\mathbb{Z}_n$ en los cuales todo elemento no nulo es inversible, o lo que es equivalente, $\mathbb{Z}_n^* = \mathbb{Z}_n - \{\overline{0}\}$, por ejemplo para $n = 2, 3, 5$.
En tales casos diremos que $\mathbb{Z}_n$ es un *cuerpo.*

***Corolario*:** $\mathbb{Z}_n$ es cuerpo $\Leftrightarrow$ n es primo.

***Demostración*:**
$\Rightarrow$) Si $\mathbb{Z}_n$ es cuerpo, entonces $\forall\ \overline{a} \neq \overline{0}$, $\overline{a}$ es inversible; por el teorema tenemos que

$$(a\ ,\ n) = 1 \quad \therefore \quad \text{si} \quad 1 \leq k < n\ , \quad (k\ ,\ n) = 1 \Rightarrow n \text{ es primo.}$$

$\Leftarrow$) Recíprocamente, si n es primo, $\forall\ k,\ 1 \leq k < n$, $(k\ ,\ n) = 1 \Rightarrow \overline{k}$ e inversible,
$\therefore \quad \mathbb{Z}_n^* = \mathbb{Z}_n - \{\overline{0}\}$, luego $\mathbb{Z}_n$ es cuerpo.

También hemos observado, que hay anillos $\mathbb{Z}_n$ en los cuales $\overline{a}\ .\overline{b} = \overline{0}$, siendo $\overline{a} \neq \overline{0} \ \wedge\ \overline{b} \neq \overline{0}$, como, por ejemplo $\overline{2}^2 = \overline{0}$ en $\mathbb{Z}_4$; $\overline{2} \cdot \overline{3} = \overline{0}$ en $\mathbb{Z}_6$; $\overline{4} \cdot \overline{7} = \overline{0}$ en $\mathbb{Z}_{14}$.

***Definición*:** $\mathbb{Z}_n$ es *dominio de integridad* si $\overline{a}\ .\overline{b} = \overline{0} \Rightarrow \overline{a} = \overline{0} \ \vee\ \overline{b} = \overline{0}$.

Ejemplos: $\mathbb{Z}_2$; $\mathbb{Z}_3$; $\mathbb{Z}_5$ **son** *dominios de integridad*
$\mathbb{Z}_4$; $\mathbb{Z}_9$; $\mathbb{Z}_6$; $\mathbb{Z}_{14}$ **no son** *dominios de integridad*

Ejercicio: Sea $p \in \mathbb{N}$, $p > 1$. Demostrar que las siguientes propiedades son equivalentes:
i . p es primo
ii. $\mathbb{Z}_p$ es dominio de integridad
iii. $\mathbb{Z}_p$ es cuerpo

Nota: No siempre es equivalente ser dominio de integridad y cuerpo; el anillo $\mathbb{Z}$ **es dominio de integridad**, pero **no es cuerpo.**
En $\mathbb{Z}$ se verifica que $a.b = 0 \Rightarrow a = 0 \ \vee\ b = 0$, pero no es cierto que todo elemento no nulo sea inversible , por ejemplo, el 2, el 3 el 15, etc., no son inversibles en $\mathbb{Z}$, es más, los **únicos** inversibles en $\mathbb{Z}$ son el 1 y el -1, con lo cual, su grupo de unidades es: $\mathbb{Z}^* = \{1, -1\}$.

Pequeño Teorema de Fermat

El *Pequeño Teorema de Fermat* afirma que para $p \in \mathbb{N}$ primo, y para $a \in \mathbb{Z}$, se verifica siempre que a^p y a tienen el mismo resto en la división por p.
Antes de demostrar esta afirmación, vamos a probar un Lema.

***Lema*:** Sea $p \in \mathbb{N}$, p primo. Entonces:

i) $\quad p \mid \binom{p}{k}$, $\forall\ k\ , 0 < k < p.$

ii) $\quad (a + b)^p \equiv a^p + b^p\ (\text{mód } p)$, $\forall\ a, b \in \mathbb{Z}$.

***Demostración*:**

i) $\binom{p}{k} = \frac{p!}{k!\cdot(p-k)!} \in \mathbb{N}$, luego $k!.(p-k)! \mid p! = p.(p-1)!$

Como $1 \le k < p$, y $k! = \prod_{i=1}^{k} i \Rightarrow \forall\, i : 1 \le i \le k < p \quad (i\,,p) = 1$

$\therefore\ (\prod_{i=1}^{k} i\,,p) = 1$, o sea $(k!\,,p) = 1$.

Análogamente, $(p-k)! = \prod_{j=1}^{p-k} j \Rightarrow \forall\, j : 1 \le j \le p-k < p$, $(j\,,p) = 1$

$\therefore\ (\prod_{j=1}^{p-k} j\,,p) = 1$, o sea $((p-k)!\,,p) = 1$.

Como $(k!\,,p) = 1 \wedge ((p-k)!\,,p) = 1 \Rightarrow (k!.(p-k)!\,,p) = 1$.

Ahora tenemos $k!.(p-k)! \mid p! = p.(p-1)! \wedge (k!.(p-k)!\,,p) = 1$

$\Rightarrow k!.(p-k)! \mid (p-1)!\ \therefore\ \frac{(p-1)!}{k!\cdot(p-k)!} \in \mathbb{N}$.

Sea $c = \frac{(p-1)!}{k!\cdot(p-k)!}$ $\therefore$ $\frac{p!}{k!\cdot(p-k)!} = p.c$ $\therefore$ $p \mid \binom{p}{k}$, $\forall\, k\,,\ 0 < k < p.$

ii) Sean $a\,,b \in \mathbb{Z}$. $(a+b)^p = \sum_{k=0}^{p}\binom{p}{k}a^k\cdot b^{p-k} = a^p + b^p + \sum_{k=1}^{p-1}\binom{p}{k}a^k\cdot b^{p-k} =$

Como $p \mid \binom{p}{k}$, $\forall\, k\,,\ 1 \le k \le p-1$, sea $\binom{p}{k} = p.c_k$ con $c_k \in \mathbb{N}$,

$= a^p + b^p + p.\sum_{k=1}^{p-1} c_k \cdot a^k \cdot b^{p-k} = a^p + b^p + p.h$, con $h \in \mathbb{Z}$

$\therefore\ (a+b)^p - (a^p + b^p) = p.h \Rightarrow (a+b)^p \equiv a^p + b^p\ (mód\ p)$.

***Teorema*:** Sean $p \in \mathbb{N}$, p primo, $a \in \mathbb{Z}$. Entonces $a^p \equiv a\ (mód\ p)$.

***Demostración*:** Primero lo demostraremos cuando $a \in \mathbb{N}$. Haremos inducción sobre *a.*

Si $a = 1$ $1^p = 1 \equiv 1\ (mód\ p)$ por ser la congruencia una relación reflexiva.

Supongamos que $a^p \equiv a\ (mód\ p)$

Queremos ver que $(a+1)^p \equiv a + 1\ (mód\ p)$.

Por el Lema $(a+1)^p \equiv a^p + 1^p = a^p + 1$

Por HI $a^p \equiv a \ (mód\ p) \Rightarrow (a+1)^p \equiv a^p + 1 \equiv a + 1 \ (mód\ p)$

$\therefore \ a^p \equiv a \ (mód\ p) \ \forall \ a \in \mathbb{N}$

Sea $a = 0$, $0^p = 0 \equiv 0 \ (mód\ p)$

Sea ahora $a \in \mathbb{N}^-$ $\therefore \ a = -n$, con $n \in \mathbb{N}$, $a^p = (-n)^p$

Distinguimos dos situaciones: $p = 2 \ \vee \ p$ primo impar.

Para $p = 2$ $a^2 = (-n)^2 = n^2 \equiv n \equiv -n = a \ (mód\ 2)$.

Para p primo impar $a^p = (-n)^p = -n^p$

Como $n^p \equiv n \ (mód\ p)$ pues $n \in \mathbb{N} \Rightarrow -n^p \equiv -n = a \ (mód\ p)$ $\therefore \ a^p \equiv a \ (mód\ p)$.
Por lo tanto $a^p \equiv a \ (mód\ p) \ \forall \ a \in \mathbb{Z}$.

***Corolario*:** Si $p \in \mathbb{N}$, p primo, $a \in \mathbb{Z}$ tal que $p \nmid a$ entonces $a^{p-1} \equiv 1 \ (mód\ p)$.

***Demostración*:** $a^p \equiv a \ (mód\ p)$, entonces $p \mid (a^p - a) = a.(a^{p-1} - 1)$.

Como $p \nmid a$ entonces $(a, p) = 1$, pues p es primo $\Rightarrow p \mid (a^{p-1} - 1)$

$\therefore \ a^{p-1} \equiv 1 \ (mód\ p)$.

Ejemplos:

1) Calcular el resto en la división por 11 de 7077^{377}.

Es claro que resulta muy complicado calcular el número 7077^{377} para después dividirlo por 11, y así encontrar el resto, por lo tanto usaremos lo aprendido.

Aplicaremos, primero, el corolario del Pequeño Teorema de Fermat.
Como 11 es primo $\wedge$ $11 \nmid 7077$, por el corolario $7077^{10} \equiv 1 \ (mód\ 11)$
Dividiendo 377 por 10, tenemos : $377 = 37.10 + 7$

Entonces, por propiedades de potencia: $7077^{377} = (7077^{10})^{37} \ . \ 7077^7$,
como $7077^{10} \equiv 1 \ (mód\ 11)$ entonces $(7077^{10})^{37} \equiv 1^{37} = 1 \ (mód\ 11)$
$\therefore \ 7077^{377} \equiv 7077^7 \ (mód\ 11)$.

Si bien estamos ahora en una situación más favorable, igual resulta engorroso calcular 7077^7 para luego dividirlo por 11 y hallar el resto, así que apliquemos ahora la aritmética de las congruencias:

$7077 = 7 \,.\, 1011$

$1011 = 91.11 + 10 \;\therefore\; 1011 \equiv 10 \equiv -1 \;(mód\ 11)$

entonces: $7077 \equiv 7.(-1) = -7 \equiv 4 \;(mód\ 11)$

$7077^7 \equiv 4^7 = (4^2)^3 . 4 \equiv 5^3 . 4 \equiv 5^2 . 20 \equiv 3.(-2) = -6 \equiv 5 \;(mód\ 11)$

Luego, el resto en la división por 11 de 7077^{377} es 5.

Nota: Tuvimos que hacer estas cuentas porque $11 \nmid 7077$; si en vez de este número hubiéramos tenido uno que fuera múltiplo de 11, no hubiéramos necesitado realizar ningún cálculo, porque si 11 divide a un número, divide a todas sus potencias, y ya sabríamos que el resto es 0.

2) Probar que $\forall\, n \in \mathbb{N} \quad \dfrac{n^7}{7} + \dfrac{n^5}{5} + \dfrac{23n}{35} \in \mathbb{N}$

$$\frac{n^7}{7} + \frac{n^5}{5} + \frac{23n}{35} = \frac{5n^7 + 7n^5 + 23n}{35} \in \mathbb{N} \iff 35 \mid (5n^7 + 7n^5 + 23n)$$

como $35 = 7.5$ y $(7 , 5) = 1$ se tiene que ,

$35 \mid (5n^7 + 7n^5 + 23n) \iff 5 \mid (5n^7 + 7n^5 + 23n) \wedge 7 \mid (5n^7 + 7n^5 + 23n)$

Veamos, primero, que $5 \mid (5n^7 + 7n^5 + 23n)$:

$5n^7 \equiv 0 \;(mód\ 5)$
$n^5 \equiv n \;(mód\ 5) \Rightarrow 7n^5 \equiv 7n \equiv 2n \;(mód\ 5)$
$23n \equiv 3n \;(mód\ 5)$

sumando: $5n^7 + 7n^5 + 23n \equiv 2n + 3n = 5n \equiv 0 \;(mód\ 5)$
$\therefore\; 5 \mid (5n^7 + 7n^5 + 23n)$.

Ahora, demostremos que $7 \mid (5n^7 + 7n^5 + 23n)$:

$n^7 \equiv n \;(mód\ 7) \Rightarrow 5n^7 \equiv 5n \;(mód\ 7)$
$7n^5 \equiv 0 \;(mód\ 7)$
$23n \equiv 2n \;(mód\ 7)$

sumando: $5n^7 + 7n^5 + 23n \equiv 5n + 2n = 7n \equiv 0 \;(mód\ 7)$

$\therefore\; 7 \mid (5n^7 + 7n^5 + 23n)$.

Por consiguiente $35 \mid (5n^7 + 7n^5 + 23n)$, luego $\dfrac{n^7}{7} + \dfrac{n^5}{5} + \dfrac{23n}{35} \in \mathbb{N}$

y esto es $\forall\, n \in \mathbb{N}$.

PIERRE DE FERMAT (1601-1665)

*La **teoría de números** es el tema que ha de dar a Fermat fama universal. Su interés por los números enteros y sus maravillosas propiedades había empezado en la década de los* 1630 *cuando Fermat leyó la traducción de Bachet de la Aritmética de Diofanto. En el estrecho margen justo al lado del problema* 8 *del libro II: "Dado un número que sea un cuadrado, descomponerlo como suma de otros dos números cuadrados", Fermat escribió su famosa conjetura:*

la ecuación $x^n + y^n = z^n$ ***no tiene soluciones enteras positivas para*** $n > 2$.

En sus propias palabras:

"....Es imposible que un cubo se pueda expresar como una suma de dos cubos o que una potencia cuarta se escriba como una suma de potencias cuartas o, en general, que un número que sea una potencia de grado mayor que dos se pueda descomponer como suma de dos potencias del mismo grado. He encontrado una demostración verdaderamente maravillosa de este resultado pero este margen es demasiado estrecho para contenerla."

La creencia actual es que Fermat había demostrado el teorema para n = 4 *(y quizás también para n =* 3*) y creía que podía generalizar su demostración para cualquier valor de n.*

El Gran Teorema de Fermat para el caso n = 3 *fue demostrado* 100 *años más tarde por Euler. La demostración de algunos otros casos particulares estuvo a cargo de grandes matemáticos como Lejeune-Dirichlet, Legendre, Lamé y Sophie Germain en el siglo* XIX. *No sabremos nunca si Fermat realmente disponía de una demostración maravillosa para cualquier valor de n. Pero en cualquier caso, el reto de demostrar el Gran Teorema de Fermat había empezado con aquella nota garabateada en el margen de un libro. La aventura terminaría* 350 *años más tarde cuando, en* 1994, *Andrew Wiles publicó la demostración del Gran Teorema de Fermat.*

El enorme interés de Fermat por los números enteros era una novedad en la Europa del siglo XVII. *Nadie tenía demasiado interés en perder el tiempo explorando propiedades de números enteros que no tenían ninguna aplicación directa. Sólo un par de problemas clásicos atraían la atención de los matemáticos de la época: el estudio de números perfectos* (*aquéllos que son iguales*

a la suma de sus divisores, exceptuando ellos mismos) *y la caracterización de las ternas pitagóricas* (*ternas de números enteros* (x, y, z) *que satisfacen el teorema de Pitágoras* $x^2 + y^2 = z^2$). *Como consecuencia del interés de Fermat en el primero de esos problemas, descubrió el que se conoce hoy en día como el Pequeño Teorema de Fermat, una verdadera joya en teoría de números, aparecido en una carta de* 1640 *y trata de la periodicidad de los restos de las potencias de* ***a*** *al dividirlas por un número primo* ***p*** *no divisor de* ***a****, de manera que al llegar a la potencia de exponente* ***p*****-1** *comienzan a repetirse consecutivamente los restos anteriores. El teorema fue demostrado por Leibniz, Euler y Gauss que generalizaron más tarde este descubrimiento en direcciones diversas.*

En términos modernos dice que si ***p*** *es un número primo y* ***a*** *es coprimo con* ***p****, entonces* $a^{p-1} \equiv 1 \mod(p)$

No deja de ser paradójico que Fermat sea recordado por su Gran Teorema, en gran parte estéril porque ningún resultado importante se deduce de él, y no por su ***Pequeño Teorema*** *que es crucial en álgebra y en la teoría de números moderna y sus aplicaciones, como es por ejemplo, la moderna criptografía, base de la seguridad de las transmisiones en Internet.*

El segundo problema, la caracterización de las ternas pitagóricas, conduce a Fermat a su interés por las descomposiciones de potencias y problemas como la descomposición de los primos de la forma $4n+1$ *como suma de dos cuadrados (de manera única), la descomposición de un entero positivo como suma de cuatro cuadrados, etc.*

Para demostrar que todo número primo de la forma $4n+1$ *es siempre suma de dos cuadrados, explica así en los márgenes del Diofanto : " si no se compone de dos cuadrados, existirá otro número primo de la misma forma menor que el anterior que tampoco se compone de dos cuadrados, y luego un tercero, etc. descendiendo al infinito hasta llegar al número 5 que es el menor de todos los números de este tipo y que por tanto no sería suma de dos cuadrados. Como esto es imposible, todos los números de esa naturaleza están compuestos de esa manera*." *Combina de esta manera el método de descenso infinito con la reducción al absurdo.*

Fermat es famoso también por los números primos que llevan su nombre, los de la forma $2^{2^n}+1$

Los primeros números de esta forma: 3, 5, 17, 257, 655537*, son primos. El siguiente para n = 5 es* 4 294 967 297 *y no es fácil, usando sólo lápiz y papel, averiguar si es primo o no. De hecho, Fermat no tuvo suficiente paciencia para comprobarlo, de lo contrario hubiera obtenido, como más tarde hizo Euler, que* 4294967297= 641 x 6700417*. Sin embargo tuvo la osadía de conjeturar que todos los números de la forma* $2^{2^n}+1$ *eran primos. Esta conjetura le tuvo en jaque toda su vida, ya que en varias ocasiones se lamentó de no haber podido obtener su demostración. Hacia el final de las*"Disquisitiones arithmeticae", *Gauss había demostrado que el polígono regular de* 17 *lados es constructible con regla y compás, llevando el tema a su final lógico al demostrar cuáles de los infinitos polígonos regulares son constructibles y cuáles no. Al haber demostrado la*

constructibilidad del polígono regular de 17 lados se planteaba, de manera natural, la de los polígonos de 257 o de 65537 lados, a lo cual contesta afirmativamente al demostrar que un polígono regular de N lados puede construirse con regla y compás si y sólo si el número N es de la forma $2^m.p_1.p_2.\ldots.p_R$, *con* $m > 0$ *y* $p_1,p_2,\ldots.p_R$ *primos de Fermat distintos.*

Teorema de Wilson

El teorma de Wilson fue atribuido a John Wilson por su profesor, Edward Waring, quien comentó que Wilson había dejado anotado este resultado en un cuaderno pero que no lo había demostrado. El propio Waring tampoco pudo hacerlo y fue Lagrange quien dio la primera prueba en 1771. *Sin embargo, el teorema debiera ser atribuido al matemático, físico y astrónomo islámico Alhazen, quien lo formuló a comienzos del siglo* XI.

Sea $p \in \mathbb{N}$, p primo. De acuerdo con lo ya visto, podemos demostrar las siguientes propiedades:

Ejercicios:

1) $\forall a \in \mathbb{N}, 1 \le a \le p-1, \exists! b \in \mathbb{N}, 1 \le b \le p-1$, tal que $a.b \equiv 1$ (*mód p*).

2) $x^2 \equiv 1$ (*mód p*) $\Leftrightarrow x \equiv 1 \vee x \equiv p-1 \equiv -1$ (*mód p*).

***Teorema* (de Wilson):** Sea $p \in \mathbb{N}$, $p > 1$. Entonces,

$$p \text{ es primo} \Leftrightarrow (p-1)! \equiv p-1 \equiv -1 \ (\textit{mód } p)$$

***Demostración*:** $\Rightarrow$) $\quad (p-1)! = \prod_{i=1}^{p-1} i = 1 \times 2 \times 3 \times \ldots\ldots \times (p-2) \times (p-1)$.

El ejercicio 1) dice que cada uno de los factores de $(p-1)!$ tiene su inverso multiplicativo, módulo p, entre esos números, y los únicos cuyos inversos son ellos mismos son el 1 y el $p-1$, por el ejercicio 2). Luego, si agrupamos cada número con su correspondiente inverso módulo p, que será distinto de él para todos los números comprendidos entre 2 y $p-2$, todos esos productos serán congruentes con 1 (*mód p*), y por consiguiente, también lo será el producto de todos ellos, o sea:

$$\prod_{i=2}^{p-2} i \equiv 1 \ (\textit{mód } p)$$

luego $$\prod_{i=1}^{p-1} i = \prod_{i=2}^{p-2} i \times (p-1) \equiv 1 \times (p-1) \equiv (p-1) \equiv -1 \ (\textit{mód } p).$$

Ejemplo: $p = 23$, $(p-1)! = 22! = \prod_{i=1}^{22} i$

$2 \times 12 = 3 \times 8 = 4 \times 6 = 24 \equiv 1$ (*mód* 23)
luego: 2 es el inverso de 12 y recíprocamente ; 3 inverso de 8, y recíprocamente;
4 inverso de 6, y recíprocamente, en todos los casos (*mód* 23).

Por lo tanto $(-2)\times(-12)\equiv 1$ (*mód* 23) entonces $21\times 11\equiv 1$ (*mód* 23) pues
$-2\equiv 21$ (*mód* 23) $\wedge$ $-12\equiv 11$ (*mód* 23) ,

así también $(-3)\times(-8)\equiv 1$ (*mód* 23) $\wedge$ $(-4)\times(-6)\equiv 1$ (*mód* 23) .
Luego $20\times 15\equiv 1$ (*mód* 23) $\wedge$ $19\times 17\equiv 1$ (*mód* 23)
Además $9\times 5 = 45\equiv -1$ (*mód* 23) $\Rightarrow (-9)\times 5\equiv 9\times(-5)\equiv 1$ (*mód* 23),
con lo cual tenemos que $14\times 5\equiv 9\times 18\equiv 1$ (*mód* 23),
o sea 5 es inverso de 14, y 9 de 18 (*mód* 23).

$7\times 10 = 70\equiv -1$ (*mód* 23) $\Rightarrow (-7)\times 10\equiv 7\times(-10)\equiv 1$ (*mód* 23) $\therefore$
$16\times 10\equiv 7\times 13\equiv 1$ (*mód* 23).

Agrupemos cada número con su correspondiente inverso (*mód* 23)

$$22! = \prod_{i=1}^{22} i =$$

$= 1\times 2\times 3\times 4\times 5\times 6\times 7\times 8\times 9\times 10\times 11\times 12\times 13\times 14\times 15\times 16\times 17\times 18\times 19\times 20\times 21\times 22 =$
$=1\times(2\times 12)\times(3\times 8)\times(4\times 6)\times(5\times 14)\times(7\times 13)\times(9\times 18)\times(10\times 16)\times(11\times 21)\times(15\times 20)\times(17\times 19)$
$\times 22\equiv 1\times 1\times 1\times 1\times 1\times 1\times 1\times 1\times 1\times 1\times 1\times 22 = 22\equiv 23-1\equiv -1$ (*mód* 23).

$\Leftarrow$) Supongamos que p no es primo, como $p>1$, entonces p es compuesto.
$\therefore\ \exists k,h\in\mathbb{N}$ tales que $p = k.h$ con $1<k,h<p$.
Si $\exists k,h\in\mathbb{N}$, con $k\neq h$, entonces $(p-1)!\equiv 0$ (*mód p*) pues

$$\prod_{i=1}^{p-1} i = 1\times 2\times 3\times\ldots\times k\times\ldots.\times h\times\ldots\times(p-1)\equiv 1\times 2\times\ldots\times p\times..\times(p-1)\equiv 0\ (mód\ p)$$

Si $\nexists k,h\in\mathbb{N}$ con $k\neq h\Rightarrow p = q^2$, con q primo.
Si $q>2$, entonces $1<q<2q<(p-1)\Rightarrow q^2\mid (p-1)!\ \therefore\ (p-1)!\equiv 0$ (*mód p*).
Si $q=2\Rightarrow p=4\ \therefore\ (p-1)! = 3! = 6\equiv 2$ (*mód 4*).

Entonces, si p no es primo $(p-1)!\not\equiv (p-1)$ (*mód p*).

Ecuaciones lineales de congruencias:

Sean las ecuaciones lineales de congruencia:

i. $7x\equiv 8$ (*mód* 10) ii) $6x\equiv 15$ (*mód* 21) iii) $4x\equiv 7$ (*mód* 10)

En el primer caso, vemos que 4 es una solución, en el segundo tenemos que – 1, 6 y 13 son soluciones no congruentes *mód* 21, y en el tercero no encontramos soluciones.
Estos ejemplos nos muestran que las ecuaciones lineales de congruencia pueden tener o no solución, y que en el caso de tenerlas, podría haber varias no congruentes; por lo tanto debemos analizar el problema para saber si podemos determinar a priori, si la ecuación dada tendrá o no solución, y en el caso de tenerla, cuántas, y si disponemos de algún método para hallarlas.
Lo primero que podemos establecer, es que si x_0 es una solución de la ecuación

$ax \equiv b\ (mód\ n)$ entonces $x_0 + k.n$ es también solución $\forall k \in \mathbb{Z}$, o sea, todos los elementos de la clase $\overline{x}_0\ (mód\ n)$ serán también solución:

Si $a.x_0 \equiv b\ (mód\ n)$ entonces $a.x_0 - b = h.n$, para algún $h \in \mathbb{Z}$,
$a.(x_0 + k.n) - b = a.x_0 + a.k.n - b = a.x_0 - b + a.k.n = h.n + a.k.n = n.(h + a.k)$,
$\Rightarrow a.(x_0 + k.n) \equiv b\ (mód\ n)\ \forall k \in \mathbb{Z}$.

Luego, si hay solución, ésta **nunca** será única, es más, habrá infinitas soluciones.
Por lo tanto, además de caracterizar las ecuaciones que sí tienen solución, deberemos analizar cuántas soluciones **no congruentes** tienen, y por consiguiente, cuáles tienen **solución única *mód n***.

***Teorema*:** La ecuación de congruencia $ax \equiv b\ (mód\ n)$ admite solución si y sólo si $(a, n) = d \mid b$.

***Demostración*:** $\Rightarrow$) Supongamos que la ecuación $ax \equiv b\ (mód\ n)$ admita una solución x_0, y sea $(a, n) = d$; entonces $a x_0 - b = hn$ para cierto $h \in \mathbb{Z}$.
Como $d \mid a \Rightarrow d \mid a x_0$; $d \mid n \Rightarrow d \mid hn \therefore d \mid b$.

$\Leftarrow$) Veamos la recíproca; supongamos ahora que $d \mid b$ donde $(a, n) = d$.
$\exists u, v \in \mathbb{Z}$ tales que $d = ua + vn$ (I).
Como $d \mid b\ \exists k \in \mathbb{Z}$ tal que $b = dk$.
Multiplicando m.a.m. la igualdad (I) por k obtenemos: $b = dk = uka + vkn$
luego $b - (uk)a = vkn$, por lo tanto $a x_0 \equiv b\ (mód\ n)$ para $x_0 = uk$, por lo que la ecuación $ax \equiv b\ (mód\ n)$ admite solución.

Ejercicio: Sea $(a, n) = d \wedge d \mid b$; sea $x_0 \in \mathbb{Z}$.
x_0 es solución de la ecuación $ax \equiv b\ (mód\ n)$ si y sólo si x_0 es solución de la ecuación
$\frac{a}{d}x \equiv \frac{b}{d}\ \ (mód\ \frac{n}{d})$.

***Teorema*:** Sea $(a, n) = d \wedge d \mid b$. La ecuación $ax \equiv b\ (mód\ n)$ admite d soluciones no congruentes; si x_0 es una solución, las demás están dadas por $x_0 + i\frac{n}{d}$ para $i = 0,1,..,d-1$.

***Demostración*:** Ya sabemos que la ecuación $ax \equiv b\ (mód\ n)$ admite solución, y supongamos que x_0 es una de ellas. Para demostrar que admite exactamente d soluciones no congruentes, debemos probar primero que todos los números enteros de la forma $x_0 + i\frac{n}{d}$ con $0 \le i \le d-1$, son también soluciones, y que son **no congruentes dos a dos**, y por último, que todo otro entero que sea solución de la ecuación será congruente $mód\ n$ con alguna de esas soluciones $x_0 + i\frac{n}{d}$.

- **Todo número de la forma $x_0 + i\frac{n}{d}$ es solución de la ecuación dada:**

Reemplacemos: $a(x_0 + i\,\frac{n}{d}) = a\,x_0 + i\,\frac{n}{d}a = a\,x_0 + isn$ donde $s = \frac{a}{d} \in \mathbb{Z}$;

como $a\,x_0 \equiv b\ (mód\ n)$, se tiene $a\,x_0 + isn \equiv b + 0 \equiv b\ (mód\ n)$, pues $isn \equiv 0\ (mód\ n)$

$\therefore\ a(x_0 + i\,\frac{n}{d}) \equiv b\ (mód\ n)$.

- $x_0 + i\,\frac{n}{d} \equiv x_0 + j\,\frac{n}{d}$ **(*mód n*) con $0 \le i, j \le d-1 \Leftrightarrow i = j$**

$\Leftrightarrow$) Supongamos, sin pérdida de generalidad, que $i \le j$.

$x_0 + i\,\frac{n}{d} \equiv x_0 + j\,\frac{n}{d} \Leftrightarrow x_0 + j\,\frac{n}{d} - (x_0 + i\,\frac{n}{d}) = hn$ para cierto $h \in \mathbb{Z}$,

$\Leftrightarrow (j - i)\,\frac{n}{d} = hn \Leftrightarrow j - i = hd \Leftrightarrow j \equiv i\ (mód\ d)$, y como $0 \le i, j \le d-1 \Leftrightarrow i = j$.

- **Si z es una solución de la ecuación $ax \equiv b$ (*mód n*) entonces $z \equiv x_0 + i\,\frac{n}{d}$ (*mód n*) para cierto i, $0 \le i \le d-1$.**

Sea z una solución de la ecuación $ax \equiv b\ (mód\ n)$, entonces $az \equiv b\ (mód\ n)$,
luego $az \equiv a\,x_0 \equiv b\ (mód\ n)$, por lo que $az - a\,x_0 = tn$ para cierto $t \in \mathbb{Z}$.

$$a(z - x_0) = tn \Rightarrow \frac{a}{d}(z - x_0) = t \cdot \frac{n}{d}$$

$$\therefore\ \frac{n}{d} \mid \frac{a}{d}(z - x_0) \ \wedge\ (\frac{a}{d}, \frac{n}{d}) = 1 \Rightarrow \frac{n}{d} \mid (z - x_0) \therefore\ \exists q \in \mathbb{Z} \text{ tal que } z - x_0 = q\frac{n}{d}$$

de donde $z = x_0 + q\frac{n}{d}$

Aplicando el Algoritmo de la División: $q = pd + r$, con $0 \le r \le d - 1$, reemplazando tenemos que:

$$z = x_0 + (pd + r)\,\frac{n}{d} = x_0 + pn + r\frac{n}{d} \equiv x_0 + r\frac{n}{d}\ (mód\ n) \quad \text{con} \quad 0 \le r \le d-1$$

Luego tenemos exactamente d soluciones no congruentes.

Ejemplos:

1) $18x \equiv 22\ (mód\ 24)$

En este caso $(18, 24) = 6 \nmid 22$ por lo tanto la ecuación no tiene solución.

2) $451x \equiv 93\ (mód\ 71)$

$451 = 6.71 + 25 \Rightarrow 451 \equiv 25\ (mód\ 71)$
$93 = 1.71 + 22 \Rightarrow 93 \equiv 22\ (mód\ 71)$

Luego la ecuación dada es equivalente a la ecuación: $25x \equiv 22\ (mód\ 71)$

$(25, 22) = 1$ por lo tanto la ecuación tiene solución única *mód* 71.

Busquemos $u, v \in \mathbb{Z}$ tales que $25u + 71v = 1$

$71 = 2.25 + 21$
$25 = 1.21 + 4$
$21 = 5.4 + 1$

$\therefore\ 1 = 21 - 5.4 = (71 - 2.25) - 5(25 - 1.21) = 71 - 7.25 + 5.\ 21 =$
$= 71 - 7.25 + 5(71 - 2.25) = 6.71 - 17.25$.

Tomando $u = -17$, $v = 6$ obtenemos $25u + 71v = 1 \Rightarrow -17.25 \equiv 1$ (*mód* 71)

$-17 \equiv 54$ (*mód* 71) $\Rightarrow 54.\ 25 \equiv 1$ (*mód* 71)

entonces $54.25x \equiv x \equiv 54.22 = 1188 \equiv 52$ (*mód* 71).

El conjunto de soluciones de la ecuación es $\overline{52} = \{ 52 + 71k \ / \ k \in \mathbb{Z} \}$.

3) $2541x \equiv 3972$ (*mód* 1719)

$2541 \equiv 822$ (*mód* 1719)
$3972 \equiv 534$ (*mód* 1719)

$\therefore$ la ecuación dada es equivalente a la ecuación: $822x \equiv 534$ (*mód* 1719)

$1719 = 2.822 + 75$
$822 = 10.75 + 72$
$75 = 1.72 + 3$
$72 = 24.3$
Entonces $(1719 , 822) = 3 \mid 534$ pues $534 = 3.178$

$\therefore$ la ecuación admite exactamente tres soluciones no congruentes.

La ecuación $822x \equiv 534$ (*mód* 1719) tiene las mismas soluciones que la ecuación:

$274\ x \equiv 178$ (*mód* 573)

pues $274 = \frac{822}{3}$, $178 = \frac{534}{3}$ y $573 = \frac{1719}{3}$, y donde $(274 , 573) = 1$

$573 = 2.274 + 25$
$274 = 10.25 + 24$
$25 = 1.24 + 1$
$1 = 25 - 1.24 = 573 - 2.274 - (274 - 10.25) = 573 - 3.\ 274 + 10.25 =$
$= 573 - 3.274 + 10(573 - 2.274) = 11.573 - 23.\ 274$.

Para $u = -23$, $v = 11$ se verifica $u.274 + v.573 = 1 \Rightarrow -23.274 \equiv 1$ (*mód* 573)
$-23 \equiv 550$ (*mód* 573) $\Rightarrow 550.274 \equiv 1$ (*mód* 573)

$\therefore$ multiplicando m.a.m por 550 la ecuación: $274\ x \equiv 178$ (*mód* 573)
obtenemos $550.274x \equiv 550.178$ (*mód* 573)

luego $x \equiv 550.178 = 97900 \equiv 490$ (*mód* 573)

x_0 = 490 es la solución única, salvo congruencias, *mód* 573 ; pero debemos buscar las tres soluciones no congruentes *mód* 1719, y ellas son:

$x_0 = 490$, $x_1 = 490 + 573 = 1063$, $x_2 = 490 + 2.573 = 1636$

Todas son no congruentes *mód* 1719 , pero están en la misma clase *mód* 573 , la clase de 490.

Nota: Resolver ecuaciones lineales de congruencia es muy sencillo cuando los números son razonablemente chicos, pero los cálculos se complican si buscamos soluciones cuando *n* es muy grande, porque de una manera u otra siempre tendremos que usar el algoritmo de Euclides para hallar el m.c.d entre dos números , y algunos $u, v \in \mathbb{Z}$ que hagan que $d = ua + vn$. Por esa razón es conveniente reducir la ecuación a otras ecuaciones con números menores, valiéndonos del TFA que nos garantiza poder factorizar en primos a *n* , ya que si $n = \prod_{i=1}^{k} p_i^{r_i}$, con los p_i primos positivos, distintos dos a dos, $r_i \in \mathbb{N}$, sabemos que $ax \equiv b\ (mód\ n) \Leftrightarrow ax \equiv b\ (mód\ p_i^{r_i})\ \forall i = 1,2,...,k$.

Ahora debemos ver cómo resolver un sistema de ecuaciones lineales de congruencias.

Sistema de Ecuaciones lineales de congruencias:

Estudiaremos cierto tipo particular de sistema de ecuaciones lineales:

$$\begin{cases} x \equiv a_1 & (mód\ n_1) \\ x \equiv a_2 & (mód\ n_2) \\ & . \\ & . \\ & . \\ x \equiv a_k & (mód\ n_k) \end{cases}$$

donde $a_1, a_2, a_3, ..., a_k \in \mathbb{Z}$, $n_1, n_2, n_3, ..., n_k \in \mathbb{N}$.

Teorema Chino del Resto (*o del Residuo*)

Sean $a_1, a_2, a_3, ..., a_k \in \mathbb{Z}$, $n_1, n_2, n_3, ..., n_k \in \mathbb{N}$, con $(n_i\ ,\ n_j) = 1$ para $i \neq j$
El sistema de ecuaciones lineales de congruencia:

$$\begin{cases} x \equiv a_1 & (mód\ n_1) \\ x \equiv a_2 & (mód\ n_2) \\ & . \\ & . \\ & . \\ x \equiv a_k & (mód\ n_k) \end{cases}$$

admite solución, y ésta es única $mód \prod_{i=1}^{k} n_i$.

***Demostración*:** Sean $m = \prod_{i=1}^{k} n_i$, $m_j = \frac{m}{n_j} = \prod_{i \neq j} n_i$, para $j = 1, 2, .., k$.

Para cada j , $(n_i , n_j) = 1 \ \forall i \neq j \ \Rightarrow \ (n_j , m_j) = 1$, por lo que m_j admite inverso multiplicativo *mód* n_j . Sea $s_j \in \mathbb{Z}$ tal que $m_j . s_j \equiv 1 \ (mód \ n_j)$.

Sea $x_0 = \sum_{i=1}^{k} a_i s_i m_i$. Veremos que x_0 es solución del sistema.

Como $n_1 \mid m_j \ \forall j > 1$ se tiene $m_j \equiv 0 \ (mód \ n_1) \ \forall j > 1 \ \therefore$

$x_0 = a_1 s_1 m_1 + a_2 s_2 m_2 + ... + a_h s_h m_h + ... + a_k s_k m_k \ \equiv \ a_1 s_1 m_1 \ \equiv \ a_1 \ (mód \ n_1)$

pues $m_1 . s_1 \equiv 1 \ (mód \ n_1)$.

Además $n_2 \mid m_j \ \forall j \neq 2 \ \Rightarrow m_j \equiv 0 \ (mód \ n_2) \ \forall j \neq 2 \ \therefore$

$x_0 = a_1 s_1 m_1 + a_2 s_2 m_2 + ... + a_h s_h m_h + ... + a_k s_k m_k \ \equiv \ a_2 s_2 m_2 \ \equiv \ a_2 \ (mód \ n_2)$

pues $m_2 . s_2 \equiv 1 \ (mód \ n_2)$.

Así, para cada h , $1 \leq h \leq k$, tenemos que $n_h \mid m_j \ \forall j \neq h$, entonces $m_j \equiv 0 \ (mód \ n_h)$ $\forall j \neq h$.

$\therefore \ x_0 = a_1 s_1 m_1 + a_2 s_2 m_2 + ... + a_h s_h m_h + ... + a_k s_k m_k \ \equiv \ a_h s_h m_h \ \equiv \ a_h \ (mód \ n_h)$

pues $m_h . s_h \equiv 1 \ (mód \ n_h)$.

Por lo tanto, x_0 es solución de cada una de las ecuaciones, luego es solución del sistema.

Sea ahora $y_0 \in \mathbb{Z}$ solución del sistema. Entonces $\forall i = 1, 2, ..k \quad y_0 \equiv a_i \ (mód \ n_i)$

Como x_0 es también solución, se tiene que $y_0 \equiv x_0 \ (mód \ n_i) \ \forall i = 1, 2, ..k$.

Entonces $n_i \mid (y_0 - x_0) \ \forall i = 1, 2, ..., k$.

Y como $(n_i , n_j) = 1 \ \forall i \neq j \ \Rightarrow \prod_{i=1}^{k} n_i \mid (y_0 - x_0)$

$\therefore \ y_0 \ \equiv \ x_0 \ (mód \prod_{i=1}^{k} n_i)$

Además, si $y = x_0 + t \prod_{i=1}^{k} n_i$, con $t \in \mathbb{Z}$,

por ser $\prod_{i=1}^{k} n_i \equiv 0 \ (mód \ n_j)$, $\forall j = 1, 2, ..., k$

se tiene $y \equiv x_0 \equiv a_j \ (mód \ n_j) \ \forall j = 1, 2, ..., k$.

Luego las soluciones del sistema son los enteros que pertenecen a la clase de $x_0 \ (mód \prod_{i=1}^{k} n_i)$.

Ejemplo: Resolver el sistema $\begin{cases} x \equiv 10 \quad (mód\ 27) \\ x \equiv 2 \quad (mód\ 25) \\ x \equiv 3 \quad (mód\ 8) \end{cases}$

$m = 27.25.8 = 5400$; $m_1 = 8.25 = 200$; $m_2 = 27.8 = 216$; $m_3 = 27.25 = 675$

$m_1 = 200 \equiv 11\ (mód\ 27)$; $m_2 = 216 \equiv 16\ (mód\ 25)$; $m_3 = 675 \equiv 3\ (mód\ 8)$

Calculemos los s_i para $i = 1, 2, 3$

$27 = 2.11 + 5$

$11 = 2.5 + 1 \Rightarrow 1 = 11 - 2.5 = 11 - 2(27 - 2.11) = 5.11 - 2.27$

$\therefore\ 5.11 \equiv 1\ (mód\ 27)$, luego $s_1 = 5$

$25 = 1.16 + 9$

$16 = 1.9 + 7$

$9 = 1.7 + 2$

$7 = 2.3 + 1$, por lo tanto

$1 = 7 - 2.3 = (16 - 9) - 3(9 - 1.7) = 16 - (25 - 1.16) - 3(25 - 1.16) + 3(16 - 1.9) =$

$= 8.16 - 4.25 - 3(25 - 1.16) = 11.16 - 7.25$

$\therefore\ 11.16 \equiv 1\ (mód\ 25)$, así $s_2 = 11$

$3.3 = 9 \equiv 1\ (mód\ 8)$, luego $s_3 = 3$

$x_0 = 10.200.5 + 2.216.11 + 675.3.3 = 20827 \equiv 4627\ (mód\ 5400)$.

El Teorema Chino del Resto sólo nos da solución a sistemas en los cuales los módulos de las ecuaciones del sistema son coprimos dos a dos; para otros sistemas deberemos hacer un estudio diferente.

***Teorema*:** Sean $a, b \in \mathbb{Z}$, $n, m \in \mathbb{N}$. El sistema:

$$\begin{cases} x \equiv a \quad (mód\ n) \\ x \equiv b \quad (mód\ m) \end{cases}$$

admite solución si y sólo si $d = (n\ ,\ m) \mid (b - a)$.

De existir la solución, es única $mód\ [\ n\ ,\ m\ ]$.

***Demostración*:** Sea $d = (n\ ,\ m)$.

$\Rightarrow$) Supongamos que el sistema admite solución, o sea que $\exists\ x_0 \in \mathbb{Z}$ tal que

$$\begin{cases} x_0 \equiv a \quad (mód\ n) \\ x_0 \equiv b \quad (mód\ m) \end{cases}$$

$\therefore\ n \mid (x_0 - a) \wedge m \mid (x_0 - b)$, y como $d = (n\ ,\ m)$ se tiene que $d \mid (x_0 - a) \wedge d \mid (x_0 - b)$

$\therefore\ d \mid [\ (x_0 - a) - (x_0 - b)\ ] = (b - a)$.

$\Leftarrow$) Sea $d = (n\ ,\ m) \mid (b - a) \Rightarrow\ \exists k \in \mathbb{Z}$ tal que $b - a = d.k\ \wedge\ \exists u, v \in \mathbb{Z}$ tales que $d = un + v\ m$

multiplicando m.a.m esta igualdad por k $\quad b - a = k.d = k.u.n + k.v.m$
así $\quad b - k.v.m = a + k.u.n$

llamando $x_0 = b - k.v.m = a + k.u.n$ se tiene que $x_0 \equiv a \ (mód\ n) \wedge x_0 \equiv b \ (mód\ m)$,
luego es solución del sistema.

Unicidad: Sea $y_0 \in \mathbb{Z}$ otra solución del sistema.
Entonces $y_0 \equiv a \equiv x_0 \ (mód\ n) \wedge y_0 \equiv b \equiv x_0 \ (mód\ m)$
$\therefore\ n \mid (x_0 - y_0) \wedge m \mid (x_0 - y_0) \Rightarrow [n, m] \mid (x_0 - y_0)$
$\therefore\ x_0 \equiv y_0 \ (mód\ [n, m])$.

Ejemplos: Resolver

1) $\begin{cases} x \equiv 45 \quad (mód\ 91) \\ x \equiv 135 \quad (mód\ 377) \end{cases}$

$(91 , 377) = 13 \nmid (135 - 45) = 90$.

El sistema **no** tiene solución.

2) $\begin{cases} x \equiv 83 \quad (mód\ 91) \\ x \equiv 512 \quad (mód\ 377) \end{cases}$

$(91 , 377) = 13 \mid (512 - 83) = 429$; $[91 , 377] = 2639$
$13 = 377 - 4.91$; $512 - 83 = 429 = 33.13 = 33.377 - 33.4.91$
$\therefore\ 512 - 33.377 = 83 - 33.4.91 = -11929 \equiv 1266 \ (mód\ 2639)$
$x_0 = 1266$ es la solución única *mód* 2639 .

Desarrollos s-ádicos

El sistema de representación de los números que usamos actualmente y nos resulta tan natural, tardó muchos siglos en perfeccionarse, pero una vez que se hubo desarrollado tal y como lo conocemos, se expandió prácticamente por todo el mundo, por la simplicidad con que se puede escribir cualquier número por más grande que éste sea, porque los símbolos que debemos recordar son relativamente pocos, y además nos permite disponer de algoritmos muy sencillos para las operaciones aritméticas básicas, tan simples que un niño de corta edad puede aprenderlos. El hecho que el sistema posicional que adoptó la humanidad fuera *decimal*, o sea en base 10 (utilizando diez símbolos o *dígitos*), probablemente se deba a procesos tradicionales heredados, dado que el hombre primitivo cuando comenzó a contar, disponía de los dedos de sus manos para hacerlo, puesto que las ventajas tan relevantes que hemos señalado las comparten buena parte de los sistemas posicionales en otras bases (cuando la base s es muy grande, la dificultad que aparece es que los símbolos a memorizar son muchos, pero los algoritmos para las operaciones elementales son igualmente sencillos).
Veremos que todo número natural se representa de manera única en cualquier base s , $s > 1$, y que los algoritmos para las operaciones aritméticas en esa base son análogos a los de base 10.

***Teorema*:** Sean $s \in \mathbb{N}$, $s > 1$, $a \in \mathbb{N}$. $\exists! n, a_0, a_1, ..., a_n \in \mathbb{N}_0$ tales que $a = \sum_{i=0}^{n} a_i s^i$

con $0 \leq a_i \leq s - 1$, $a_n \neq 0$.

***Demostración*:** Haremos inducción sobre a.

Si $a = 1$, $1 = 0.s + 1$. Dado que $s > 1$, tomando $n = 0$ y $a_0 = 1$ verifican el teorema, y están unívocamente determinados porque son cociente y resto, respectivamente, en la división de 1 por s .

Sea $a > 1$, supongamos que se verifica la hipótesis para todo b, $1 \le b \le a - 1$.
Queremos demostrarlo para a.

- Si $a < s$, $a = 0.s + a$, y cociente 0 y resto a están unívocamente determinados.
- Si $a = s$, $a = 1.s + 0$, y cociente 1 y resto 0 están unívocamente determinados.

- Si $a > s$, aplicando el Algoritmo de la División, $\exists! b, r \in \mathbb{Z}$ tales que
  $a = b.s + r$ con $0 \le r < s$.
  $0 < s - r < b.s = a - r \le a \Rightarrow b > 0$ pues $s > 0$.
  Como $s > 1$, tenemos que $b < b.s \le a$, así $1 \le b < a$ y por HI $\exists! n, b_0, b_1, ..., b_n \in \mathbb{N}_0$ tales que $b = \sum_{i=0}^{n} b_i \cdot s^i$ con $0 \le b_i < s$, $b_n \neq 0$.
  Reemplazando b tenemos que $a = s. \sum_{i=0}^{n} b_i \cdot s^i + r = \sum_{i=0}^{n} b_i \cdot s^{i+1} + r =$
  $= \sum_{i=1}^{n+1} b_{i-1} \cdot s^i + r$.
  Llamando $a_0 = r$, $a_i = b_{i-1}$ para $i = 1,2,\ldots, n + 1$, tenemos que
  $a = \sum_{i=0}^{n+1} a_i \cdot s^i$ con $0 \le a_i \le s - 1$, $i = 0,1,2,\ldots, n + 1$, $a_{n+1} \neq 0$.
  como queríamos demostrar.

***Definición*:** Se dice que $a_n a_{n-1} a_{n-2} \ldots . a_1 a_0$ es la *representación en base* s del número a y se lo nota $a = (a_n a_{n-1} a_{n-2} \ldots . a_1 a_0)_s$.
Cuando $s = 10$ tenemos la *representación decimal* de un número, que es la usualmente utilizada en nuestros días, y lo notamos directamente así: $a = a_n a_{n-1} a_{n-2} \ldots . a_1 a_0$

Ejemplos: $3248 = 3.10^3 + 2.10^2 + 4.10 + 8$
$14 = 1.2^3 + 1.2^2 + 1.2 + 0 \therefore 14 = (1110)_2$
$14 = 1.3^2 + 1.3 + 2 \therefore 14 = (112)_3$
$14 = 3.4 + 2 \therefore 14 = (32)_4$

***Cómo buscar la representación en una base s de cierto número a* :**

El método está dado por el mismo teorema de existencia de la representación en base s de a , hay que dividir por s iterativamente, y los sucesivos restos que se obtienen nos dan los "dígitos" correspondientes (les llamamos *dígitos* por analogía con los símbolos del desarrollo decimal, pero obviamente en base s no son diez, sino s los símbolos que representen los números desde 0 hasta $s - 1$). Para $s \le 10$ los símbolos que utilizaremos serán los mismos que para la base 10, sólo utilizaremos desde el 0 hasta $s - 1$; cuando $s > 10$ deberemos agregar otros símbolos, y por comodidad serán letras del alfabeto, en el orden alfabético. Si s fuera muy grande y no alcanzaran

las letras del alfabeto, se pueden elegir otros símbolos hasta completar; desde el punto de vista teórico esto es posible, pero en la práctica no se utilizan bases tan grandes, ni otros símbolos ajenos a los que nos son familiares, porque sería muy difícil reconocer, no sólo ya el número expresado, sino también los números que son representados por esos símbolos.
Vamos a mostrar con ejemplos, cómo encontrar el desarrollo en base *s* de *a* :

Ejemplos:

1) $a = 285$ $s = 6$

285	6		
45	47	6	
3	5	7	6
		1	1

$285 = (1153)_6$

2) $a = 347$ $s = 2$

347	2								
14	173	2							
07	13	86	2						
1	1	06	43	2					
		0	03	21	2				
			1	01	10	2			
					0	5	2		
						1	2	2	
							0	1	

$347 = (101011011)_2$

3) $a = 1438$ $s = 12$
Como tenemos sólo 10 símbolos numéricos y necesitamos 12, agregaremos dos letras: *A* y *B* .

Escribamos la tabla de equivalencias:

10	**12**
0	0
1	1
2	2
3	3
4	4
5	5
6	6
7	7
8	8
9	9
10	*A*
11	*B*

$$\begin{array}{r|l} 1438 & 12 \\ \hline 23 & 119 \quad \big|12 \\ \hline 118 & 11=\boxed{B} \quad \boxed{9} \\ 10 = \boxed{A} & \end{array}$$

$1438 = (9BA)_{12}$

Comentario: La notación posicional introdujo una excepcional ventaja pues permitió obtener algoritmos muy sencillos para realizar las operaciones elementales: suma, resta, multiplicación y división, y ese éxito fue la razón por la que se impusiera a punto tal que desplazó a todos los demás sistemas de numeración que se utilizaron hasta esa época. La sencillez de los algoritmos no sólo es tal cuando la base es 10, sino el procedimiento es el mismo para cualquier s , la dificultad que nos puede representar en la actualidad, está dada por la "identificación" que tenemos del *número* con *su notación decimal*.
Veamos, con algunos ejemplos, cómo utilizar los algoritmos en otras bases:

Ejemplos:

1) Base $s = 2$
En base 2: 1 + 1 = 10, 1 + 1 + 1 = 11, 1 + 1 + 1 + 1 = 100

$$\begin{array}{r} 1001101 \\ + \quad 1101111 \\ \hline 10111100 \end{array} \qquad \begin{array}{r} 10001 \\ - \quad 1111 \\ \hline 10 \end{array}$$

$$\begin{array}{r} 1011 \\ \times\ 101 \\ \hline 1011 \\ 10110 \\ \hline 110111 \end{array}$$

$$\begin{array}{r|l} 1001101 & 101 \\ \hline -101 & 1111 \\ \hline 1001 & \\ -\ 101 & \\ \hline 1000 & \\ -\ 101 & \\ \hline 111 & \\ -\ 101 & \\ \hline 10 & \end{array}$$

2) En base $s = 5$

$$\begin{array}{r} 24231 \\ + \quad 43204 \\ \hline 122440 \end{array} \qquad \begin{array}{r} 434401 \\ - \quad 332043 \\ \hline 102303 \end{array}$$

Pues 1 + 4 = 10 ; 4 + 3 = 12 ; 11 – 3 = 3 ; 10 – 1 = 4

$$\begin{array}{r} 434 \\ \text{x } 24 \\ \hline 3401 \\ 1423 \\ \hline 23131 \end{array}$$

$4x1 = 4$
$4x2 = 4 + 4 = 13$
$4x3 = 13 + 4 = 22$
$4x4 = 22 + 4 = 31$
$22 + 3 = 30$
$2x3 = 11$

$$\begin{array}{r|l} 4302 & 34 \\ -34 & 110 \\ \hline 040 & \\ -34 & \\ \hline 012 & \end{array}$$

Reglas de divisibilidad

La notación posicional nos permite formular reglas de divisibilidad para ciertos casos, ellas nos facilitan la tarea de decidir si cierto número es divisible o no por otro, sin necesidad de realizar la operación.

Por ejemplo, para $m \in \mathbb{N}$, tenemos que:

i. El resto en la división por 2 de *m* es el mismo que el de su cifra de unidades (en la representación decimal). Por tanto, $2 \mid m$ sii la cifra de sus unidades es un número par.

ii. El resto en la división por 5 de *m* es el mismo que el de su cifra de unidades (en la representación decimal). Por tanto, $5 \mid m$ sii la cifra de sus unidades es 0 o 5.

iii. El resto en la división por 3 de *m* es el mismo que el de la suma de sus cifras decimales. Por tanto, para $m = \sum_{i=0}^{n} a_i 10^i$, con $0 \le a_i \le 9$, $3 \mid m$ sii $3 \mid \sum_{i=0}^{n} a_i$.

iv. El resto en la división por 9 de *m* es el mismo que el de la suma de sus cifras decimales. Por tanto, para $m = \sum_{i=0}^{n} a_i 10^i$, con $0 \le a_i \le 9$, $9 \mid m$ sii $9 \mid \sum_{i=0}^{n} a_i$.

v. El resto en la división por 4 de *m* es el mismo que el del número formado por sus dos últimas cifras decimales.

Por tanto, para $m = \sum_{i=0}^{n} a_i 10^i$, con $0 \le a_i \le 9$, $4 \mid m$ sii $4 \mid a_1 a_0$.

vi. El resto en la división por 8 de *m* es el mismo que el del número formado por sus tres últimas cifras decimales.

Por tanto, para $m = \sum_{i=0}^{n} a_i 10^i$, con $0 \le a_i \le 9$, $8 \mid m$ sii $8 \mid a_2 a_1 a_0$.

Vamos a demostrar v. a modo de ejemplo, y las demás se dejan como ejercicios.

***Demostración de v.*:**

Sea $m = \sum_{i=0}^{n} a_i 10^i$, con $0 \le a_i \le 9$

$100 = 4.25$; $1000 = 4.250$; en general $4 \mid 10^k \ \forall k \ge 2$.

Vamos a demostrarlo:

Tenemos que $4 \mid 10^2 \wedge 10^2 \mid 10^k \; \forall k \geq 2 \quad \Rightarrow \quad 4 \mid 10^k \; \forall k \geq 2$

Como $m = \sum_{i=0}^{n} a_i 10^i = \sum_{i=2}^{n} a_i 10^i + a_1 10 + a_0 = 10^2 \sum_{i=2}^{n} a_i 10^{i-2} + a_1 10 + a_0 =$

$= 10^2 \sum_{i=0}^{n-2} a_{i+2} 10^i + a_1 10 + a_0$

$4 \mid 10^2 \Rightarrow 10^2 \equiv 0 \; (mód\; 4) \; \therefore \; 10^2 \sum_{i=0}^{n-2} a_{i+2} 10^i \equiv 0 \; (mód\; 4)$

así $m = \sum_{i=0}^{n} a_i 10^i = \sum_{i=2}^{n} a_i 10^i + a_1 10 + a_0 \equiv a_1 10 + a_0 \; (mód\; 4)$.

Por lo tanto $m \equiv a_1 a_0 \; (mód\; 4)$.

Luego el resto en la división por 4 de *m* es el mismo que el del número formado por sus dos últimas cifras en su desarrollo decimal.
Como *m* y $a_1 a_0$ tienen el mismo resto en la división por cuatro, éste será cero en ambos casos, o será 1, o 2 o 3, en ambos casos, con lo cual $4 \mid m$ sii $4 \mid a_1 a_0$.

Método del Campesino Ruso

El Método del Campesino Ruso, es un sistema utilizado, hasta hace poco tiempo atrás, por campesinos de muchas regiones de Rusia, para multiplicar dos números enteros sin necesidad de hacer uso de los algoritmos asociados a la notación decimal, ni de aprender tablas de multiplicar. En realidad el método no es originario de Rusia, se han encontrado indicios de haber sido utilizado en épocas lejanas en Alemania, Francia e Inglaterra, seguramente llevado por los romanos que también lo utilizaban, y sus orígenes se remontan al antiguo Egipto del año 2000 a.c..
El Método del Campesino Ruso para multiplicar dos números naturales consiste en realizar duplicaciones sucesivas de uno de los números y divisiones por 2, sucesivas, del otro; graficaremos el método con un ejemplo:

Calcular 87×73

Se colocan en sendas columnas los números a multiplicar 87 y 73; mientras uno de ellos es duplicado sucesivamente, el otro es dividido por 2, también sucesivamente; en la división es descartado el resto 1 que se obtiene al dividir por 2 los números impares. Se seleccionan aquellos números de la columna de las duplicaciones, que se encuentren en las mismas filas que los números impares de la columna de las divisiones (en el ejemplo marcados con un *) y se los suma.

* 87	73
* 43	146
* 21	292
10	584
* 5	1168
2	2336
* 1	4672

$$73 + 146 + 292 + 1168 + 4672 = 6351 = 87 \times 73$$

Método egipcio

Los papiros de Moscú que datan de aproximadamente del año 1850 a.c, y de Rhind o Ahmes de, aproximadamente el año 1650 a.c. , muestran que los antiguos egipcios utilizaban un método similar al del Campesino Ruso, del que posiblemente éste se haya basado, no sólo para multiplicar, sino también para dividir.

Para multiplicar 47×96.

*1	96
*2	192
*4	384
*8	768
16	1536
*32	3072

Duplicamos 96 sucesivamente, tantas veces hasta alcanzar la mayor potencia de 2 menor que 47.

Como $47=32+8+4+2+1$, se suman las duplicaciones correspondientes a esas potencias de 2.

$$3072+768+384+192+96=4512=47\times 96$$

Calcular $1793\div 53$.

Duplicamos 53 tantas veces hasta llegar al mayor número posible menor o igual que 1793:

$$1793=1696+97=1696+53+44$$

*1	53
2	106
4	212
8	424
16	848
*32	1696

En la fila de las potencias de 2 los correspondientes a 1696 y 53 son respectivamente 32 y 1

$$32+1=33$$

Luego el cociente es 33 y el resto es 44

$$1793=33\times 53+44.$$

Otro ejemplo:

Calcular el cociente y el resto de dividir 954 por 41.

$$954=656+298=656+164+134=$$
$$=656+164+82+52=$$
$$=656+164+82+41+11$$

$$16+4+2+1=23$$

Luego $954=41\times 23+11$

*1	41
*2	82
*4	164
8	328
*16	656

Para el lector entusiasta…

a) Verifique los métodos dados con otras multiplicaciones : 136×58 ; 105×220.
b) Verifique el método para encontrar cociente y resto en la división de : 1467 por 85 y 159 por 38.
c) Justifique los métodos.

Ejercicios

1. Probar que si $m, n \in \mathbb{Z}$ entonces:
   1.1. $m + n \in \mathbb{Z}$.
   1.2. $m - n \in \mathbb{Z}$.
   1.3. $m.n \in \mathbb{Z}$.
   1.4. Si $n \neq 0$ ¿$m.n^{-1} \in \mathbb{Z}$?

2. Sean $a, b \in \mathbb{Z}$ probar que: $a.b = 1$ si y sólo si $a = b = 1 \vee a = b = -1$.

3. Analizar la V o F de las siguientes afirmaciones para
   $a, b, c, d, n, k, k_1, k_2, m \in \mathbb{Z}$, no nulos cuando corresponda. Si son V demostrar y si son F buscar contraejemplos.
   i) $k \mid a \,.\, b \Rightarrow k \mid a \vee k \mid b$.
   ii) $a \mid b \wedge b \mid a \Rightarrow |a| = |b|$.
   iii) $k \mid a \wedge k \mid b \Rightarrow k \mid (a + b) \wedge k \mid (a - b)$.
   iv) $k \mid (a + b) \Rightarrow k \mid a \vee k \mid b$.
   v) $a \mid (b + c) \wedge a \mid b \Rightarrow a \mid c$.
   vi) $k_1 \mid b \wedge k_2 \mid b \Rightarrow (k_1 \,.\, k_2) \mid b$.
   vii) $k \mid a \Rightarrow k \mid m.a$.
   viii) $a \mid b.c \Rightarrow a \mid b \vee a \mid c$.
   ix) $a \mid b \Rightarrow -a \mid b \wedge a \mid -b$.
   x) $a \mid 1 \vee a \mid -1 \Rightarrow a = 1 \vee a = -1$.
   xi) $a \mid 0$, $\forall a \in \mathbb{Z}$, $a \neq 0$.

4. Aplicar el algoritmo de la división en $\mathbb{Z}$, $m = b.q + r$, con $0 \leq r \leq |b|$ en los siguientes casos:

   i) $m = 13 \quad b = 5$ ii) $m = -27 \quad b = 11$ iii) $m = 1 \quad b = 0$
   iv) $m = 1 \quad b = -1$ v) $m = -1 \quad b = 2$ vi) $m = -11 \quad b = -119$

5. Conociendo el resto de la división de m por a , calcular el resto de la división de:
   i) m por $-a$ ii) $-m$ por $-a$ iii) $-m$ por a

6. Demostrar que 5 y 7 son primos.

7. Sabiendo que el resto de la división de un entero a por 7 es 5, calcular el resto de la división por 7 de los enteros:
   $2a$ $14a - 1$ $11 - a$ a^2 $a^2 - 1$

8. Calcular todos los restos posibles de la división de un entero z^2 por: a) 7 b) 5.

9. Deducir del ejercicio anterior que 7 divide a $m^2 + n^2$ si y sólo si 7 divide a m y a n.

10. Demostrar que n^2 es par si y sólo si n es par, $n \in \mathbb{N}$

11. ¿Cuáles de los siguientes enteros son pares , para $n \in \mathbb{N}$? Justificar:

    $3n^2 + 1$; ; $n.(n + 1)$; $(n - 1) \,.\, (n + 1)$; $n^3 - n$; $(-1)^{n-1} \,.\, 3 + (-1)^n \,.\, 3$

12. Sabiendo que el resto de la división de 520 por un $n \in \mathbb{N}$ es 4, y el resto de dividir 1125 por n es 9, determinar n.

13. Demostrar que si $a, b \in \mathbb{Z}$ y $13 \mid (b - a)$ entonces $13 \mid a^3 - b^3$. ¿Vale la recíproca?

13. Probar que para todo $n \in \mathbb{N}$:

i) $4^n - 1$ es divisible por 3 ii) $3^{2n+1} + 2^{n+2}$ es múltiplo de 7

iii) $10^{3^n} - 1$ es divisible por 3^n iv) $5^{2^n} - 1$ es divisible por 24

15. Probar que para todo $a \in \mathbb{Z}$, $(a^2 - a + 1) \mid [a^{2n+1} + (a - 1)^{n+2}]$.

16. Demostrar que para todo $n \in \mathbb{N}$ **:**

i) $7^n - 2^n$ es múltiplo de 5. ii) $n^3 + (n + 1)^3 + (n + 2)^3$ es múltiplo de 9.

iii) $(a + b)^n - b^n$ es múltiplo de a.

17. Sea $a \in \mathbb{Z}$ impar. Demostrar que existe un primo p tal que $p \mid (a^3 - 1)$ y $p \mid (a + 1)$. ¿Vale un enunciado análogo si no se pide que a sea impar?

18. Expresar el máximo común divisor de a y b como $ra + sb$, $r, s \in \mathbb{Z}$, en los siguientes casos:

i) $a = 125$, $b = 27$ ii) $a = -78$, $b = 22$

iii) $a = -45$, $b = -20$ iv) $a = 24$, $b = 35$

19. En cada uno de los siguientes casos calcular $d = (a, b)$. Encontrar además, en cada caso, tres pares de (u, v), con $u, v \in \mathbb{Z}$, tales que $d = u.a + v.b$

i. $a = 210$; $b = 567$ iv. $a = 15 \times 36$; $b = 15 \times 22$

ii. $a = 480$; $b = -17$ v. $a = 28$; $b = 750$

iii. $a = -26$; $b = 0$ vi. $a = 3^{18} + 1$; $b = 3^{18} - 1$

20. Sean $a, b, c \in \mathbb{Z}$, $d, k \in \mathbb{N}$. Probar:

i) $(a, b) = d \Rightarrow \left(\frac{a}{d}, \frac{b}{d}\right) = 1$. ii) $(a, b) = d \Rightarrow (ka, kb) = kd$.

iii) $(a, b) = d \wedge (c, b) = 1 \Rightarrow (ac, b) = d$. iv) $(a, b) = 1 \wedge a \mid b \cdot c \Rightarrow a \mid c$.

v) $(a,b) = 1, \quad a \mid c \wedge b \mid c \Rightarrow a.b \mid c$ vi) Para $a \neq 0, (a,b) = |a| \Leftrightarrow a \mid b$

vii) Si $b = q.a + r \Rightarrow (a,b) = (a,r)$ En particular $(a - b, a) = (a, b) = (a + b, a)$.

viii) Generalización: si $a_i \neq 0$, $a_i \mid c \ \forall i$, $i = 1,2,..n$, y $(a_i, a_j) = 1$, para $i \neq j$,

entonces $\prod_{i=1}^{n} a_i \mid c$.

ix) $p, q \in \mathbb{N}$ primos, $(p, q) = 1 \Leftrightarrow p \neq q$.

x) $(a, c) = (b, c) = 1 \Rightarrow (ab, c) = 1$.

xi) Sea p primo, tal que $p \mid \prod_{i=1}^{n} a_i$, con los $a_i \in \mathbb{Z}$, entonces $\exists j$, $1 \leq j \leq n$, tal que $p \mid a_j$.

xii) Sea $p \in \mathbb{N}$, $p > 1$; p es primo $\Leftrightarrow (p , k) = 1 \ \forall\, k$, $1 \leq k < p$.

xiii) $[a , b] = [\,|a| , |b|\,]$, $\forall a, b \in \mathbb{Z} - \{0\}$.

xiv) $[a , b] = |b| \Leftrightarrow a \mid b$.

xv) Sean $a, b \in \mathbb{Z}$, $m \in \mathbb{N}$, tales que $a \mid m \wedge b \mid m$. Entonces:

$$m = [a , b] \Leftrightarrow \left(\frac{m}{a} , \frac{m}{b}\right) = 1 .$$

21. Analizar la V o F de las siguientes afirmaciones para $a, b, c, d, n \in \mathbb{Z}$.

Las que son V demostrarlas y las que son F buscar contraejemplo.

i) Sean $a \in \mathbb{Z}$, $n \in \mathbb{Z}$, $0 < a < n$, $(a , n) = 1 \Rightarrow (n - a , n) = 1$.

ii) Sean $a \in \mathbb{Z}$, $b \in \mathbb{Z}$, $n \in \mathbb{Z}$, $(a , n) = 1$, $(b , n) = 1 \Rightarrow (a.b , n) = 1$.

iii) Sean $a, b, c, d \in \mathbb{Z}$, $(a , b) = 1 \wedge (c , d) = 1 \Rightarrow (a . c , b . d) = 1$.

22. Demostrar que si $a, b \in \mathbb{Z}$ son coprimos y $c \in \mathbb{Z}$, la ecuación $ax + by = c$ siempre puede ser resuelta para $x, y \in \mathbb{Z}$. ¿ La solución es única?. ¿Vale un enunciado análogo si a y b no son coprimos?

23. Para $a \in \mathbb{Z}$, encontrar los posibles valores de:
i. $(a , a + 1)$; ii. $(a - 1 , a + 1)$; iii. $(4a , 2a + 3)$

24. Encontrar $x, y \in \mathbb{Z}$ tales que:

i) $-117 x + 38 y = 1102$ ii) $15 x - 14 y = 213$ iii) $80x + 50y = 810$

iv) $n x - (n + 1) . y = n^2$, $n \in \mathbb{N}$. v) $122 x - 14 y = -422$

25. Problema: Un granjero compró un cierto número de vacas a \$80 cada una y un cierto número de cerdos a \$50 cada uno. En total pagó \$ 810. ¿Cuántas vacas y cuántos cerdos compró?

26. Problema: ¿De cuántas maneras se pueden cambiar 40 pesos de cierta unidad monetaria en monedas de 10 y 25 centavos?

27. Sean $p \in \mathbb{Z}$, p primo, $m, n \in \mathbb{Z}$, $m \neq 0, n \neq 0$, tales que $p \mid m.n$.
Demostrar que $p \mid m$ ó $p \mid n$.

28. Demostrar que si $(a , b) = 1$ entonces $(a + b , a.b) = 1$ y $(a^2 - b^2 , a.b) = 1$.

29. Probar que si $(a^2 + b^2 , a.b) = 1$ entonces $(a + b , a.b) = 1$.

30. Sabiendo que $(a , b) = 1$ ¿qué puede decirse de $(2.a , 3.b)$?

31. Si $(a , b) = 14$, calcular los posibles valores de:

i. $(a , a + b)$; ii. $(5a , 5b)$; iii. $(7a , 14b)$

32. Demostrar que $(a^2 + 3 , a^2 - 2) = 1$, $\forall a \in \mathbb{Z}$.

33. i. ¿Qué números naturales a, $a < 300$, satisfacen la condición $(a\ ,\ 360) = 20$?
ii. ¿Y la condición $[a\ ,\ 156] = 2340$?

34. Encontrar los $a, b \in \mathbb{N}$ tales que $[\ a\ ,\ b\ ] = 756 \quad \wedge \quad (\ a\ ,\ b\ ) = 36$.

35. Sean $a, b \in \mathbb{Z}$ tales que $\left(a^2 + b^2\ ;\ 9072\right) = 504$ y $[\ 5a + b\ ;\ 336\ ] = 1008$; calcular $(a\ ;\ b)$.

36. Problema: 1800 tornillos pesan tanto como 6930 tuercas. ¿Cuál es el menor número de tuercas y de tornillos para los cuales las tuercas pesan igual que los tornillos?

37. Escribir los siguientes enteros como producto de primos:

1472 ; 210^4 ; 18365 ; $1810^2 \cdot 21^3$

38. Demostrar que no existen $m, n \in \mathbb{N}$ tales que:

$m^2 = 2n^2$; $m^2 = 12n^2$; $m^3 = 4n^3$

39. Determinar el número de divisores positivos de los siguientes números: 68 ; 113 ; 97

40. Calcular el mínimo común múltiplo de los pares de enteros del ejercicio 18.

41. Determinar el menor de los enteros impares que tenga:
i. 17 divisores positivos.
ii. 24 divisores positivos.

42. Problema: Dos viajantes de comercio visitan periódicamente por un día cierta ciudad, uno lo hace cada 105 días y el otro cada 132 días. Hoy, martes, se encontraron y procuraron recordar cuándo se habían visto por última vez en esa ciudad. ¿Puede decir cuántos días han transcurrido desde entonces y qué día de la semana era?

43. i) Probar que si $2^m + 1$ es primo, $m \in \mathbb{N}$, m es de la forma 2^n, $n \in \mathbb{N} \cup \{0\}$,

(los números de la forma $2^{2^m} + 1$ se denominan *números de Fermat*).

ii) Demostrar que si $n \in \mathbb{N}$ tal que $2^n - 1$ es primo entonces n es primo (los números de la forma $2^n - 1$ se denominan *números de Mersenne*). ¿Vale la recíproca?

44. i) Expresar en bases $s = 3$, 5, 7 los números 1915 y 2423.

ii) Determinar los desarrollos 2- , 3- , 7- , 11- ádicos de los números (10-ádicos) 12, 17, 129.

iii) ¿Qué enteros están representados por: $(\ 1560\ )_8$; $(\ 3815\ )_9$

iv) Efectuar las siguientes operaciones:

a) $(\ 2165\ )_7 + (\ 255\ )_7$ b) $(\ 241\ )_6 \cdot (\ 1513\ )_6$

45. i. Desarrollar en bases 2 , 7 , y 16 los números: 254, 1023, 2401
ii. ¿Cuáles son los siguientes de los números que se dan a continuación?:

a. $(4)_5$ c. $(8088)_9$

b. $(44)_5$ d. $(AB)_{12}$

¿ y los anteriores?

iii. En base 12, ¿cuál es el mayor y por cuánto?
9A o A9 BA o BB 9B o B1

46. Resolver:
ii. $(654)_7 \,.\, (135)_7 + (266)_7 - (421)_7$
iii. $(11100111)_2 \div (11)_2 + (101)_2 - (1001)_2$
iv. $(121)_3 \,.\, (110)_3 + (1121)_3 - (222)_3$
v. $(A213)_{11} \div (819)_{11}$
vi. $(81A3)_{12} - (2B9)_{12}$

47. Completar los siguientes enunciados:
i. Con un dígito binario se puede escribir hasta el número……
ii. Con dos dígitos binarios se puede escribir hasta el número……..
iii. Con tres dígitos binarios se puede escribir hasta el número……..
iv. Con *n* dígitos binarios se puede escribir hasta el número……..

48. ¿Es par o impar el número $(7A)_{12}$?

49. Enunciar la regla de divisibilidad por 3 en base 2. Análogamente para la regla de divisibilidad por 9 en base 6.

50. ¿Es $(1836)_{12}$ divisible por 13 (escrito en base 10)?

51. ¿Cuáles de las siguientes congruencias son verdaderas?:

$3 \equiv -1$ (*mód* 2) $-7 \equiv -28$ (*mód* 7) $111 \equiv -1$ (*mód* 14)

52. Sea $m \in \mathbb{Z}$ impar, probar que:

i) $m^2 \equiv 1$ (*mód* 4) ii) $m^2 \equiv 1$ (*mód* 8)

53. Mostrar con ejemplos que la implicación $a \,.\, c \equiv a \,.\, d$ (*mód m*) $\Rightarrow$ $c \equiv d$ (*mód m*)
no es verdadera.

54. Escribir las tablas de suma y producto en $\mathbb{Z}_3$, $\mathbb{Z}_4$, $\mathbb{Z}_5$ y $\mathbb{Z}_6$. Determinar en cada caso los elementos inversibles.

55. Sea $n \in \mathbb{N}$. Demostrar
i. $\overline{u}, \overline{v} \in \mathbb{Z}_n^* \Rightarrow \overline{u} \,.\, \overline{v} \in \mathbb{Z}_n^* \wedge (\overline{u} \,.\, \overline{v})^{-1} = \overline{v}^{-1} . \overline{u}^{-1}$
ii. $\overline{1} \in \mathbb{Z}_n^* \wedge \overline{1}^{-1} = \overline{1}$
iii. Si $\overline{u} \in \mathbb{Z}_n^* \Rightarrow \overline{u}^{-1} \in \mathbb{Z}_n^* \wedge (\overline{u}^{-1})^{-1} = \overline{u}$

56. Sea $p \in \mathbb{N}$, $p > 1$. Demostrar que las siguientes propiedades son equivalentes:
i. p es primo
ii. $\mathbb{Z}_p$ es dominio de integridad
iii. $\mathbb{Z}_p$ es cuerpo

57. Demostrar que si $a^2 + b^2 + c^2 \equiv 0$ (*mód* 5) entonces $a.\, b.\, c \equiv 0$ (*mód* 5)

58. Calcular los restos de la división de:

i) 7^{12} por 11 ii) 3^8 por 5 iii) 2^{21} por 13 iv) 8^{25} por 127

v) 4^{7856} por 56 vi) $5 \cdot 7^{50} + 7 \cdot 5^{60}$ por 11

59. Hallar la cifra de las unidades de 17^{15} en su desarrollo decimal.

60. a) Calcular los restos posibles de la división por 7 de 10^{10^n}, con n natural. Justificar.

b) Determinar el resto de la división por 7 de $10 + 10^{10} + 10^{10^2} + ... + 10^{10^{10}}$.

61. Para $m \in \mathbb{N}$, demostrar que, en relación a su representación decimal:

i. El resto en la división por 2 de m es el mismo que el de su cifra de unidades. Por tanto, $2 \mid m$ sii la cifra de sus unidades es un número par.

ii. El resto en la división por 5 de m es el mismo que el de su cifra de unidades. Por tanto, $5 \mid m$ sii la cifra de sus unidades es 0 o 5 .

iii. El resto en la división por 3 de m es el mismo que el de la suma de sus cifras. Por tanto, para $m = \sum_{i=0}^{n} a_i 10^i$, con $0 \le a_i \le 9$, $3 \mid m$ sii $3 \mid \sum_{i=0}^{n} a_i$.

iv. El resto en la división por 9 de m es el mismo que el de la suma de sus cifras. Por tanto, para $m = \sum_{i=0}^{n} a_i 10^i$, con $0 \le a_i \le 9$, $9 \mid m$ sii $9 \mid \sum_{i=0}^{n} a_i$.

v. El resto en la división por 4 de m es el mismo que el del número formado por sus dos últimas cifras. Por tanto, para $m = \sum_{i=0}^{n} a_i 10^i$, con $0 \le a_i \le 9$, $4 \mid m$ sii $4 \mid a_1 a_0$.

vi. El resto en la división por 8 de m es el mismo que el del número formado por sus tres últimas cifras. Por tanto, para $m = \sum_{i=0}^{n} a_i 10^i$, con $0 \le a_i \le 9$, $8 \mid m$ sii $8 \mid a_2 a_1 a_0$.

vii. Un número es múltiplo de 10 sii la cifra de sus unidades es 0; es múltiplo de 100 sii sus dos últimas cifras son nulas; ……; es múltiplo de 10^k sii sus últimas k cifras son nulas .

62. a) Calcular el resto de la división de $(172432589732)^2$ por 9 .

b) Enunciar y demostrar un criterio de divisibilidad por 11.

c) Enunciar y demostrar criterios de divisibilidad por : 2^k y 5^k para $k \in \mathbb{N}$.

63. Sea $n = 10\,a + b$ probar que n es divisible por:

i) 7 sii $a - 2b$ lo es ii) 13 sii $a + 4b$ lo es iii) 17 sii $a - 5b$ lo es

64. i) Si $n \in \mathbb{Z}$, demostrar que $n^5 - n$ es múltiplo de 30.

ii) Si $x \in \mathbb{Z}$ es tal que el resto de dividir x por 2 y por 3 es 1, probar que existe un $y \in \mathbb{Z}$ tal que $x^2 - 1 = 36\,y^2 + 12\,y$.

65. i) Sean $n \in \mathbb{N}$, $a \in \mathbb{Z}$. Demostrar que para todo $b \in \mathbb{Z}$ la ecuación $a.x \equiv b$ (mód n) admite solución y es única sii (a , n) = 1.

ii) Deducir que si n es primo todo $\overline{a} \neq 0$ en $\mathbb{Z}_n$ es inversible.

iii) Caracterizar los elementos inversibles en $\mathbb{Z}_n$.

66. Resolver las siguientes ecuaciones de congruencia en el caso que tengan solución:

i) $7x \equiv 2\,(\,mód 3\,)$ ii) $15x \equiv -6\,(\,mód 3\,)$ iii) $6x \equiv 5\,(\,mód 3\,)$

iv) $6x+3 \equiv 1\,(\,mód 10\,)$ v) $1266x+7 \equiv 1\,(\,mód 39\,)$ vi) $122x \equiv -5\,(\,mód 3\,)$

vii) $15x-3 \equiv 21\,(\,mód 2\,)$ viii) $12x \equiv 15\,(\,mód 8\,)$

ix) $330x \equiv 42\,(\,mód 273\,)$ x) $180x \equiv -18\,(\,mód 30\,)$

67. Encontrar todos los $x \in \mathbb{Z}$ tales que :

i) $x^2 \equiv 1$ (*mód* 4) ii) $x^2 \equiv x$ (*mód* 12) iii) $x^2 \equiv 3$ (*mód* 3)

iv) $x^2 \equiv 0$ (*mód* 12) v) $22x^2 + x + 10 \equiv 1$ (*mód* 3)

68. Probar que si $n \in \mathbb{N}$, $\nexists\, a \in \mathbb{Z}$ tal que $70n^2 + 56\,n + 42 = a^2$.

69. i) Probar que $n^{49} + n^{28} + n^{21} + n^{14} \equiv 1$ (*mód* 7) $\Rightarrow n \equiv 10$ (*mód* 7) .

ii) Hallar todos los $n \in \mathbb{Z}$ tales que $n^{50} + n^{20} + n^{15} + n^4 + 1 \equiv 0$ (*mód* 5) .

70. Sean p, $q \in \mathbb{N}$, primos distintos. Probar que : $p^{q-1} + q^{p-1} \equiv 1$ (*mód* $p.q$) .

71. Problema: En la fecha de nacimiento de personas famosas se esconde el número 9. Por ejemplo, Miguel nació el 8 de diciembre de 1953, si ponemos 8121953 y luego cambiamos el orden de las cifras de este número, por ejemplo 1218953; luego restamos del número mayor el menor

$$\begin{array}{r} 8121953 \\ - \\ 1218953 \\ \hline 6903000 \end{array}$$

Sumamos las cifras de este último número, y da 18, 1 + 8 = 9 .

Pruebe con otras personas famosas (puede probar si es usted una persona famosa) y vea qué pasa. Justifique.

72. Problema: Una mujer con una canasta de huevos fue atropellada por una bicicleta. La mujer se presentó a cobrarle al padre del ciclista y le dijo que no sabía cuántos huevos tenía, pero que cuando los contó de 2 en 2 sobraba un huevo, y lo mismo ocurrió cuando los contó de 3 en 3, de 4 en 4 , de 5 en 5 y de 6 en 6. ¿Cuál es el número mínimo de huevos que podría haber llevado en la canasta?

73. a) Determinar el menor número natural m que satisface simultáneamente las siguientes condiciones: $m \equiv 5 \quad (4), \quad m \equiv 7 \quad (5), \quad m \equiv 4 \quad (7)$

b) Determinar el menor número natural *x* que verifica simultáneamente:

$$2x \equiv 3 \quad (5), \quad 5x \equiv 2 \quad (6), \quad 3x \equiv 1 \quad (7)$$

c) ¿Cuáles son los primeros cuatro números naturales consecutivos divisibles por 4, 5, 7 y 9 respectivamente?

74. Problema: Un cliente paga $ 48 por un artículo; para pagar dispone de un billete de $ 100 y tres monedas de $ 1, mientras que el comerciante cuenta con seis billetes de $ 10 y siete de $ 5 para dar el vuelto. ¿De cuántas maneras diferentes puede darle el cambio el comerciante?

75. Problema: Un niño juega con un cierto número de cubos. Le faltan 5 cubos para construir una caja de base rectangular que contengan 16 cubos, le sobra uno si forma una caja de base rectangular que contenga 25 cubos, y no le sobra ninguno si construye una caja de base rectangular con 21 cubos. Determinar la cantidad mínima de cubos con que el niño juega.

76. Problema: Una bolsa contiene un cierto número de bolitas. Si se sacan de a 2,3,4,5 o 6 por vez, queda sólo una bolita, pero si se sacan de a 7 por vez no queda ninguna. Encontrar el menor número posible de bolitas que puede haber en la bolsa.

77. ¿Para qué valores $a \in \mathbb{Z}$ es $(2.a + 1)^{100}$ divisible por 7?

78. ¿Puede ser el número $\overbrace{1111....1}^{300 veces}$ un cuadrado?

79. Encontrar las cifras (en la representación decimal) de las unidades y de las decenas de 7^{83}.

80. El producto de un número natural de tres cifras por 7 termina (a la derecha) en 638. Encontrar ese número.

81. Encontrar los números naturales de cuatro cifras que al dividirlos por 8 y 125 dan restos 7 y 4 respectivamente.

82. Calcular: i. 7^{1015} (31) ii. 7^{1000} (65)

83. Determinar cuatro pares de $s,t \in \mathbb{N}$, $s > 1$, $t > 1$, tales que $(14)_s = (22)_t$

84. El producto de un número natural de tres cifras por 7 termina (a la derecha) en 638. Encontrar ese número.

85. i. Sea $p \in \mathbb{N}$ primo. Probar que si $\exists n \in \mathbb{N} \wedge \exists a \in \mathbb{Z}$ tales que

$$a^2 \equiv a \ (p^n) \Rightarrow a \equiv 0 \vee a \equiv 1 \ (p^n)$$

ii. Determinar todos los $a \in \mathbb{N}$, $0 \le a \le 360$, tales que $a^2 \equiv a \quad (360)$.

86. Hallar los restos en la división de:
i. 15! por 17 ii. 2.26! por 29 iii. 19^{523} por 715

87. i. Factorizar en producto de naturales primos el número 50! sin realizar el producto.
ii. Idem i. para 100!
iii. Determinar la cantidad de ceros en que termina el desarrollo decimal de 100!
iv. Idem iii. para 500!

88. Demostrar que $\forall n \in \mathbb{N} \quad \left(\frac{n(n+1)}{2},\ 2n+1 \right) = 1$.

89. Sean $a_1, a_2, a_3, ..., a_n \in \mathbb{Z}$, no nulos, $n > 2$, $d \in \mathbb{N}$ tal que $d \mid a_i \quad \forall i = 1, 2, ..., n$; demostrar que: $d = (a_1,\ a_2,\ a_3, ..., a_n) \Leftrightarrow d = (\ d_1\ ,\ a_n)$, con $d_1 = (a_1,\ a_2,\ a_3, ..., a_{n-1})$

90. Probar que 61! + 1 y 63! + 1 son múltiplos de 71.

91. Probar sin hacer inducción, que $\forall n \in \mathbb{N}$:
i. $\frac{n^5}{5} + \frac{n^3}{3} + \frac{7n}{15} \in \mathbb{N}$ ii. $\frac{n^7}{7} + \frac{n^3}{3} + \frac{11n}{21} \in \mathbb{N}$ iii. $\frac{n^{11}}{11} + \frac{n^{13}}{13} + \frac{119n}{143} \in \mathbb{N}$

92. Sean a, $b \in \mathbb{Z}$. Mostrar que si $(a\ ,\ b) = 3$, entonces $(5^2\ a^3 b\ ,\ a^4 + b^4\ ) = 3^4$

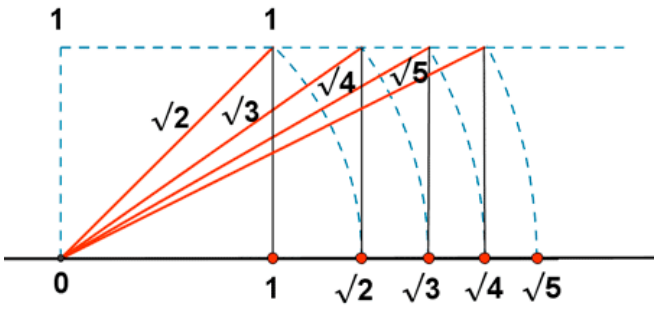
93. Hallar los enteros a que satisfacen simultáneamente: $6a \equiv 2^{117}$ (*mód* 20) $\wedge$ $14a \equiv 3$ (*mód* 15)

CAPÍTULO VI

NÚMEROS RACIONALES COMPLETITUD DEL CUERPO DE LOS REALES

Hacia el año 2000 a.C., los egipcios utilizaban algunas fracciones sencillas tales como $\frac{1}{2}; \frac{1}{3}; \frac{2}{3} \ldots$

En siglo V a.C., los griegos pitagóricos, que hasta entonces pensaban que los números naturales y las fracciones regían el universo, descubrieron la existencia de segmentos, como por ejemplo, la medida de la diagonal de un cuadrado de lado 1, *cuya medida no puede expresarse como fracción. Existía otro tipo de números: los irracionales*



Hemos visto que en $\mathbb{Z}$ podemos resolver **siempre** la ecuación: $a + x = b$ sin importar quiénes sean a , $b \in \mathbb{Z}$, y que la solución es **única**; sin embargo la ecuación: $a.x = b$ no siempre tiene solución en $\mathbb{Z}$, aun siendo $a \neq 0$; quiere decir que el conjunto $\mathbb{Z}$ es insuficiente para encontrar soluciones a esta última ecuación, y por ello debemos *extenderlo* a otro conjunto en el cual sea posible resolverla.

***Definición*:** Llamamos *conjunto de números racionales*, y lo simbolizamos con $\mathbb{Q}$, al conjunto:

$$\mathbb{Q} = \left\{ m.n^{-1} / \ m, n \in \mathbb{Z}, \ n \neq 0 \right\}$$

Nota: si $m, n \in \mathbb{Z} \ \wedge \ n \neq 0$, n tiene inverso multiplicativo en $\mathbb{R}$, luego el producto $m.n^{-1}$ está bien definido en $\mathbb{R}$.

Notación: al producto $m.n^{-1}$ lo escribiremos $\frac{m}{n}$, luego el conjunto $\mathbb{Q}$ se define

$$\mathbb{Q} = \left\{ \frac{m}{n} \ / \quad m, n \in \mathbb{Z} \ \wedge \ n \neq 0 \right\}$$

Cada *fracción* $\frac{m}{n}$ determina *unívocamente* un *número racional,* pero dos fracciones distintas pueden dar el mismo número racional; por ejemplo $\frac{m}{n} = \frac{m.k}{n.k} \quad \forall k \in \mathbb{Z} - \{0\}$, puesto que

$$\frac{m.k}{n.k} = m.k.(n.k)^{-1} = m.k.n^{-1}.k^{-1} = m.n^{-1}.k.k^{-1} = m.n^{-1} = \frac{m}{n}$$

Ejercicios:

1) Demostrar que para $m, n, r, s \in \mathbb{Z}$, $n \neq 0$, $s \neq 0$,

$$\frac{m}{n} = \frac{r}{s} \Leftrightarrow m.s = n.r \ .$$

2) Demostrar que para cada fracción $\frac{m}{n}$ $\exists! \, r \in \mathbb{Z} \wedge s \in \mathbb{N}$ tales que $\frac{m}{n} = \frac{r}{s}$ con $(r \ , s) = 1$.

***Definición*:** La fracción $\frac{r}{s}$ se dice *irreducible* si $(r \ , s) = 1$.

Comentario: El ejercicio 2) muestra que cada número racional se puede representar por una *única* fracción irreducible; en este caso sí tenemos una *correspondencia biunívoca,* la de los números racionales con las fracciones irreducibles.

Si $m \in \mathbb{Z}$, $m = m \ .1 = m \ .1^{-1} = \frac{m}{1}$, y ésta es la fracción irreducible que lo representa, por lo tanto $\mathbb{Z} \subset \mathbb{Q}$, o lo que es lo mismo: $\mathbb{Q}$ *extiende a* $\mathbb{Z}$.

En particular $0 = \frac{0}{1}$, y $\frac{m}{n} = 0 \Leftrightarrow m = 0$ (demostrarlo). Por lo tanto, si $\frac{m}{n} \neq 0$, quiere decir que $m \neq 0$, luego está definido el número racional $\frac{n}{m}$, que, a su vez, es no nulo.

Ejercicio: Demostrar que la suma y el producto de números racionales es, a su vez, un número racional, o sea:

Para $\frac{m}{n}, \frac{r}{s} \in \mathbb{Q}$, $\frac{m}{n} + \frac{r}{s} \in \mathbb{Q} \quad \wedge \quad \frac{m}{n} \cdot \frac{r}{s} \in \mathbb{Q}$.

Sugerencia: Demostrar que $\frac{m}{n} + \frac{r}{s} = \frac{m.s + n.r}{s.n} \wedge \frac{m}{n} \cdot \frac{r}{s} = \frac{m.r}{n.s}$

Por lo tanto la suma y el producto son dos operaciones en $\mathbb{Q}$:

$$+: \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q} \qquad (x , y) \to x + y$$

$$\cdot : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q} \qquad (x , y) \to x \cdot y$$

que verifican las siguientes propiedades:

Suma:

- asociativa
- conmutativa
- tiene elemento neutro: 0
- todo elemento tiene inverso aditivo u opuesto: $-\left(\frac{m}{n}\right) = \frac{-m}{n}$

Por verificar todas estas propiedades decimos que ($\mathbb{Q}$, +) es un *grupo abeliano.*

Producto:

- asociativo
- conmutativo
- tiene elemento neutro: 1
- todo elemento no nulo tiene inverso: $\frac{m}{n} . \frac{n}{m} = 1 \Rightarrow \frac{n}{m} = \left(\frac{m}{n}\right)^{-1}$
- además el producto es distributivo respecto de la suma: $x.(y + z) = x.y + x.z$

Por haber dos operaciones en $\mathbb{Q}$ que verifican todas las propiedades enunciadas, decimos que ($\mathbb{Q}$, + , .) es un cuerpo.

Hemos comenzado definiendo el Cuerpo Ordenado de Números Reales, en dicho conjunto distinguimos el conjunto de Números Naturales, luego definimos el de los Números Enteros, y ahora hicimos lo propio con el de los Racionales, y vemos que obtenemos también un cuerpo ordenado, porque claramente se verifican en $\mathbb{Q}$ todas las propiedades relativas al orden; luego es razonable preguntarse si $\mathbb{Q}$ no es igual a $\mathbb{R}$, o sea, si hemos llegado a caracterizar a los números reales como cociente de enteros. Inmediatamente podemos responder negativamente a esa pregunta, porque ya hemos visto que hay números reales que no se pueden escribir como cociente de enteros, por ejemplo el número real positivo cuyo cuadrado es 2 , que lo escribimos $\sqrt{2}$, sabemos que existe porque es lo que mide la hipotenusa de un triángulo rectángulo isósceles de lados 1, y también sabemos que $\nexists m, n \in \mathbb{N}$ tales que $m^2 = 2n^2$, o sea, 2 no es el cuadrado de ningún número racional, por lo tanto $\mathbb{Q} \subsetneq \mathbb{R}$. Que $\mathbb{Q}$ sea un subconjunto propio de $\mathbb{R}$, y que ambos sean cuerpos ordenados, está indicando que esos axiomas no caracterizan al conjunto de números reales como creímos en un principio, nos falta algún otro axioma para poder definirlo:

Axioma de Completitud:

Todo subconjunto no vacío de $\mathbb{R}$ *, acotado superiormente, admite supremo.*

***Teorema*:** Sea $A \subset \mathbb{R}$, $A \neq \phi$ y acotado superiormente por s. Las siguientes dos propiedades son equivalentes:

i. $s = sup\, A$

ii. $\forall \varepsilon > 0 \quad \exists a \in A$ tal que $s - \varepsilon < a \leq s$

***Demostración*:** i. $\Rightarrow$ ii.)

Sea $\varepsilon > 0$, como $s = sup\, A$, s es la menor de las cotas superiores de A, por lo tanto, los números menores que él no pueden ser cotas superiores de A; como $s - \varepsilon < s$ entonces $s - \varepsilon$ no es cota superior de $A \therefore \exists a \in A$ tal que $s - \varepsilon < a$, además $a \leq s$, porque s sí es cota superior de *A*.

ii. $\Rightarrow$ i.) Por hipótesis *s* es cota superior de A, para ver que es el supremo debemos ver que es la menor de las cotas superiores, o lo que es lo mismo, que los números menores que *s* no pueden ser cotas superiores de *A*.
Sea $t < s$, sea $\varepsilon = s - t > 0$ entonces $t = s - \varepsilon$; por ii. $\exists a \in A$ tal que $s - \varepsilon < a$, luego $\exists a \in A$ tal que $t < a$ por lo tanto t no es cota superior de A, y así *s* es la menor de las cotas superiores de $A \therefore s = sup\, A$.

Ejercicios:

1) Demostrar que todo subconjunto no vacío de $\mathbb{R}$, acotado inferiormente, admite ínfimo.

2) Demostrar que si $A \subset \mathbb{R}$, $A \neq \phi$ y acotado inferiormente por t, las siguientes dos propiedades son equivalentes:

i. $t = ínf\, A$

ii. $\forall \varepsilon > 0 \quad \exists a \in A$ tal que $t \leq a < t + \varepsilon$

Definición*:** Con los axiomas de cuerpo ordenado y el axioma de completitud, caracterizamos al cuerpo de los números reales como un ***cuerpo ordenado completo.

Teorema de Arquimedianidad

En el capítulo referido al conjunto de Números Naturales vimos que $\mathbb{N}$ no está acotado superiormente por ningún número natural, y obviamente tampoco lo está por ningún número entero, pero no habíamos podido demostrar que $\mathbb{N}$ no es un conjunto acotado superiormente en $\mathbb{R}$; el axioma de completitud nos brinda un herramienta para poder hacerlo.

*Arquímedes (*287 *a.c.*-212 *a.c)*

***Teorema*:** $\mathbb{N}$ no está acotado superiormente en $\mathbb{R}$, o sea $\forall x \in \mathbb{R} \quad \exists n \in \mathbb{N}$ tal que $n > x$.

***Demostración*:** Vamos a demostrarlo por *el absurdo*.
Supongamos que $\mathbb{N}$ sea un conjunto acotado superiormente en $\mathbb{R}$; por el axioma de completitud, $\mathbb{N}$ tiene un supremo s.
Si $s = sup\,\mathbb{N}$, como $s \notin \mathbb{N}$ porque $\mathbb{N}$ no admite cotas superiores naturales, $n < s \ \forall n \in \mathbb{N}$ entonces $n + 1 < s \ \forall n \in \mathbb{N}$, o sea que $n < s - 1 \ \forall n \in \mathbb{N}$ $\therefore$ $s - 1$ es una cota superior de $\mathbb{N}$, pero $s - 1 < s$!! (absurdo!) pues s es el supremo de $\mathbb{N}$.
Luego $\mathbb{N}$ no admite cotas superiores en $\mathbb{R}$.

***Corolario1*:** $\forall a, b \in \mathbb{R}$, $a > 0$, $\exists n \in \mathbb{N}$ tal que $na > b$.

***Demostración*:** Como $a > 0 \ \wedge \ \frac{b}{a} = b.a^{-1} \in \mathbb{R}$, por el teorema de Arquimedianidad,

$\exists n \in \mathbb{N}$ tal que $n > \frac{b}{a}$, entonces $na > b$ por ser $a > 0$.

***Corolario2*:** $\forall x > 0 \ \exists n \in \mathbb{N}$ tal que $0 < \frac{1}{n} < x$.

***Demostración*:** Sea $x > 0$, por el Corolario 1 $\exists n \in \mathbb{N}$ tal que $nx > 1$, luego $0 < \frac{1}{n} < x$

***Corolario3*: ($\mathbb{Q}$ es denso en $\mathbb{R}$)** $\forall x, y \in \mathbb{R}, x < y$, $\exists r \in \mathbb{Q}$ tal que $x < r < y$.

***Demostración*:**

- Primero consideremos que $0 < x < y$.

Siendo $y - x > 0$, por el Corolario 1 $\exists n \in \mathbb{N}$ tal que $n(y - x) > 1$ $\therefore$ $ny > nx + 1$. Como $nx > 0$, por el teorema de Arquimedianidad, $\exists k \in \mathbb{N}$ tal que $k > nx$; sea $m = mín \ \{ k \in \mathbb{N} \ / \ nx < k \}$ (la existencia de este mínimo está garantizada por la buena ordenación de $\mathbb{N}$).
Entonces $nx < m$; queremos ver que $m < ny$.
Si no fuera así, o sea, si $m \geq ny > nx + 1$ sería $m - 1 > nx$, y como $m > 1$
pues es $m > 1 + nx$, entonces $m - 1 \in \mathbb{N} \ \wedge \ m - 1 < m$!! (absurdo!)
pues $m = mín \ \{ k \in \mathbb{N} \ / \ nx < k \}$ $\therefore$ $m < ny$.

Como $nx < m < ny$ se tiene $x < \frac{m}{n} < y \ \wedge \ \frac{m}{n} \in \mathbb{Q}$

- Sea ahora $0 = x < y$

Por el Corolario 2 $\exists n \in \mathbb{N}$ tal que $0 < \frac{1}{n} < y \ \wedge \ \frac{1}{n} \in \mathbb{Q}$

- Si $x < 0 < y$, $0 \in \mathbb{Q}$

- Si $x < y \leq 0$ entonces $0 \leq -y < -x$; por lo visto en los casos anteriores $\exists r \in \mathbb{Q}$ tal que $-y < r < -x$ $\therefore$ $x < -r < y \ \wedge \ -r \in \mathbb{Q}$

Luego, hemos demostrado que si $x < y$ $\exists r \in \mathbb{Q}$ tal que $x < r < y$. Esta propiedad de los racionales en los reales se expresa diciendo que $\mathbb{Q}$ *es denso en* $\mathbb{R}$.

Raíces cuadradas en $\mathbb{R}$ **:**

***Definición*:** Sea $x \in \mathbb{R}$; x es un *cuadrado* en $\mathbb{R}$ si $\exists y \in \mathbb{R}$ tal que $y^2 = x$.

***Observación*:** si x es un cuadrado en $\mathbb{R}$ entonces $x \geq 0$ porque ya vimos que $\forall y \in \mathbb{R}$ se verifica que $y^2 \geq 0$.

0 es un cuadrado porque $0^2 = 0$.

Veremos que todo $x > 0$ es también un cuadrado en $\mathbb{R}$.

Antes observemos que si $x > 0$ es un cuadrado en $\mathbb{R}$, e y es tal que $y^2 = x$ entonces $(-y)^2 = x$; siendo x positivo , $y \neq 0$, luego entre $y \wedge -y$ uno y sólo uno es positivo. Además éstos son los únicos números reales cuyos cuadrados dan x , puesto que si $y^2 = z^2$, tenemos que

$(y - z).(y + z) = 0 \Rightarrow y - z = 0 \vee y + z = 0 \quad \therefore \quad z = y \vee z = -y.$

***Teorema*:** $\forall x > 0 \ \exists! y > 0$ tal que $y^2 = x$.

***Demostración*:** La unicidad de y ya ha sido demostrada en la observación anterior; nos resta verificar la existencia.

- Supongamos, primero, que $x > 1$.

Sea el conjunto $A = \left\{ z \in \mathbb{R}_{>0} \ / \quad z^2 \leq x \right\}$.

$A \neq \phi$ puesto que $1 \in A$, y acotado superiormente por x , ya que $z \in A \Rightarrow z^2 \leq x$

y como $x > 1$, se verifica que $x < x^2 \ \therefore \ z^2 < x^2$, y como ambos son positivos, entonces $z < x$.

Como A es no vacío y acotado superiormente en $\mathbb{R}$, por el axioma de completitud, A admite supremo.

Sea $s = sup\ A$, $s > 1$; por la propiedad de tricotomía, se verifica una y sólo una de estas tres situaciones : $s^2 < x \vee s^2 > x \vee s^2 = x$.

- Supongamos que $s^2 < x \Rightarrow x - s^2 > 0$, y por lo tanto $\dfrac{x - s^2}{1 + 2s} > 0$

$\therefore \ \exists \varepsilon \in \mathbb{R}, \quad 0 < \varepsilon < 1$ tal que $\varepsilon < \dfrac{x - s^2}{1 + 2s}$

$\therefore \ \varepsilon (1 + 2s) < x - s^2 \ \therefore \ \varepsilon^2 + 2\varepsilon s + s^2 < \varepsilon + 2\varepsilon s + s^2 < x$ puesto que al ser $\varepsilon < 1$, se verifica que $\varepsilon^2 < \varepsilon$.

Así tenemos que $(s + \varepsilon)^2 < x \Rightarrow s + \varepsilon \in A$, pero $s < s + \varepsilon$!! (absurdo!) pues s es cota superior de A.

- Supongamos ahora $s^2 > x$ entonces $s^2 - x > 0 \ \therefore \ \dfrac{s^2 - x}{2s} > 0$

$\exists \varepsilon \in \mathbb{R}, \quad 0 < \varepsilon < 1$ tal que $\varepsilon < \dfrac{s^2 - x}{2s}$, luego $2\varepsilon s < s^2 - x$

y por tanto $x < s^2 - 2\varepsilon s < s^2 - 2\varepsilon s + \varepsilon^2 = (s - \varepsilon)^2$

Si $z \in A$ entonces $z^2 < x < (s - \varepsilon)^2$, y como $z > 0 \wedge s - \varepsilon > 0$, tenemos que $z < s - \varepsilon \ \therefore$ $s - \varepsilon$ es cota superior de A !! (absurdo!) pues $s - \varepsilon < s \ \wedge \ s = sup\ A$.

Como $s^2 \not< x \ \wedge \ x \not< s^2$ se tiene $s^2 = x$ $\therefore$ x es un cuadrado en $\mathbb{R}$.

- Si $x = 1$, x es un cuadrado pues $1^2 = 1$.
- Si $0 < x < 1$ entonces $\frac{1}{x} > 1$; por lo demostrado anteriormente, $\exists s > 0$ tal que $s^2 = \frac{1}{x}$ $\therefore$ $x = \frac{1}{s^2} = \left(\frac{1}{s}\right)^2$

Por lo tanto $\forall x > 0 \quad \exists! y > 0$ tal que $y^2 = x$.

***Definición*:** Sea $x \geq 0$. Llamamos *raíz cuadrada de x,* y lo notamos $\sqrt{x}$, al único número real $y \geq 0$ tal que $y^2 = x$.

$$y = \sqrt{x}$$

Como $\forall x > 0$ hay dos números reales, uno positivo y el otro su opuesto, cuyos cuadrados dan x, a esos dos números los notamos respectivamente: $\sqrt{x} \ \wedge -\sqrt{x}$

El símbolo de la raíz cuadrada ($\sqrt{\ }$) fue introducido en 1525 por el matemático Christoph Rudolff. Se conjetura que no es más que una forma estilizada de la letra "r", que representa la palabra latina radix (raíz), alargándola con un trazo horizontal hasta adoptar el aspecto actual.

***Definición*:** Sea $n \in \mathbb{N}$, $n > 2$, $x \in \mathbb{R}$; se dice que *x es una potencia n-ésima* si $\exists y \in \mathbb{R}$ tal que $y^n = x$.

***Observación*:** Cuando n es par $y^n \geq 0 \ \forall y \in \mathbb{R}$, y como $y^n = 0 \Leftrightarrow y = 0$, tenemos que $\forall y \neq 0$ se verifica que $y^n > 0$. Por lo tanto, para n par, si x es una potencia n-ésima entonces $x \geq 0$. También, como en el caso $n = 2$, tenemos que $y^n = (-y)^n$, uno de estos números es positivo y el otro es negativo.
Cuando n es impar esa propiedad no es válida, pues
$y^n > 0$ si $y > 0$, $y^n = 0$ si $y = 0 \ \wedge \ y^n < 0$ si $y < 0$; además $-y^n = (-y)^n$
por lo tanto basta determinar cuáles son las potencias n-ésimas positivas para determinarlas todas.

Ejercicios:

1) Demostrar que para $z, y \in \mathbb{R} \quad z^n - y^n = (z - y).\sum_{i=0}^{n-1} z^i y^{n-1-i}$

2) Demostrar que si $z > 0 \ \wedge \ y > 0$, $\sum_{i=0}^{n-1} z^i y^{n-1-i} > 0$.

3) Demostrar para $z, y \in \mathbb{R}_{>0}$, $n \in \mathbb{N}$, $z^n = y^n \Leftrightarrow z = y$

4) Demostrar para $z, y \in \mathbb{R}_{>0}$, $n \in \mathbb{N}$, $z^n < y^n \Leftrightarrow z < y$

Demostración de 3):

Sean z , $y \in \mathbb{R}_{>0}$ tales que $z^n = y^n \Rightarrow z^n - y^n = 0 = (z-y).\sum_{i=0}^{n-1} z^i y^{n-1-i}$, y como $\sum_{i=0}^{n-1} z^i y^{n-1-i} > 0$

$\Rightarrow z - y = 0 \therefore z = y$.

La recíproca es trivial.

Nota: si $x > 0$ es una potencia *n*-ésima entonces $\exists! \, y > 0$ tal que $y^n = x$.

Sólo nos resta demostrar que todo número real no negativo es una potencia *n*-ésima; eso es lo que afirma el siguiente teorema, cuya demostración es conceptualmente análoga al teorema de existencia de raíces cuadradas.

***Teorema*:** $\forall x > 0 \; \exists! \, y > 0$ tal que $y^n = x$.

***Demostración*:** La unicidad de y ya ha sido demostrada en el ejercicio anterior; nos resta verificar la existencia.

- Supongamos, primero, que $x > 1$.

Sea el conjunto $A = \left\{ z \in \mathbb{R}_{>0} \; / \quad z^n \le x \right\}$.

$A \neq \phi$ puesto que $1 \in A$, y acotado superiormente por x , ya que $z \in A \Rightarrow z^n \le x$

y como $x > 1$, se verifica que $x < x^n \therefore z^n < x^n$, y como ambos son positivos, entonces $z < x$.

Como A es no vacío y acotado superiormente en $\mathbb{R}$, por el axioma de completitud, A admite supremo.

Sea $s = sup \; A$, $s > 1$; por la propiedad de tricotomía, se verifica una y sólo una de estas tres situaciones : $s^n < x \vee s^n > x \vee s^n = x$.

- Supongamos que $s^n < x \Rightarrow x - s^n > 0$, y por lo tanto $\dfrac{x - s^n}{\sum_{i=0}^{n-1} \binom{n}{i} s^i} > 0$

$\therefore \exists \varepsilon \in \mathbb{R}, \quad 0 < \varepsilon < 1$ tal que $\varepsilon < \dfrac{x - s^n}{\sum_{i=0}^{n-1} \binom{n}{i} s^i}$

$\therefore \; \varepsilon \sum_{i=0}^{n-1} \binom{n}{i} s^i < x - s^n \; \therefore \; \sum_{i=0}^{n} \binom{n}{i} s^i \varepsilon^{n-i} < \varepsilon + \sum_{i=1}^{n-1} \binom{n}{i} \varepsilon s^i + s^n < x$ puesto que al ser $\varepsilon < 1$, se verifica que $\varepsilon^i < \varepsilon \;\; \forall i > 1$.

Así tenemos que $(s+\varepsilon)^n < x \Rightarrow s + \varepsilon \in A$, pero $s < s + \varepsilon$!! (absurdo!) pues s es cota superior de *A*.

- Supongamos ahora $s^n > x$ entonces $s^n - x > 0 \therefore \dfrac{s^n - x}{\sum_{i=1}^{n-1} \binom{n}{i} s^i} > 0$

$\exists \varepsilon \in \mathbb{R}$, $0 < \varepsilon < 1$ tal que $\varepsilon < \dfrac{s^n - x}{\sum_{i=1}^{n-1} \binom{n}{i} s^i}$, luego $\varepsilon \sum_{i=1}^{n-1} \binom{n}{i} s^i < s^n - x$

y por tanto $x < s^n - \varepsilon \sum_{i=1}^{n-1} \binom{n}{i} s^i = s^n + \sum_{i=1}^{n-1} \binom{n}{i} s^i (-\varepsilon) < \sum_{i=0}^{n} \binom{n}{i} s^i (-\varepsilon)^{n-i} = (s-\varepsilon)^n$.

Si $z \in A$ entonces $z^n < x < (s-\varepsilon)^n$, y como $z > 0 \wedge s - \varepsilon > 0$, tenemos que $z < s - \varepsilon$ $\therefore$ $s - \varepsilon$ es cota superior de A !! (absurdo!) pues $s - \varepsilon < s \wedge s = sup\ A$.

Como $s^n \not< x \quad \wedge \quad x \not< s^n$ se tiene $s^n = x$ $\therefore$ x es una potencia n-ésima en $\mathbb{R}$.

Si $x = 1$, x es una potencia n-ésima pues $1^n = 1$.
Si $0 < x < 1$ entonces $\dfrac{1}{x} > 1$; por lo demostrado anteriormente,

$\exists s > 0$ tal que $s^n = \dfrac{1}{x}$ $\therefore$ $x = \dfrac{1}{s^n} = \left(\dfrac{1}{s}\right)^n$

Por lo tanto $\forall x > 0\ \exists! y > 0$ tal que $y^n = x$.

***Definición*:** Sea $x \geq 0$. Llamamos *raíz n-ésima de x,* y lo notamos $\sqrt[n]{x}$, al único número real $y \geq 0$ tal que $y^n = x$.

Notación: $y = \sqrt[n]{x}$

Si n es par el otro número real cuya potencia n-ésima da x es $-\sqrt[n]{x}$, que es negativo.
Si n es impar $\forall x \in \mathbb{R}\ \exists! y \in \mathbb{R}$ tal que $y^n = x$, $y > 0 \Leftrightarrow x > 0$, $y = 0 \Leftrightarrow x = 0$,
$y < 0 \Leftrightarrow x < 0$.

Propiedades de la raíz n-ésima:

Sean a , $b \in \mathbb{R}_{>0}$, $n, m \in \mathbb{N}$. Probar que:

- **i.** $\left(\sqrt{a}\right)^2 = a$
- **ii.** $\sqrt[n]{a \cdot b} = \sqrt[n]{a} \cdot \sqrt[n]{b}$
- **iii.** $\sqrt[n]{a^{-1}} = \left(\sqrt[n]{a}\right)^{-1}$
- **iv.** $\sqrt[m]{\sqrt[n]{a}} = \sqrt[n.m]{a}$
- **v.** $a < b \Leftrightarrow \sqrt[n]{a} < \sqrt[n]{b}$
- **vi.** $1 < a$, $n < m \Rightarrow \sqrt[m]{a} < \sqrt[n]{a}$

***Demostración*:** Se deja como ejercicio.

Potencia racional de un número real

***Definición*:** Sean $n, m \in \mathbb{N}$, $x \in \mathbb{R}$, $x \geq 0$; definimos $x^{\frac{m}{n}} =: \left(\sqrt[n]{x}\right)^m$.

Nota: Cuando n es impar no necesitamos imponer la condición $x \geq 0$, en este caso podemos definir $x^{\frac{m}{n}} =: \left(\sqrt[n]{x}\right)^m \quad \forall x \in \mathbb{R}$.

Si $m \in \mathbb{Z} \ \wedge \ m \leq 0$ sólo podemos definir $x^{\frac{m}{n}} =: \left(\sqrt[n]{x}\right)^m$ cuando $x > 0$ para n par, y $x \neq 0$ para n impar.

***Propiedades de la potencia racional*:**

Sean $a, b \in \mathbb{R}_{>0}$, $n, q \in \mathbb{N}$, $m, p \in \mathbb{Z}$, $r, s \in \mathbb{Q}$. Demostrar que:

i. $\frac{m}{n} = \frac{p}{q} \Rightarrow a^{\frac{m}{n}} = a^{\frac{p}{q}}$ (Esto dice que la potencia de exponente racional $\frac{m}{n}$ está bien definida)
ii. $a^{\frac{m}{n}} = \sqrt[n]{a^m}$
iii. $a^r \, . \, a^s = a^{r+s}$
iv. $\frac{a^r}{a^s} = a^{r-s}$
v. $(a^r)^s = a^{r.s}$
vi. $(a.b)^r = a^r . \, b^r$
vii. $a^{-r} = (a^r)^{-1}$

***Demostración*:** Se deja como ejercicio.

Para pensar: ¿Podemos afirmar que siempre es $\sqrt{x^2} = \left(\sqrt{x}\right)^2$?

Números racionales y números irracionales

Ya hemos visto que hay ciertos números reales que no son racionales, por ejemplo $\sqrt{2} \notin \mathbb{Q}$; todos aquellos números reales que no son racionales se denominan ***irracionales***. Si simbolizamos con $\mathbb{I}$ a tal conjunto, tenemos que $\mathbb{I} = \mathbb{R} - \mathbb{Q}$, y por lo tanto que $\mathbb{R} = \mathbb{Q} \cup \mathbb{I}$ (unión disjunta).

No es sencillo demostrar que un determinado número es irracional, en especial los del tipo : 2^e, e^π , π^e , $\pi^{\sqrt{2}}$ (e es la base de los *logaritmos neperianos*, y la definición de potencia que justifica las notaciones de los números que hemos mencionado es $a^x =: e^{x.\ln a}$, para $a \in \mathbb{R}_{>0}$). La irracionalidad de e y de π fue demostrada en 1761 por Lambert; en 1929 Gelfond probó que e^π es trascendente (por lo tanto irracional) y los otros números no se sabe aun si son o no irracionales. Mucho más sencillo resulta probar que $\sqrt{10}$, $\sqrt[3]{4}$ o $\sqrt[5]{8}$ son irracionales, es más, es sencillo demostrar que $\forall r \in \mathbb{Q}_{>0} \ \sqrt[n]{r} \notin \mathbb{Q}$ para casi todo $n \in \mathbb{N}$.

Números algebraicos y trascendentes

***Definición*:** Sea $a \in \mathbb{R}$, *a* se dice *algebraico* si existen $r_0, r_1, r_2, ..., r_n \in \mathbb{Q}$, no todos nulos, tales que : $r_n a^n + r_{n-1} a^{n-1} + ... + r_2 a^2 + r_1 a + r_0 = 0$.

***Definición*:** Sea $a \in \mathbb{R}$. *a* se dice *trascendente* si no es algebraico, o sea si
$r_n a^n + r_{n-1} a^{n-1} + ... + r_2 a^2 + r_1 a + r_0 = 0$ con $r_i \in \mathbb{Q}$, $\forall i$, $i = 0,1,2,\ldots n$
$\Rightarrow r_i = 0 \ \forall i$, $i = 0,1,2,\ldots n$.

Ejemplos: $\sqrt{10}$, $\sqrt[3]{4}$ o $\sqrt[5]{8}$ son algebraicos puesto que :
$\sqrt{10}$ es solución de la ecuación polinomial, con coeficientes en $\mathbb{Q}$: $x^2 - 10 = 0$;
$\sqrt[3]{4}$ es solución de la ecuación polinomial, con coeficientes en $\mathbb{Q}$: $x^3 - 4 = 0$;
$\sqrt[5]{8}$ es solución de la ecuación polinomial, con coeficientes en $\mathbb{Q}$: $x^5 - 8 = 0$.

e y π son trascendentes ; la trascendencia de *e* fue probada por primera vez por Hermite en 1873, y la de π por Lindemann en 1882.

Nota: Todo número racional es algebraico, puesto que si $r \in \mathbb{Q}$, *r* es solución de la ecuación polinomial en $\mathbb{Q}$: $x - r = 0$.

Si llamamos $\mathbb{A}$ al conjunto de números algebraicos, y $\mathbb{T}$ al conjunto de números trascendentes, tenemos que $\mathbb{R} = \mathbb{A} \cup \mathbb{T}$ (unión disjunta) y $\mathbb{Q} \subsetneq \mathbb{A}$ porque ya vimos que todo número racional es algebraico y que existen números irracionales que también son algebraicos.
Aunque, quizás por la dificultad que tenemos en dar ejemplos, parecería que, desde el punto de vista *cuantitativo*, hay más números algebraicos que trascendentes, nada más alejado de la realidad, el conjunto $\mathbb{T}$ *tiene un número mucho mayor de elementos que* $\mathbb{A}$; ese hecho lo expresamos diciendo que *card* $\mathbb{A}$ < *card* $\mathbb{T}$ (el cardinal de $\mathbb{A}$ es menor que el de $\mathbb{T}$).

Algunos irracionales famosos

El número π

π viene de la palabra griega peripheria que significa circunferencia. El nombre π lo comenzó a usar Euler en el siglo XVII.
Arquímedes de Siracusa (287-212 a.C.), nacido en Siracusa, en la Magna Grecia, la actual Sicilia, fue el más grande de los matemáticos de la antigüedad y será recordado por su obra sobre círculos, cilindros y esferas que ahora asociamos con el número π. Claro que los griegos no trabajaban directamente con π, sino que lo veían geométricamente como la razón entre la circunferencia de un círculo y su diámetro.
Culturas anteriores habían advertido que dicha razón es siempre la misma, aproximadamente $3\frac{1}{7}$.
Los babilonios habían observado que $\frac{25}{8} < \pi < \frac{22}{7}$. Arquímedes fue mucho más lejos, sus resultados iban acompañados de demostraciones rigurosas. Hasta donde sabían los griegos, la razón entre la circunferencia de un círculo y su diámetro podría ser irracional, pero él comparó la circunferencia de un círculo con los perímetros de dos series de polígonos: una situada en el

interior del círculo y la otra a su alrededor, utilizando polígonos inscriptos de 96 lados, demostró que $3\frac{10}{71} < \pi < 3\frac{1}{7}$.

En el siglo XVI, Francisco Vieta calculó π con 10 decimales, y en 1596 el alemán Ludolf von Ceulen calculó 35 de sus cifras decimales.

En 1761 el físico y matemático alemán Johan Heinrich Lambert demostró que π es irracional.

En 1882 C.L.F. Lindemann de Munich, publica en un artículo de los Mathematische Annalen la demostración de manera concluyente que π es un número **trascendente**.

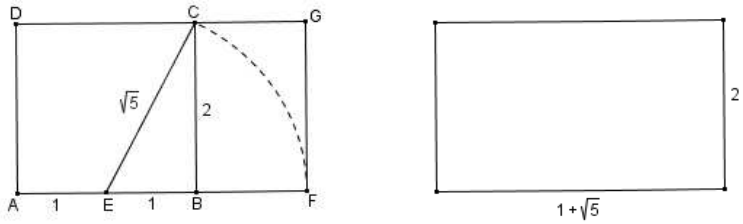
La trascendencia de π surge del antiguo problema de la cuadratura del círculo. El problema consistía en construir un cuadrado de área igual a un círculo dado utilizando regla y compás. Este antiguo problema griego no tiene solución.

El número de oro

Se dice que dos números enteros positivos *a* y *b* están en **razón áurea** si y sólo si $\frac{a+b}{a} = \frac{a}{b} = \Phi$.

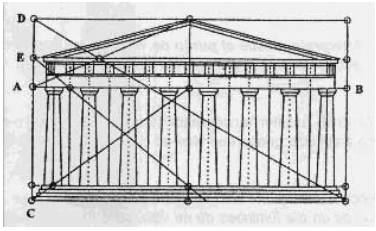
En particular, para $b = 1$ resolver $\frac{a+1}{a} = \frac{a}{1}$, es equivalente a resolver la ecuación $a^2 - a - 1 = 0$, siendo el número irracional $\Phi = \frac{1+\sqrt{5}}{2}$ su solución positiva conocida como **número de oro**. Por otro lado es oportuno observar que, por ser solución de una ecuación a coeficientes enteros, resulta que Φ es **algebraico**.

Rectángulo áureo: El rectángulo de la figura es áureo pues sus lados $\overline{AF}$ y $\overline{FG}$ están en la proporción del número áureo.



Su propiedad elemental es que si al rectángulo dado se le quita el cuadrado ABCD se obtiene otro rectángulo **semejante** al primero, en nuestro dibujo será el rectángulo BFGC semejante al rectángulo AFGD.

Φ es la llamada **razón áurea**; número de oro o número de Fidias, llamado también así, dado que fue él quien lo empleó para diseñar **El Partenón.**

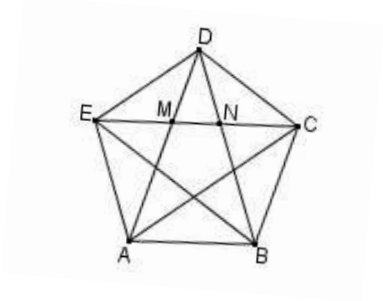


Hacia el 530 a.C, Pitágoras (582 a.C - 500 a.C.), filósofo y matemático griego, se instaló en Crotona, una colonia griega al sur de Italia, donde fundó un movimiento con propósitos religiosos, políticos y filosóficos, conocido como pitagorismo. Entre las amplias investigaciones matemáticas realizadas por los pitagóricos se encuentran sus estudios de los números pares e impares, de los números primos y de los cuadrados, esenciales en la teoría de números. Desde este punto de vista aritmético, cultivaron el concepto de número, que llegó a ser para ellos el principio crucial de toda proporción, orden y armonía en el universo.

La estrella pentagonal o pentágono estrellado era el símbolo de los seguidores de Pitágoras. Los pitagóricos pensaban que el mundo estaba configurado según un orden numérico, donde sólo tenían cabida los números fraccionarios, sin embargo, la casualidad hizo que en su propio símbolo se encontrara un número irracional: **el número de oro.**

Por ejemplo, la relación entre la diagonal del pentágono y su lado es el número de oro: $\frac{\overline{AC}}{\overline{AB}} = \frac{1+\sqrt{5}}{2}$

También podemos comprobar que los segmentos EM, MC y EC están en proporción áurea y que el pentágono que se forma en el cruce de las diagonales es proporcional al original.



Representación decimal de un número real

Dado un punto en la recta, $x > 0$, buscaremos una representación para ese número (con los 10 símbolos con que contamos), que caracterice totalmente a x.
Como x es un número bien determinado en la semirrecta real positiva, existe un único $n \in \mathbb{N}_0$, tal que $n \le x < n+1$; a ese n lo llamamos *la parte entera de x* :

$[x] = n$; $x - [x] = (x)$ es lo que llamamos *parte decimal de x* y verifica que $0 \le (x) < 1$

Ejercicio: Si $x = k + y = h + z$ con $k, h \in \mathbb{Z}$, $0 \le y < 1$, $0 \le z < 1$ entonces $k = h \wedge y = z$

Así $x = [x] + (x)$ en forma unívoca, con $[x] \in \mathbb{N}_0 \wedge (x) \in [0,1)$

Para $[x] = n$ ya hemos encontrado una representación decimal (en cualquier base s) , así que ahora buscaremos una representación decimal para los x , $0 < x < 1$

Sea entonces $x \in \mathbb{R}$, $0 < x < 1$

Podemos partir el intervalo [0, 1) en diez subintervalos iguales:

$$[0,1) = \bigcup_{i=0}^{9} \left[\frac{i}{10}, \frac{i+1}{10} \right)$$

Como $x \in [0, 1)$, los subintervalos son disjuntos dos a dos y cubren a todo el intervalo original, existe un único $a_{-1} \in \mathbb{N}_0$, $0 \le a_{-1} \le 9$, tal que

$$x \in \left[\frac{a_{-1}}{10}, \frac{a_{-1}+1}{10} \right)$$

Volvemos a partir este intervalo en 10 subintervalos de igual longitud, que, a su vez, es una centésima de la longitud del intervalo original:

$$\left[\frac{a_{-1}}{10}, \frac{a_{-1}+1}{10} \right) = \bigcup_{i=0}^{9} \left[\frac{a_{-1}}{10} + \frac{i}{10^2}, \frac{a_{-1}}{10} + \frac{i+1}{10^2} \right)$$

Nuevamente, ésta es una partición del intervalo $\left[\frac{a_{-1}}{10}, \frac{a_{-1}+1}{10} \right)$

por lo tanto existe un único a_{-2}, con $0 \le a_{-2} \le 9$, tal que $x \in \left[\frac{a_{-1}}{10} + \frac{a_{-2}}{10^2}, \frac{a_{-1}}{10} + \frac{a_{-2}+1}{10^2} \right)$

continuando con la partición sucesivamente, obtenemos una sucesión $a_{-1}, a_{-2}, ..., a_{-k} \in \mathbb{N}_0$ con $0 \le a_{-i} \le 9$ tal que $x \in \left[\frac{a_{-1}}{10} + \frac{a_{-2}}{10^2} + ... + \frac{a_{-k}}{10^k}, \frac{a_{-1}}{10} + \frac{a_{-2}}{10^2} + ... + \frac{a_{-k}+1}{10^k} \right)$

Si para algún k ocurriera que $x = \frac{a_{-1}}{10} + \frac{a_{-2}}{10^2} + ... + \frac{a_{-k}}{10^k}$

ya encontramos la expresión decimal exacta de x y escribiremos $x = 0, a_{-1}a_{-2}....a_{-k}$.

Si esto no ocurriera para ningún k, continuando con las particiones de intervalos, obtenemos dos sucesiones:

$$b_k = \frac{a_{-1}}{10} + \frac{a_{-2}}{10^2} + ... + \frac{a_{-k}}{10^k}$$

$$c_k = \frac{a_{-1}}{10} + \frac{a_{-2}}{10^2} + ... + \frac{a_{-k}+1}{10^k}$$

donde $b_k < x < c_k \quad \forall\, k \in \mathbb{N}$

$(b_k)_{k\in\mathbb{N}}$ es monótona creciente, pues $b_k \le b_{k+1} \ \forall\, k \in \mathbb{N}$

y $(c_k)_{k\in\mathbb{N}}$ es monótona decreciente, pues $c_k > c_{k+1} \quad \forall\, k \in \mathbb{N}$

y ambas están acotadas, $(b_k)_{k\in\mathbb{N}}$ superiormente por x, y $(c_k)_{k\in\mathbb{N}}$ inferiormente también por x.

Además $0 \le x - b_k < \frac{1}{10^k}$ y $0 < c_k - x \le \frac{1}{10^k} \ \forall\, k \in \mathbb{N}$

Luego $x = sup\,\{ b_k : k \in \mathbb{N} \} = ínf\,\{ c_k : k \in \mathbb{N} \}$.

Como $(b_k)_{k\in\mathbb{N}}$ y $(c_k)_{k\in\mathbb{N}}$ son sucesiones monótonas y acotadas, tienen límite, y ese límite es obviamente x.

b_k se denomina la aproximación a x por defecto con un error menor que $\frac{1}{10^k}$, y

c_k la aproximación a x por exceso con un error no mayor que $\frac{1}{10^k}$.

Tanto b_k como c_k son números racionales, pero x podría no serlo.

Representaremos a x como:

$$x = 0, a_{-1}a_{-2}....a_{-k}....$$

y diremos que ésta es su *representación decimal*.

Nótese que

$$x = \frac{a_{-1}}{10} + \frac{a_{-2}}{10^2} + \frac{a_{-3}}{10^3} + ... + \frac{a_{-k}}{10^k} + ... = a_{-1}10^{-1} + a_{-2}10^{-2} + a_{-3}10^{-3} + ... + a_{-k}10^{-k} + ...$$

La serie $\sum_{k\in\mathbb{N}} a_{-k}10^{-k}$ es una serie convergente, porque la sucesión de sus sumas parciales $(b_k)_{k\in\mathbb{N}}$, es convergente, y converge a x, luego podemos decir que $x = \sum_{k\in\mathbb{N}} a_{-k}10^{-k}$

Hay números cuya representación decimal es "finita" y otros, sin ser finita, está bien determinada pues conocemos exactamente cuáles serán todas sus cifras decimales. Estos números son los que tienen representación decimal "periódica".

Por ejemplo:

$$\frac{1}{4} = 0,25 \qquad \frac{1}{8} = 0,125 \qquad \frac{1}{5} = 0,2$$
$$\frac{1}{25} = 0,04 \qquad \frac{1}{10} = 0,1 \qquad \frac{3}{50} = \frac{6}{100} = 0,06$$

tienen representación *decimal finita*,

en cambio, son *periódicas* las representaciones decimales de:

$$\frac{1}{6} = 0,1666...66.. \qquad \frac{1}{3} = 0,3333...33..$$
$$\frac{1}{11} = 0,090909...09... \qquad \frac{3}{7} = 0,428571428571....428571...$$

donde los puntos suspensivos indican que ese número, o grupo de números, se repetirá indefinidamente en el mismo orden. A ese grupo de números es lo que llamamos *período*.

Definición: Decimos que un número x, $0 < x < 1$, tiene *representación decimal periódica* si

$$x = 0, a_{-1}a_{-2}....a_{-k}a_{-(k+1)}....a_{-(k+h)}...$$

donde $\exists\ k, h \in \mathbb{N}$ tales que

$$a_{-(k+1)} = a_{-(k+h+1)} = a_{-(k+2h+1)} = ... = a_{-(k+nh+1)} = ...$$
$$a_{-(k+2)} = a_{-(k+h+2)} = a_{-(k+2h+2)} = ... = a_{-(k+nh+2)} = ...$$
$$.....$$
$$a_{-(k+h)} = a_{-(k+2h)} = a_{-(k+3h)} = ... = a_{-(k+(n+1)h)} = ...$$

La sucesión $a_{-(k+1)}a_{-(k+2)}a_{-(k+3)}....a_{-(k+h)}$ se denomina el *período de x* y *h* es la *longitud del período*.

Notación: $x = 0, a_{-1}a_{-2}a_{-3}...a_{-k}\overline{a_{-k+1}a_{-(k+2)}a_{-(k+3)}...a_{-(k+h)}}$

Todo número decimal finito, se puede considerar un decimal periódico, con período cero, (o sea $h = 1$, y $a_{-(k+1)} = 0$).

La sucesión $a_{-1}a_{-2}...a_{-k}$ se denomina "*la parte decimal no periódica de x*"; esta parte podría no existir, en cuyo caso se dice que el número es *periódico puro*.

Un número periódico puro tiene representación decimal: $x = 0,\overline{a_1a_2a_3.....a_k}$

Como vimos al comienzo, todo número real positivo se escribe de manera única como

$x = [\,x\,] + (\,x\,)$, con $[\,x\,] \in \mathbb{N}_0 \ \wedge \ (\,x\,) \in [\,0,1\,)$

Por ser $[\,x\,] \in \mathbb{N}_0 \ \exists!\, n \in \mathbb{N}_0 \ \wedge \ a_0, a_1, ..., a_n \in \mathbb{N}_0 \ con \ 0 \le a_i \le 9 \ \ \forall i = 0,1,2,...,n \,,\ a_n \neq 0$

tales que $[\,x\,] = \sum_{i=0}^{n} a_i 10^i$

Como $(\,x\,) \in [\,0,1\,)$, por lo que vimos antes, existe una única sucesión $(a_{-k})_{k\in\mathbb{N}}$ y $0 \le a_{-i} \le 9 \ \forall i \in \mathbb{N}$ tal que $(\,x\,) = \sum_{k\in\mathbb{N}} a_{-k} 10^{-k}$.

***Definición*:** Para cualquier $x \in \mathbb{R}$, $x \ge 0$,
decimos que la sucesión $a_n a_{n-1} a_{n-2} ....a_1 a_0 a_{-1} a_{-2} ....a_{-k} .....$ es la *representación decimal de x* cuando $x = \sum_{i=0}^{n} a_i 10^i + \sum_{k\in\mathbb{N}} a_{-k} 10^{-k}$ con los $a_i \in \mathbb{N}_0 \ \ 0 \le a_i \le 9 \quad \forall i \in \mathbb{N}^- \cup \{\,0,1,2,....,n\}$.

***Definición*:** Un número $x \in \mathbb{R}$, $x \ge 0$, se dice *de representación decimal periódica*, si su parte decimal tiene representación decimal periódica.

Los desarrollos decimales de los números racionales se pueden caracterizar completamente, como lo demuestra el siguiente teorema:

Teorema: Todo número racional tiene una representación decimal periódica (pudiendo ser finita) y recíprocamente, todo número que admite una representación decimal periódica, es racional.

***Demostración*:**

Sea $x \in \mathbb{Q}$, $x > 0$, $\exists\ m, n \in \mathbb{N}$, tales que $x = \frac{m}{n}$, $(\,m\,,\,n\,) = 1$

Por el Algoritmo de la División de Euclides, tenemos que $m = cn + r,\ c, r \in \mathbb{Z} \quad 0 \le r < n$

- Si $r = 0$ entonces $\frac{m}{n} = c \in \mathbb{N}$

Por lo tanto $\exists!\, n \in \mathbb{N}_0 \ \wedge \ a_0, a_1, ..., a_n \in \mathbb{N}_0 \quad con \ \ 0 \le a_i \le 9 \quad \forall i = 0,1,2,...,n \,,\ a_n \neq 0$

tales que $\frac{m}{n} = \sum_{i=0}^{n} a_i 10^i$

- Si $r > 0$ $\qquad \frac{m}{n} = c + \frac{r}{n}$ $\qquad , r < n$

por el Algoritmo de la División, se tiene $10\,r = a_{-1}\,n + r_1 \qquad 0 \le r_1 < n\,,\ a_{-1} \in \mathbb{Z}$

entonces $\dfrac{m}{n} = c + \dfrac{r}{n} = c + \dfrac{10r}{10n} = c + \dfrac{a_{-1}}{10} + \dfrac{r_1}{10n}$

Debemos ver que $0 \le a_{-1} \le 9$:

a) Veamos que $0 \le a_{-1}$.

Como $r, n \in \mathbb{N}$, entonces $10r\,, n \in \mathbb{N}$

- si $10r > n \Rightarrow r_1 < n < 10r$

luego $10\,r - r_1 \in \mathbb{N}$ y $10\,r - r_1 = a_{-1}\,n$

por lo tanto $n \mid (10r - r_1)$, como $(10r - r_1) \in \mathbb{N} \ \wedge \ n \in \mathbb{N}$, entonces $a_{-1} \in \mathbb{N}$.

- si $10\,r = n$ entonces $10r = 1.n + 0$ por lo tanto $a_{-1} = 1$.
- si $10\,r < n$, $10\,r = 0\,.\,n + r_1$ con $0 < r_1 = 10r < n$ y $a_{-1} = 0$.

Luego $a_{-1} \ge 0$.

b) Veamos que $a_{-1} \le 9$.

Como $0 < r < n$, $0 < 10\,r < 10\,n$ entonces $0 < \dfrac{10r}{n} < 10$

$10\,r = a_{-1}\,n + r_1$ por lo tanto $\dfrac{10r}{n} = a_{-1} + \dfrac{r_1}{n}$

como $0 \le r_1 < n$ entonces $0 \le \dfrac{r_1}{n} < 1$.

Así $a_{-1} = \dfrac{10r}{n} - \dfrac{r_1}{n} < \dfrac{10r}{n} < 10$ y como $a_{-1} \in \mathbb{Z}$, entonces $a_{-1} \le 9$.

Volvamos a la expresión anterior: $\dfrac{m}{n} = c + \dfrac{r}{n} = c + \dfrac{10r}{10n} = c + \dfrac{a_{-1}}{10} + \dfrac{r_1}{10n}$

Si $r_1 = 0$ $\dfrac{m}{n} = c + \dfrac{a_{-1}}{10} = c, a_{-1}$ y $\dfrac{m}{n}$ tiene una representación decimal finita.

Si $r_1 > 0 \qquad 10\,r_1 = a_{-2}\,n + r_2 \qquad , 0 \le r_2 < n \qquad , 0 \le a_{-2} \le 9$ (por el mismo razonamiento anterior).

$$\frac{m}{n} = c + \frac{a_{-1}}{10} + \frac{r_1}{10n} = c + \frac{a_{-1}}{10} + \frac{10r_1}{10^2 n} = c + \frac{a_{-1}}{10} + \frac{a_{-2}}{10^2} + \frac{r_2}{10^2 n}$$

Si $r_2 = 0$ $\quad \frac{m}{n} = c + \frac{a_{-1}}{10} + \frac{a_{-2}}{10^2} = c, a_{-1}a_{-2}$ que es una representación decimal finita.

Si $r_2 > 0$ $\quad 10\, r_2 = a_{-3}\, n + r_3 \qquad 0 \le r_3 < n, \quad 0 \le a_{-3} \le 9$

$$\frac{m}{n} = c + \frac{a_{-1}}{10} + \frac{a_{-2}}{10^2} + \frac{10 r_2}{10^3 n} = c + \frac{a_{-1}}{10} + \frac{a_{-2}}{10^2} + \frac{a_{-3}}{10^3} + \frac{r_3}{10^3 n}$$

y así sucesivamente,

$m = c\, n + r$	$0 \le r < n$	
$10r = a_{-1}\, n + r_1$	$0 \le r_1 < n$	$0 \le a_{-1} \le 9$
$10\, r_1 = a_{-2}\, n + r_2$	$0 \le r_2 < n$	$0 \le a_{-2} \le 9$
$10\, r_2 = a_{-3}\, n + r_3$	$0 \le r_3 < n$	$0 \le a_{-3} \le 9$
.....		
$10\, r_{k-1} = a_{-k}\, n + r_k$	$0 \le r_k < n$	$0 \le a_{-k} \le 9$
$10\, r_k = a_{-(k+1)}\, n + r_{k+1}$	$0 \le r_{k+1} < n$	$0 \le a_{-(k+1))} \le 9$

Si $\exists\, h \in \mathbb{N}$ tal que $\quad 10\, r_{h-1} = a_{-h}\, n + r_h \quad$ con $\quad r_h = 0\,, \quad 0 \le a_{-h} \le 9,$

obtenemos que $\frac{m}{n}$ tiene una representación decimal finita : $\frac{m}{n} = c, a_{-1}a_{-2}...a_{-h}$

Si $\forall\, h \in \mathbb{N}$, $r_h \neq 0$, como los $r_i \in \mathbb{N}$ y $r_i < n$, a lo sumo después de $n - 1$ divisiones obtenemos un resto igual a alguno de los anteriores, o sea $\exists\, k, h \in \mathbb{N}$ tales que $r_k = r_{k+h}$.

$$10\, r_k = a_{-(k+1)}\, n + r_{k+1}$$

$$10\, r_{k+h} = a_{-(k+h+1)}\, n + r_{k+h+1}$$

Entonces $10\, r_k = 10\, r_{k+h}$, puesto que el Algoritmo de la División asegura la unicidad del cociente y del resto en la división de un número por otro,

resulta $\quad a_{-(k+1)} = a_{-(k+h+1)} \quad$ y $\quad r_{k+1} = r_{k+h+1}$

Luego $10\, r_{k+1} = 10\, r_{k+h+1}$

$$10\, r_{k+1} = a_{-(k+2))} n + r_{k+2}$$

$$10\, r_{k+h+1} = a_{-(k+h+2)}\, n + r_{k+h+2}$$

luego $\qquad a_{-(k+2)} = a_{-(k+h+2)} \quad$ y $\quad r_{k+2} = r_{k+h+2}$

así $\qquad 10\, r_{k+2} = 10\, r_{k+h+2}$

de lo que obtenemos $\qquad a_{-(k+3)} = a_{-(k+h+3)}$ y $r_{k+3} = r_{k+h+3}$

y así sucesivamente.

Las sucesivas divisiones nos dan:

$m = cn + r$
$10r = a_{-1}n + r_1$
$10r_1 = a_{-2}n + r_2$
.....
$10r_{k-1} = a_{-k}n + r_k$
$10r_k = a_{-(k+1)}n + r_{k+1}$
$10r_{k+1} = a_{-(k+2)}n + r_{k+2}$
.....
$10r_{k+h-1} = a_{-(k+h)}n + r_{k+h}$, $r_{k+h} = r_k$
$10r_{k+h} = a_{-(k+h+1)}n + r_{k+h+1} \Leftrightarrow 10r_k = a_{-(k+1)}n + r_{k+1}$
$10r_{k+h+1} = a_{-(k+h+2)})n + r_{k+h+2} \Leftrightarrow 10r_{k+1} = a_{-(k+2)}n + r_{k+2}$
.....
$10r_{k+2h-1} = a_{-(k+2h)}n + r_{k+2h} \Leftrightarrow 10r_{k+h-1} = a_{-(k+h)}n + r_{k+h}$,
$r_{k+2h} = r_{k+h} = r_k$
$10r_{k+2h} = a_{-(k+2h+1)}n + r_{k+2h+1} \Leftrightarrow 10r_k = a_{-(k+1)}n + r_{k+1}$
.....

y así se repite indefinidamente, quedando:

$a_{-(k+1)} = a_{-(k+h+1)} = a_{-(k+2h+1)} = ... = a_{-(k+ih+1)} = \ldots.$
$a_{-(k+2)} = a_{-(k+h+2)} = a_{-(k+2h+2)} = ... = a_{-(k+ih+2)} = \ldots.$
.....
$a_{-(k+h-1)} = a_{-(k+2h-1)} = a_{-(k+3h-1)} = ... = a_{-(k+(i+1)h-1)} = \ldots.$
$a_{-(k+h)} = a_{-(k+2h)} = a_{-(k+3h)} = ... = a_{-(k+(i+1)h)} = \ldots.$

luego $a_{-(k+1)}$ ..... $a_{-(k+h)}$ $a_{-(k+h-1)}$ es el período en la representación decimal de $\frac{m}{n}$ y así,

$$\frac{m}{n} = c, a_{-1}...a_{-k}\overline{a_{-(k+1)}...a_{-(k+h)}}$$

Recíprocamente, si x admite una representación decimal periódica, tenemos:

1. Si es decimal finita

$x = a_h a_{h-1}....a_1 a_0, a_{-1}a_{-2}....a_{-k}$, $0 \le a_i \le 9$, $i = -k, -(k-1)..-1,0,1,2,...,h$

$x = a_h 10^h + a_{h-1}10^{h-1} + ...+ a_1 10 + a_0 + a_{-1}10^{-1}a_{-2}10^{-2} + ...+ a_{-k}10^{-k}$

$10^k x = a_h 10^{h+k} + a_{h-1}10^{h+k-1} + ...+ a_1 10^{k+1} + a_0 10^k + a_{-1}10^{k-1}a_{-2}10^{k-2} + ...+ a_{-(k-1)}10 + a_{-k}$

luego $10^k x = m \in \mathbb{N}$

entonces $x = \frac{m}{10^k} \in \mathbb{Q}$

2. Si x es decimal periódico, no finito; consideremos primero a x periódico puro

$$x = 0, \overline{a_{-1}a_{-2}...a_{-k}}$$

$$x = a_{-1}10^{-1} + a_{-2}10^{-2} + ... + a_{-(k-1)}10^{-(k-1)} + a_{-k}10^{-k} + a_{-1}10^{-(k+1)} + a_{-2}10^{-(k+2)} + ... +$$
$$+ a_{-k}10^{-2k} + ... + a_{-1}10^{-(2k+1)} + ...$$

$$10^k x = a_{-1}10^{k-1} + a_{-2}10^{k-2} + ... + a_{-(k-1)}10^{-1} + a_{-k} + a_{-1}10^{-1} + a_{-2}10^{-2} + ... + a_{-k}10^{-k} + ... +$$
$$+ a_{-1}10^{-(k+1)} + a_{-2}10^{-(k+2)} + ...$$

En notación decimal, tenemos que:

$x = 0, a_{-1}a_{-2}.....a_{-k}a_{-1}a_{-2}....a_{-k}...$

$10^k x = a_{-1}a_{-2}.....a_{-k}, a_{-1}a_{-2}....a_{-k}a_{-1}a_{-2}...a_{-k}a_{-1}...$

luego $10^k x - x = a_{-1}a_{-2}.....a_{-k} = a_{-1}10^{k-1} + a_{-2}10^{k-2} + ... + a_{-(k-1)}10 + a_{-k} \in \mathbb{N}$

entonces $(10^k - 1)\, x = m \in \mathbb{N}$

así $x = \dfrac{m}{10^k - 1} = \dfrac{m}{\underbrace{99...9}_{k \ veces}} \in \mathbb{Q}$

3. Si x es cualquier número decimal periódico

$x = n, a_{-1}....a_{-k}\,\overline{a_{-(k+1)}....a_{-(k+h)}}$ $\qquad n = [\,x\,] \in \mathbb{N}_0$ ([x] parte entera de x)

$x = n,\ a_{-1}....a_{-k} + 0, \underbrace{0....0}_{k \ veces}\,\overline{a_{-(k+1)}....a_{-(k+h)}}$

$n,\ a_{-1}....a_{-k} \in \mathbb{Q}$ porque es un número decimal finito (por lo visto en 1).

Sea $x' = 0, \underbrace{0....0}_{k \ veces}\,\overline{a_{-(k+1)}....a_{-(k+h)}}$

$10^k x' = 0, \overline{a_{-(k+1)}....a_{-(k+h)}}$, luego $10^k x'$ es decimal periódico puro; por lo visto en (2) tenemos que $10^k x' \in \mathbb{Q} \Rightarrow x' \in \mathbb{Q}$

Así x es suma de dos números racionales, luego es un número racional.
Escribamos a x como cociente de números naturales. Para ello, reemplazamos según lo visto anteriormente:

$$n, a_{-1}a_{-2}...a_{-k} = n + \frac{a_{-1}a_{-2}.....a_{-k}}{10^k}$$

por lo tanto $\qquad x = n + \dfrac{a_{-1}a_{-2}...a_{-k}}{10^k} + x'$

con $\qquad x' = \dfrac{0, \overline{a_{-(k+1)}...a_{-(k+h)}}}{10^k} = \dfrac{a_{-(k+1)}...a_{-(k+h)}}{10^k(10^h - 1)}$

Así queda demostrado que los números racionales se caracterizan por ser aquéllos cuya representación decimal es periódica.

Observación: Nótese que las "*cifras decimales*" de un determinado número *x* están dadas por los términos de la sucesión $(b_k)_{k\in\mathbb{N}}$ y $b_k \le x \qquad \forall\, k \in \mathbb{N}$.

Como $b_k = [x] + \frac{a_{-1}}{10} + \frac{a_{-2}}{10^2} + ... + \frac{a_{-k}}{10^k}$ con $0 \le a_{-i} \le 9 \quad \forall\, i \in \mathbb{N}$;
no puede ocurrir que $\exists\ n_0 \in \mathbb{N}$ tal que $a_{-n} = 9\ \forall\ n \ge n_0$, pues si esto ocurriera,

$$c_{n_0} = [x] + \frac{a_{-1}}{10} + \frac{a_{-2}}{10^2} + ... + \frac{a_{-(n_0-1)}}{10^{n_0-1}} + \frac{a_{-n_0}+1}{10^{n_0}}$$

como $a_{-n_0} = 9 \quad \Rightarrow \quad \frac{a_{-n_0}+1}{10^{n_0}} = \frac{1}{10^{n_0-1}}$

$$c_{n_0} = [x] + \frac{a_{-1}}{10} + \frac{a_{-2}}{10^2} + ... + \frac{a_{-(n_0-1)}}{10^{n_0-1}} + \frac{1}{10^{n_0-1}} = [x] + \frac{a_{-1}}{10} + \frac{a_{-2}}{10^2} + ... + \frac{a_{-(n_0-1)}+1}{10^{n_0-1}}$$

$$c_{n_0+1} = [x] + \frac{a_{-1}}{10} + \frac{a_{-2}}{10^2} + ... + \frac{a_{-(n_0-1)}}{10^{n_0-1}} + \frac{a_{-n_0}}{10^{n_0}} + \frac{a_{-(n_0+1)}+1}{10^{n_0+1}}$$

como $a_{-(n_0+1)} = 9 \Rightarrow \frac{a_{-(n_0+1)}+1}{10^{n_0+1}} = \frac{9+1}{10^{n_0+1}} = \frac{1}{10^{n_0}}$

$$\frac{a_{-n_0}}{10^{n_0}} + \frac{a_{-(n_0+1)}+1}{10^{n_0+1}} = \frac{9}{10^{n_0}} + \frac{1}{10^{n_0}} = \frac{1}{10^{n_0-1}}$$

así $c_{n_0+1} = [x] + \frac{a_{-1}}{10} + \frac{a_{-2}}{10^2} + ... + \frac{a_{-(n_0-1)}}{10^{n_0-1}} + \frac{1}{10^{n_0-1}} = c_{n_0}$

Razonando por inducción, podemos demostrar que $c_n = c_{n_0} \qquad \forall\ n \ge n_0$
Entonces $\lim_{n\to\infty} c_n = c_{n_0}$

pero $\lim_{n\to\infty} c_n = x \quad \Rightarrow \quad x = c_{n_0}$

pero $x < c_n\ \forall\ n \in \mathbb{N}$, lo que genera una contradicción; por lo tanto, ningún número puede ser periódico, con período 9.

Si las cifras decimales las definiéramos a través de la sucesión $(c_k)_{k\in\mathbb{N}}$, obtendríamos que los números podrían tener período 9, pero nunca serían decimales exactos, o sea, con período 0. Obviamente, esto depende de la definición que se haga de las cifras decimales de un determinado número, pero claramente la ventaja de obtener un período 9 es despreciable ante la de poder expresar un número con cifras decimales exactas.

Ahora veamos:

¿Cuáles son los números racionales de la forma $\frac{m}{n}$, con (m , n) = 1, que admiten representación decimal finita?

Si $\frac{m}{n}$ admite representación decimal finita, $\exists k \in \mathbb{N}$ tal que

$$\frac{m}{n} = c + \frac{a_{-1}}{10} + \frac{a_{-2}}{10^2} + \ldots + \frac{a_{-k}}{10^k} \qquad c \in \mathbb{N}_0$$

Luego $10^k \cdot \frac{m}{n} \in \mathbb{N}$, entonces $n \mid 10^k$, pues $(n, m) = 1$

Así $n = 2^t 5^s$ para ciertos $t, s \in \mathbb{N}_0$

Veamos que la condición es suficiente:

Si $n = 2^t 5^s$ $t, s \in \mathbb{N}_0$, y $h = máx\ \{t, s\}$,

Sea la representación decimal de $\frac{m}{n}$, con $(n, m) = 1$,

$$\frac{m}{n} = c + \frac{a_{-1}}{10} + \frac{a_{-2}}{10^2} + \ldots + \frac{a_{-(h-1)}}{10^{h-1}} + \frac{a_{-h}}{10^h} + \frac{a_{-(h+1)}}{10^{h+1}} + \ldots + \frac{a_{-k}}{10^k} + \ldots . \ , c \in \mathbb{N}_0$$

como $n \mid 10^h$ entonces $10^h \cdot \frac{m}{n} \in \mathbb{N}$

$$10^h \frac{m}{n} = c10^h + a_{-1}10^{h-1} + a_{-2}10^{h-2} + \ldots . + a_{-(h-1)}10 + a_{-h} + \frac{a_{-(h+1)}}{10} + \frac{a_{-(h+2)}}{10^2} + \ldots + \frac{a_{-k}}{10^{k-h}} + \ldots$$

Como $10^h \frac{m}{n} \in \mathbb{N}$ y $0 \le \frac{a_{-(h+1)}}{10} + \frac{a_{-(h+2)}}{10^2} + \ldots + \frac{a_{-k}}{10^{k-h}} + \ldots + \ldots < 1$

entonces $\frac{a_{-(h+1)}}{10} + \frac{a_{-(h+2)}}{10^2} + \ldots + \frac{a_{-k}}{10^{k-h}} + \ldots . = 0$

y así $a_{-k} = 0 \qquad \forall\ k \ge h + 1$

luego $\frac{m}{n} = c + \frac{a_{-1}}{10} + \ldots + \frac{a_{-h}}{10^h}$

Conclusión: un número racional $\frac{m}{n}$, $m, n \in \mathbb{N}$, $(n, m) = 1$ admite representación decimal finita sii $n = 2^t 5^s$, con $t, s \in \mathbb{N}_0$.

Ejemplos:

1. Encontrar la representación decimal de $\frac{3}{16}$

$$3 = 0.16 + 3$$
$$30 = 1.16 + 14$$
$$140 = 8.16 + 12$$
$$120 = 7.16 + 8$$
$$80 = 5.16 + 0$$

Luego obtenemos que $\frac{3}{16} = 0{,}1875$ (representación decimal finita).

$$\frac{3}{16} = \frac{30}{16.10} = \frac{1.16+14}{16.10} = \frac{1}{10} + \frac{14}{16.10} = \frac{1}{10} + \frac{140}{16.10^2} = \frac{1}{10} + \frac{8.16+12}{16.10^2} =$$

$$= \frac{1}{10} + \frac{8}{10^2} + \frac{12}{16.10^2} = \frac{1}{10} + \frac{8}{10^2} + \frac{120}{16.10^3} = \frac{1}{10} + \frac{8}{10^2} + \frac{7.16+8}{16.10^3} =$$

$$= \frac{1}{10} + \frac{8}{10^2} + \frac{7}{10^3} + \frac{8}{16.10^3} = \frac{1}{10} + \frac{8}{10^2} + \frac{7}{10^3} + \frac{80}{16.10^4} = \frac{1}{10} + \frac{8}{10^2} + \frac{7}{10^3} + \frac{5.16+0}{16.10^4} =$$

$$= \frac{1}{10} + \frac{8}{10^2} + \frac{7}{10^3} + \frac{5}{10^4}$$

Obsérvese que este proceso es el que realizamos mediante el algoritmo de la división que utilizamos:

30	16
140	0,1875
120	
80	
0	

2. Encontrar la representación decimal de $x = \frac{5}{7}$

$5 = 0.7 + \mathbf{5}$
$50 = 7.7 + 1$
$10 = 1.7 + 3$
$30 = 4.7 + 2$
$20 = 2.7 + 6$
$60 = 8.7 + 4$
$40 = 5.7 + \mathbf{5}$

$$x = \frac{5}{7} = \frac{50}{7.10} = \frac{7.7+1}{7.10} = \frac{7}{10} + \frac{1}{7.10} = \frac{7}{10} + \frac{10}{7.10^2} = \frac{7}{10} + \frac{1.7+3}{7.10^2} = \frac{7}{10} + \frac{1}{10^2} + \frac{3}{7.10^2} =$$
$$= \frac{7}{10} + \frac{1}{10^2} + \frac{30}{7.10^3} = \frac{7}{10} + \frac{1}{10^2} + \frac{4.7+2}{7.10^3} = \frac{7}{10} + \frac{1}{10^2} + \frac{4}{10^3} + \frac{2}{7.10^3} =$$
$$= \frac{7}{10} + \frac{1}{10^2} + \frac{4}{10^3} + \frac{20}{7.10^4} = \frac{7}{10} + \frac{1}{10^2} + \frac{4}{10^3} + \frac{2.7+6}{7.10^4} = \frac{7}{10} + \frac{1}{10^2} + \frac{4}{10^3} + \frac{2}{10^4} + \frac{6}{7.10^4} =$$
$$= \frac{7}{10} + \frac{1}{10^2} + \frac{4}{10^3} + \frac{2}{10^4} + \frac{60}{7.10^5} = \frac{7}{10} + \frac{1}{10^2} + \frac{4}{10^3} + \frac{2}{10^4} + \frac{8.7+4}{7.10^5} =$$
$$= \frac{7}{10} + \frac{1}{10^2} + \frac{4}{10^3} + \frac{2}{10^4} + \frac{60}{7.10^5} = \frac{7}{10} + \frac{1}{10^2} + \frac{4}{10^3} + \frac{2}{10^4} + \frac{8.7+4}{7.10^5} =$$

$$= \frac{7}{10} + \frac{1}{10^2} + \frac{4}{10^3} + \frac{2}{10^4} + \frac{8}{10^5} + \frac{4}{7.10^5} = \frac{7}{10} + \frac{1}{10^2} + \frac{4}{10^3} + \frac{2}{10^4} + \frac{8}{10^5} + \frac{40}{7.10^6} =$$
$$= \frac{7}{10} + \frac{1}{10^2} + \frac{4}{10^3} + \frac{2}{10^4} + \frac{8}{10^5} + \frac{5.7+5}{7.10^6} = \frac{7}{10} + \frac{1}{10^2} + \frac{4}{10^3} + \frac{2}{10^4} + \frac{8}{10^5} + \frac{5}{10^6} + \frac{5}{7.10^6} =$$
$$= \frac{7}{10} + \frac{1}{10^2} + \frac{4}{10^3} + \frac{2}{10^4} + \frac{8}{10^5} + \frac{5}{10^6} + \frac{50}{7.10^6} = ...$$

50	7
10	0,714285
30	
20	
60	
40	
5	

Luego la representación decimal es $\frac{5}{7} = 0,\overline{714285}$

3. Encontrar la representación decimal de $x = \sqrt{3}$ ·

Para determinar la representación decimal de $\sqrt{3}$ nos basaremos en la conocida propiedad de números reales: $x \geq 0$, $y \geq 0$, $x \leq y \Leftrightarrow x^2 \leq y^2$.

$1 < \sqrt{3} < 2 \Leftrightarrow 1 < 3 < 4$

Partimos el intervalo $(1, 2)$ en 10 subintervalos de longitud $\frac{1}{10}$; para saber en cuál se ubica $\sqrt{3}$ utilizamos la equivalencia mencionada:

$(1 + \frac{1}{10})^2 = \frac{121}{100} < 3$; $(1 + \frac{2}{10})^2 = \frac{144}{100} < 3$; $(1 + \frac{3}{10})^2 = \frac{169}{100} < 3$;

$(1 + \frac{4}{10})^2 = \frac{196}{100} < 3$; $(1 + \frac{5}{10})^2 = \frac{225}{100} < 3$; $(1 + \frac{6}{10})^2 = \frac{256}{100} < 3$;

$(1 + \frac{7}{10})^2 = \frac{289}{100} < 3$; $(1 + \frac{8}{10})^2 = \frac{324}{100} > 3$

por lo ya visto $1 + \frac{7}{10} < \sqrt{3} < 1 + \frac{8}{10} \Leftrightarrow (1 + \frac{7}{10})^2 < 3 < (1 + \frac{8}{10})^2$

con lo que $\sqrt{3} \in (1 + \frac{7}{10}, 1 + \frac{8}{10})$; subdividimos este intervalo en 10 subintervalos de longitud $\frac{1}{10}$ y queremos establecer en cuál de ellos se ubica.

$(1 + \frac{7}{10} + \frac{1}{10^2})^2 = \frac{29241}{10^4} < 3$; $(1 + \frac{7}{10} + \frac{2}{10^2})^2 = \frac{29584}{10^4} < 3$;

$(1 + \frac{7}{10} + \frac{3}{10^2})^2 = \frac{29929}{10^4} < 3$; $(1 + \frac{7}{10} + \frac{4}{10^2})^2 = \frac{30276}{10^4} > 3$

continuando con el proceso:

$$1+\frac{7}{10}+\frac{3}{10^2}<\sqrt{3}<1+\frac{7}{10}+\frac{4}{10^2} \Leftrightarrow (1+\frac{7}{10}+\frac{3}{10^2})^2<3<(1+\frac{7}{10}+\frac{4}{10^2})^2$$

$$(1+\frac{7}{10}+\frac{3}{10^2}+\frac{1}{10^3})^2=\frac{2996361}{10^6}<3 ; \qquad (1+\frac{7}{10}+\frac{3}{10^2}+\frac{2}{10^3})^2=\frac{2999824}{10^6}<3$$

$$(1+\frac{7}{10}+\frac{3}{10^2}+\frac{3}{10^3})^2=\frac{3003289}{10^6}>3$$

$$1+\frac{7}{10}+\frac{3}{10^2}+\frac{2}{10^3}<\sqrt{3}<1+\frac{7}{10}+\frac{3}{10^2}+\frac{3}{10^3}$$

$$\Leftrightarrow (1+\frac{7}{10}+\frac{3}{10^2}+\frac{2}{10^3})^2<3<(1+\frac{7}{10}+\frac{3}{10^2}+\frac{3}{10^3})^2$$

$$(1+\frac{7}{10}+\frac{3}{10^2}+\frac{2}{10^3}+\frac{1}{10^4})^2=\frac{300017041}{10^8}>3$$

luego $1+\frac{7}{10}+\frac{3}{10^2}+\frac{2}{10^3}<\sqrt{3}<1+\frac{7}{10}+\frac{3}{10^2}+\frac{2}{10^3}+\frac{1}{10^4}$

$$1+\frac{7}{10}+\frac{3}{10^2}+\frac{2}{10^3}+\frac{5}{10^5}<\sqrt{3}<1+\frac{7}{10}+\frac{3}{10^2}+\frac{2}{10^3}+\frac{6}{10^5}$$ pues

$$(\frac{173205}{10^5})^2=\frac{29999972025}{10^{10}}<3<\frac{30000318436}{10^{10}}=(\frac{173206}{10^5})^2$$

$\therefore$ la representación decimal con cinco decimales exactos es $\sqrt{3} \approx 1,73205$.

Generalización de la representación de un número real a una base s, $s \in \mathbb{N}$, s > 1

De la misma manera que nos planteamos esa pregunta cuando hablamos de números enteros, surge inmediatamente el interrogante de por qué representación decimal; qué pasaría si en vez de dividir cada intervalo entero en 10 partes iguales lo hiciéramos en tres, cinco o veinte. Aquí la respuesta es la misma que en el caso de números enteros, el número diez ocupa un lugar de privilegio por cuestiones culturales, porque históricamente se utilizaron 10 símbolos, no porque teóricamente tenga una propiedad especial, que lo distinga de otros números, e impida que se realice un razonamiento análogo con ellos.

Sea $s \in \mathbb{N}$, $s > 1$.
Para $x \in \mathbb{R}$, $x > 0$, existe un único $n \in \mathbb{N}_0 : n \le x < n+1$ donde $[x] = n$
Así $x = [x] + (x)$ en forma unívoca, con $[x] \in \mathbb{N}_0 \wedge (x) \in [0,1)$
Para $[x] = n$ ya hemos encontrado una representación en base s, así que ahora buscaremos una representación en base s para los x, $0 < x < 1$

Sea entonces $x \in \mathbb{R}$, $0 < x < 1$

Partimos el intervalo [0, 1) en *s* subintervalos de igual longitud.

$$[\,0,1\,)=\bigcup_{i=0}^{s-1}\left[\ \frac{i}{s}\ ,\ \frac{i+1}{s}\right)$$

Como ésta es una partición, existe un único $a_{-1}\in\mathbb{N}_0$, $\quad 0\le a_{-1}\le s-1$,

tal que $x\in\left[\ \frac{a_{-1}}{s},\ \frac{a_{-1}+1}{s}\right)$

Subdividimos este intervalo en *s* subintervalos de igual longitud.

$$\left[\ \frac{a_{-1}}{s},\ \frac{a_{-1}+1}{s}\right)=\ \bigcup_{i=0}^{s-1}\ \left[\ \frac{a_{-1}}{s}+\frac{i}{s^2}\ ,\ \frac{a_{-1}}{s}+\frac{(i+1)}{s^2}\right)$$

Nuevamente existe un único $a_{-2}\in\mathbb{N}_0$, $0\le a_{-2}\le s-1$

tal que $x\in\left[\ \frac{a_{-1}}{s}+\frac{a_{-2}}{s^2}\ ,\ \frac{a_{-1}}{s}+\frac{a_{-2}+1}{s^2}\right)$

y así sucesivamente; después de k pasos, obtenemos una sucesión finita a_{-1}, a_{-2},....., $a_{-k}\in\mathbb{N}_0$,

$0\le a_{-i}\le s-1$ tal que $\quad x\in\left[\ \frac{a_{-1}}{s}+\frac{a_{-2}}{s^2}+\ldots+\frac{a_{-k}}{s^k},\ \frac{a_{-1}}{s}+\frac{a_{-2}}{s^2}+\ldots+\frac{a_{-(k-1)}}{s^{k-1}}+\frac{a_{-k}+1}{s^k}\right)$

la sucesión $(b_k)_{k\in\mathbb{N}}$, $\qquad b_k=\frac{a_{-1}}{s}+\frac{a_{-2}}{s^2}+\ldots+\frac{a_{-k}}{s^k}$

es monótona creciente y $\qquad b_k\le x\qquad\forall\,k\in\mathbb{N}$

Además $0\le x-b_k<\frac{1}{s^k}$

La sucesión $(c_k)_{k\in\mathbb{N}}$ donde $\qquad c_k=\frac{a_{-1}}{s}+\frac{a_{-2}}{s^2}+\ldots+\frac{a_{-(k-1)}}{s^{k-1}}+\frac{a_{-k}+1}{s^k}$

es monótona decreciente y $\quad x<c_k\quad\forall\,k\in\mathbb{N}$

Además $\quad 0<c_k-x\le\frac{1}{s^k}$

Así que $x=\lim_{k\to\infty}b_k=\lim_{k\to\infty}c_k$

La representación en base *s* está dada por la sucesión $(b_k)_{k\in\mathbb{N}}$.

Se dice que $(x)_s=0,a_{-1}a_{-2}....a_{-k}...$ ($(x)_s$ se lee la *representación en base* ***s*** *de* ***x***).

Para cualquier $x\in\mathbb{R}$, $x>0$, teniendo que $[\,x\,]=a_hs^h+a_{h-1}s^{h-1}+....+a_1s+a_0$

obtenemos que $x=a_hs^h+a_{h-1}s^{h-1}+\ldots+a_1s+a_0+\frac{a_{-1}}{s}+\frac{a_{-2}}{s^2}+\ldots+\frac{a_{-k}}{s^k}+.....$

$0\le a_i<s,\ \forall\ i\le h$, $i\in\mathbb{Z}$

Nota: En base *s* se puede definir, como en base 10, los conceptos de representación *finita* y *periódica*.

Podemos enunciar un teorema similar a la caracterización dada para la representación decimal periódica, cuya demostración se realiza en forma completamente análoga a ella:

Teorema: Todo número racional tiene una representación en base *s* periódica (pudiendo ser finita) y recíprocamente, todo número que admite una representación en base *s* periódica, es racional.

Cuando queremos encontrar la representación en base *s* de un número racional $\frac{m}{n}$, procedemos en forma análoga a la realizada para la representación decimal.

$m = c\,n + r$	$0 \le r < n$
$s\,r = a_{-1}\,n + r_1$	$0 \le r_1 < n\ 0 \le a_{-1} < s$ (por un razonamiento
$s\,r_1 = a_{-2}\,n + r_2$	$0 \le r_2 < n\ 0 \le a_{-2} < s$ análogo al realizado en el
.....	desarrollo decimal)
$s\,r_{k-1} = a_{-k}\,n + r_k$	$0 \le r_k < n$

$$\frac{m}{n} = c + \frac{r}{n} = c + \frac{rs}{s \cdot n} = c + \frac{a_{-1}}{s} + \frac{r_1}{s \cdot n} = c + \frac{a_{-1}}{s} + \frac{r_1 s}{s^2 \cdot n} = c + \frac{a_{-1}}{s} + \frac{a_{-2}}{s^2} + \frac{r_2}{s^2 \cdot n} =$$
$$= c + \frac{a_{-1}}{s} + \frac{a_{-2}}{s^2} + \frac{r_2 \cdot s}{s^3 \cdot n} = c + \frac{a_{-1}}{s} + \frac{a_{-2}}{s^2} + \ldots + \frac{a_{-k}}{s^k} + \frac{r_k}{s^k \cdot n}$$

Nótese que los restos son números enteros comprendidos entre 0 y $n - 1$, por lo que, o bien alguno es cero, o en algún momento, deberá coincidir con alguno anterior, por lo que vemos que en base *s* también se caracterizan los números racionales por ser aquéllos que tienen representación en base *s*, finita o periódica. (La demostración de este teorema en base *s* es análoga a la realizada en base 10, reemplazando este número por *s* en cada uno de los pasos.)

Lo que obviamente variará para un número racional es que admita representación periódica o finita en una o en otra base.

Por ejemplo:

$$\left(\frac{1}{7}\right)_{10} = 0,\overline{142857} \qquad \left(\frac{1}{7}\right)_{7} = 0,1 \qquad \left(\frac{1}{7}\right)_{3} = 0,\overline{010212}$$

Entonces, ¿cuáles serán los números con representación finita en base *s*?

Si $s = p_1^{r_1}\ p_2^{r_2} \ldots p_k^{r_k}$ $\quad r_i \in \mathbb{N}$, $p_i \in \mathbb{N}$ primos

$\frac{m}{n}$ admite representación finita en base *s* sii $\exists\, h \in \mathbb{N}$ tal que $n \mid s^h$,

o sea, sii $n = p_1^{d_1}\ p_2^{d_2} \ldots p_k^{d_k}$ $\quad d_i \in \mathbb{N}_0$

La demostración la proponemos como ejercicio.

Aplicación: La no numerabilidad del conjunto de los números reales

Recordemos algunas definiciones dadas en el capítulo II:

> Sea $\mathcal{F}$ un conjunto de conjuntos (conjunto cuyos elementos son, a su vez, conjuntos). Vamos a definir en $\mathcal{F}$ una relación de equivalencia:
>
> $$A \approx B \Leftrightarrow \quad \exists\, f : A \to B \text{ función biyectiva}$$

Se lee: *A es coordinable con B si y sólo si existe una función biyectiva de A sobre B*, o sea si *A* y *B* tienen el mismo cardinal.

***Definición*:** Un conjunto *A* se dice *numerable* si es coordinable con el conjunto de números naturales $\mathbb{N}$, o sea si su cardinal es $\aleph_0$.

Hemos visto también en ese capítulo que el conjunto $\mathbb{Z}$ de los números enteros es numerable.

Veamos que el conjunto $\mathbb{Q}$ de números racionales es numerable.

No haremos una demostración rigurosa, pero describiremos la idea.

> *Se nos ha sugerido que al llegar aquí, el lector cansado, cierra el libro con un suspiro…. y se va al cine. Sólo podemos adelantarle, para calmarlo, que esta demostración, como la que sigue sobre la no contabilidad de los números reales, es difícil. Ud. puede rechinar sus dientes y tratar de entender todo lo que pueda de ellas, o bien prescindir de ambas. Lo esencial antes de retirarse, es saber que Cantor descubrió que las fracciones racionales son contables, pero que el conjunto de los números reales no lo es. De este modo, y a pesar de lo que le dicte el sentido común, no hay más fracciones que números enteros y hay más números reales entre 0 y 1, que elementos en toda la clase de los números enteros.*
> *(Matemáticas e Imaginación-Edward Kasner & James Newman. pág 58)*

Para ver que $\mathbb{Q}$ es numerable debemos poder demostrar que existe una aplicación biyectiva de $\mathbb{N}$ sobre $\mathbb{Q}$. Para ello, escribiremos a los racionales positivos como una sucesión, definida de manera tal de asegurarnos que todos ellos estén alcanzados por algún término de la sucesión.
Utilizando el método de Cantor, disponemos los números racionales en una "matriz" infinita:

$$\begin{array}{ccccccccc}
\frac{1}{1} & \frac{1}{2} & \frac{1}{3} & \frac{1}{4} & \frac{1}{5} & . & . & . \\
\frac{2}{1} & \frac{2}{2} & \frac{2}{3} & \frac{2}{4} & \frac{2}{5} & . & . & . \\
\frac{3}{1} & \frac{3}{2} & \frac{3}{3} & \frac{3}{4} & \frac{3}{5} & . & . & . \\
\frac{4}{1} & \frac{4}{2} & \frac{4}{3} & \frac{4}{4} & \frac{4}{5} & . & . & . \\
\frac{5}{1} & \frac{5}{2} & \frac{5}{3} & \frac{5}{4} & \frac{5}{5} & . & . & . \\
. & . & . & . & . & . & . & . \\
. & . & . & . & . & . & . & . \\
. & . & . & . & . & . & . & .
\end{array}$$

y se los enumera como sigue

$$\frac{1}{1}\to\frac{1}{2}\to\frac{2}{1}\to\frac{1}{3}\to\frac{2}{2}\to\frac{3}{1}\to\frac{1}{4}\to\frac{2}{3}\to\frac{3}{2}\to\frac{4}{1}\to\frac{1}{5}\to\frac{2}{4}\to\frac{3}{3}\to\frac{4}{2}\to\frac{5}{1}\to.....$$

Claramente cada número racional positivo está en alguna fila y en alguna columna de esta matriz, y con esta enumeración en diagonal se los recorre a todos.
La sucesión así definida, claramente no es inyectiva, puesto que distintas fracciones representan el mismo número racional positivo, con lo cual cada uno de ellos no está en un solo lugar de la matriz, por ejemplo $\frac{1}{1}=\frac{2}{2}=\frac{3}{3}=\frac{4}{4}=....$, o $\frac{1}{2}=\frac{2}{4}=\frac{3}{6}=...=\frac{5}{10}=...$, pero esta sucesión suryectiva y no inyectiva nos dice que *card* $(\mathbb{Q}^+) \leq$ *card* $(\mathbb{N})$, porque existe una función suryectiva de $\mathbb{N}$ sobre $\mathbb{Q}^+$, pero como, $\mathbb{N} \subset \mathbb{Q}^+$ tenemos que
card $(\mathbb{Q}^+) \geq$ *card* $(\mathbb{N})$, con lo cual se obtiene que *card* $(\mathbb{Q}^+)$ = *card* $(\mathbb{N})$. Análogamente podemos demostrar que *card* $(\mathbb{Q}^-)$ = *card* $(\mathbb{N})$. Como $\mathbb{Q}=\mathbb{Q}^+\cup\mathbb{Q}^-\cup\{0\}$ y la unión de conjuntos numerables es un conjunto numerable, como así también la unión de conjuntos numerables con conjuntos finitos (propiedad que no demostraremos pero puede consultar en bibliografía sobre Teoría de Conjuntos), tenemos que *card* $(\mathbb{Q})$ = *card* $(\mathbb{N})$.

- Ahora, veremos que el conjunto $\mathbb{R}$ de los números reales **no** es numerable.

La demostración de este hecho se realiza mediante el denominado **Método de Diagonalización de Cantor** o **Método de Diagonal de Cantor,** pues fue ideada por Georg Cantor .

***Teorema*:** El intervalo $(0,1)$ no es un conjunto numerable.

***Demostración* :** Supongamos que $(0,1)$ fuera un conjunto numerable, entonces existiría una función biyectiva $f:\mathbb{N}\to(0,1)$.

Sea $f(1)=0,\ a_1^1a_2^1a_3^1.....a_n^1.....$ (escrito en notación decimal)
$f(2)=0,\ a_1^2a_2^2a_3^2.....a_n^2....$
.
.

.

$f(m) = 0,\ a_1^m a_2^m a_3^m .....a_n^m .....$

.

.

Como f es suryectiva todo número de $(0, 1)$ es algún $f(m)$.

Definamos ahora el siguiente número: $r = 0,\ b_1 b_2 b_3 .....b_n ....$

tal que los b_i verifican : $b_1 \neq a_1^1$, $b_2 \neq a_2^2$, $b_3 \neq a_3^3$ …., en general $b_n \neq a_n^n$ $\forall n \in \mathbb{N}$.

$f(1) \neq r$ pues $b_1 \neq a_1^1$; $f(2) \neq r$ pues $b_2 \neq a_2^2$, $f(3) \neq r$ pues $b_3 \neq a_3^3$,

en general $\forall n \in \mathbb{N}$ $f(n) \neq r$ pues $b_n \neq a_n^n$.

$\therefore$ ninguna sucesión $(s_i)_{i \in \mathbb{N}}$ puede cubrir el intervalo $(0, 1)$.

Conclusión: El intervalo $(0, 1)$ no puede estar en correspondencia biunívoca con el conjunto $\mathbb{N}$, luego **no es numerable.**

- $(0, 1)$ es coordinable con el conjunto $\mathbb{R}_{>0}$ pues la aplicación $e^{\frac{1}{x}}$ es una biyección del conjunto $\mathbb{R}_{>0}$ sobre $(0, 1)$ $\therefore$ $\mathbb{R}_{>0}$ **no es numerable**.
- $\mathbb{R}$ es coordinable con $\mathbb{R}_{>0}$ pues la aplicación *ln x* es una biyección de $\mathbb{R}_{>0}$ sobre $\mathbb{R}$ $\therefore$ $\mathbb{R}$ **no es numerable.**

***Ejercicios*:**

1. i) Probar que la suma y producto de racionales es racional.

   ii) Probar que si $\frac{p}{q} \in \mathbb{Q}$ y $\frac{p}{q} \neq 0$ entonces $\left(\frac{p}{q}\right)^{-1} \in \mathbb{Q}$

   iii) ¿Es cierto que la suma y producto de irracionales es siempre irracional?

2. Demostrar aplicando el Teorema Fundamental de la Aritmética que los siguientes números son irracionales:

   $\sqrt{2}$, $\sqrt{10}$, $\sqrt{12}$, $\sqrt{2}+\frac{1}{\sqrt{2}}$, $\sqrt{2}+\sqrt{3}$, $\sqrt{2}+\sqrt{3}+4$

   $\sqrt{p}$, $\sqrt[n]{p}$, $n, p \in \mathbb{N}$, p primo.

3. i. Demostrar que para $m, n, r, s \in \mathbb{Z}$, $n \neq 0$, $s \neq 0$,

$$\frac{m}{n} = \frac{r}{s} \Leftrightarrow m.s = n.r$$

   ii. Demostrar que para cada fracción $\frac{m}{n}$ $\exists! r \in \mathbb{Z} \wedge s \in \mathbb{N}$ tales que $\frac{m}{n} = \frac{r}{s}$ con $(r , s) = 1$.

4. a) Demostrar que si $m, n \in \mathbb{Q}$, $m \neq 0$, ó $n \neq 0$, entonces $m\sqrt{2} + n\sqrt{3}$ es irracional.

   b) Idem con $\frac{m}{n\sqrt{2}+\sqrt{3}}$, $m \neq 0$

   c) Probar que si $a, b, c \in \mathbb{Q}$ son tales que $a\sqrt{2} + b\sqrt{3} + c\sqrt{5} = 0$ entonces $a = b = c = 0$.

   d) Probar que $\sqrt{\sqrt[3]{5} - \sqrt[3]{4}} = \frac{1}{3}(\sqrt[3]{2} + \sqrt[3]{20} - \sqrt[3]{25})$.

5. Ordenar las siguientes sucesiones de números racionales:

   i) $\frac{-3}{2}, \frac{-5}{2}, \frac{-11}{9}$ ii) $\frac{21}{3}, \frac{41}{18}, \frac{13}{7}$ iii) $\frac{2}{5}, \frac{1}{9}, \frac{3}{6}, \frac{2}{8}$

6. Demostrar que todo subconjunto no vacío de $\mathbb{R}$, acotado inferiormente, admite ínfimo.

7. Demostrar que si $A \subset \mathbb{R}$, $A \neq \phi$ y acotado inferiormente por t , las siguientes dos propiedades son equivalentes:

   i. $t = \text{ínf } A$ ii. $\forall \varepsilon > 0 \quad \exists a \in A$ tal que $t \leq a < t + \varepsilon$

8. Sean $x, y \in \mathbb{R}$.

   i) Probar que si $x < y$ entonces $x < \frac{x+y}{2} < y$

   ii) Deducir que si $x, y \in \mathbb{Q}$ $x < y$, existe un racional q tal que $x < q < y$.

9. Sean $x, y \in \mathbb{R}$, $x < y$.

   i) Demostrar que $x < x + \frac{y-x}{\sqrt{2}} < y$

   ii) Deducir que si $r, r' \in \mathbb{Q}$ $r < r'$, existe un irracional t tal que $r < t < r'$.

iii) Deducir que si $x, y \in \mathbb{R}$, $x < y$, existe un $t \notin \mathbb{Q}$ tal que $x < t < y$.

10. Demostrar que:

i. Para $z, y \in \mathbb{R}$ $z^n - y^n = (z-y).\sum_{i=0}^{n-1} z^i y^{n-1-i}$

ii. Si $z > 0 \wedge y > 0$, $\sum_{i=0}^{n-1} z^i y^{n-1-i} > 0$.

iii. Si $z, y \in \mathbb{R}_{>0}$, $n \in \mathbb{N}$, $z^n = y^n \Leftrightarrow z = y$.

iv) Si $z, y \in \mathbb{R}_{>0}$, $n \in \mathbb{N}$, $z^n < y^n \Leftrightarrow z < y$.

11. Sean $s, \varepsilon \in \mathbb{R}$, $s > 1$, $0 < \varepsilon < 1$, $n \in \mathbb{N}$. Demostrar que:

$$s^n + \sum_{i=1}^{n-1} \binom{n}{i} s^i (-\varepsilon) < \sum_{i=0}^{n} \binom{n}{i} s^i (-\varepsilon)^{n-i} = (s-\varepsilon)^n .$$

12. Probar que los siguientes números son irracionales (asumiendo la irracionalidad de π):

i. $\pi + \sqrt{3}$ ii. $\sqrt{\pi}$ iii. $\frac{1}{\pi}$

13. Sea $q \in \mathbb{Q}$.

i) Probar que existe $m \in \mathbb{N}$ tal que $q < m$.

ii) En cada uno de los casos siguientes determinar un $m \in \mathbb{Z}$, tal que $m \leq q < m + 1$.

a) $q = \frac{12}{5}$ b) $q = \frac{31}{7}$ c) $q = \frac{-231}{19}$

14. Sean a, b racionales $a < b$. Probar que $a < \frac{2a+b}{3} < b$

15. Asumiendo la trascendencia de π , demostrar la trascendencia de :

i. $2 + \pi$ ii. $\frac{1}{\pi}$

16. Calcular en cada caso, si existen ínfimo y/o supremo de A:

i) $A = \{ x \in \mathbb{R} : |x - 1| < 1 \}$ ii) $A = \{ x \in \mathbb{R} : x^2 < 1 \}$

iii) $A = \left\{ \frac{n}{n+1} / \quad n \in \mathbb{N} \right\}$ iv) $A = \left\{ \frac{n+1}{n} / \quad n \in \mathbb{N} \right\}$

v) $A = (a, b)$, $a < b$

17. Sean $a, b \in \mathbb{R}_{>0,}$ $n, m \in \mathbb{N}$. Probar:

i) $\sqrt[n]{a.b} = \sqrt[n]{a}.\sqrt[n]{b}$ iii) $\sqrt[m]{\sqrt[n]{a}} = \sqrt[n.m]{a}$

ii) $\sqrt[n]{a^{-1}} = \left(\sqrt[n]{a} \right)^{-1}$ iv) $a < b \Leftrightarrow \sqrt[n]{a} < \sqrt[n]{b}$

v) $1 < a, \quad n < m \Rightarrow \sqrt[m]{a} < \sqrt[n]{a}$

18. Sean $a, b \in \mathbb{R}_{>0}$, $n, q \in \mathbb{N}$, $m, p \in \mathbb{Z}$, $r, s \in \mathbb{Q}$. Demostrar que:

Si $\frac{m}{n} = \frac{p}{q} \Rightarrow a^{\frac{m}{n}} = a^{\frac{p}{q}}$ (Esto dice que la potencia $\frac{m}{n}$ está bien definida).

19. Sean $a, b \in \mathbb{R}$, $r, s \in \mathbb{Q}$. Probar la validez de las siguientes propiedades:

i) $a^r . a^s = a^{r+s}$

ii) $a^r / a^s = a^{r-s}$

iii) $(a^r)^s = a^{r.s}$

iv) $(a.b)^r = a^r . b^r$

v) $a^{-r} = (a^r)^{-1}$

20. Problema: Antes de llegar al comercio minorista, una cierta manufacturación pasa por la mano de dos intermediarios que trabajan con márgenes de utilidad del 20% y del 30% respectivamente. Si el precio que debe pagar el mayorista es de $ 1560. ¿Cuál es el precio de fábrica?

21. Si $x = k + y = h + z$ con $k, h \in \mathbb{Z}$, $0 \leq y < 1$, $0 \leq z < 1$ entonces $k = h \ \wedge \ y = z$.

22. Hallar la representación decimal de : $\frac{1}{7}$; $\frac{15}{4}$; $\frac{17}{6}$; $\frac{6}{17}$.

23. Encontrar el número racional cuya representación decimal es : 1,422525252….

24. Hallar la representación en las bases indicadas, de los números:

i. $\frac{1}{17}$ en base 12

ii. $\frac{4}{5}$ en base 3

iii. $\frac{1}{3}$ en base 3

iv. $\frac{1}{5}$ en base 5

25. Hallar el número racional cuya representación:

i. en base 7 es 0,123

ii. en base 6 es 0,012

iii. en base 12 es 0,A

26. ¿En qué bases será finito el desarrollo de $\frac{7}{30}$?

27. i. Encontrar la representación en bases 3, 5 y 10 de $\sqrt{2}$, con, al menos, tres cifras.

ii. Idem para $\sqrt{3}$ en bases 2, 3 y 4

CAPÍTULO VII

ESTRUCTURAS ALGEBRAICAS
GRUPOS, ANILLOS Y CUERPOS

"Alrededor de 1850 las matemáticas sufrieron uno de los cambios más trascendentales de su historia, aunque ello no se hizo entonces evidente. Antes de 1800, los principales objetos de estudio matemático eran relativamente concretos: números, triángulos, esferas. El álgebra utilizaba fórmulas para representar manipulaciones con números, pero las propias fórmulas se veían como representaciones simbólicas de procesos, no como cosas en sí mismas. Pero hacia 1900, fórmulas y transformaciones se veían como cosas, no como procesos, y los objetos del álgebra eran mucho más abstractos y más generales…"

(Historia de las Matemáticas, Ian Stewart)

Suponemos que el lector está familiarizado con la Aritmética del conjunto $\mathbb{Z}$ de los números enteros (y con las propiedades de la suma y el producto de los números racionales y reales) y de $\mathbb{Z}_n$, conoce sus similitudes y diferencias; por ello consideramos pertinente introducir nociones básicas de ciertas estructuras algebraicas fundamentales: grupos, anillos y cuerpos, que permitan realizar un estudio más abstracto de los ejemplos conocidos y de otros que veremos en lo sucesivo.

***Leyes de composición*:**

***Definición*:** Sea G un conjunto no vacío. Una operación en G (o *ley de composición en G*) es una función $\psi : G \times G \to G$ que a cada par ordenado $(a, b) \to a * b$, donde $a * b$ representa la imagen del par (a, b) por la función ψ.

Ejemplos: Son ampliamente conocidas las siguientes leyes de composición:

i) $+ : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$, $(a, b) \to a + b$ ii) $\cdot : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$, $(a, b) \to a \cdot b$ iii) $+ : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$, $(a, b) \to a + b$

iv) Para $\mathfrak{F}(A) = \{ f \ / \ f : A \to A \ \text{función} \}$, $\circ : \mathfrak{F}(A) \times \mathfrak{F}(A) \to \mathfrak{F}(A)$ tal que $(f, g) \to g \circ f$ (composición de funciones en A).

***Definiciones*:** Sean $G \neq \phi$, $*$ una operación en G.

- Decimos que $*$ es *asociativa* si $a * (b * c) = (a * b) * c \ \forall\, a,b,c \in G$.
- Decimos que $*$ es *conmutativa* si $a * b = b * a \ \forall\, a,b \in G$.
- Decimos que G posee un elemento neutro para $*$ si $\exists e \in G$ tal que $a * e = e * a = a \ \forall\, a \in G$.
- Si G posee un elemento neutro e para $*$, decimos que $a \in G$ *es inversible por* $*$ si $\exists\, a' \in G$ tal que $a * a' = a' * a = e$.

Ejemplos: En los ejemplos anteriores i), ii), iii) son asociativas, conmutativas y tienen en cada caso su elemento neutro, en i) e iii) todo elemento tiene inverso, pero en ii) sólo el 1 y el –1 son inversibles.
La operación del ejemplo iv) es asociativa, no conmutativa (en general) , tiene elemento neutro, la aplicación identidad: id_A, y en general, no todo elemento es inversible (sabemos que para que una función f sea inversible es necesario y suficiente que sea biyectiva).

***Proposición*:** Sean $G \neq \phi$, $*$ una operación en G. Si $*$ admite elemento neutro en G, éste es único.

***Demostración*:**
Supongamos que hubiera dos neutros e_1 y $e_2 \in G$. Entonces

$a * e_1 = e_1 * a = a$, $\forall\, a \in G$ y $a * e_2 = e_2 * a = a$, $\forall\, a \in G$

en particular $e_1 = e_1 * e_2 = e_2$.

Monoides y grupos

***Definición*:** Sean $G \neq \phi$, $*$ una operación en *G*. El par ordenado $(G , *)$ se denomina *monoide* si la operación $*$ es asociativa y tiene elemento neutro en *G*.
Si la operación es además conmutativa, se dice que es un *monoide conmutativo*.

Observación: la estructura algebraica, en este caso monoide pero la observación es válida para todas las demás, se define como un par ordenado (o una terna, en otros casos) en el cual no sólo importa el conjunto sino que es fundamental la/s operación/es definida/s en él, porque, como hemos visto en ejemplos precedentes, sobre un mismo conjunto pueden definirse distintas operaciones, y no todas ellas con las mismas propiedades, lo que producen estructuras muy diferentes. Hecha esta aclaración, también indicamos que *por abuso de lenguaje*, en muchos casos haremos mención del monoide o grupo *G,* del anillo *A* o del cuerpo *K*, sin especificar la operación (o las operaciones) porque la/s sobreentenderemos para facilitar las notaciones, pero asumiendo en nuestro discurso que está/n implícita/s.

***Corolario*:** En todo monoide, el neutro que existe, es **única**.

Ejemplos: $(\mathbb{N}, \cdot)$, $(\mathbb{Z}, +)$, $(\mathbb{Z}, \cdot)$, $(\mathbb{Q}, +)$, $(\mathbb{Q}, \cdot)$, $(\mathbb{R}, +)$, $(\mathbb{R}, \cdot)$, $(\mathbb{Z}_n, +)$, $(\mathbb{Z}_n, \cdot)$, para $n \in \mathbb{N}$, $(\mathfrak{F}(A), \circ)$, son todos monoides.
$(\mathbb{N}, +)$ **no** es un monoide porque no hay en $\mathbb{N}$ un neutro para la suma.

***Definición*:** Sea $(G , *)$ un monoide, *e* su elemento neutro. Diremos que $(G , *)$ es un *grupo* si todo elemento de *G* es inversible, o sea si $\forall a \in G \ \exists a' \in G$ tal que $a * a' = a' * a = e$

Evariste Galois (1811-1832)

Con Ruffini aparece la nueva idea de "grupo", que llamaba "permutaciones", y que Cauchy desarrolló bajo el nombre de "sistemas conjugados de sustituciones", pero el cabal fundador de la teoría de grupos es Evariste Galois, uno de los matemáticos precoces de mayor genio, cuya vida breve y agitada fue fiel reflejo de la época romántica en que le tocó actuar.
…la noche anterior al duelo, en el que muere, lega a un amigo, en notas apresuradas, su testamento científico, donde le pide que, si su adversario vence, haga conocer sus descubrimientos a Gauss o a Jacobi para que expresen su opinión "no respecto de la verdad, sino de la importancia de los teoremas. Espero que más tarde alguien encuentre provechoso descifrar todo este lío". Este lío (ce gâchis) es hoy la teoría de grupos.
Historia de la Matemática.- vol 2- Julio Rey Pastor y José Babini

***Proposición*:** Sea $(G , *)$ un grupo. El inverso de cada elemento de *G* es **único.**

***Demostración*:** Supongamos que para un $a \in G \ \exists a', a'' \in G$ tales que

$$a * a' = a' * a = e \ \wedge \ a * a'' = a'' * a = e .$$

Entonces, aplicando las definiciones de inverso y de elemento neutro, y la propiedad asociativa, obtenemos que:

$$a' = a' * e = a' * (a * a'') = (a' * a) * a'' = e * a'' = a''$$

Notación: En un grupo, escribiremos al inverso de cada elemento *a* como a^{-1} , excepto en aquellos casos concretos en que ya tengan una notación específica, como lo es el inverso aditivo u opuesto de un número entero (racional o real) a que lo escribimos $-a$.

Ejemplos: $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{Z}_n, +)$ son todos grupos.
$(\mathbb{N}, \cdot)$, $(\mathbb{Z}, \cdot)$, $(\mathbb{Q}, \cdot)$, $(\mathbb{R}, \cdot)$, $(\mathbb{Z}_n, \cdot)$, $(\mathfrak{F}(A), \circ)$ **no** son grupos pues en ellos no todo elemento tiene inverso. En $\mathbb{N}$ el único inversible para $\cdot$ es el 1, en $\mathbb{Z}$ los inversibles para $\cdot$ son sólo 1 y –1 , en $\mathbb{Q}$ y $\mathbb{R}$, 0 no es inversible para $\cdot$ por lo tanto no todos son inversibles. En $\mathbb{Z}_n$ los elementos inversibles son las $\overline{a}$ tales que (a , n) = 1 , que para cualquier n no son todos los a , con $0 < a < n$; pero aun siendo n primo, 0 no es inversible.
En $\mathfrak{F}(A)$ ya resaltamos que no toda función es inversible, sólo las biyectivas. El conjunto $S_X = \{ f : X \to X \ / \ f \ es \ biyectiva \}$, con la operación $\circ$ (composición de funciones) constituye un grupo. Cuando X es finito al conjunto se lo designa S_n , donde n es el cardinal de X, y a sus elementos $\sigma \in S_n$ se los denomina *permutaciones.*

Un grupo muy pequeño

Entre los grupos que tienen un número finito de elementos los más pequeños son los que tienen sólo dos elementos. Si consideramos el conjunto $A = \{\alpha, \beta\}$ y la operación ^ definida según la siguiente tabla:

^	α	β
α	α	β
β	β	α

Es claro y sencillo de comprobar que la operación es asociativa; que el elemento neutro es α , ya que α ^ β = β ^ α = β y que cada elemento tiene su inverso (el inverso de α es α y el inverso de β es β), por lo que (A , ^) es grupo. Además es un grupo conmutativo.
Se trata de un grupo más interesante de lo que parece si reemplazamos α y β por los bits informáticos 0 y 1 respectivamente.
En realidad, el grupo más pequeño que existe es el formado por un único elemento que es a su vez elemento neutro e inverso de sí mismo al que los matemáticos denominan el grupo trivial.

***Propiedades*:** Sean (G , $*$) un grupo, $a, b \in G$. Se verifican las siguientes propiedades:
i. $e^{-1} = e$
ii. $(a.b)^{-1} = b^{-1}.a^{-1}$
iii. $(a^{-1})^{-1} = a$

***Demostración*:** Se deja como ejercicio.

***Definición*:** Sean (G , $\cdot$) un grupo, $a \in G$, $n \in \mathbb{N}$. Definiremos a^n inductivamente por:

$$a^n =: \begin{cases} a^1 = a \\ a^{n+1} = a^n.a \end{cases}$$

***Propiedades*:** Sean (G , $\cdot$) un grupo, $a \in G$, $n, m \in \mathbb{N}$. Se verifican las siguientes propiedades:
i. $a^n.a^m = a^{n+m}$
ii. $(a^n)^m = a^{n.m}$

***Demostración*:** Se deja como ejercicio.

***Definición*:** Sean $(G, \cdot)$ un grupo, e su neutro, $a \in G$, $n \in \mathbb{N}$. Definimos $a^0 =: e$ y $a^{-n} =: (a^n)^{-1}$.

Ejercicio: $a^{-n} = (a^{-1})^n$.

***Propiedades*:** Sean $(G, \cdot)$ un grupo, $a \in G$, $n, m \in \mathbb{N}_0$. Se verifican las siguientes propiedades:

i. $a^{-n}.a^{-m} = a^{-(n+m)}$.
ii. $a^n.a^{-m} = a^{n-m}$.
iii. $(a^{-n})^m = (a^n)^{-m} = a^{-n.m}$.
iv. $(a^{-n})^{-m} = a^{n.m}$.

***Demostración*:** Se deja como ejercicio.

***Definición*:** Sea $(G, \cdot)$ un grupo, $H \subset G$. Se dice que H es un *subgrupo* de G si $H \neq \phi$, y $\forall x, y \in H$ se verifica que $x.y^{-1} \in H$.

Notación: Cuando queramos indicar que H es un subgrupo de G se notará: $H \underset{sg}{\subset} G$

Ejemplos:

1. Todo grupo G admite los llamados *subgrupos triviales*: G ; $\{e\}$ (El subgrupo $\{e\}$ se denomina *el subgrupo nulo*; cuando se especifica que un subgrupo H es *no nulo* se escribe $H \neq 0$).
2. En el grupo $(\mathbb{Z}, +)$, los subconjuntos:
   $n\mathbb{Z} = \{a \in \mathbb{Z} \ / \ n \mid a\} = \{nk \ / \ k \in \mathbb{Z}\}$ son todos subgrupos, $n \in \mathbb{N}_0$.
3. $\mathbb{Z} \underset{sg}{\subset} \mathbb{Q} \underset{sg}{\subset} \mathbb{R}$, todos ellos considerados con la operación $+$.

Ejercicio: Demostrar que $n\mathbb{Z} = (-n)\mathbb{Z} \ \ \forall n \in \mathbb{N}$

***Teorema*:** Sean $(G, \cdot)$ un grupo, $H \subset G$. Entonces $H \underset{sg}{\subset} G$ si y sólo si H verifica

$$\begin{cases} e \in H \\ si \ \ x, y \in H \Rightarrow x.y \in H \\ si \ \ x \in H \Rightarrow x^{-1} \in H \end{cases}$$

***Demostración*:** $\Rightarrow$) Supongamos que H es un subgrupo de G, por lo tanto $H \neq \phi$, con lo cual tiene, al menos, un elemento x.

Por la definición de subgrupo, y como $x \in H$, se verifica que $x.x^{-1} \in H$, pero $x.x^{-1} = e$, así $e \in H$.

Sea ahora cualquier $y \in H$, como ya establecimos que $e \in H$, por definición de subgrupo, tenemos que $e.y^{-1} \in H$, pero $e.y^{-1} = y^{-1}$, por ser e neutro, luego demostramos que $y \in H \Rightarrow y^{-1} \in H$.

Sean ahora dos elementos cualesquiera $x, y \in H$; como $y \in H \Rightarrow y^{-1} \in H$. Utilizando nuevamente la definición, tenemos que $x.(y^{-1})^{-1} \in H$, pero $(y^{-1})^{-1} = y$ por lo tanto $x.y \in H$, como queríamos probar.

$\Leftarrow$) Sea ahora H un subconjunto del grupo G que verifica

$$\begin{cases} e \in H \\ si \;\; x, y \in H \Rightarrow x.y \in H \\ si \;\; x \in H \Rightarrow x^{-1} \in H \end{cases}$$

Veamos que es un subgrupo de G : $H \neq \phi$ puesto que, por hipótesis, $e \in H$.

Ahora debemos demostrar que $x , y \in H \Rightarrow x.y^{-1} \in H.$

Si $y \in H$, por hipótesis $y^{-1} \in H$, y también por hipótesis, $x , y^{-1} \in H \Rightarrow x.y^{-1} \in H.$

Con lo cual hemos demostrado que H verifica la definición, por lo tanto $H \underset{sg}{\subset} G$

***Corolario*:** Sean (G , $\cdot$) un grupo, $H \underset{sg}{\subset} G$; (H , $\cdot$) es a la vez un grupo (donde con "$\cdot$" indicamos también la operación en H inducida por la de G).

***Demostración*:** Por la equivalencia demostrada anteriormente, la función $\cdot$ restringida a $H \times H$ se aplica sobre H , con lo cual es también una operación en H.
También la equivalencia demostrada dice que si tengo un subgrupo H, éste tiene elemento neutro, y todo elemento de H tiene su inverso en H; como la operación $\cdot$ ya es asociativa en G, lo será también su restricción a H. Por lo tanto, la operación en H verifica todas las propiedades que permiten que se estructure como un grupo.

***Proposición*:** Sean (G , $\cdot$) un grupo, $a \in G$. El conjunto $H = \left\{ a^n \;/\; n \in \mathbb{Z} \right\}$ es un subgrupo de G.

***Demostración*:** Se deja como ejercicio porque resulta como consecuencia directa de las propiedades enunciadas anteriormente.

***Definición*:** Sea (G , $\cdot$) un grupo. El grupo se dice *abeliano* si la operación es además conmutativa.

Los grupos abelianos son así llamados en honor al matemático noruego Niels Henrik Abel.
Este matemático fue quien introdujo el concepto de los grupos conmutativos en un artículo del primer número de la revista matemática Journal de Crelle, en 1826*, que versaba sobre la asociatividad.*
Abel investigó la estructura de los grupos conmutativos y mostró que son producto de grupos cíclicos. No obstante, no sería el concepto de grupo el tema que más se destacara de su trabajo.

Niels Henrik Abel (1802-1829)

Ejemplos: ($\mathbb{Z}$, +) , ($\mathbb{Q}$, +) , ($\mathbb{R}$, +) , ($\mathbb{Z}_n$, +) son todos grupos abelianos.

(S_n , $\circ$) no es grupo abeliano para $n > 2$.

Nota: Los ejemplos precedentes muestran que los grupos (abelianos o no) pueden ser finitos o infinitos. Cuando un grupo G es finito (o sea, el conjunto G es finito) se denomina *orden de G* al cardinal de G.
En símbolos $o(G) = card (G)$.

Ejemplo: $o(\mathbb{Z}_n) = n$.

***Corolario*:** El subgrupo $H = \{ a^n \ / \ n \in \mathbb{Z} \}$ de G es siempre un grupo abeliano.

***Demostración*:** Se deja como ejercicio.

***Definición*:** Sean $(G , \cdot)$ un grupo, $a \in G$; el grupo $H = \{ a^n \ / \ n \in \mathbb{Z} \}$ se denomina *grupo cíclico generado por a* , y lo notaremos (*a*) (también se suele escribir $\langle a \rangle$).

Definición*:** Sea H un grupo cíclico, $a \in H$, se dice que ***a** genera a H,* o que ***a es *generador de H* si $H = (a)$, o sea, si $\forall\, b \in H \ \exists\, n \in \mathbb{Z}$ tal que $b = a^n$.

***Definición*:** Sean $(G , \cdot)$ un grupo, $a \in G$, $a \neq e$. Si $\exists\, k \in \mathbb{N}$ tal que $a^k = e$; sea $n = mín\{ k \in \mathbb{N} \ / \ a^k = e \}$; n se denomina *el orden* de a , y se escribe $n = ord(a)$.

***Proposición*:** Si $(G , \cdot)$ es un grupo y $a \in G$ de orden n , entonces:
i. Para $m \in \mathbb{Z}$, $a^m = e \iff n \mid m$.
ii. Para $k, h \in \mathbb{Z}$, $a^k = a^h \iff k \equiv h \ (mód\ n)$.

***Demostración*:**
i. $\Leftarrow$) Si $m \in \mathbb{Z}$ es tal que $n \mid m$, $\exists q \in \mathbb{Z}$ tal que $m = q.n$, entonces $a^m = a^{q.n} = (a^n)^q = e^q = e$

$\Rightarrow$) Supongamos ahora $m \in \mathbb{Z}$ tal que $a^m = e$; por el Algoritmo de la División $m = q.n + r$ con $q, r \in \mathbb{Z}$ y $0 \leq r < n$
luego $e = a^m = (a^n)^q . a^r = e^q . a^r = a^r$ con lo que $a^r = e$, pero $r < n$, por lo que $r \notin \mathbb{N}$, por la minimalidad de n , entonces $r = 0$ y así $n \mid m$.

ii. Sean $k, h \in \mathbb{Z}$, $a^k = a^h \iff a^{k-h} = a^k a^{-h} = e \iff n \mid (k - h) \iff k \equiv h \ (mód\ n)$.

***Corolario*:** Si $(G , \cdot)$ es un grupo y $a \in G$ es de orden n , entonces el grupo cíclico generado por a, $(a) = \{ a^n \ / \ n \in \mathbb{Z} \}$ tiene orden n .

***Demostración*:**
Por lo demostrado en la proposición anterior $(a) = \{ a^0 = e, a, a^2, a^3, ..., a^{n-1} \}$ pues cada $a^k = a^r$ donde r es el resto de k en la división por n , y restos distintos r, s , en la división por n dan potencias de a distintas, o sea si $r \neq s$, $0 \leq r , s < n$ entonces $a^r \neq a^s$.

Notación: Por analogía con los ejemplos más naturales de los grupos abelianos, que son los que dimos anteriormente, y porque éstos constituyen una parte importante de otras estructuras en las que intervienen más de una operación, a la operación de los grupos abelianos se la suele notar con el símbolo + , a su neutro con 0 , y al inverso de cada elemento a como $-a$.

Cuando éste sea el caso, escribiremos en notación *aditiva* en vez de la notación *multiplicativa* que usamos anteriormente:

Notación multiplicativa

i. $e^{-1} = e$
ii. $(a.b)^{-1} = b^{-1}.a^{-1}$
iii. $(a^{-1})^{-1} = a$
iv. $a^n = \begin{cases} a^1 = a \\ a^{n+1} = a^n.a \end{cases}$
v. $a^n.a^m = a^{n+.m}$
vi. $(a^n)^m = a^{n.m}$
vii. $a^0 = e$, $a^{-n} = (a^n)^{-1}$
viii. $a^{-n}.a^{-m} = a^{-(n+m)}$
ix. $a^n.a^{-m} = a^{n-m}$
x. $a^{-n})^m = (a^n)^{-m} = a^{-n.m}$
xi. $(a^{-n})^{-m} = a^{n.m}$

Notación aditiva

i) $-0 = 0$
ii) $-(a + b) = [(-a) + (-b)]$
iii) $-(-a) = a$
iv) $na = \begin{cases} 1a = a \\ (n+1)a = na + a \end{cases}$
v) $na + ma = (n + m)a$
vi) $n(ma) = (nm)a = (mn)a$
vii) $0a = 0$, $(-n)a = -na$
viii) $(-n)a + (-m)a = -(n + m)a$
ix) $na + (-m)a = (n - m)a$
x) $m(-na) = (-m)na = -nma$
xi) $(-m)[(-n)a] = nma$

Nota: Cuando en la notación aditiva se escribe $0a = 0$ hay que tener bien claro que el cero de la izquierda es el número entero, mientras que el de la derecha es el neutro de la operación en el grupo

Notación aditiva de la definición de subgrupo:

***Definición*:** Sea $(G , +)$ un grupo abeliano, $H \subset G$. Se dice que H es un *subgrupo* de G si $H \neq \phi$, y $\forall\, x , y \in H$ se verifica que $x - y \in H$.

Nota: Claramente todo subgrupo de un grupo abeliano es también abeliano.

La versión "abeliana" de la caracterización de los subconjuntos de G que son subgrupos es:

***Teorema*:** Sean $(G , +)$ un grupo abeliano, $H \subset G$. Entonces $H \underset{sg}{\subset} G$ si y sólo si H verifica:

$$\begin{cases} 0 \in H \\ si \;\; x, y \in H \Rightarrow x + y \in H \\ si \;\; x \in H \Rightarrow -x \in H \end{cases}$$

Ejercicio: Sean $(G , +)$ un grupo abeliano, $a, b \in G$, $n \in \mathbb{N}$. Demostrar que $n(a + b) = na + nb$.

Cuando el grupo G sea abeliano, al grupo cíclico generado por a lo escribiremos:

$$(a) = H = \{ na \;/\; n \in \mathbb{Z} \} .$$

Ejemplos:

1. Los grupos $n\mathbb{Z}$ definidos antes son subgrupos cíclicos de $\mathbb{Z}$, $n\mathbb{Z} = (n)$; en particular $\mathbb{Z} = (1)$.
2. Los grupos $(\mathbb{Z}_n , +)$ son cíclicos y de orden n , $\mathbb{Z}_n = (\bar{1})$.

Nota: Los ejemplos precedentes muestran que los grupos cíclicos también pueden ser finitos o infinitos.

Ejercicios:

1. Sea $(G, \cdot)$ un grupo, $H \underset{sg}{\subset} G$, $a \in H$. Demostrar que $(a) \underset{sg}{\subset} H$, o sea, (a) es el *menor* subgrupo de G que contiene al elemento a.

2. ¿Cuáles son los generadores de $\mathbb{Z}$? ¿y los de $n\mathbb{Z}$?

3. Determinar los generadores de los grupos cíclicos: $\mathbb{Z}_2$, $\mathbb{Z}_3$, $\mathbb{Z}_4$, $\mathbb{Z}_5$, $\mathbb{Z}_9$, $\mathbb{Z}_{10}$. Analice los resultados de los ejemplos dados y elabore conclusiones.

4. Determinar los subgrupos de los grupos del ejercicio *3*. ¿Son cíclicos? ¿Cuáles son sus órdenes?

5. Demostrar que la intersección de subgrupos de *G* es un subgrupo de *G*. ¿Es la unión de subgrupos de G un subgrupo de *G*?

Aplicación*: *Los subgrupos de $\mathbb{Z}$.

***Teorema*:** Los subgrupos del grupo aditivo $\mathbb{Z}$ son los $n\mathbb{Z}$, $n \in \mathbb{N}_0$.

***Demostración*:** Ya hemos visto que los $n\mathbb{Z}$, $n \in \mathbb{N}_0$, son subgrupos de $\mathbb{Z}$; nos resta demostrar que son los únicos, o sea, que si un subconjunto *H* de $\mathbb{Z}$ es un subgrupo, entonces $\exists\ n \in \mathbb{N}_0$ tal que $H = n\mathbb{Z}$

Sea $H \underset{sg}{\subset} \mathbb{Z}$, si $H \neq 0$, entonces $H \cap \mathbb{N} \neq \phi$, puesto que si $x \in H \wedge x \neq 0$ entonces $-x \in H$, y $x \in \mathbb{N} \vee -x \in \mathbb{N}$.

Por ser $\mathbb{N}$ un conjunto bien ordenado, $H \cap \mathbb{N}$ tiene mínimo *n.*

Como $n \in H \Rightarrow n\mathbb{Z} \subset H$.

Vamos a demostrar que $H \subset n\mathbb{Z}$.

Sea $x \in H$, aplicando el Algoritmo de la División en $\mathbb{Z}$ tenemos $x = nq + r$ con $0 \leq r < n$

luego $r = x - nq$; $n \in H \Rightarrow nq \in H$, $\wedge\ x \in H \therefore r = x - nq \in H$, por ser $H \underset{sg}{\subset} \mathbb{Z}$; $r < n \wedge$

$n = mín\ H \cap \mathbb{N} \Rightarrow r \notin \mathbb{N} \therefore r = 0$.

Así $x = nq \wedge x \in n\mathbb{Z} \quad \therefore \quad H \subset n\mathbb{Z}$.

Por lo tanto hemos demostrado que los subgrupos del grupo aditivo $\mathbb{Z}$ son los $n\mathbb{Z}$, para $n \in \mathbb{N}_0$.

Ejercicios:

1. Demostrar que $n\mathbb{Z} \subset m\mathbb{Z}$ si y sólo si $m \mid n$.
2. Si se considera el conjunto de los subgrupos propios no nulos de $\mathbb{Z}$

$$\mathbb{S}(\mathbb{Z}) = \{ n\mathbb{Z} \ / \ n \in \mathbb{N} \wedge n > 1 \}.$$

2.a- $\mathbb{S}(\mathbb{Z})$ ¿ tiene máximo /o mínimo, pensado al conjunto ordenado por inclusión?

2.b- Encontrar en $\mathbb{S}(\mathbb{Z})$, si existen, elementos maximales y minimales.

***Corolario*:** Hay una correspondencia biunívoca entre los subgrupos de $\mathbb{Z}$ y $\mathbb{N}_0$.

***Demostración*:** Ya vimos que para cada $n \in \mathbb{N}_0$ hay un subgrupo de $\mathbb{Z}$, el $n\mathbb{Z}$, y que además éstos son sus únicos subgrupos. Falta demostrar que si

$$n \neq m \Rightarrow n\mathbb{Z} \neq m\mathbb{Z} \text{ para } n, m \in \mathbb{N}_0 .$$

Supongamos que para $n, m \in \mathbb{N}_0$ $n\mathbb{Z} = m\mathbb{Z}$. Entonces $n \in m\mathbb{Z} \wedge m \in n\mathbb{Z}$

$\therefore (n, m \in \mathbb{N} \wedge n \mid m \wedge m \mid n) \vee n = m = 0$.

Si $n, m \in \mathbb{N} \wedge n \mid m \wedge m \mid n \Rightarrow n = m$.

Así que en cualquier caso, si $n\mathbb{Z} = m\mathbb{Z} \Rightarrow n = m$.

Todos los ejemplos de grupos que hemos visto son grupos abelianos, pero existe una gran variedad de grupos no abelianos para cuyo estudio se recurre a estrategias bastante diferentes. Nos detendremos en un ejemplo importante de uno de estos grupos.

Grupo de permutaciones de n elementos o Grupo Simétrico

Sea $S_n = \{ \sigma \ / \ \sigma : \{1,2,3,...,n\} \to \{1,2,3,...,n\} \ biyectiva \}$. $(S_n \ , \circ)$, donde $\circ$ es la composición de funciones, es un grupo llamado *grupo de permutaciones de n elementos* o *grupo símétrico.* A sus elementos los designaremos con las letras $\sigma, \varsigma, \tau, \delta,$ etc. y los llamaremos *permutaciones.*

Una permutación $\sigma : \{1,2,3,...,n\} \to \{1,2,3,...,n\}$ es tal que $i \to \sigma(i)$, y la escribiremos $\sigma = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \dots & \sigma(n) \end{pmatrix}$. Si $\sigma, \tau \in S_n$, la operación $\tau \circ \sigma$ la notaremos así:

$$\tau \circ \sigma = \sigma\tau = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix} \begin{pmatrix} 1 & 2 & \dots & n \\ \tau(1) & \tau(2) & \dots & \tau(n) \end{pmatrix} = \begin{pmatrix} 1 & 2 & \dots & n \\ \tau\circ\sigma(1) & \tau\circ\sigma(2) & \dots & \tau\circ\sigma(n) \end{pmatrix}$$ La permutación

identidad es $\begin{pmatrix} 1 & 2 & 3 & \dots & n \\ 1 & 2 & 3 & \dots & n \end{pmatrix}$ y la llamaremos 1.

Ejemplo: $S_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \right\}$

$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$ que se interpreta $\begin{matrix} 1 \to 3 \to 3 \\ 2 \to 1 \to 2 \\ 3 \to 2 \to 1 \end{matrix}$

El grupo S_n es no abeliano para $n > 2$, por ejemplo en S_3

$$\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}\neq\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}.$$

***Teorema*:** El grupo simétrico S_n es finito y $ord(S_n) = n!$.

***Demostración*:** La haremos por inducción sobre n .
Para $n = 1$, claramente $S_1 = \{1\}$ luego $ord\,(S_1) = 1 = 1!$
Supongamos, por hipótesis inductiva, que $ord(S_n) = n!$, queremos ver que $ord(S_{n+1}) = (n + 1)\,!$.
Sea $\sigma \in S_{n+1}$ tal que $\sigma(n+1) = n+1$, la restricción $\overline{\sigma} = \sigma\big|_{\{1,2,3,\ldots,n\}} \in S_n$;
recíprocamente, para cada $\alpha \in S_n$ se puede encontrar una $\tau \in S_{n+1}$ tal que $\overline{\tau} = \alpha$, simplemente definiendo $\tau : \{1,2,3,\ldots,n,n+1\} \to \{1,2,3,\ldots,n,n+1\}$ tal que $\tau(i) = \begin{cases}\alpha(i) & si \quad 1 \le i \le n\\ n+1 & si \quad i = n+1\end{cases}$.
Llamando $H_{n+1} = \{\sigma \in S_{n+1} \;/\; \sigma(n+1) = n+1\}$, la función $\theta : H_{n+1} \to S_n$ definida por $\theta(\sigma) = \overline{\sigma}$ es una correspondencia biunívoca; por lo cual $card\,(H_{n+1}) = card\,(S_n) = n\,!$ (HI).
Sea ahora para cada i , $1 \le i \le n$, $H_i = \{\sigma \in S_{n+1} \;/\; \sigma(n+1) = i\}$, claramente $H_i \cap H_j = \phi$ $\forall i, j$, $i \neq j$, $1 \le i$, $j \le n + 1$. Además, para $1 \le i \le n$, la aplicación $\varphi_i : H_i \to H_{n+1}$ definida por $\tau \to \rho_i \circ \tau$, donde $\tau \in H_i$ y $\rho_i \in S_{n+1}$ es tal que

$$\rho_i(j) = \begin{cases} n+1 & si \quad j = i\\ i & si \quad j = n+1\\ j & si \quad j \neq i \wedge j \neq n+1\end{cases}$$

$\rho_i \circ \tau \in H_{n+1}$ pues $\rho_i \circ \tau \in S_{n+1}$ y además $(\rho_i \circ \tau)(n+1) = \rho_i(\tau(n+1)) = \rho_i(i) = n+1$.
La aplicación φ_i es biyectiva porque ρ_i es una permutación, con lo cual
$card\,(H_i) = card\,(H_{n+1}) = n\,!$ $\forall i$, $1 \le i \le n$; además $S_{n+1} = \bigcup_{i=1}^{n+1} H_i$, unión disjunta dos a dos, por lo cual $ord(S_{n+1}) = card(S_{n+1}) = \sum_{i=1}^{n+1} card(H_i) = (n + 1)\; n\,! = (n + 1)\,!$;
lo que demuestra nuestra afirmación.

Veamos aspectos importantes relativos a S_n, para lo cual introduciremos algunas definiciones.

Notación: escribiremos la permutación σ tal que $\sigma(i) = a_i$, con $a_i \in \mathbb{N}$, $1 \le a_i \le n$,

$$\sigma = \begin{pmatrix}1&2&3&\ldots&n\\ a_1&a_2&a_3&\ldots&a_n\end{pmatrix}.$$

***Definición*:** Sea $k \in \mathbb{N}$, $1 < k \le n$. Se llama *ciclo de longitud k* o *k-ciclo* , a una permutación σ que deja fijos $n - k$ elementos y que los k elementos restantes son movidos por la permutación de la manera siguiente:
$\sigma(i_1) = i_2$, $\sigma(i_2) = i_3$, $\sigma(i_3) = i_4$, . .., $\sigma(i_{k-1}) = i_k$, $\sigma(i_k) = i_1$, que también se representa

$$i_1 \to i_2 \to i_3 \to i_4 \to \ldots. \to i_{k-1} \to i_k \to i_1$$

Al ciclo descripto lo notaremos $(i_1, i_2, i_3, i_4, \ldots., i_{k-1}, i_k)$ indicando sólo los elementos movidos por la permutación, y obviando los que quedan fijos.

Al conjunto $\{ i_1 , i_2 , i_3 , i_4 , ..., i_{k-1} , i_k \}$ se lo denomina *soporte* del ciclo. Claramente ciclos distintos pueden tener igual soporte (Ver ejemplos posteriores).

Un ciclo se puede representar de diferentes maneras, por ejemplo el 3-ciclo en S_4
$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix}$ se puede representar (2 , 4 , 3) o bien (3 , 2 , 4) o (4 , 3 , 2).
El inverso de un *k*-ciclo es a su vez, un *k*-ciclo:
Si σ es un *k*-ciclo $(i_1 , i_2 , i_3 , i_4 , ..., i_{k-1} , i_k)$, esto significa que σ aplica

$$\begin{cases} i_1 \to i_2 \\ i_2 \to i_3 \\ i_3 \to i_4 \\ \quad . \\ \quad . \\ \quad . \\ i_{k-1} \to i_k \\ i_k \to i_1 \end{cases} ; \quad \sigma^{-1} \text{ aplica } \begin{cases} i_2 \to i_1 \\ i_3 \to i_2 \\ i_4 \to i_3 \\ \quad . \\ \quad . \\ \quad . \\ i_k \to i_{k-1} \\ i_1 \to i_k \end{cases} \text{, o sea es el ciclo } (i_1, i_k , i_{k-1}, ..., i_3, i_2)$$

Por lo tanto, el ciclo inverso se obtiene escribiendo la lista de elementos del ciclo dado, en sentido inverso.

***Definición*:** Un ciclo de longitud 2 o 2-ciclo se denomina *transposición*.
Si σ es una transposición entonces $\sigma^2 = 1$, o lo que es equivalente, $\sigma^{-1} = \sigma$.

Ejemplos:
1. En S_3 : (1 , 2) , (1 , 3) y (2 , 3) son las transposiciones
(1 , 3 , 2) , (1 , 2 , 3) son los 3-ciclos
(1 , 3 , 2) es el inverso de (1 , 2 , 3) .
2. En S_4 : (1,2) , (1 , 3) , (1 , 4) , (2 , 3) , (2 , 4) , (3 , 4) son las transposiciones;
(1 , 2 , 3) , (1 , 3 , 2) , (1 , 2 , 4) , (1 , 4 , 2) , (1 , 3 , 4) , (1 , 4 , 3) , (2 , 3 , 4) , (2 , 4 , 3) son los 3-ciclos;
(1 , 2 , 3 , 4) , (1 , 3 , 2, 4) , (1 , 2 , 4 , 3) , (1 , 3 , 4 , 2) , (1 , 4 , 2 , 3) , (1 , 4 , 3 , 2) son los 4-ciclos;
(1 , 2 , 3) es el inverso de (1 , 3 , 2) ; (1 , 2 , 4) es el inverso de (1 , 4 , 2) ;
(1 , 3 , 4) es el inverso de (1 , 4 , 3) ; (2 , 3 , 4) es el inverso de (2 , 4 , 3) ; (1 , 4 , 3 , 2) es el inverso de (1 , 2 , 3 , 4) ; (1 , 3 , 2, 4) es el inverso de (1 , 4 , 2 , 3) ; (1 , 2 , 4 , 3) es el inverso de (1 , 3 , 4 , 2).

***Proposición*:** El orden de un ciclo coincide con su longitud.

***Demostración*:** Sea $\sigma \in S_n$ un ciclo de longitud *k* , y $\{ i_1 , i_2 , i_3 , i_4 , ..., i_{k-1} , i_k \}$ su soporte.

$$\begin{cases} \sigma(i_1) = i_2 \\ \sigma(i_2) = i_3 \\ \sigma(i_3) = i_4 \\ \quad . \\ \quad . \\ \quad . \\ \sigma(i_{k-1}) = i_k \\ \sigma(i_k) = i_1 \end{cases} ; \begin{cases} \sigma^2(i_1) = i_3 \\ \sigma^2(i_2) = i_4 \\ \sigma^2(i_3) = i_5 \\ \quad . \\ \quad . \\ \quad . \\ \sigma^2(i_{k-1}) = i_1 \\ \sigma^2(i_k) = i_2 \end{cases} , \begin{cases} \sigma^3(i_1) = i_4 \\ \sigma^3(i_2) = i_5 \\ \quad . \\ \quad . \\ \quad . \\ \sigma^3(i_{k-2}) = i_1 \\ \sigma^3(i_{k-1}) = i_2 \\ \sigma^3(i_k) = i_3 \end{cases} ; \ldots ; \begin{cases} \sigma^j(i_1) = i_{j+1} \\ \sigma^j(i_2) = i_{j+2} \\ \quad . \\ \quad . \\ \quad . \\ \sigma^j(i_{k-j}) = i_k \\ \sigma^j(i_{k-j+1}) = i_1 \\ \quad . \\ \quad . \\ \quad . \\ \sigma^j(i_{k-1}) = i_{j-1} \\ \sigma^j(i_k) = i_j \end{cases}$$

$$\begin{cases} \sigma^{k-1}(i_1) = i_k \\ \sigma^{k-1}(i_2) = i_1 \\ \sigma^{k-1}(i_3) = i_2 \\ \quad . \\ \quad . \\ \quad . \\ \sigma^{k-1}(i_{k-1}) = i_{k-2} \\ \sigma^{k-1}(i_k) = i_{k-1} \end{cases} ; \begin{cases} \sigma^k(i_1) = i_1 \\ \sigma^k(i_2) = i_2 \\ \sigma^k(i_3) = i_3 \\ \quad . \\ \quad . \\ \quad . \\ \sigma^k(i_{k-1}) = i_{k-1} \\ \sigma^k(i_k) = i_k \end{cases}$$

o sea $\sigma^k = 1 \ \wedge \ \sigma^j \neq 1 \ \ \forall j = 1, 2, ..., k-1 \ \therefore \ ord(\sigma) = k$.

***Definición*:** Dos ciclos de S_n se dicen *disjuntos* si sus soportes son conjuntos disjuntos.

Observación: σ y τ son dos ciclos disjuntos si y sólo si se verifica que, para $1 \leq x \leq n$,

$$\begin{cases} \sigma(x) \neq x \ \Rightarrow \ \tau(x) = x \\ \tau(x) \neq x \ \Rightarrow \sigma(x) = x \end{cases}$$

***Proposición*:** Dos ciclos disjuntos de S_n conmutan.

***Demostración*:** Si σ y τ son dos ciclos disjuntos de soportes *A* y *B* respectivamente, entonces $A \cap B = \phi$.

Sea $x \in \{ 1, 2, 3, ..., n \}$, calculemos $(\tau \circ \sigma)(x)$ y $(\sigma \circ \tau)(x)$.

✓ Sea $x \in A$, entonces $(\tau \circ \sigma)(x) = \tau(\sigma(x))$; como $x \in A$, entonces $\sigma(x) \in A$, luego $\sigma(x) \notin B$, con lo cual $\tau(\sigma(x)) = \sigma(x)$.

Por otra parte $(\sigma\circ\tau)(x) = \sigma(\tau(x)) = \sigma(x)$, pues si $x\in A$, entonces $\sigma(x)\neq x$ de donde $\tau(x) = x$. Por lo tanto $(\tau\circ\sigma)(x) = (\sigma\circ\tau)(x)\ \ \forall x\in A$.

✓ Sea $x\in B$, $(\tau\circ\sigma)(x) = \tau(\sigma(x)) = \tau(x)$, pues si $x\in B \Rightarrow\ x\notin A\ \wedge\ \sigma(x) = x$

$(\sigma\circ\tau)(x) = \sigma(\tau(x)) = \tau(x)$, pues si $x\in B$ se tiene que $\tau(x)\in B\ \Rightarrow \tau(x)\notin A$ $\wedge\ \sigma(\tau(x)) = \tau(x)$. Así $(\tau\circ\sigma)(x) = (\sigma\circ\tau)(x)\ \ \forall x\in B$.

✓ Sea $x\notin A\cup B$, $\tau(x) = \sigma(x) = x$, luego $(\tau\circ\sigma)(x) = \tau(x) = x\ \wedge$ $(\sigma\circ\tau)(x) = \sigma(\tau(x)) = \sigma(x) = x$, luego $(\tau\circ\sigma)(x) = (\sigma\circ\tau)(x)\ \ \forall x\notin A\cup B$.

Así hemos demostrado que $\sigma\circ\tau = \tau\circ\sigma$.

***Teorema*:** En S_n toda permutación $\sigma\neq 1$ es producto finito de ciclos disjuntos. Además la descomposición es única salvo el orden de los factores.

***Demostración*:**
Existencia de la factorización:
Sea $\sigma\neq 1$, $\sigma:\{1,2,3,...,n\}\to\{1,2,3,...,n\}$ biyectiva, $j\to\sigma(j) = i_j$; como $\sigma\neq 1\ \exists j$, $1\le j\le n$, tal que $\sigma(j)\neq j$. Sea $i_1 = mín\{\ j\ /\ 1\le j\le n\ \wedge\ \sigma(j)\neq j\ \}$
Como i_1 es un índice movido por la permutación σ , será $\sigma(i_1) = i_2$, $\sigma(i_2) = i_3$, $\sigma(i_3) = i_4$, . .., $\sigma(i_{s-1}) = i_s$ …., o , con la notación anterior

$$i_1\to i_2\to i_3\to i_4\to ....\to i_{s-1}\to i_s\to ....$$

Esta sucesión es finita porque los i_t pertenecen a un conjunto finito y son distintos dos a dos porque σ es biyectiva, con lo cual $\exists h$, $1\le h\le n$ tal que $i_h = i_s$ para algún $s < h$.
Sea $k+1 = mín\{\ h\in\mathbb{N}\ /\ \exists s < h\ \ tal\ que\ \ i_s = i_h\ \}$ y sea $t < k$ tal que $i_t = i_{k+1}$;
$t = 1$, pues si $t > 1$, $\sigma(i_{t-1}) = i_t = i_{k+1} = \sigma(i_k)$ de donde $i_k = i_{t-1}$, lo que contradice la elección de $k+1$. Entonces $\sigma(i_k) = i_1$ y tenemos el k-ciclo

$$i_1\to i_2\to i_3\to i_4\to ....\to i_{k-1}\to i_k\to i_1$$

Si $k = n$, σ es un n-ciclo, y no hay nada más que demostrar.
Si $k < n$ y $\sigma(j) = j\ \ \forall j\in\{1,2,...,n\}-\{i_1,i_2,...,i_k\}$, entonces σ es un k-ciclo; si en cambio $\exists\, j\in\{1,2,...,n\}-\{i_1,i_2,...,i_k\}$ tal que $\sigma(j)\neq j$, tomemos j_1 el mínimo con esa propiedad, como antes tendremos una sucesión de elementos movidos por σ

$$j_1\to j_2\to j_3\to j_4\to ....\to j_{r-1}\to j_r\to ....$$

e igual que antes, esta sucesión es finita, con elementos distintos dos a dos

$$j_1\to j_2\to j_3\to j_4\to ....\to j_{h-1}\to j_h\to j_1$$

con lo cual es un h-ciclo.
Si $\exists\, j\in\{1,2,...,n\}-\{i_1,i_2,...,i_k,j_1,j_2,...,j_h\}$ tal que $\sigma(j)\neq j$ sea q_1 el mínimo con esa propiedad, y se reitera el proceso. Continuamos así hasta agotar los j que son movidos por la permutación y quedan afuera de los ciclos encontrados.

Los ciclos encontrados son disjuntos dos a dos: por construcción los primeros elementos de cada ciclo son diferentes y no pertenecen al soporte de cada uno de los otros ciclos. Si existiera, por ejemplo, un $i_r = j_u$, $r > 1$, $u > 1$ entonces $\sigma(i_{r-1}) = \sigma(j_{u-1})$, con lo cual $i_{r-1} = j_{u-1}$, y así sucesivamente, con lo que llegaríamos a que $i_1 = j_t \vee i_q = j_1$ para algún *t* o algún *q* !!(absurdo).
Claramente $\sigma = (i_1, i_2, i_3, i_4, ..., i_{k-1}, i_k)\,(j_1, j_2, j_3, ..., j_{h-1}, j_h) \ldots (l_1, l_2, l_3, ..., l_{s-1}, l_s)$.

Unicidad:
Sea $c_1c_2...c_r = d_1d_2...d_s$ dos descomposiciones de σ como ciclos disjuntos.
Haremos inducción sobre *r* :
Si $r = 1$, $c_1 = d_1d_2...d_s$. Como los ciclos son disjuntos, el primer elemento de c_1 pertenece al soporte de uno y sólo uno de los d_j , que como son ciclos que conmutan, podemos suponer que es d_1 . Como los elementos del soporte de c_1 son movidos dentro de ese conjunto, entonces $c_1 = d_1$. Si $s > 1$ entonces $1 = d_2d_3...d_s$!!(absurdo) pues la *id* no mueve elementos, entonces $s = 1$.

HI: Supongamos que todo producto de r ciclos disjuntos se factorice de manera única.

Sea ahora $c_1c_2...c_rc_{r+1} = d_1d_2...d_s$. Razonando como antes, el primer elemento del soporte de c_1 debe estar en el soporte de algún d_j , que al ser ciclos disjuntos, conmutan, luego podemos suponer que es d_1 , con lo cual (como antes) tendremos que $c_1 = d_1$. Como los ciclos son inversibles, $c_1c_2...c_rc_{r+1} = d_1d_2...d_s \Rightarrow c_2c_3...c_rc_{r+1} = d_2d_3...d_s$, y por HI, $r = s - 1$ y para cada i , $2 \le i \le r + 1$ $\exists\, j_i$, $2 \le j_i \le s = r + 1$ tal que $c_i = d_{j_i}$.
Luego, la descomposición en ciclos disjuntos es única, salvo por el orden en que están escritos.

Nota: Si σ y τ son dos permutaciones en S_n que conmutan, entonces

$$(\tau \circ \sigma)^k = \tau^k \circ \sigma^k .$$

Si $k = 2$ $\quad (\tau \circ \sigma)^2 = (\tau \circ \sigma) \circ (\tau \circ \sigma) = \tau \circ \sigma \circ \tau \circ \sigma = \tau \circ \tau \circ \sigma \circ \sigma = \tau^2 \circ \sigma^2$.
Razonando por inducción se demuestra $\forall k \ge 2$.

***Proposición*:** Si $c_1, c_2, ..., c_r$ son ciclos disjuntos, de órdenes $k_1, k_2, ..., k_r$ respectivamente, entonces el $o(c_1c_2...c_r) = [\,k_1\,, k_2\,, \ldots, k_r\,]$ (mínimo común múltiplo de $k_1\,, k_2\,, \ldots, k_r$)

***Demostración*:** Sea $k = [\,k_1\,, k_2\,, \ldots, k_r\,]$ $\quad (c_1c_2...c_r)^k = c_1^k c_2^k ... c_r^k = 1.1....1 = 1$, pues $k_i \mid k \;\; \forall i = 1, 2, ..., r$, entonces $o(c_1c_2...c_r) \mid k = [\,k_1\,, k_2\,, \ldots, k_r\,]$
Si $(c_1c_2....c_r)^m = 1$ entonces $c_1^m c_2^m c_3^m ... c_r^m = 1$. Si $\exists\, j$, $1 \le j \le r$ tal que $c_j^m \ne 1$ entonces c_j^m mueve elementos en el soporte de c_j , y su inverso mueve elementos en ese mismo conjunto!! (absurdo) pues el soporte de c_j es disjunto con el conjunto de los elementos movidos por

$c_1^m c_2^m,..c_{j-1}^m c_{j+1}^m ... c_r^m$. Luego $c_j^m = 1$, por lo que $k_j \mid m \quad \forall j = 1,2,...,r$, entonces $k = [\, k_1 , k_2 , ... , k_r \,] \mid m$.

Luego $o(c_1 c_2 ... c_r) = [\, k_1 , k_2 , ... , k_r \,]$.

Ejemplos:

i. $\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 5 & 1 & 6 & 4 & 7 & 3 \end{pmatrix}$ es el 7-ciclo (1, 2, 5, 4, 6, 7, 3), $o(\sigma_1) = 7$

ii. $\sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 2 & 5 & 7 & 1 & 4 & 6 \end{pmatrix}$; $\sigma_2 =$ (1, 3, 5)(4, 7, 6) , $o(\sigma_2) = 3$

iii. $\sigma_3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 6 & 2 & 5 & 4 & 3 \end{pmatrix}$; $\sigma_3 =$ (2, 6, 3)(4, 5) , $o(\sigma_3) = 6$

***Proposición*:** Todo ciclo es producto de transposiciones.

***Demostración*:** El ciclo $(i_1 , i_2 , i_3 , i_4 , ..., i_{k-1} , i_k) = (i_{k-1}, i_k)(i_{k-2}, i_{k-1}).....(i_2, i_3)(i_1, i_2)$
pues si llamamos $\tau_j = (i_j , i_{j+1})$, $j = 1,2,\ldots, k$

$\tau_{k-2} \circ \tau_{k-1} = \tau_{k-1}\tau_{k-2}$ mueve los índices $\begin{cases} i_{k-1} \xrightarrow{\tau_{k-1}} i_k \xrightarrow{\tau_{k-2}} i_k \\ i_{k-2} \xrightarrow{\tau_{k-1}} i_{k-2} \xrightarrow{\tau_{k-2}} i_{k-1} \\ i_k \xrightarrow{\tau_{k-1}} i_{k-1} \xrightarrow{\tau_{k-2}} i_{k-2} \end{cases}$ y los demás quedan fijos

$\tau_{k-1}\tau_{k-2}\tau_{k-3}$ mueve los índices $\begin{cases} i_{k-3} \xrightarrow{\tau_{k-1}} i_{k-3} \xrightarrow{\tau_{k-2}} i_{k-3} \xrightarrow{\tau_{k-3}} i_{k-2} \\ i_{k-2} \xrightarrow{\tau_{k-1}} i_{k-2} \xrightarrow{\tau_{k-2}} i_{k-1} \xrightarrow{\tau_{k-3}} i_{k-1} \\ i_{k-1} \xrightarrow{\tau_{k-1}} i_k \xrightarrow{\tau_{k-2}} i_k \xrightarrow{\tau_{k-3}} i_k \\ i_k \xrightarrow{\tau_{k-1}} i_{k-1} \xrightarrow{\tau_{k-2}} i_{k-2} \xrightarrow{\tau_{k-3}} i_{k-3} \end{cases}$ y los demás quedan fijos.

Y así sucesivamente…

$\tau_{k-1}\tau_{k-2}\tau_{k-3}....\tau_2\tau_1$ mueve los índices:

$$\begin{cases} i_1 \xrightarrow{\tau_{k-1}} i_1 \xrightarrow{\tau_{k-2}} i_1 \xrightarrow{\tau_{k-3}} i_1 \;.......\; i_1 \xrightarrow{\tau_3} i_1 \xrightarrow{\tau_2} i_1 \xrightarrow{\tau_1} i_2 \\ i_2 \xrightarrow{\tau_{k-1}} i_2 \xrightarrow{\tau_{k-2}} i_2 \xrightarrow{\tau_{k-3}} i_2 \;.......\; i_2 \xrightarrow{\tau_3} i_2 \xrightarrow{\tau_2} i_3 \xrightarrow{\tau_1} i_3 \\ i_3 \xrightarrow{\tau_{k-1}} i_3 \xrightarrow{\tau_{k-2}} i_3 \xrightarrow{\tau_{k-3}} i_3 \;.......\; i_3 \xrightarrow{\tau_3} i_4 \xrightarrow{\tau_2} i_4 \xrightarrow{\tau_1} i_4 \\ \qquad . \\ \qquad . \\ \qquad . \\ i_{k-3} \xrightarrow{\tau_{k-1}} i_{k-3} \xrightarrow{\tau_{k-2}} i_{k-3} \xrightarrow{\tau_{k-3}} i_{k-2} \xrightarrow{\tau_{k-4}} i_{k-2} \;....\; i_{k-2} \xrightarrow{\tau_2} i_{k-2} \xrightarrow{\tau_1} i_{k-2} \\ i_{k-2} \xrightarrow{\tau_{k-1}} i_{k-2} \xrightarrow{\tau_{k-2}} i_{k-1} \xrightarrow{\tau_{k-3}} i_{k-1} \;.....\; i_{k-1} \xrightarrow{\tau_2} i_{k-1} \xrightarrow{\tau_1} i_{k-1} \\ i_{k-1} \xrightarrow{\tau_{k-1}} i_k \xrightarrow{\tau_{k-2}} i_k \xrightarrow{\tau_{k-3}} i_k \;......\; i_k \xrightarrow{\tau_2} i_k \xrightarrow{\tau_1} i_k \\ i_k \xrightarrow{\tau_{k-1}} i_{k-1} \xrightarrow{\tau_{k-2}} i_{k-2} \xrightarrow{\tau_{k-3}} i_{k-3} \;......\; i_4 \xrightarrow{\tau_3} i_3 \xrightarrow{\tau_2} i_2 \xrightarrow{\tau_1} i_1 \end{cases}$$

y los demás quedan fijos, siendo así el ciclo $(i_1, i_2, i_3, i_4, ..., i_{k-1}, i_k)$.

***Corolario*:** Toda permutación se puede escribir como producto de transposiciones.

Nota: La descomposición de una permutación en producto de transposiciones no es única, pero sí se puede demostrar que cualesquiera sean las descomposiciones de σ todas tendrán un número par de transposiciones o todas un número impar; no es posible encontrar una descomposición con un número par de transposiciones y otra con un número impar de ellas para la misma permutación.
La no unicidad de la descomposición de una permutación en producto de transposiciones no contradice el teorema demostrado anteriormente, que toda permutación se factoriza como producto de únicos ciclos disjuntos, pudiendo sólo alterarse el orden de éstos, porque las transposiciones que aparecen en la descomposición de la permutación son ciclos sí, pero no necesariamente disjuntos dos a dos.

- ❖ Queremos analizar, ahora, cuál es el efecto de una transposición sobre un ciclo
  - ✓ *La transposición mueve dos elementos de un ciclo*

1. $(k, i_1, i_2, i_3, ..., i_r, h, j_1, j_2, ..., j_s)(k, h) = (k, i_1, i_2, ..., i_r)(h, j_1 j_2, ..., j_s)$

   pues $\begin{pmatrix} k & i_1 & i_2 & . & . & . & i_{r-1} & i_r & h & j_1 & j_2 & . & . & . & j_{s-1} & j_s \\ i_1 & i_2 & i_3 & . & . & . & i_r & h & j_1 & j_2 & j_3 & . & . & . & j_s & k \end{pmatrix} \begin{pmatrix} . & . & k & . & . & h & . & . \\ . & . & h & . & . & k & . & . \end{pmatrix} =$

   $= \begin{pmatrix} k & i_1 & i_2 & . & . & . & i_r \\ i_1 & i_2 & i_3 & . & . & . & k \end{pmatrix} \begin{pmatrix} h & j_1 & j_2 & . & . & . & j_s \\ j_1 & j_2 & j_3 & . & . & . & h \end{pmatrix}$

2. $(k, i_1, i_2, ..., i_r, h)(k, h) = (k, i_1, i_2, ..., i_r)$

   $\begin{pmatrix} k & i_1 & . & . & . & i_{r-1} & i_r & h \\ i_1 & i_2 & . & . & . & i_r & h & k \end{pmatrix} \begin{pmatrix} . & . & k & . & . & h & . & . \\ . & . & h & . & . & k & . & . \end{pmatrix} =$

   $= \begin{pmatrix} k & i_1 & . & . & . & i_{r-1} & i_r & h \\ i_1 & i_2 & . & . & . & i_r & k & h \end{pmatrix} = (k, i_1, i_2, ..., i_r)$

  - ✓ *La transposición mueve elementos de ciclos distintos*

3. $(k, i_1, i_2, ..., i_r)(h, j_1 j_2, ..., j_s)(k, h) = (k, i_1, i_2, i_3, ..., i_r, h, j_1, j_2, ..., j_s)$

   Por 1. tenemos la identidad

   $(k, i_1, i_2, i_3, ..., i_r, h, j_1, j_2, ..., j_s)(k, h) = (k, i_1, i_2, ..., i_r)(h, j_1 j_2, ..., j_s)$

   multiplicando ambos miembros de la igualdad por (k, h)

   $(k, i_1, i_2, i_3, ..., i_r, h, j_1, j_2, ..., j_s)(k, h)^2 = (k, i_1, i_2, ..., i_r)(h, j_1 j_2, ..., j_s)(k, h)$

   siendo $(k, h)^2 = 1$, obtenemos la igualdad buscada.

4. $(k, h)(k, i_1, i_2, ..., i_r) = (k, i_1, i_2, ..., i_r, h)$.

   Para demostrar esta identidad se razona de la misma manera que en 3.

Sea $\sigma \in S_n$, si $\sigma \neq 1$, $\sigma = c_1, c_2, ..., c_r$, donde los c_j son ciclos disjuntos dos a dos, de órdenes $k_1, k_2, ..., k_r$ respectivamente. Llamaremos $N(\sigma)$ al número asociado a la permutación σ, definido por: $N(\sigma) = \sum_{j=1}^{r} k_j - r$, o sea, la suma de las longitudes de los ciclos disjuntos que la

factorizan menos el número de ellos. Observemos que $N(\sigma)$ está unívocamente determinado por σ dado que la factorización en ciclos disjuntos es única (salvo por el orden en que se operan).
Definimos, además, $N(1)=0$.
Si τ es una transposición, claramente $N(\tau)=1$.

***Proposición*:** Sea $\sigma \in S_n$, $\sigma \neq 1$. Si σ se escribe como producto de *m* transposiciones, entonces $m \equiv N(\sigma) \pmod 2$.

***Demostración*:** Veamos, primero, que si τ es una transposición, $N(\sigma\tau)=N(\sigma)\pm 1$.

- Si τ no mueve los índices de los ciclos de σ, τ es un ciclo disjunto de los c_j, con lo cual la factorización en ciclos disjuntos de $\sigma\tau = c_1, c_2, ..., c_r\ \tau$, de donde

$$N(\sigma\tau)=\sum_{j=1}^{r} k_j + 2 - (r+1) = N(\sigma)+1 .$$

- Si τ mueve sólo un índice de los ciclos de σ, estamos en la situación 4. analizada previamente, en la cual $c_s\tau$ es un ciclo (c_s el ciclo afectado por τ).

Por lo tanto $N(\sigma)=\sum_{j=1}^{r} k_j + 1 - r = N(\sigma)+1$ pues $c_s\tau$ es un (k_s+1)-ciclo.

- Si τ mueve los índices de ciclos diferentes de σ, si c_s y c_t son los ciclos afectados por τ , por 3. tenemos que $c_s c_t \tau$ es un $(c_s + c_t)$ - ciclo, y $\sigma\tau$ se factoriza como producto de $r-1$ ciclos, por lo que

$$N(\sigma\tau)=\sum_{j=1}^{r} k_j - (r-1) = N(\sigma)+1 .$$

- Si τ mueve dos índices de un ciclos de σ, estamos en alguna de las situaciones de 1. o 2. En el caso 1. , $\sigma\tau$ se escribe como producto de (*r* + 1) ciclos disjuntos, donde la suma de las longitudes de los ciclos que factorizan σ coincide con la suma de las longitudes de los ciclos que factorizan $\sigma\tau$, por lo cual $N(\sigma\tau)=N(\sigma)-1$.

  En el caso 2. , la cantidad de ciclos que factorizan σ es la misma que la de $\sigma\tau$; si c_s es el ciclo cuyos índices son movidos por la transposición τ, el ciclo $c_s\tau$ tiene longitud $k_s - 1$, con lo cual $N(\sigma\tau)=N(\sigma)-1$.

Demostremos ahora que si σ se escribe como producto de *m* transposiciones, entonces $m \equiv N(\sigma) \pmod 2$. Haremos inducción sobre *m* .
Si *m* = 1 , σ es una transposición y $N(\sigma)=1$.
Sea *m* > 1 y supongamos que toda permutación que se escriba como producto de *m* – 1 transposiciones verifica la hipótesis.
Sea $\sigma = \tau_m \tau_{m-1} .... \tau_2 \tau_1$, donde τ_j son transposiciones $\forall j = 1, 2, ..., m$.
Si llamamos $\rho = \tau_{m-1} \tau_{m-2} .... \tau_2 \tau_1$, $\rho \in S_n$ y se escribe como producto de *m* – 1 transposiciones; por hipótesis inductiva $N(\rho) \equiv m-1 \pmod 2$, y como $\sigma = \tau_m \rho$, entonces $N(\sigma) = N(\rho) \pm 1$, por lo tanto $m \equiv N(\sigma) \pmod 2$.

***Corolario*:** Dos descomposiciones de una permutación en producto de transposiciones tienen ambas un número par de ellas, o bien un número impar.

***Demostración*:** Es inmediata a partir de la proposición, pues el número $N(\sigma)$ está unívocamente determinado por la permutación σ.

***Definición*:** Sea $\sigma \in S_n$. Se dice que σ es una *permutación par* si se descompone como producto de un número par de transposiciones; en caso contrario, se dice que la permutación es *impar* .

***Definición*:** Se llama *signo* de la permutación σ a $sg(\sigma) = \begin{cases} 1 & si\ \sigma\ es\ par \\ -1 & si\ \sigma\ es\ impar \end{cases}$

$sg(1) = 1$ puesto que $\tau\tau = 1$ para toda transposición τ ; $sg(\tau) = -1$.

Ejemplos:

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 6 & 2 & 1 & 9 & 8 & 3 & 7 & 5 & 4 \end{pmatrix} = (1,6,3)(4,9)(5,8) = (6,3)(1,6)(4,9)(5,8)$$

puesto que (1, 6, 3) = (6, 3)(1, 6) $\therefore\ sg(\sigma_1) = 1$, o sea, σ_1 es una permutación par.

$$\sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 6 & 9 & 4 & 1 & 8 & 3 & 5 & 7 & 2 \end{pmatrix} = (1,6,3,4)(2,9)(5,8,7) =$$

$$= (3,4)(6,3)(1,6)(2,9)(8,7)(5,8)$$ por ser (1, 6, 3, 4) = (3, 4)(6, 3)(1, 6)

y (5, 8, 7) = (8, 7)(5, 8) $\therefore\ sg(\sigma_2) = 1$, σ_2 es una permutación par.

$$\sigma_3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 6 & 9 & 8 & 1 & 4 & 3 & 5 & 7 & 2 \end{pmatrix} = (1,6,3,8,7,5,4)(2,9) =$$

= (5, 4)(7,5)(8, 7)(3, 8)(6, 3)(1, 6)(2, 9)

$\therefore\ sg(\sigma_3) = -1$, σ_3 es una permutación impar.

Homomorfismo de grupos:

***Definición*:** Sean $(G, *)$, $(H, \bullet)$ grupos; $f : G \to H$ una función.

Decimos que *f* es un *homomorfismo de grupos* si verifica:

$$f(a * a') = f(a) \bullet f(a')\ \forall a, a' \in A .$$

Ejemplos: Son homomorfismos de grupos:

1. $f : \mathbb{Z} \to n\mathbb{Z}$ definida por $f(k) = nk$.
2. $\varphi : \mathbb{Z} \to \mathbb{Z}_n$ definida por $\varphi(k) = \overline{k}$, $\forall k \in \mathbb{Z}$, (proyección canónica al cociente) .
3. $ln : \mathbb{R}_{>0} \to \mathbb{R}$ (logaritmo natural) del grupo $(\mathbb{R}_{>0}, \cdot)$ en el grupo $(\mathbb{R}, +)$.
4. $\exp_2 : \mathbb{R} \to \mathbb{R}^*$, $x \to 2^x$, del grupo $(\mathbb{R}, +)$ en el grupo $(\mathbb{R}^*, \cdot)$.

5. $id : G \to G$, $id(x) = x$ (homomorfismo identidad).
6. Si $H \underset{sg}{\subset} G$, $i : H \to G$, $i(x) = x$ (homomorfismo inclusión).

***Propiedades*:** Sean $(G, *)$, $(H, \bullet)$ grupos con neutros e y e' respectivamente; $f : G \to H$ homomorfismo de grupos. Entonces:

i. $f(e) = e'$.
ii. $f(a^{-1}) = (f(a))^{-1} \ \forall a \in G$.
iii. En general $f(a^n) = (f(a^n)) \ \forall n \in \mathbb{Z}$.

***Demostración*:**

i. $f(e) = f(e * e) = f(e) \bullet f(e)$

como $f(e) \in H$, y H es un grupo, $f(e)$ tiene inverso; operando m.a.m. $(f(e))^{-1}$

$$(f(e))^{-1} \bullet f(e) = (f(e))^{-1} \bullet [f(e) \bullet f(e)] = [(f(e))^{-1} \bullet f(e)] \bullet f(e)$$
$$e' = e' \bullet f(e) = f(e)$$
$$\therefore \ f(e) = e' .$$

ii. $a^{-1} * a = a * a^{-1} = e \Rightarrow f(a^{-1} * a) = f(a * a^{-1}) = f(e) = e'$.

como f es homomorfismo de grupos

$$f(a^{-1} * a) = f(a^{-1}) \bullet f(a) = f(a * a^{-1}) = f(a) \bullet f(a^{-1}) = e' .$$

Luego $f(a^{-1})$ es el inverso de $f(a)$ $\therefore$ $f(a^{-1}) = (f(a))^{-1}$.

iii. Queda como ejercicio.

***Teorema*:** Sean $(G, *)$, $(H, \bullet)$, $(T, \otimes)$ grupos; $f : G \to H$, $g : H \to T$ homomorfismos de grupos. Entonces la función $g \circ f : G \to T$ es también un homomorfismo de grupos.

***Demostración*:** Debemos demostrar que si

$$x_1 , x_2 \in G \Rightarrow (g \circ f)(x_1 * x_2) = (g \circ f)(x_1) \otimes (g \circ f)(x_2)$$

por definición de composición $(g \circ f)(x_1 * x_2) = g(f((x_1 * x_2))) =$

por ser f un homomorfismo de grupos $= g(f(x_1) \bullet f(x_2)) =$

por ser g un homomorfismo de grupos $= g(f(x_1)) \otimes (g(f(x_2))) =$

$$= (g \circ f)(x_1) \otimes (g \circ f)(x_2)$$

como se quería demostrar.

***Definiciones*:** Sean G , H grupos; $f : G \to H$ homomorfismo de grupos. Decimos que:

- f es *monomorfismo* si f es inyectiva.
- f es *epimorfismo* si f es suryectiva.
- f es *isomorfismo* si f es biyectiva.
- f es *endomorfismo* si los grupos G y H coinciden.

- f es *automorfismo* si es endomorfismo biyectivo.

> *Los escritos de Galois, y sólo parcialmente, no se conocieron hasta 1846 por obra de Liouville; Jules Tannery los completó en 1910. En esos escritos asoman la idea de "cuerpo" desarrolladas luego por Riemann y Dedekind, que Galois introduce con motivo de los hoy llamados "imaginarios de Galois", y las propiedades más importantes de la teoría de grupos, nombre que él acuña en el sentido actual de clase cerrada respecto de la adición y sustracción. Sin duda que esta noción, en especial referida al grupo de sustituciones, estaba esbozada en los trabajos de Lagrange y Vandermonde del siglo XVIII y en los de Gauss, Abel, Ruffini y Cauchy del XIX, e implícita en problemas de teoría de las ecuaciones, teoría de números y de transformaciones geométricas, pero será Galois quien muestre una idea clara de la teoría general, con las nociones de subgrupo y de isomorfismo.*
>
> Historia de la Matemática.- vol 2- Julio Rey Pastor y José Babini.

Ejemplos: En los ejemplos anteriores, $\varphi : \mathbb{Z} \to \mathbb{Z}_n$ es epimorfismo;
$id_G : G \to G$ es automorfismo,
$f : \mathbb{Z} \to n\mathbb{Z}$, $ln : \mathbb{R}_{>0} \to \mathbb{R}$ son isomorfismos;
$i : H \to G$, $\exp_2 : \mathbb{R} \to \mathbb{R}^*$ son monomorfismos.

Ejercicios:
1. La composición de monomorfismos es un monomorfismo.
2. La composición de epimorfismos es un epimorfismo.
3. La composición de isomorfismos es un isomorfismo.
4. La función inversa de un isomorfismo es también un isomorfismo.

***Definición*:** Dos grupos G y H se dicen *isomorfos* si $\exists f$, $f : G \to H$ isomorfismo de grupos.

Notación: Cuando G y H sean isomorfos, lo notaremos $G \approx H$

Ejercicio: El isomorfismo de grupos es una relación de equivalencia.

***Definición*:** Sean G , H grupos; $f : G \to H$ homomorfismo de grupos. Llamamos *núcleo de f* al conjunto $Ker(f) = \{ x \in G \ / \ f(x) = e' \}$, donde e' es el neutro de H.

***Proposición*:** Con las notaciones anteriores, tenemos que $Ker(f) \underset{sg}{\subset} G$ e $Im(f) \underset{sg}{\subset} H$.

***Demostración*:** $Ker(f) \neq \phi$ puesto que $f(e) = e'$, entonces $e \in Ker(f)$.

Sean $x , y \in Ker(f)$, $x * y^{-1} \overset{?}{\in} Ker(f)$.
Para responder esa pregunta debemos calcular $f(x * y^{-1})$

$f(x * y^{-1}) = f(x) \bullet f(y^{-1}) = f(x) \bullet (f(y))^{-1} = e' \bullet (e')^{-1} = (e')^{-1} = e'$ luego $x * y^{-1} \in Ker(f)$.

Por lo tanto $Ker(f) \underset{sg}{\subset} G$.

Para demostrar que $Im(f) \underset{sg}{\subset} H$, observemos primero que $Im(f) \neq \phi$ puesto que $f(e) = e'$

y así $e' \in Im(f)$.

Si $v, w \in Im(f)$ $\exists x , y \in G$ tales que $f(x) = v \wedge f(y) = w$

$v \bullet w^{-1} = f(x) \bullet (f(y))^{-1} = f(x) \bullet f(y^{-1}) = f(x * y^{-1}) \Rightarrow v \bullet w^{-1} \in Im(f)$

$\therefore Im(f) \underset{sg}{\subset} H.$

***Proposición*:** Sean G , H grupos, $f : G \to H$ homomorfismo de grupos.
f es monomorfismo si y sólo si $Ker(f) = \{ e \}$.

***Demostración*:** $\Rightarrow$) Sea f monomorfismo, por lo tanto es inyectiva.

Si $x \in Ker(f) \Rightarrow f(x) = e' = f(e)$, y por ser inyectiva $x = e$.

$\Leftarrow$) Supongamos que $Ker(f) = \{ e \}$, queremos ver que f es inyectiva.

Sean $x , y \in G$ tales que $f(x) = f(y) \Rightarrow f(x) \bullet (f(y))^{-1} = e'$

pero $f(x) \bullet (f(y))^{-1} = f(x * y^{-1}) = e' \Rightarrow x * y^{-1} \in Ker(f)$, como $Ker(f) = \{ e \}$,

$x * y^{-1} = e$, operando m.a.m. por y obtenemos que $x = y$, luego f es inyectiva.

***Proposición*:** Sean $(G , *)$, $(H , \bullet)$ grupos con neutros e y e' respectivamente;
$f : G \to H$ homomorfismo de grupos, $G' \underset{sg}{\subset} G$, $H' \underset{sg}{\subset} H$. Entonces:

i. $f(G') \underset{sg}{\subset} H.$

ii. $f^{-1}(H') \underset{sg}{\subset} G.$

***Demostración*:**

i. $f(G') = \{ f(x) \ / \ x \in G' \} \neq \phi$ puesto que $e \in G'$ por ser $G' \underset{sg}{\subset} G \wedge f(e) = e'$

$\Rightarrow e' \in f(G')$.

Si $v , w \in f(G')$ $\exists x , y \in G'$ tales que $f(x) = v \wedge f(y) = w$, ¿ $v \bullet w^{-1} \in f(G')$?

$v \bullet w^{-1} = f(x) \bullet (f(y))^{-1} = f(x) \bullet f(y^{-1}) = f(x * y^{-1})$

$\Rightarrow v \bullet w^{-1} \in f(G')$ pues $x * y^{-1} \in G'$ por ser $G' \underset{sg}{\subset} G$

$\therefore f(G') \underset{sg}{\subset} H.$

ii. $f^{-1}(H') = \{ x \in G \ / \ f(x) \in H' \} \neq \phi$ puesto que $e' \in H'$ por ser $H' \underset{sg}{\subset} H \wedge$

$f(e) = e' \Rightarrow e \in f^{-1}(H')$.

Sean $x , y \in f^{-1}(H') \therefore f(x) \in H' \wedge f(y) \in H'$; ¿ $x * y^{-1} \in f^{-1}(H')$?

$f(x * y^{-1}) = f(x) \bullet f(y^{-1}) = f(x) \bullet (f(y))^{-1} \in H'$ por ser $H' \underset{sg}{\subset} H \therefore x * y^{-1} \in f^{-1}(H')$, y así

$f^{-1}(H') \underset{sg}{\subset} G$.

Ejercicio: Demostrar que todo grupo cíclico finito de orden n es isomorfo a $\mathbb{Z}_n$, y que los grupos cíclicos infinitos son isomorfos a $\mathbb{Z}$.

Anillos y cuerpos

***Definición*:** Sea A un conjunto no vacío, o sea, $A \neq \phi$. Sean + y $\cdot$ dos operaciones en A:

$+ : A \times A \to A$, $\quad \cdot : A \times A \to A$

$(a , b) \to a + b$ $\quad (a , b) \to a . b$

que verifican las siguientes propiedades:

Suma: (A , +) grupo abeliano.

Producto: $\cdot$

- asociativo: $a.(b.c) = (a.b).c$, $\forall a, b, c \in A$

y se verifica además:

Decimos que la terna (A , + , $\cdot$) es un *anillo.*

Si la operación $\cdot$ es además:

- conmutativa: $a.b = b.a$, $\forall a, b \in A$
  el anillo (A , + , $\cdot$) es un *anillo conmutativo.*

Si la operación $\cdot$ cumple con la:

- Existencia de elemento neutro: $\exists e' \in A$ tal que $a . e' = e'. a = a$, $\forall a \in A$,
  el anillo (A , + , $\cdot$) es un *anillo con identidad.*

- Distributividad de $\cdot$ respecto de + : $a.(b + c) = a.b + a.c$,
  $(a + b).c = a.c + b.c$ $\forall a, b, c \in A$

En el caso que cumpla todas las propiedades enunciadas, decimos que (A , + , $\cdot$) es un *anillo conmutativo con identidad.*

Nota: Como ya dijimos anteriormente, por abuso de notación, cuando sobreentendamos las operaciones definidas en A, diremos *el anillo A*, pero debe quedar bien claro que para la estructura importan tanto el conjunto cuanto las operaciones.

Emma Noether

El concepto de anillo fue introducido indistintamente por Richard Dedekind (1831-1916) *y Leopold Kronecker(1821-1891). Este último los llamaba "Orders". El nombre de anillo fue utilizado por primera vez por David Hilbert en 1897 en un trabajo titulado "The Theory of Algebraic Nimber Fields"….. En su sentido abstracto, el concepto de anillo fue introducido por Abraham Fraenkel* (1891-1965) *en 1914, pero con una formulación muy diferente de la que usamos actualmente. Fue en* 1917*, gracias al importante trabajo de Emma Noether* (1882-1935) *con su "Teoría de ideales en Anillos", cuando el concepto se extendió por la comunidad matemática. Muchos historiadores de la Matemática coinciden en valorar los teoremas de Noether en el campo del Álgebra Abstracta, como lo fueron en su momento los de Euclides en el campo de la Geometría.*

http://www.sangakoo.com/blog/estructuras-algebraicas/

***Propiedades*:** Sea A un anillo.

i. El neutro de la suma es **único.**
ii. El inverso aditivo u opuesto de cada elemento es **único.**
iii. El neutro del producto, cuando existe, es **único.**

***Demostración*:** Estas propiedades ya fueros demostradas para monoides en general, luego valen en los casos de anillos y de anillos con identidad en particular.

Nota: Por ser $(A, +)$ un grupo abeliano, llamaremos 0 al neutro respecto de esta operación, y $-a$ al inverso aditivo de cada $a \in A$. Al neutro del producto, cuando exista, lo simbolizaremos con 1.

Ejemplos: $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{Z}_n, +, \cdot)$ $\forall n \in \mathbb{N}$, son anillos conmutativos con identidad.

***Definición*:** Sea A un anillo, $B \subset A$. B es un *subanillo* de A si verifica:

i. $B \neq \phi$.
ii. $x, y \in B \Rightarrow x - y \in B \wedge x \,.\, y \in B$.

Si A es un anillo con identidad, $B \subset A$. B es un *subanillo con identidad* de A si además verifica:

iii. $1 \in B$.

Notación: $B \underset{suba.}{\subset} A$.

Ejemplos: $\mathbb{Z} \underset{suba.}{\subset} \mathbb{Q}$, $\mathbb{Q} \underset{suba.}{\subset} \mathbb{R}$.

Nota: Cuando $B \underset{suba.}{\subset} A$, B es un anillo con las operaciones inducidas, dado que para $x, y \in B$ por ii. se verifica que $x - x = 0 \in B \therefore 0 - x = -x \in B \wedge x - (-y) = x + y \in B$.
Luego las funciones + y $\cdot$ restringidas a $B \times B$ se aplican sobre B, por lo tanto son operaciones en B, que verifican todas las propiedades para hacer de B un anillo; si A fuese un anillo con identidad, y si por iii. $1 \in B$, se verifican todas las propiedades que sindican a B como un anillo conmutativo con identidad.

Ejercicios: Sea A un anillo, y cuando corresponda, un anillo con identidad; $a, b \in A$.

Demostrar que:

i. $a \cdot 0 = 0$.
ii. $-(-a) = a$.
iii. $(-a) \cdot b = a \cdot (-b) = -a.b$.
iv. $(-1) \cdot a = -a$.
v. $(-a).(-b) = a.b$.

***Elementos inversibles en un anillo*:**

Definición: Sea A un anillo con identidad , $a \in A$.
a se dice *inversible en A* si $\exists b \in A$ tal que $a.b = b.a = 1$.
b se llama *inverso* de a y se lo nota $b = a^{-1}$.

Notas:

- el 0 nunca puede ser inversible pues $0.c = 0 \ \forall c \in A$.
- Si a es inversible, el inverso de a es **único** (ya demostrado).

Notaremos al inverso de a, cuando exista, como a^{-1}.

Llamaremos $A^* = \{ a \in A / \quad a \text{ es inversible} \}$.

- $A^* \neq \phi$ pues $1^{-1} = 1$ ya que $1.1 = 1 \Rightarrow 1 \in A^*$.
- Si $a \in A^* \Rightarrow a^{-1} \in A^*$, pues $(a^{-1})^{-1} = a$.
- Si $a, b \in A^* \Rightarrow a.b \in A^*$, puesto que $(a.b)^{-1} = b^{-1}.a^{-1}$.

Por verificarse las propiedades precedentes, tenemos que $\cdot$ es una operación en A^*, y como ella es asociativa, tiene elemento neutro, el 1, y todo elemento de A^* tiene inverso en A^*, entonces $(A^*, \cdot)$ es un grupo, que llamaremos *grupo de unidades de A.*

Nota: En el caso de los anillos conmutativos con identidad, su grupo de unidades es también un grupo abeliano, pero se notará siempre en forma multiplicativa pues su operación es la restricción del producto en A . Si el anillo no fuera conmutativo, el grupo de unidades no sería necesariamente abeliano.

Ejemplos: $\mathbb{Z}^* = \{1, -1\}$; $\mathbb{Q}^* = \mathbb{Q} - \{0\}$; $\mathbb{R}^* = \mathbb{R} - \{0\}$; $\mathbb{Z}_n^* = \{ \overline{a} \ / \ (a, n) = 1 \}$

***Definición*:** Sea A un anillo conmutativo con identidad; si $A^* = A - \{0\}$ diremos que A es un *cuerpo.*

Ejemplos: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{Z}_p$, con $p \in \mathbb{N}$ primo, son cuerpos.

Richard Dedekind
(1831 - 1916)

El concepto de cuerpo estaba implícito ya en la obra de Abel y de Galois, pero Dedekind parece haber sido el primero en dar, en 1879, una definición explícita de un cuerpo de números: un conjunto de números que forma un grupo abeliano con respecto a la suma y con respecto a la multiplicación (excepto en lo que se refiere al inverso del cero), y tal que la multiplicación es distributiva con respecto a la suma.
(Historia de la Matemática, Carl B. Boyer).

***Definición*:** Sea A un anillo conmutativo con identidad . Diremos que A es *dominio de integridad*, o que es *íntegro* si satisface que:

$$a\ ,\ b \in A \text{ son tales que } a.b = 0 \Rightarrow a = 0 \vee b = 0$$

o lo que es equivalente:

$$\text{si } a \neq 0 \wedge b \neq 0 \Rightarrow a.b \neq 0\ .$$

Ejemplos: $\mathbb{Z}$; $\mathbb{Q}$; $\mathbb{R}$; $\mathbb{Z}_p$, con $p \in \mathbb{N}$ primo , son dominios de integridad.

$\mathbb{Z}_n$, con n compuesto, **no** es dominio de integridad.

Ejercicio: Demostrar que los subanillos con identidad de un dominio de integridad son también dominios de integridad.

***Proposición*:** Todo cuerpo es dominio de integridad.

***Demostración*:** Sea K un cuerpo , y sean $x\ ,\ y \in K$ tales que $x.y = 0$.

Si $x = 0$ no hay nada que demostrar.

Si $x \neq 0$, como K es cuerpo, x es inversible $\therefore\ \exists x^{-1} \in K$.

Multiplicando la igualdad $x.y = 0$ m.a.m por x^{-1}

$\therefore\ x^{-1}.\ x\ .\ y = x^{-1}.\ 0 = 0$, como $x^{-1}.\ x = 1$, tenemos que $1\ .\ y = 0 \Rightarrow y = 0$, que es lo que queríamos demostrar.

Luego K es dominio de integridad.

Nota: La recíproca no es cierta, pues $\mathbb{Z}$ es dominio de integridad y no es cuerpo.

Cuerpo de cocientes o de fracciones de un dominio de integridad

Así como el anillo de enteros $\mathbb{Z}$ puede ser extendido al cuerpo $\mathbb{Q}$ de números racionales, queremos saber si para cualquier dominio de integridad A existe un cuerpo K que lo contenga. Para demostrar que esta pregunta tiene respuesta afirmativa, haremos una construcción análoga a la que se realiza para definir el conjunto $\mathbb{Q}$ a partir $\mathbb{Z}$ definiendo una relación de equivalencia apropiada (ver Capítulo II, segunda parte).

***Definición*:** Un anillo con identidad A puede sumergirse en un anillo B (obviamente con identidad) si existe un monomorfismo con identidad de A en B . En este caso A será isomorfo (como anillo

con identidad) a un subanillo de *B*. En tal caso, también suele decirse que hay una inmersión de *A* en *B*.

Comentario: Si un dominio de integridad *A* está contenido en un cuerpo *K*, $\forall a,b \in A$, con $b \neq 0$, se verificará que $ab^{-1} \in K$, puesto que si $b \neq 0$, como $b \in A \ \wedge \ A \subset K$, entonces $b \in K$, luego $b^{-1} \in K$, por ser *K* cuerpo, por lo que a, $b^{-1} \in K \ \Rightarrow \ ab^{-1} \in K$.

Notación: Escribiremos al elemento ab^{-1} como $\frac{a}{b}$.

***Teorema*:** Todo dominio de integridad *A* puede sumergirse en un cuerpo.

***Demostración*:** Sea *A* dominio de integridad. Definiremos en $A \times (A - \{0\})$ la siguiente relación:

$$(a, b) \sim (c, d) \quad \Leftrightarrow \quad ad = bc \ .$$

Esta es una relación de equivalencia (demostrarlo).

Cada clase de equivalencia es: $\overline{(a,b)} = \{ (c,d) \in A \times (A - \{0\}) \ / \ ad = bc \ \}$

y el conjunto cociente, que llamaremos $K = {A \times (A - \{0\}) \big/ \sim}$.

Definiremos en *K* dos operaciones, a partir de las operaciones del dominio *A* .

Suma: $\overline{(a,b)} + \overline{(c,d)} = \overline{(ad + bc, bd)}$

Producto: $\overline{(a,b)} \, . \, \overline{(c,d)} = \overline{(ac, bd)}$

¿Estas operaciones están bien definidas?, o sea, si $(a,b) \sim (a',b') \ \wedge \ (c,d) \sim (c',d')$

¿se verifica $(ad + bc, \ bd) \sim (a'd' + b'c', \ b'd') \ \wedge \ (ac, \ bd) \sim (a'c', \ b'd')$?

Para demostrarlo debemos ver:

1. $ab' = ba' \ \wedge \ cd' = dc' \ \Rightarrow \ (ad + bc)b'd' = (a'd' + b'c')bd$.
2. $ab' = ba' \ \wedge \ cd' = dc' \ \Rightarrow \ acb'd' = a'c'bd$.

Demostremos:

1. $(ad + bc)b'd' = adb'd' + bcb'd' = (ab')dd' + (cd')bb' = (ba')dd' + (dc')bb' =$
$= (a'd' + b'c')bd$.
2. $acb'd' = ab'cd' = ba'c'd = a'c'bd$.

K , con estas operaciones, se estructura como un cuerpo (demostrarlo), donde $\overline{(0,1)}$ es el neutro para la suma (o sea el 0 de *K*) , y $\overline{(1,1)}$ es el neutro para el producto (o sea el 1 de *K*).

¿Cómo son las clases $\overline{(0,1)}$ y $\overline{(1,1)}$, o sea, cuáles son los elementos que las constituyen?

$$(a, b) \sim (0,1) \quad \Leftrightarrow \quad a.1 = 0.b = 0 \quad \Leftrightarrow \quad a = 0$$

luego $\overline{(0,1)} = \{ (0,b) \ / \ b \in A - \{0\} \}$

$$(a, b) \sim (1,1) \quad \Leftrightarrow \quad a.1 = b.1 \quad \Leftrightarrow \quad a = b$$

por tanto $\overline{(1,1)} = \{ (a,a) \ / \ a \in A - \{0\} \}$

En consecuencia $\overline{(a,b)} \neq \overline{(0,1)} \quad \Leftrightarrow \quad a \neq 0$, por lo que $\overline{(b,a)}$ está definida, y en virtud de la definición del producto, $\overline{(a,b)}^{-1} = \overline{(b,a)}$

Definiremos una inmersión de *A* en *K* :

La aplicación $\mathfrak{J} : A \to K$ definida por $\mathfrak{J}(a) = \overline{(a,1)}$
es un monomorfismo de anillos con identidad, dado que:

$\mathfrak{J}(a+b) = \overline{(a+b,1)} = \overline{(a,1)} + \overline{(b,1)} = \mathfrak{J}(a) + \mathfrak{J}(b)$ por definición de suma en *K*

$\mathfrak{J}(a.b) = \overline{(a.b,1)} = \overline{(a,1)}.\overline{(b,1)} = \mathfrak{J}(a).\mathfrak{J}(b)$ por definición de producto en *K*.

Además es monomorfismo puesto que $Ker(\mathfrak{J}) = \{\, a \in A \;\; / \;\; \mathfrak{J}(a) = 0 \,\} = \{\, 0 \,\}$ ya que

$\mathfrak{J}(a) = \overline{(a,1)} = \overline{(0,1)} \quad \Leftrightarrow \quad a = 0$.

De esta manera el dominio de integridad *A* se *identifica* con un subanillo con identidad de *K* , que es la imagen isomórfica de de *A* en *K* por la inmersión $\mathfrak{J}$. A través de esta inmersión, identificaremos cada $a \in A$ con su imagen $\overline{(a,1)}$, y para cada $b \in A - \{0\}$, escribiremos b^{-1} al elemento $\overline{(1,b)}$ de *K* .

Escribiremos a los elementos $\overline{(a,b)}$ de *K* , con $a \in A, b \in A - \{0\}$, como $\frac{a}{b}$.

Observación: $\frac{a}{b} = \overline{(a,b)} = \overline{(a,1)}.\overline{(1,b)} = a.b^{-1}$ **.**

***Corolario*:** El cuerpo *K* definido en el teorema, es el "menor" cuerpo que contiene a *A*, o sea, si *L* es un cuerpo que contiene a *A*, también contiene a *K*.

***Demostración*:** Sea *L* un cuerpo tal que $A \subset L$, y sea $\frac{a}{b} \in K$, como $a \in A, b \in A - \{0\}$, entonces

$a \in L, b \in L - \{0\}$, luego $a \in L,\ b^{-1} \in L - \{0\}$, por lo que $ab^{-1} \in L \ \wedge \ ab^{-1} = \frac{a}{b}$.

Así $K \subset L$.

Ejemplo: $\mathbb{Q}$ es el cuerpo de cocientes de $\mathbb{Z}$.

Ejercicios:

1**.** Sea *A* dominio de integridad. La relación en $A \times (A - \{0\})$ definida por:

$$(a,b) \sim (c,d) \quad \Leftrightarrow \quad ad = bc \ .$$

es una relación de equivalencia.

2. Demostrar que las operaciones definidas en $K = {A \times (A - \{0\}) \big/ \sim}$:

Suma: $\overline{(a,b)} + \overline{(c,d)} = \overline{(ad+bc, bd)}$

Producto: $\overline{(a,b)} \,.\, \overline{(c,d)} = \overline{(ac,bd)}$

lo estructuran como cuerpo.

Divisibilidad en un dominio de integridad

***Definición*:** Sea *A* dominio de integridad, $a, b \in A, \quad a \neq 0$; se dice que *a divide* a *b* o que *b* es *múltiplo* de *a*, si $\exists c \in A$ tal que $b = a \cdot c$.

Cuando un tal *c* existe es **única**:
Supongamos que $\exists c, d \in A$ tales que $b = a \cdot c = a \cdot d$,

entonces $0 = a \cdot c - a \cdot d = a \cdot (c - d)$, como A es dominio de integridad $\wedge$ $a \neq 0$ entonces $c - d = 0$ con lo cual $c = d$.

***Propiedades*:** Sea A dominio de integridad, $a, b \in A$, $a \neq 0$.
i. $1 \mid b$, $-1 \mid b$.
ii. $a \mid a$, $a \mid -a$, $-a \mid a$.
iii. $a \mid b \Rightarrow a \mid -b \wedge -a \mid b$.
iv. $a \mid b \Rightarrow a \mid bc \quad \forall c \in A$.
v. Para $c \in A$, $b \neq 0$, $a \mid b \wedge b \mid c \Rightarrow a \mid c$ (transitiva).
vi. Para $b \neq 0$, $a \mid b \wedge b \mid a \Leftrightarrow \exists u \in A^*$ tal que $b = ua$.
vii. Para $c \in A$, $a \mid b \wedge a \mid c \Rightarrow a \mid (b + c)$.
viii. Para $c \in A$, $a \mid (b + c) \wedge a \mid b \Rightarrow a \mid c$.

***Definición*:** Sea A dominio de integridad, $a, b \in A$.
a se dice *asociado* a b si $\exists u \in A^*$ tal que $b = ua$.

La relación en A : $a \sim b \Leftrightarrow a$ es asociado a b , es una relación de equivalencia.

Observación: Por el ejercicio vi. para $a, b \in A - \{0\}$, a y b son asociados sii $a \mid b \wedge b \mid a$
Los asociados a 1 son todos los elementos inversibles de A.

Cuadrados en un dominio de integridad

***Definición*:** Sea A dominio de integridad, $x \in A$; x es un *cuadrado* en A si $\exists y \in A$ tal que $y^2 = x$.

***Observación*:** 0 es un cuadrado porque $0^2 = 0$. Análogamente 1 también lo es.
Observemos que si x es un cuadrado en A, e y es tal que $y^2 = x \Rightarrow (-y)^2 = x$; $y \wedge -y$ son los únicos con esa propiedad , puesto que si $y^2 = z^2$, tenemos que $(y - z).(y + z) = 0 \Rightarrow y - z = 0 \vee y + z = 0 \quad \therefore \quad z = y \vee z = -y$.

Nota: Puede ocurrir que $y = -y$, por ejemplo en $\mathbb{Z}_2$, en cuyo caso habrá a lo sumo un $y \in A$ tal que $y^2 = x$, si en cambio en A se verifica que $y = -y \Leftrightarrow y = 0$, para cada $x \in A$, $x \neq 0$, no existe ninguno o existen dos y tales que $y^2 = x$.

Ejemplos: 1) En $\mathbb{R}$ los cuadrados son todos los números no negativos.
En $\mathbb{Q}$ los cuadrados son no negativos, pero no todos ellos, 2 no es cuadrado, $\frac{1}{5}$ tampoco lo es. Análogamente para $\mathbb{Z}$.
2) En $\mathbb{Z}_2$ todos son cuadrados; en $\mathbb{Z}_3$ los cuadrados son $\{\overline{0}, \overline{1}\}$; en $\mathbb{Z}_5$ los cuadrados son $\{\overline{0}, \overline{1}, \overline{4}\}$, y como $\overline{4} = -\overline{1}$, $-\overline{1}$ es un cuadrado en $\mathbb{Z}_5$; en $\mathbb{Z}_7$ los cuadrados son $\{\overline{0}, \overline{1}, \overline{2}, \overline{4}\}$, o sea, $-\overline{1}$ no es un cuadrado en $\mathbb{Z}_7$.

***Definición*:** Sea $p \in \mathbb{N}$ primo, $a \in \mathbb{Z}$. Se dice que a es *residuo cuadrático módulo p* (RC *mód p*) si $\exists x \in \mathbb{Z}$ tal que $x^2 \equiv a \ (p)$, o sea si $\overline{a}$ es un cuadrado en $\mathbb{Z}_p$.

Cuando *a* no es RC (*mód p*) se dice que es *no RC* (*mód p*).

Ejemplos: 0, 1 y todos los a^2 son residuos cuadráticos (*mód p*) $\forall p$ natural primo, – 1 es residuo cuadrático *mód* 5, pero no *mód* 3 o *mód* 7 .

Notación: Sea $a \in \mathbb{Z}$ tal que $p \nmid a$, para indicar si es o no RC(*mód p*) se utiliza el *Símbolo de Legendre* $\left(\frac{a}{p}\right)$ definido por: $\left(\frac{a}{p}\right) = \begin{cases} 1 & si \quad a\ es\ RC\ (mód\ p) \\ -1 & si \quad es\ no\ RC\ (mód\ p) \end{cases}$

Ejercicios:
1. Para *p* primo positivo impar, $a \in \mathbb{N}$, $1 \le a \le p-1$, la mitad de ellos son RC (*p*) y la otra mitad son no RC (*p*).
2. Sea $a = bc$, con $a, b, c \in \mathbb{Z}$, $p \in \mathbb{N}$ primo tal que $p \nmid a$.
Entonces *a* es RC (*mód p*) si y sólo si *b* y *c* son ambos RC (*mód p*) o ambos no RC (*mód p*) , o lo que es equivalente:

$$\left(\frac{cd}{p}\right) = \left(\frac{c}{p}\right)\left(\frac{d}{p}\right)$$

Ideales

***Definición*:** Sea *A* anillo conmutativo con identidad, $I \subset A$. Decimos que *I* es un *ideal* de *A* si verifica:
i. $I \underset{sg}{\subset} A$.
ii. $\forall x \in I \ \wedge \ \forall y \in A \quad xy \in I$.

Ernst Eduard Kummer
(1810 - 1893)

El interés en la idea abstracta de estructura y la aparición de nuevas álgebras, especialmente durante la segunda mitad del siglo XIX, condujo también a amplias generalizaciones en el campo de los números y su aritmética… Gauss extendió la idea de número entero ordinario a los llamados enteros de Gauss, que son los números complejos de la forma a+bi, con a y b enteros. Dedekind la generalizó a su vez en su teoría de los "enteros algebraicos", es decir, números que son raíces de ecuaciones polinómicas con coeficientes enteros y tales que el coeficiente del término de mayor grado sea 1. Tales sistemas de "enteros" no constituyen cuerpos, desde luego, puesto que los elementos no nulos no tienen inversos para la multiplicación, en general. Sí tienen algo en común con los cuerpos, de hecho, ya que verifican todas las restantes propiedades de un cuerpo de números; se dice, pues, que forman un "dominio de integridad". Tales generalizaciones de la idea de entero costaron un precio, sin embargo, que fue la pérdida de la propiedad de factorización única. Debido a ello, Dedekind y otro matemático contemporáneo, Ernst Eduard Kummer (1810-1893), introdujeron en la aritmética el concepto de "ideal", basado en la idea de "anillo". ("Historia de la Matemática", C. Boyer*)*

Nota: Si *I* es un ideal de *A* , $I \neq \phi$ por ser un subgrupo de *A*.

Ejercicio: Si *I* es un ideal de $A \ \wedge \quad a \in I$, todos los asociados de *a* son también elementos de *I.*

Ejemplos:
1. Todo anillo *A* admite dos ideales: *A* y 0 (subgrupo nulo), llamados i*deales triviales*.
2. Si $a \in A$, el conjunto $I = \{ ak \ / \ k \in A \}$ es un ideal de *A* .

Notación: $I = (a)$.

3. Si *J* es ideal de *A* , $a \in J$, entonces $(a) \subset J$, o sea (a) es el "menor" ideal de *A* que contiene a *a* .

Nota: Los ideales de *A* no son subanillos (con identidad) de *A*, excepto el mismo *A*,
pues si *I* es ideal de *A* tal que $I \subsetneq A \ \wedge \ 1 \in I$ entonces $\forall x \in A \ \ x = x \cdot 1 \in I$ con lo cual $I = A$!!
En general, si I es un ideal de *A* para el cual $\exists u \in A^*$ tal que $u \in I$ entonces $I = A$.

Ejemplos: Los ideales de $\mathbb{Z}$ son los $n\mathbb{Z}$, con $n \in \mathbb{N}_0$, dado que éstos son los subgrupos de $\mathbb{Z}$, y además son ideales.

***Definición*:** Sea *A* anillo conmutativo con identidad, $I \subsetneq A$. Decimos que *I* es un ideal *maximal* de *A* si verifica: si J es un ideal de A tal que $I \subset J$ entonces $I = J \ \vee \ J = A$.

Nota: Un ideal es *ideal maximal* si es un elemento maximal en el conjunto de los ideales propios ordenado por inclusión.

Ejercicio: Los ideales maximales de $\mathbb{Z}$ son los $p\mathbb{Z}$, con $p \in \mathbb{N}$ primo.

***Teorema*:** En todo anillo conmutativo con identidad existen ideales maximales propios.

***Demostración*:** Para demostrar este teorema haremos uso de un lema fundamental de la matemática llamado *Lema de Zorn.*

***Lema de Zorn*:** Si en un conjunto ordenado $(\mathrm{E}, \prec)$ toda *cadena* (subconjunto de E totalmente ordenado) tiene cota superior, entonces en E existe un elemento maximal.

Max August Zorn
(1906 - 1993)

Max Zorn nació el 6 de junio de 1906 en Krefeld, Alemania occidental y falleció el 9 de marzo de 1993 en Indiana, EEUU. Asistió a la Universidad de Hamburgo, donde estudió con Artin . Recibió su Ph.D. en Hamburgo en abril de 1930 con una tesis sobre álgebras alternativas. En esta etapa, fue galardonado con un premio de la Universidad de Hamburgo. Fue nombrado como asistente en Halle, pero no tuvo la oportunidad de trabajar allí por mucho tiempo, ya que, en 1933, se vio obligado a abandonar Alemania debido a las políticas nazis.
Zorn emigró a los Estados Unidos y trabajó en la Universidad de Yale desde 1934 hasta 1936 , período en el cual propuso el "Lema de Zorn".
Por supuesto no fue él quien llamó a su resultado "Lema de Zorn", sino que lo presentó como un "principio máximo" en un breve documento titulado "Un comentario sobre el método de álgebra transfinito" que publicó en el Boletín de la Sociedad Americana de Matemáticas en 1935.
El nombre "Lema de Zorn" se debió al químico y matemático John Tukey (1915-2000).

Sea $\Gamma = \{ I \subsetneq A \ / \ I \ es \ ideal \ de \ A \}$, ordenamos Γ por inclusión.

$(\Gamma, \subset)$ es un conjunto ordenado, queremos ver que en Γ toda cadena tiene cota superior, para deducir, por el Lema de Zorn, que existe un elemento maximal.
Sea $\{J_i\}_{i\in R}$ una cadena en Γ, luego $\forall i, j \in R \quad J_i \subset J_j \ \vee \ J_j \subset J_i$.
Entonces el conjunto $H = \bigcup_{i\in R} J_i$ es un ideal de *A* (ejercicio) $\wedge \quad H \subsetneq A$, por lo tanto $H \in \Gamma$; claramente *H* es una cota superior de la cadena $\{J_i\}_{i\in R}$ pues $J_i \subset H \quad \forall i \in R$.
Entonces, por el Lema de Zorn, existe en Γ un elemento maximal *M* que es un ideal maximal de *A.*

Ejercicio: Sea *I* ideal propio de *A*, demostrar que existe un ideal maximal *M* tal que $I \subset M$ (o sea, todo ideal propio está contenido en un ideal maximal).
Pista: razonar en forma similar al teorema.

***Definición*:** Un ideal *I* de *A* se dice *principal* si $\exists a \in I$ tal que $I = (a)$, o sea $\forall x \in I \quad \exists k \in A$ tal que $x = ka$.

***Definición*:** Si $I = (a)$, *a* es un *generador* de *I.* En general, si *I* es un ideal principal, un elemento $b \in I$ es un *generador* de *I* si $\forall x \in I \quad \exists k \in A$ tal que $x = ka$
O sea, *b* genera al ideal principal *I* , si $\forall x \in I$ se verifica que $b \mid x$.

Ejercicio: Si $I = (a)$, demostrar que los generadores de *I* son asociados de *a* .

Ejercicio: $(a) \subset (b) \quad \Leftrightarrow \quad b \mid a$. En particular $(a) = (b) \quad \Leftrightarrow$ *a* y *b* son asociados.

Ejemplo: Los $n\mathbb{Z}$ son ideales principales de $\mathbb{Z}$, con $n \ \wedge \ -n$ como generadores.

***Definición*:** Un dominio de integridad *A* se dice *dominio principal* si todo ideal de *A* es principal.

Ejemplo: $\mathbb{Z}$ es un dominio principal.

***Definición*:** Sea *A* dominio de integridad, $p \in A$. *p* se dice *primo* en *A* , si verifica:
i. $p \neq 0 \ \wedge \ p \notin A^*$.
ii cada vez que $p \mid a \cdot b$, con $a, b \in A$, entonces $p \mid a \ \vee \ p \mid b$.

***Definición*:** Sea *A* dominio de integridad, $p \in A$. *p* se dice *irreducible o extremal* en *A* si sus únicos divisores son las unidades y los asociados a *p*, o sea si verifica que

si $q \mid p$ entonces $q \in A^* \ \vee \ q = up$ con $u \in A^*$.

***Proposición*:** Sea *A* dominio de integridad, $p \in A$. Si *p* es primo en *A* entonces es irreducible en *A*

***Demostración*:** Sea *p* primo en *A* y sea $p = a \cdot b$, con $a, b \in A$, por ser *p* primo entonces $p \mid a \ \vee \ p \mid b$, pero $a \mid p \ \wedge \ b \mid p$.
Así ($p \mid a \ \wedge \ a \mid p$) $\vee$ ($p \mid b \ \wedge \ b \mid p$) $\therefore$ ($b \in A^* \ \wedge$ *a* asociado a *p*) $\vee$
($a \in A^* \ \wedge$ *b* asociado a *p*) con lo cual *p* es irreducible.

***Definición*:** Sea *A* dominio de integridad, $a,b\in A$, $a\neq 0 \vee b\neq 0$, sea $g\in A-\{0\}$, se dice que g es un *máximo común divisor* (m.c.d.) de a y b, si:

i. $g\mid a \wedge g\mid b$.

ii. Si $c\mid a \wedge c\mid b \Rightarrow c\mid g$.

Ejercicio: Dos m.c.d. de *a* y *b* son asociados. Recíprocamente, si g es un m.c.d. de a y b entonces todo asociado a g también lo es.

***Teorema*:** Sea *A* un dominio principal $\forall a,b\in A$, $a\neq 0 \vee b\neq 0$, existe un m.c.d. de *a* y *b*. Si *g* es un tal m.c.d. de *a* y *b* entonces $\exists u,v\in A$ tales que $g=ua+vb$.

***Demostración*:** Sea $I=\{ka+hb \;/\; k,h\in A\}$

I es un ideal de *A*, $I\neq 0$ pues $a\in I \wedge b\in I$.

Como *A* es un dominio principal, *I* es ideal principal, $\exists g\in I$, $g\neq 0$, tal que $I=(g)$ $\therefore$ $\exists u,v\in A$ tales que $g=ua+vb$.

Como $a\in I=(g) \Rightarrow (a)\subset(g) \therefore g\mid a$,

análogamente $b\in I=(g) \Rightarrow (b)\subset(g) \therefore g\mid b$, luego g verifica i.

Sea, ahora, $c\in A$ tal que $c\mid a \wedge c\mid b$, entonces $a=ck \wedge b=hc$ para ciertos $k,h\in A$ $\therefore$ $g=ua+vb=ukc+vhc=(uk+vh)c$ con $uk+vh\in A$, así $c\mid g$ por lo cual se verifica ii. y g es un m.c.d. de a y b $\wedge$ $\exists u,v\in A$ tales que $g=ua+vb$.

***Definición*:** Sea *A* un dominio principal, $a,b\in A$, $a\neq 0 \vee b\neq 0$, *a* y *b* se dicen *coprimos* o *primos entre sí*, si su m.c.d. es 1. En tal caso el ideal $I=\{ka+hb \;/\; k,h\in A\}=(1)=A$ por lo cual la notación $(a\,,b)=1$, no lleva a ninguna contradicción, dado que $\exists u,v\in A$ tales que $1=ua+vb$, por más que cualquier otra unidad de *A* sea también un m.c.d. de *a* y *b*. Recíprocamente, si $\exists u,v\in A$ tales que $1=ua+vb$, entonces $(a\,,b)=1$.

***Proposición*:** Sea *A* dominio principal, $p\in A$, irreducible en *A*, entonces $\forall a\in A$ se verifica una y sólo una de estas dos propiedades: $p\mid a \vee (a\,,p)=1$.

***Demostración*:** Sea $a\in A$, si $p\mid a$ ya está, no hay nada más que demostrar.

Si $p\nmid a$, sea g un m.c.d. de p y a, $\exists u,v\in A$ tales que $g=ua+vp$.

Como $g\mid p$ y p es irreducible en *A* entonces $g\in A^* \vee g=wp$ con $w\in A^*$.

Si $g\in A^*$ entonces $(a\,,p)=1$, que es lo que queríamos demostrar.

Si $g=wp$ con $w\in A^*$, como $g\mid a$ entonces $p\mid a$, por ser p y g asociados !!

Luego, la única posibilidad es que $g\in A^*$, o sea, $(a\,,p)=1$.

***Corolario*:** Sea *A* dominio principal, $p\in A$. *p* es primo en *A* si y sólo si es irreducible en *A*.

***Demostración*:** $\Rightarrow$) ya fue demostrada para cualquier dominio de integridad *A*.

$\Leftarrow$) Sea p irreducible en *A*, y sean $a,b\in A$ tales que $p\mid a\cdot b$.

Si $p\mid a$ ya está, no hay nada más que demostrar.

Si $p \nmid a$, entonces $(a\,,\,p)=1$, luego $\exists u,v\in A$ tales que $1=ua+vp$, multiplicando ambos miembros de la igualdad por b, se tiene que $b=uab+vpb$, y como $p\mid a\cdot b$ y $p\mid vpb$ entonces $p\mid b$, como queríamos demostrar. Así p es primo en A.

Ejercicios: Sea A dominio principal.

1. Si $p\in A$ es primo y $p\mid\prod_{i=}^{n}a_i$, con $a_i\in A\ \forall i=1,...,n$, entonces $\exists j$, $1\le j\le n$ tal que $p\mid a_j$.

2. Si $a\mid bc\ \wedge\ (a\,,b)=1$ entonces $a\mid c$.

***Proposición*:** Sea A dominio principal, p es primo en A si y sólo si (p) es un ideal maximal de A.

***Demostración*:** $\Rightarrow$) Sea p primo en A, y sea $I=(p)$; claramente $I\subsetneq A$ pues si $1\in I$ entonces p sería asociado a 1, lo que es imposible porque p es primo.

Sea J ideal de A tal que $I\subset J$. Como A es dominio principal $\exists x\in A$ tal que $J=(x)$. $I\subset J$ $\Rightarrow x\mid p\ \therefore\ x\in A^*\ \vee\ x=up$ con $u\in A^*$, o sea $J=A\ \vee\ J=I$

Luego $I=(p)$ es maximal.

$\Leftarrow$) Sea $I=(p)$ ideal maximal en A.

Sea $p=a\cdot b$ entonces $(p)\subset(a)\ \wedge\ (p)\subset(b)$. Si $a\notin A^*$ entonces $(a)\subsetneq A$, y como $I=(p)$ es ideal maximal entonces $I=(p)=(a)\ \therefore\ a$ y p son asociados y b es una unidad de A. Análogamente si $b\notin A^*$. Luego p es primo en A.

***Corolario*:** Sea A dominio principal , $\forall a\in A-A^*\ \exists p\in A$ primo tal que $p\mid a$.

***Demostración*:** Sea $a\in A-A^*$.

Si $a=0$, y p es primo en A, $a=0=0\cdot p$, luego $p\mid 0$.

Si $a\neq 0$, $(a)\neq 0\ \wedge\ (a)\subsetneq A$ por no ser a una unidad de A, luego existe un ideal J maximal de A tal que $(a)\subset J$. Como A es dominio principal $\exists p\in A$ tal que $J=(p)$ y como J es maximal entonces p es primo; además $(a)\subset(p)$ implica que $p\mid a$, con lo cual se establece el corolario.

Dominios euclidianos

***Definición*:** Sea A un dominio de integridad, se dice que es un *dominio euclidiano* si existe una función $d:A-\{0\}\to\mathbb{N}_0$ tal que:

i. $d(a)\le d(ab)\quad\forall a,b\in A-\{0\}$.

ii. $\forall a,b\in A-\{0\}\ \ \exists q,r\in A$ tales que $b=qa+r$ con $r=0\ \ \vee\ \ d(r)<d(a)$.

El anillo $\mathbb{Z}$ es un ejemplo de dominio euclidiano, en el cual la función d definida por $d(a)=|\,a\,|\ \ \forall a\in\mathbb{Z}-\{0\}$, cumple con las dos condiciones pedidas.

***Proposición*:** Sea A un dominio euclidiano, y sean $a,b\in A-\{0\}$. Si $b\notin A^*$, entonces $d(a)<d(ab)$.

***Demostración*:** Sea $I=(a)$, como $a\neq 0 \Rightarrow I\neq 0$ (ideal nulo).

Por ser *A* euclidiano, $d(a)\leq d(ak) \quad \forall k\in A-\{0\}$, por lo cual $d(a)=mín\{d(b)/b\in I-\{0\}\}$
Este $d(a)$ siempre existe puesto que $d(x)\in\mathbb{N}_0 \quad \forall x\in I-\{0\}$, y $\mathbb{N}_0$ es bien ordenado.
Si $d(a)=d(ak)$ para algún $k\in A-\{0\}$, sea $x\in I-\{0\}$, entonces $\exists q,r\in A$ tales que $x=qka+r$ con $r=0 \ \vee \ d(r)<d(ak)=d(a)$, como $x\in I-\{0\} \ \wedge \ qak\in I$ entonces $r\in I$ por lo que $d(a)\leq d(r) \ \vee \ r=0$ por lo que $r=0 \ \therefore \ x\in(ak)$
Entonces $I\subset(ak)$, pero $(ak)\subset(a)=I$, con lo cual *ak* es un generador de I, por lo que concluimos que *a* y *ak* son asociados $\therefore \ k\in A^*$.
Entonces, si $a,b\in A-\{0\} \ \wedge \ b\notin A^*$, se verifica que $d(a)<d(ab)$.

***Teorema*:** Todo dominio euclidiano es dominio principal.

***Demostración*:** Sea I ideal de *A*, $I\neq 0$, (claramente el ideal nulo es principal).
Sea $a\in I$ tal que $d(a)$ es mínimo en $I-\{0\}$, y sea $b\in I-\{0\}$; por ser *A* euclidiano $\exists q,r\in A$ tales que $b=qa+r$ con $r=0 \ \vee \ d(r)<d(a)$, como $b\in I \ \wedge \ a\in I \Rightarrow b\in I \ \wedge \ aq\in I$ luego $r\in I$, con lo cual $d(a)\leq d(r) \ \vee \ r=0$.
Así $r=0$ y $b=qa\in(a)$; como $a\in I$ entonces $(a)\subset I \ \therefore \ I=(a)$ y así *I* es principal; esto es para todo I ideal de *A*, por lo que *A* es dominio principal.

***Definición*:** Sea *A* un dominio de integridad, se dice que es un *dominio factorial* o *dominio de factorización única* si $\forall a\in A-\{0\}, \ a\notin A^*$ existen finitos irreducibles $p_1, p_2, ..., p_n\in A$, tales que $a=\prod_{i=1}^{n} p_i$. Este factorización es única, excepto por el orden y/o asociados a los irreducibles, o sea, si $\prod_{i=1}^{n} p_i=\prod_{j=1}^{m} q_j$, donde $p_1, p_2, ..., p_n, q_1, q_2, ..., q_m\in A$ irreducibles, entonces $n=m \quad \wedge \ \forall i, \ i=1,...,n \ \exists j_i, \ 1\leq j_i\leq n$, tal que $p_i=u_i q_{j_i}$ con $u_i\in A^*$.

***Teorema*:** Todo dominio euclidiano es dominio de factorización única.

***Demostración*:** *Existencia de la factorización*:

Sea $a\in A-\{0\}, \ a\notin A^*$, si *a* es irreducible no hay nada que demostrar; si *a* es reducible, $\exists p_1\in A$ primo (y por tanto, irreducible), tal que $a=p_1\cdot a_1$ donde $a_1\in A-\{0\} \ \wedge \ a_1\notin A^*$; si a_1 es primo, ya está la factorización; si no lo es $\exists p_2\in A$ primo, tal que $a_1=p_2\cdot a_2$ donde $a_2\in A-\{0\} \ \wedge \ a_2\notin A^*$, si a_2 es primo, la factorización de *a* es: $a=p_1p_2a_2$, si no lo es $\exists p_3\in A$ primo, tal que $a_2=p_3\cdot a_3$ donde $a_3\in A-\{0\} \ \wedge \ a_3\notin A^*$. Este proceso es finito pues en cada paso encontramos un a_i tal que $a=p_1p_2...p_ia_i$ con los p_j primos y los

$a_j \neq 0 \ \wedge \ a_j \notin A^*$, para $j = 1,...,i$. Observemos que en cada paso $a_{j+1} \mid a_j$ con lo cual $d(a_{j+1}) < d(a_j)$ pues ellos no son asociados. El conjunto $\{ k \in \mathbb{N}_0 \ / \ k < d(a) \}$ es finito, por lo tanto $\exists i$ tal que $a = p_1 p_2 ... p_i a_i$ con los p_j primos para $j = 1,...,i$, y también a_i primo, lo que nos da la factorización en primos (o irreducibles) de *a*.

Unicidad de la factorización:

Debemos demostrar que si $\prod_{i=1}^{n} p_i = \prod_{j=1}^{m} q_j$, donde $p_1, p_2, ..., p_n, q_1, q_2, ..., q_m \in A$ irreducibles, entonces $n = m \ \wedge \ \forall i, \ i = 1,...,n \ \exists j_i, \ 1 \leq j_i \leq n$, tal que $p_i = u_i q_{j_i}$ con $u_i \in A^*$.

Lo haremos por inducción sobre *n* :

Si $n = 1$, $p_1 = \prod_{j=1}^{m} q_j$ donde $p_1, q_1, q_2, ..., q_m \in A$ son primos (o irreducibles).

Si $m > 1$ entonces $q_1 \mid p_1$ donde $q_1 \notin A^*$ ni es asociado a p_1, pues $d(q_1) < d(p_1)$!! (absurdo) con lo cual $m = 1 \ \wedge \ q_1 = p_1$.

HI: Supongamos que toda factorización de *n* primos sea única en el sentido del teorema.

Sea una factorización de *n* + 1 primos .

$\prod_{i=1}^{n+1} p_i = \prod_{j=1}^{m} q_j$ con $p_1, p_2, ..., p_n, q_1, q_2, ..., q_m \in A$ primos

$p_1 \mid \prod_{j=1}^{m} q_j$, y como p_1 es primo $\exists j_1 \ \ 1 \leq j_1 \leq m$ tal que $p_1 \mid q_{j_1}$, y como ambos son primos, entonces son asociados $\therefore \ \exists u_1 \in A^*$ tal que $q_{j_1} = u_1 p_1$.

Cancelando p_1 de la identidad $\prod_{i=1}^{n+1} p_i = \prod_{j=1}^{m} q_j$ obtenemos $p_2 p_3 ... p_n p_{n+1} = u_1 q_1 q_2 ... q_{j_i - 1} q_{j_i + 1} ... q_m$

En el primer miembro de la igualdad hay un producto de *n* primos, por HI el segundo miembro de la igualdad tiene también *n* primos, y son los mismos, salvo asociados, que los del primer miembro, excepto quizás por el orden en que están escritos.

Por lo tanto $m - 1 = n$ con lo que $m = n + 1$ y para cada $i = 1, 2, ..., n+1 \ \exists j_i, \ 1 \leq j_i \leq n+1$, tal que $p_i = u_i q_{j_i}$ con $u_i \in A^*$.

Nota: Todo dominio principal es también dominio factorial, pero la demostración es un poco más difícil.

Característica de un cuerpo

Sea *K* un cuerpo, supongamos que $\exists n \in \mathbb{N}$ tal que *n* 1= 0 (el $1 \in K$), entonces sea

$m = mín\{ n \in \mathbb{N} \ / \ n1 = 0 \}$.

Veamos que *m* es primo. Como *m* > 1 si no es primo, $\exists p \in \mathbb{N}$ primo tal que $p \mid m \ \wedge \ 1 < p < m$; $m = p.k$ con $1 < k < m$.

$0 = m1 = pk\ 1 = (p1).(k1)$, y como K es cuerpo entonces $p1 = 0$ ó $k1 = 0$!! (absurdo) pues $p < m$ y $k < m$ y m es mínimo con esa propiedad, luego m es primo.

Además $ma = 0$, para todo a en K, puesto que $ma = (m1).a = 0$

***Definición*:** Si K es un cuerpo y p es un natural primo tal que $p1 = 0$ entonces el cuerpo K se dice de característica p . Si en cambio $p1 \neq 0$ para todo primo p (o sea para todo n natural) el cuerpo K se dice de característica 0.

Notación: $car\ K = p$ ó $car\ K = 0$

Ejercicio: Sea K cuerpo. Si existen $a \in K - \{0\}$ y $n \in \mathbb{N}$ tales que $na = 0$ entonces $car\ K = p$ para un primo positivo p que divida a n .

Ejemplos: $\mathbb{Q}$ y $\mathbb{R}$ son cuerpos de característica 0 ; $\mathbb{Z}_p$ es cuerpo de característica p , para cada primo p.

El primo de la característica está unívocamente determinado, pues si p y q fueran dos primos distintos tales que $p1 = q1 = 0$, como ambos son primos y distintos son coprimos, luego $\exists u, v \in \mathbb{Z}$ tales que $up + vq = 1 \Rightarrow up1 + vq1 = 1$ (en este caso el 1 de K) con lo cual $1 = 0$ (en K) !! (absurdo, porque K es un cuerpo).

Luego si $car\ K = p$, $\forall q$ primo, $q \neq p$, $q1 \neq 0$; si $car\ K = 0$, $\forall q$ primo, $q1 \neq 0$.

Ejercicios:
1. Si $car\ K = p$, p primo, demostrar que para $n \in \mathbb{N}$, $n1 = 0 \Leftrightarrow p \mid n$.
2. $car\ K = 2$ si y sólo si existe un a no nulo en K tal que $a = -a$.
Si $car\ K = 2$, $a = -a$ para todo a en K .

Homomorfismos de anillos:

***Definición*:** Sean A , B anillos; $f : A \to B$ una función.
Decimos que f es un *homomorfismo de anillos* si verifica:

- **i.** $f(a + a') = f(a) + f(a')\ \forall a, a' \in A$.
- **ii.** $f(a\ .\ a') = f(a)\ .\ f(a')\ \forall a, a' \in A$.

Si A , B son anillos con identidad, decimos que f es un *homomorfismo de anillos con identidad* si verifica:

- **i.** $f(a + a') = f(a) + f(a')\ \forall a, a' \in A$.
- **ii.** $f(a\ .\ a') = f(a)\ .\ f(a')\ \forall a, a' \in A$.
- **iii.** $f(1) = 1$.

Nota: Si f es un homomorfismo de anillos, es un homomorfismo de los grupos subyacentes.

Ejemplos: 1) $\varphi : \mathbb{Z} \to \mathbb{Z}_n$, definida por $\varphi(k) = \overline{k}$, $\forall k \in \mathbb{Z}$, es homomorfismo de anillos con identidad.
2) A anillo con identidad, $id_A : A \to A$, $id_A(a) = a$, $\forall a \in A$, es homomorfismo de anillos con identidad.

3) A , B anillos con identidad, $A \underset{suba.}{\subset} B$, $i : A \to B$, $i(a) = a$, $\forall a \in A$, es homomorfismo de anillos con identidad.

***Propiedades*:** Sean A , B anillos ; $f : A \to B$ homomorfismo de anillos. Entonces:

i. $f(0) = 0$.
ii. $f(-a) = -f(a)$ $\forall a \in A$.

***Demostración*:** Por ser los homomorfismos de anillos también homomorfismos de grupos, se consideran aquéllos como un caso particular de éstos.

***Definiciones*:** Sean A , B anillos; $f : A \to B$ homomorfismo de anillos. Decimos que:

- f es *monomorfismo* si f es inyectiva.
- f es *epimorfismo* si f es suryectiva.
- f es *isomorfismo* si f es biyectiva.
- f es un *endomorfismo* si es un homomorfismo del anillo A en sí mismo.
- f es un *automorfismo* si es un endomorfismo isomórfico, o sea un isomorfismo de un anillo en sí mismo.

Ejemplos: En los ejemplos anteriores, $\varphi : \mathbb{Z} \to \mathbb{Z}_n$ es epimorfismo;
$id_A : A \to A$ es automorfismo ; $i : A \to B$ es monomorfismo.

Ejercicios:

1. Demostrar que la composición de homomorfismos de anillos es un homomorfismo de anillos.
2. Demostrar que la composición de monomorfismos de anillos es un monomorfismo de anillos.
3. Demostrar que la composición de epimorfismos de anillos es un epimorfismo de anillos.
4. Demostrar que la composición de isomorfismos de anillos es un isomorfismo de anillos.
5. Demostrar que la función inversa de un isomorfismo de anillos es un isomorfismo de anillos.

***Definición*:** Dos anillos A y B se dicen *isomorfos* si $\exists f$, $f : A \to B$ isomorfismo de anillos.

Notación: Cuando A y B sean isomorfos, lo notaremos $A \approx B$.

Ejercicio: El isomorfismo de anillos es una relación de equivalencia.

***Definición*:** Sean A , B anillos ; $f : A \to B$ homomorfismo de anillos . Llamamos *núcleo de f* al conjunto $Ker(f) = \{ x \in A \ / \ f(x) = 0 \}$.

Nota: El núcleo de un homomorfismo verifica que $0 \in Ker(f)$ pues $f(0) = 0$; además, si $a , a' \in Ker(f) \Rightarrow a + a' \in Ker(f) \wedge -a \in Ker(f) \wedge a.a' \in Ker(f)$ (demostrarlo), luego el $Ker(f)$ es un subanillo de A , pero si A y B son anillos con identidad y f un homomorfismo de anillos con identidad, como $1 \notin Ker(f)$ pues $f(1) = 1$,entonces $Ker(f)$ **no** es un subanillo con identidad del anillo A. En cambio $Im(f) = \{ f(x) \ / \ x \in A \} \underset{suba.}{\subset} B$ en cualquier caso.

***Proposición*:** Sean A , B anillos; $f : A \to B$ homomorfismo de anillos .

f es monomorfismo si y sólo si $Ker(f) = \{ 0 \}$.

***Demostración*:** Es un caso particular de homomorfismo de grupos.

Problemas para pensar:

1. ¿Cuántos subanillos tiene $\mathbb{Z}$?, y ¿cuántos subanillos con identidad tiene $\mathbb{Z}$?, ¿cuántos endomorfismos de anillos con identidad puedo definir en $\mathbb{Z}$?
2. ¿Puedo definir un homomorfismo de anillos con identidad de $\mathbb{Z}_n$ en $\mathbb{Z}_m$ cuando $n \neq m$?, ¿y cuando $n = m$? , ¿cuántos?
3. Demostrar que hay un único automorfismo de anillos con identidad de $\mathbb{Q}$ que es el automorfismo $id_{\mathbb{Q}}$.
4. ¿Cuántos homomorfismos de anillos con identidad puedo definir de $\mathbb{Z}$ en $\mathbb{Q}$?, ¿y de $\mathbb{Z}$ en $\mathbb{R}$?
5. Si K es un cuerpo, A un anillo con identidad (no necesariamente un cuerpo) ¿puede un homomorfismo de anillos con identidad de K en A no ser un monomorfismo?
6. ¿Cuántos homomorfismos de anillos con identidad puedo definir de $\mathbb{Q}$ en $\mathbb{Z}$?
   ¿y de $\mathbb{R}$ en $\mathbb{Z}$?

Ejercicios:

1. Para los conjuntos y operaciones dadas en cada caso, analizar las propiedades de éstas y decir en qué casos tenemos un monoide y/o grupo, especificando si es abeliano o no:

i. $G = \mathbb{Z}$, $x * y = x + y + x.y$
ii. $G = \mathbb{N}$, $x * y = (x, y) = mcd\{x, y\}$
iii. $G = \mathbb{Z}$, $x * y = x + 1$

2. ¿Cuáles de los siguientes subconjuntos de $\mathbb{Z}_{13}^*$ forman un subgrupo con respecto a la multiplicación?

i. $\{\overline{1}, \overline{12}\}$ ii. $\{\overline{1}, \overline{2}, \overline{4}, \overline{6}, \overline{8}, \overline{10}, \overline{12}\}$

3. ¿Cuáles de los siguientes conjuntos, junto con la operación que se indica en cada caso, forman grupo?

i. $S = \{x \in \mathbb{Z} \ / \ x < 0\}$, operación: +
ii. $T = \{5x \ / \ x \in \mathbb{Z}\}$, operación: +
iii. $U = \{\overline{a} \in \mathbb{Z}_n \ / \ (a, n) = 1\}$, operación: ·

4. Sean $(G , *)$ un monoide conmutativo, $a, b \in G$. Demostrar que $\forall n \in \mathbb{N}$ $(a * b)^n = a^n * b^n$ (En particular si $(G , +)$ es un grupo abeliano $n(a + b) = na + nb$).

5. Sean $(G , \cdot)$ un grupo, e el neutro, $a, b \in G$. Demostrar que se verifican las siguientes propiedades:

i. $e^{-1} = e$
ii. $(a . b)^{-1} = b^{-1}. a^{-1}$
iii. $(a^{-1})^{-1} = a$

6. Sea $(G , \cdot)$ un monoide. Demostrar que es un grupo si y sólo si las ecuaciones $ax = b \ \wedge \ xa = b$ admiten solución $\forall a, b \in G$. Demostrar que en cada caso la solución es única.

7. Sea $(G , \cdot)$ un grupo con neutro 1. Demostrar que:

i. Si $a, b, c \in G$, $a.b = a.c \ \vee \ b.a = c.a \Rightarrow b = c$.
ii. $a.b = b.a \Leftrightarrow a^{-1}. b^{-1} = b^{-1}. a^{-1}$.
iii. $x \in G$, $x^2 = x \ \Leftrightarrow \ x = 1$.

8. Sea $(G , \cdot)$ un grupo. Probar que si $\forall x \in G \ x^2 = 1 \ \Rightarrow G$ es abeliano.

9. Sean $(G , \cdot)$ un grupo, $a \in G$, $n, m \in \mathbb{Z}$. Demostrar las siguientes propiedades:

i. $a^{-n} = (a^{-1})^n$
ii. $a^n.a^m = a^{n+m}$
iii. $(a^n)^m = a^{n.m}$

10. Probar que $n\mathbb{Z} \underset{sg}{\subset} \mathbb{Z} \ \forall n \in \mathbb{Z}$, y que $n\mathbb{Z} = (-n)\mathbb{Z} \ \forall n \in \mathbb{N}$. ¿Qué subgrupos se obtienen para $n = 0$ y $n = 1$?

11. i. Decir si es verdadero o falso que:

a. $2\mathbb{Z} \underset{sg}{\subset} 6\mathbb{Z}$ b. $3\mathbb{Z} \underset{sg}{\subset} 6\mathbb{Z}$ c. $6\mathbb{Z} \underset{sg}{\subset} 2\mathbb{Z}$

d. $6\mathbb{Z} \underset{sg}{\subset} 3\mathbb{Z}$ e. $6\mathbb{Z} \underset{sg}{\subset} 8\mathbb{Z}$ f. $9\mathbb{Z} \underset{sg}{\subset} 6\mathbb{Z}$

Justificar en cada caso.

ii. Establecer condiciones necesarias y suficientes sobre n , $m \in \mathbb{N}$ para que $n\mathbb{Z} \underset{sg}{\subset} m\mathbb{Z}$, y demostrarlas.

12. Sea el conjunto $\mathbb{S}(\mathbb{Z}) = \{ n\mathbb{Z} \ / \ n \in \mathbb{N} \ \wedge \ n > 1 \}$ de los subgrupos no triviales de $\mathbb{Z}$, ordenado por inclusión. Encontrar elementos maximales y/o minimales, si los hubiera.

13. i. Determinar los subgrupos de los siguientes grupos aditivos: $\mathbb{Z}_2$, $\mathbb{Z}_3$, $\mathbb{Z}_4$, $\mathbb{Z}_5$, $\mathbb{Z}_9$, $\mathbb{Z}_{10}$.
ii. Los subgrupos encontrados en el inciso i) ¿son cíclicos?

14. Determinar cuáles de los siguientes subconjuntos del grupo aditivo $\mathbb{R}$ son subgrupos:

i. $H = \{ x \ / \ x \geq 0 \}$ ii. $G = \left\{ r\sqrt{5} \ / \ r \in \mathbb{Q} \right\}$

iii. $S = \left\{ r + s\sqrt{2} \ / \ r, s \in \mathbb{Q} \right\}$ iv. $T = \left\{ \frac{n}{2} \ / \ n \in \mathbb{Z} \right\}$

v. $U = \left\{ \frac{n}{2^i 5^j} \ / \ n \in \mathbb{Z},\ i, j \in \mathbb{N}_0 \right\}$ vi. $V = \left\{ \frac{n}{m} \ / \ n \in \mathbb{Z},\ m \in \mathbb{N} \ impar \right\}$

vii. $W = \left\{ \frac{n}{m} \ / \ n \in \mathbb{Z} \ par,\ m \in \mathbb{N} \right\}$

15. Descomponer las siguientes permutaciones en ciclos disjuntos y calcular sus órdenes:

i. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 3 & 1 & 6 & 5 \end{pmatrix}$; ii. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 1 & 4 & 2 & 5 \end{pmatrix}$; iii. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 7 & 5 & 2 & 6 & 1 & 4 \end{pmatrix}$

iv. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 5 & 7 & 4 & 8 & 2 & 1 & 6 \end{pmatrix}$; v. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 4 & 3 & 2 & 7 & 6 & 9 & 1 & 10 & 8 & 5 \end{pmatrix}$

16. i. Si $\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 7 & 5 & 2 & 6 & 1 & 4 \end{pmatrix}$, calcular σ_1^{1000}

ii. Para $\sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 5 & 7 & 4 & 8 & 2 & 1 & 6 \end{pmatrix}$, calcular σ_2^{914}

17. Escribir las permutaciones anteriores como producto de transposiciones y calcular sus signos.

18. Determinar en función de *n* la paridad de la permutación:

$$\begin{pmatrix} 1 & 2 & 3 & \ldots & n-2 & n-1 & n \\ n & n-1 & n-2 & \ldots & 3 & 2 & 1 \end{pmatrix}$$

19. Sea en S_n el conjunto $G_j = \{ \sigma \in S_n \ / \ \sigma(j) = j \}$ con $1 \leq j \leq n$. Demostrar que $G_j \underset{sg}{\subset} S_n$.

20. Probar que si σ es una permutación y $(i_1, i_2, i_3, i_4, ..., i_{k-1}, i_k)$ es un ciclo, se verifica que $\sigma^{-1}(i_1, i_2, i_3, ..., i_{r-1}, i_r)\sigma = (\sigma(i_1), \sigma(i_2), ..., \sigma(i_{r-1}), \sigma(i_r))$.

21. i. Demostrar que $(k, h) = (1, k)\,(1, h)\,(1, k)$.
ii. Mostrar que S_n está generado por el conjunto de transposiciones $\{(1, j) \ / \ j = 1, 2, ..., n\}$.

22. i. Demostrar que $(1, k + 1) = (k, k+1)\,(1, k)\,(k, k + 1)$.
ii. Mostrar que S_n está generado por el conjunto de transposiciones $\{(j, j+1) / \ j = 1, 2, ..., n-1\}$.

23. Dar ejemplos de:
i. un monomorfismo de grupos que no sea epimorfismo.
ii. un epimorfismo de grupos que no sea monomorfismo.
iii. un isomorfismo de grupos que no sea automorfismo.
iv. un endomorfismo de grupos que no sea automorfismo.
v. un automorfismo no trivial de grupos.

24. Sea $f : G \to H$ un homomorfismo de grupos. Demostrar que $\forall a \in G$, $f(a^n) = (f(a^n)) \ \forall n \in \mathbb{Z}$.

25. ¿Se puede definir homomorfismos de grupos de:

i. $\mathbb{Z}$ en $\mathbb{Z}_n$	ii. $\mathbb{Z}_n$ en $\mathbb{Z}$	iii. $\mathbb{Z}_2$ en $\mathbb{Z}_4$	iv. $\mathbb{Z}_4$ en $\mathbb{Z}_2$
v. $\mathbb{Z}_3$ en $\mathbb{Z}_5$	vi. $\mathbb{Z}_5$ en $\mathbb{Z}_2$	vii. $\mathbb{Z}_5$ en $\mathbb{Z}_{10}$	viii. $\mathbb{Z}_{10}$ en $\mathbb{Z}_5$
ix. $\mathbb{Z}_3$ en $\mathbb{Z}_9$	x. $\mathbb{Z}_9$ en $\mathbb{Z}_3$	xi. $\mathbb{Z}_4$ en $\mathbb{Z}_{10}$?	

Justificar.

26. Enunciar condiciones necesarias y suficientes sobre n , $m \in \mathbb{N}$ para que exista un homomorfismo de grupos de $\mathbb{Z}_n$ en $\mathbb{Z}_m$ ¿Cuándo este homomorfismo puede ser monomorfismo?, ¿y epimorfismo?, ¿e isomorfismo?

27. Sean los grupos aditivos de $\mathbb{Z}$ y $\mathbb{Q}$.
i. Demostrar que hay un único homomorfismo de grupos de $\mathbb{Q}$ en $\mathbb{Z}$ que es el idénticamente nulo, o sea si $f : \mathbb{Q} \to \mathbb{Z}$ es un homorfismo de los grupos aditivos correspondientes, entonces $f \equiv 0$ ($f(x) = 0 \ \forall x \in \mathbb{Q}$).

ii. Si $f : \mathbb{Z} \to \mathbb{Q}$ es un homomorfismo de grupos tal que $f(1) = 1$ entonces f es el homomorfismo inclusión de $\mathbb{Z}$ en $\mathbb{Q}$, o sea $f(x) = x \ \forall x \in \mathbb{Z}$.

iii. Si f y g son dos homomorfismos de grupos de $\mathbb{Z} \to \mathbb{Q}$ tales que $f(1) = g(1) \Rightarrow f = g$.

28. Sean $(G , *)$, $(H , \bullet)$, $(T , \otimes)$ grupos; $f : G \to H$, $g : H \to T$ homomorfismos de grupos. Demostrar:
i. f y g monomorfismos $\Rightarrow$ $g \circ f : G \to T$ monomorfismo.
ii. f y g epimorfismos $\Rightarrow$ $g \circ f : G \to T$ epimorfismo.
iii. f y g isomorfismos $\Rightarrow$ $g \circ f : G \to T$ isomorfismo.
iv. f isomorfismo $\Rightarrow$ f^{-1} isomorfismo.

29. Demostrar que todo grupo cíclico finito de orden *n* es isomorfo a $\mathbb{Z}_n$, y que los grupos cíclicos infinitos son isomorfos a $\mathbb{Z}$.

30. Demostrar que la aplicación $\phi : S_n \to \{1,-1\}$ definida por $\phi(\sigma) = sg(\sigma)$ es un homomorfismo del grupo simétrico S_n en el grupo multiplicativo $\{1,-1\}$. ¿Es epimorfismo?, ¿cuál es el núcleo?

31. Sean *A* un anillo, a , $b \in A$. Demostrar las siguientes propiedades:
i. $a \,.0 = 0$
ii. $-(-a) = a$
iii. $(-a)\,.\,b = a\,.\,(-b) = -a.b$
iv. $(-1)\,.\,a = -a$
v. $(-a).(-b) = a.b$

32. Caracterizar los subanillos con identidad del anillo $\mathbb{Z}$. Análogamente para el anillo $\mathbb{Z}_n$.

33. Demostrar que los subanillos con identidad de un dominio de integridad son también dominio de integridad.

34. Sea *A* dominio de integridad, $a,b \in A$, $a \neq 0$. Demostrar:
i. $1 \mid b$, $-1 \mid b$.
ii. $a \mid a$, $a \mid -a$, $-a \mid a$.
iii. $a \mid b \Rightarrow a \mid -b \;\wedge\; -a \mid b$.
iv. $a \mid b \;\Rightarrow\; a \mid bc \quad \forall c \in A$.
v. Para $c \in A$, $b \neq 0$, $a \mid b \;\wedge\; b \mid c \;\Rightarrow\; a \mid c$ (transitiva).
vi. Para $b \neq 0$, $a \mid b \;\wedge\; b \mid a \;\Leftrightarrow\; \exists u \in A^*$ tal que $b = ua$.
vii. Para $c \in A$, $a \mid b \;\wedge\; a \mid c \;\Rightarrow\; a \mid (b+c)$.
viii. Para $c \in A$, $a \mid (b+c) \;\wedge\; a \mid b \;\Rightarrow\; a \mid c$.

35. La relación en *A* : $a \sim b \;\Leftrightarrow$ "a es asociado a b ", es una relación de equivalencia.

36. Sea *A* dominio de integridad. La relación en $A \times (A - \{0\})$ definida por:

$$(a,b) \sim (c,d) \;\Leftrightarrow\; ad = bc$$

es una relación de equivalencia.

37. Demostrar que las operaciones definidas en $K = {A \times (A - \{0\}) \big/ \sim}$:

Suma: $\overline{(a,b)} + \overline{(c,d)} = \overline{(ad+bc, bd)}$
Producto: $\overline{(a,b)}\,.\,\overline{(c,d)} = \overline{(ac,bd)}$
lo estructuran como cuerpo.

38. i Sea $a \in A$, el conjunto $I = \{ ak \;/\; k \in A \}$ es un ideal de *A* .
ii. Si *J* es ideal de *A* , $a \in J$, entonces $(a) \subset J$, o sea (a) es el "menor" ideal de *A* que contiene a a .

39. Sea A un dominio de integridad, sea $\{ J_i \}_{i \in R}$ una cadena de ideales en A, demostrar que el conjunto $H = \bigcup_{i \in R} J_i$ es un ideal de A.

40. Sea I ideal propio de A, demostrar que existe un ideal maximal M tal que $I \subset M$ (o sea, todo ideal propio está contenido en un ideal maximal).
Pista: razonar en forma similar al teorema precedente al Lema de Zorn.

41. Sea A dominio de integridad, I ideal de A.
i. Si $I = (a)$, demostrar que los generadores de I son los asociados de a.
ii. $(a) \subset (b) \iff b \mid a$. En particular $(a) = (b) \iff a$ y b son asociados.

42. Sea A dominio de integridad.
i. $p \in A$ es irreducible, entonces lo son todos sus asociados.
ii. $p \in A$ es primo, entonces lo son todos sus asociados.

43. Sea A dominio de integridad, $a, b \in A$, $a \neq 0 \vee b \neq 0$. Demostrar que dos m.c.d. de a y b son asociados. Recíprocamente, si g es un m.c.d. de a y b entonces todo asociado a g también lo es.

44. Sea A dominio principal, demostrar:
i. Si $p \in A$ es primo y $p \mid \prod_{i=}^{n} a_i$, con $a_i \in A \ \forall i = 1, ..., n$, entonces $\exists j$, $1 \leq j \leq n$ tal que $p \mid a_j$.
ii. Si $a \mid bc \ \wedge \ (a, b) = 1$ entonces $a \mid c$.

45. Sea A dominio euclidiano, $a, b \in A - \{0\}$. Si a y b son asociados entonces $d(a) = d(b)$.

46. Sea K cuerpo.
i. Si $car\ K = p$, p primo, demostrar que para $n \in \mathbb{N}$, $n1 = 0 \iff p \mid n$
ii. $car\ K = 2$ si y sólo si existe un a no nulo en K tal que $a = -a$.
Si $car\ K = 2$, $a = -a$ para todo a en K.
iii. Si existen $a \in K - \{0\}$ y $n \in \mathbb{N}$ tales que $na = 0$ entonces $car\ K = p$ para un primo positivo p que divida a n.

47. A partir del ejercicio 25 caracterizar completamente los endomorfismos de anillos con identidad de los anillos $\mathbb{Z}$ y $\mathbb{Z}_n$.

48. i. Definir, si es posible, tres homomorfismos de anillos con identidad de $\mathbb{Z} \to \mathbb{Q}$. ¿Es posible definir un homomorfismo de anillos con identidad de $\mathbb{Q} \to \mathbb{Z}$?
ii. Caracterizar los homomorfismos de anillos con identidad de $\mathbb{Z} \to \mathbb{Z}_n$ y de $\mathbb{Z}_n \to \mathbb{Z}$.
iii. Demostrar que el único automorfismo del cuerpo $\mathbb{Q}$ es la identidad.

49.i. Demostrar que la composición de homomorfismos de anillos con identidad es un homomorfismo de anillos con identidad.
ii. Demostrar que la inversa de un isomomorfismo de anillos con identidad es también un isomorfismo de anillos con identidad.

50. De los subconjuntos de $\mathbb{R}$ del ejercicio 14. , decir cuáles de ellos son subanillos con identidad del anillo $\mathbb{R}$ y establecer cuáles son subcuerpos.

51. Sean *K* un cuerpo y *A* un anillo con identidad. Demostrar que todo homomorfismo de anillos con identidad de $K \to A$ es monomorfismo.

52. Determinar los cuadrados en $\mathbb{Z}_n$ para $2 \leq n \leq 15$.

53. i. Demostrar que la aplicación $\theta : (\mathbb{Z}_n^*, \cdot) \to (\mathbb{Z}_n^*, \cdot)$ definida por $\theta(x) = x^2$, es un homomorfismo de grupos.

ii. Para $p \in \mathbb{N}$, *p* primo, determinar el $Ker(\theta)$. ¿Y para *n* no primo?

iii. Para $p \in \mathbb{N}$, *p* primo, ¿cuál es el $o(Im(\theta))$?

54. Demostrar que:

i. Para *p* primo positivo impar, $a \in \mathbb{N}$, $1 \leq a \leq p-1$, la mitad de ellos son RC (*p*) y la otra mitad son no RC (*p*).

ii. Sea $a = bc$, con $a, b, c \in \mathbb{Z}$, $p \in \mathbb{N}$ primo tal que $p \nmid a$. Entonces *a* es RC (*mód p*) si y sólo si *b* y *c* son ambos RC (*mód p*) o ambos no RC (*mód p*) , o lo que es equivalente:

$$\left(\frac{cd}{p}\right) = \left(\frac{c}{p}\right)\left(\frac{d}{p}\right).$$

iii. ***Criterio de Euler* :** Sea $a \in \mathbb{Z}$, $p \in \mathbb{N}$ primo tal que $p \nmid a$. Entonces:

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \quad (mód\ p).$$

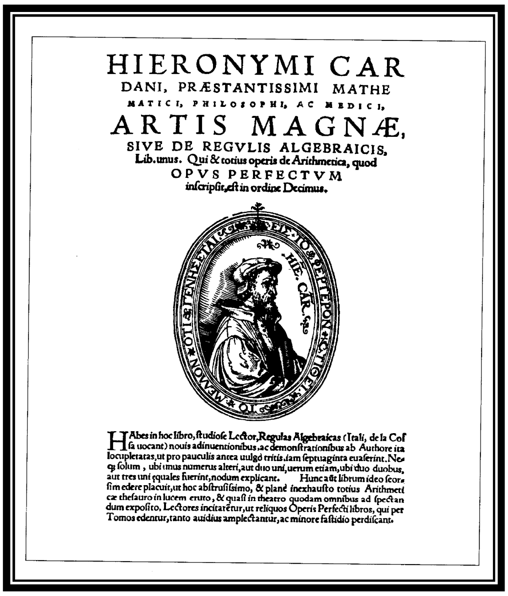
Pista: Observar que $a^{p-1} \equiv 1 \ (p)$ entonces $a^{\frac{p-1}{2}} \equiv 1 \quad \vee \quad a^{\frac{p-1}{2}} \equiv -1 \quad (mód\ p)$

Además, recordar $x^{\frac{p-1}{2}} - 1 = 0$ tiene, cuanto más, $\frac{p-1}{2}$ soluciones en $\mathbb{Z}_p$

(ver capítulo de Polinomios).

CAPÍTULO VIII

ANILLO DE POLINOMIOS


HIERONYMI CAR
DANI, PRÆSTANTISSIMI MATHE
MATICI, PHILOSOPHI, AC MEDICI,
ARTIS MAGNÆ,
SIVE DE REGVLIS ALGEBRAICIS,
Lib. unus. Qui & totius operis de Arithmetica, quod
OPVS PERFECTVM
inscripsit, est in ordine Decimus.

HIE. CAR.

HAbes in hoc libro, studiose Lector, Regulas Algebraicas (Itali, de la Cos
sa uocant) nouis adinuentionibus, ac demonstrationibus ab Authore ita
locupletatas, ut pro pauculis antea uulgò tritis, iam septuaginta euaserint. Ne-
que solum, ubi unus numerus alteri, aut duo uni, uerum etiam, ubi duo duobus,
aut tres uni æquales fuerint, nodum explicant. Hunc aût librum ideo seor-
sim edere placuit, ut hoc abstrusissimo, & planè inexhausto totius Arithmeti
cæ thesauro in lucem eruto, & quasi in theatro quodam omnibus ad spectan
dum exposito, Lectores incitaretur, ut reliquos Operis Perfecti libros, qui per
Tomos edentur, tanto auidius amplectantur, ac minore fastidio perdiscant.

En el año 1545 se divulgó la solución de la ecuación cúbica y de la cuártica, gracias a la publicación del Ars Magna de Jerónimo Cardano (1501-1576). Sin embargo no fue Cardano el descubridor original de la solución de la ecuación cúbica ni de la cuártica, tal como él mismo admite francamente en su libro. La sugerencia para resolver la cúbica la obtuvo de Niccolo Tartaglia (1500-1557) y la de la ecuación cuártica la descubrió el antiguo secretario de Cardano, Ludovico Ferrari. (1522-1565). Lo que no menciona Cardano en el Ars Magna es que le había jurado a Tartaglia, quien intentaba publicar la solución de la cúbica como la parte culminante de su futuro tratado de Algebra, no develar el secreto. Asimismo, Tartaglia había publicado una traducción de Arquímedes (1543) derivada de la de Moerbeke como si fuera propia y, en su obra Quesiti et inventioni diverse (1546), había dado la ley del plano inclinado, presumiblemente derivada de la obra de Jordano Nemorario, sin aclarar su autor. Posiblemente, el mismo Tartaglia, haya obtenido la resolución de la cúbica de alguna fuente anterior. En definitiva, ni Cardano ni Tartaglia fueron los primeros en hacer el descubrimiento, sino alguien que casi nadie recuerda hoy: Scipione del Ferro (1465-1526), profesor de Matemática en Bolonia, que no publicó la solución, pero se la reveló antes de morir a uno de sus alumnos. A mediados del siglo XIX, mediante el estudio de las funciones elípticas y contemporáneamente con Charles Hermite (1822-1901), Leopold Kronecker (1823-1891) dio una solución de la ecuación de quinto grado.

Un objetivo central del Álgebra es resolver ecuaciones *polinomiales*, determinar, si es posible, cuándo y dónde tienen solución, y cuando las tienen, cuántas. Para poder encarar el estudio de la *resolución de ecuaciones polinomiales* y dar algunas respuestas a los problemas que se plantean, necesitamos definir una nueva estructura algebraica, *el anillo de polinomios*, construir en él una *aritmética* que se asemeje lo más posible, bajo ciertas condiciones, a la desarrollada en el anillo $\mathbb{Z}$ de los números enteros.

.

Anillos de expresiones polinomiales

En lo que sigue, los anillos a los que haremos referencia serán **siempre** anillos conmutativos con identidad, los subanillos de éstos, serán subanillos con identidad, y los homomorfismos serán homomorfismos de anillos con identidad.

***Definición*:** Sean A , B anillos conmutativos con identidad; $A \underset{suba.}{\subset} B$, $b \in B$,

llamaremos *expresión polinomial en b con coeficientes en A* a un elemento de B del tipo: $p(b) = a_n b^n + a_{n-1} b^{n-1} + a_{n-2} b^{n-2} + ... + a_2 b^2 + a_1 b + a_0$ con $a_i \in A \ \forall\, i = 0,1,2,\ldots,n$.

Al conjunto de expresiones polinomiales en b con coeficientes en A lo notaremos $A[b]$.

***Proposición*:** $A[b]$ es un subanillo de B que contiene a A y a b.

***Demostración*:** $A \subset A[b]$ es inmediato, pues si $a \in A$, $a = a + 0.b \in A[b]$ ya que $0 \in A$.

Sean $p(b)$, $q(b) \in A[b]$, queremos ver que $p(b) + q(b) \in A[b]$ $\wedge$ $p(b) \,.\, q(b) \in A[b]$, porque ya sabemos que $1 \in A[b]$ porque $1 \in A$.

$$p(b) = \sum_{i=0}^{n} a_i b^i \quad , \quad q(b) = \sum_{i=0}^{n} c_i b^i \ \text{, con} \quad a_i \ , \ c_i \in A \quad \forall\, i = 0,1,2,\ldots,n$$

Por las propiedades asociativa y conmutativa de la suma, y distributiva tenemos que

$$p(b) + q(b) = \sum_{i=0}^{n} (a_i + c_i) b^i \in A[b] \quad \text{pues} \quad a_i + c_i \in A \quad \forall\, i = 0,1,2,\ldots,n$$

para $c \in A$, $cb^k . p(b) = \sum_{i=0}^{n} c a_i b^{i+k} \in A[b]$ pues $c\, a_i \in A \quad \forall\, i = 0,1,2,\ldots,n$

entonces para $q(b) = \sum_{j=0}^{m} c_j b^j \in A[b]$

$$q(b) \,.\, p(b) = (\sum_{j=0}^{m} c_j b^j)(\sum_{i=0}^{n} a_i b^i) = \sum_{j=0}^{m} c_j b^j \sum_{i=0}^{n} a_i b^i = \sum_{j=0}^{m} \sum_{i=0}^{n} c_j a_i b^{i+j} = \sum_{k=0}^{n+m} (\sum_{i+j=k} c_j a_i) b^k \in A[b].$$

Como $1 \in A \ \wedge \ -1 \in A$

$$-\, p(b) = (-1).\, p(b) \in A[b] \quad \therefore \quad p(b) - q(b) = p(b) + (-\, q(b)) \in A[b]$$

$\therefore$ $A[b] \underset{suba.}{\subset} B$. Además $b = 1.b + 0 \in A[b]$.

***Definición*:** Al anillo $A[b]$ lo llamaremos *anillo de expresiones polinomiales en b con coeficientes en A.*

***Definición*:** Sean A , B anillos conmutativos con identidad; $A \underset{suba.}{\subset} B$. Sea $b \in B$; b se dice *algebraico sobre A*, si existe una expresión polinomial $p(b)$ con coeficientes en A, no todos nulos, tal que $p(b) = 0$. En símbolos:

$\exists\ a_i \in A$, $i = 0,1,2,\ldots,n$, no todos nulos, tales que

$$a_n b^n + a_{n-1} b^{n-1} + a_{n-2} b^{n-2} + \ldots.. + a_2 b^2 + a_1 b + a_0 = 0$$

***Definición*:** Sean A , B anillos conmutativos con identidad; $A \underset{suba.}{\subset} B$. Sea $b \in B$;

b se dice *trascendente sobre A* si no es algebraico sobre A , o sea, para $a_i \in A$

$$a_n b^n + a_{n-1} b^{n-1} + a_{n-2} b^{n-2} + \ldots.. + a_2 b^2 + a_1 b + a_0 = 0 \quad \Rightarrow \quad a_i = 0 \ \forall\ i = 0,1,2,\ldots,n$$

Nota: Los números reales algebraicos son *los algebraicos sobre* $\mathbb{Q}$, y los trascendentes son los *trascendentes sobre* $\mathbb{Q}$, pensando a $\mathbb{Q}$ como subanillo de $\mathbb{R}$.

***Proposición*:** Sean A , B anillos conmutativos con identidad; $A \underset{suba.}{\subset} B$. Sea $b \in B$ trascendente sobre A . Son equivalentes:

- **i.** b es trascendente sobre A.
- **ii.** dos expresiones polinomiales en b , $p(b), q(b) \in A[b]$ coinciden si y sólo si coinciden todos sus coeficientes, o sea si $p(b) = \sum_{i=0}^{n} a_i b^i$, $q(b) = \sum_{i=0}^{n} c_i b^i \in A[b]$,

$$p(b) = \sum_{i=0}^{n} a_i b^i = q(b) = \sum_{i=0}^{n} c_i b^i \quad \Leftrightarrow \quad a_i = c_i \quad \forall\ i = 0,1,2,\ldots,n.$$

***Demostración*: i. $\Rightarrow$ ii.**)

Sean $p(b) = \sum_{i=0}^{n} a_i b^i$, $q(b) = \sum_{i=0}^{n} c_i b^i \in A[b]$ tales que $p(b) = q(b)$

entonces $p(b) - q(b) = 0 \ \therefore \ \sum_{i=0}^{n} (a_i - c_i) b^i = 0$, y como b es trascendente sobre A

tenemos que $a_i - c_i = 0 \quad \forall\ i = 0,1,2,\ldots,n \ \therefore \ a_i = c_i \ \forall\ i = 0,1,2,\ldots,n.$

Claramente $a_i = c_i \ \forall\ i = 0,1,2,\ldots,n \ \Rightarrow \ p(b) = q(b).$

ii. $\Rightarrow$ i.) Es trivial, porque la definición de trascendente es un caso particular de **ii.** ,

ya que $a_n b^n + a_{n-1} b^{n-1} + a_{n-2} b^{n-2} + \ldots.. + a_2 b^2 + a_1 b + a_0 = 0 = 0.b^n + 0.b^{n-1} + \ldots + 0.b + 0$

$\Rightarrow \ a_i = 0 \ \forall\ i = 0,1,2,\ldots,n.$

Nota: La proposición precedente nos dice que si tenemos un elemento b trascendente sobre A, cada expresión polinomial en b con coeficientes en A está *unívocamente* determinada por sus coeficientes.

Contraejemplo: Observemos que cuando el elemento es algebraico no tenemos la unicidad de las expresiones polinomiales con relación a los coeficientes.
Por ejemplo, en $\mathbb{Q}[\sqrt{2}]$, donde sabemos que $\sqrt{2}$ es algebraico, las expresiones polinomiales en $\sqrt{2}$: $p(b) = 3(\sqrt{2})^3 + 5(\sqrt{2})^2 - 3\sqrt{2} + 4$;

$q(b) = (\sqrt{2})^5 - 3(\sqrt{2})^4 + 2(\sqrt{2})^2 - \sqrt{2} + 22$, verifican que $p(b) = q(b) = 3\sqrt{2} + 14$.

Vemos como tres expresiones polinomiales diferentes, porque tienen distintos coeficientes, dan, sin embargo, el mismo número real.

***Teorema*:** Sean A , B anillos conmutativos con identidad; $A \underset{suba.}{\subset} B$. Sean $b, c \in B$ trascendentes sobre A . Entonces $A[b] \approx A[c]$.

***Demostración*:** Sea $\psi : A[b] \to A[c]$ definida por $\psi(\sum_{i=0}^{n} a_i b^i) = \sum_{i=0}^{n} a_i c^i$

ψ está bien definida porque $p(b)$ está unívocamente determinado por sus coeficientes, por ser b trascendente sobre A.

ψ es homomorfismo de anillos con identidad puesto que:

$$\psi(p(b) + q(b)) = \psi(\sum_{i=0}^{n} a_i b^i + \sum_{i=0}^{n} d_i b^i) = \psi(\sum_{i=0}^{n} (a_i + d_i) b^i) = \sum_{i=0}^{n} (a_i + d_i) c^i =$$

$$= \sum_{i=0}^{n} a_i c^i + \sum_{i=0}^{n} d_i c^i = \psi(\sum_{i=0}^{n} a_i b^i) + \psi(\sum_{i=0}^{n} d_i b^i) = \psi(p(b)) + \psi(q(b))$$

Sean $p(b) = \sum_{i=0}^{n} a_i b^i$, $q(b) = \sum_{j=0}^{m} d_j b^j$; $\psi(p(b) \,.\, q(b)) = \psi((\sum_{i=0}^{n} a_i b^i).(\sum_{j=0}^{m} d_j b^j)) =$

$$= \psi(\sum_{k=0}^{n+m} (\sum_{i+j=k} a_i d_j) b^k = \sum_{k=0}^{n+m} (\sum_{i+j=k} a_i d_j) c^k = (\sum_{i=0}^{n} a_i c^i).(\sum_{j=0}^{m} d_j c^j) = \psi(p(b)) \,.\, \psi(q(b)) \,.$$

Además $\psi(a) = a \quad \forall a \in A$, luego $\psi(1) = 1 \ \wedge \ \psi(0) = 0$. Luego ψ es homomorfismo de anillos con identidad.

Falta demostrar que ψ es biyectiva.

ψ es monomorfismo puesto que si $p(b) \in Ker(\psi)$, con $p(b) = \sum_{i=0}^{n} a_i b^i$,

se tiene que $\sum_{i=0}^{n} a_i c^i = 0$, pero como c es trascendente sobre A , eso significa que

$a_i = 0 \quad \forall\, i = 0,1,2,\ldots,n \quad \therefore \quad p(b) = 0$.

ψ es epimorfismo puesto que si $t(c)\in A[c]$, $t(c) = \sum_{i=0}^{k} e_i c^i$, claramente se ve que

$t(c) = \psi(\sum_{i=0}^{k} e_i b^i) \in Im(\psi)$, con lo cual probamos que ψ es suryectiva.

Por lo tanto ψ es un isomorfismo de anillos con identidad $\therefore$ $A[b] \approx A[c]$.

Nota: Si en el enunciado del teorema precedente hubiésemos tomado A , B , C anillos con identidad; $A \underset{suba.}{\subset} B \ \wedge \ A \underset{suba.}{\subset} C$, $b\in B$, $c\in C$ ambos trascendentes sobre A , podríamos haber demostrado $A[b] \approx A[c]$ en forma totalmente análoga a la realizada para demostrar el teorema precedente, lo que muestra que el anillo de expresiones polinomiales en b con coeficientes en A depende fundamentalmente de b y de A , no del anillo B que contiene a b y a A.

***Definición*:** Sean A , B anillos conmutativos con identidad tales que $A \underset{suba.}{\subset} B$, $b\in B$ trascendente sobre A.

Se denomina *anillo de polinomios en una indeterminada x con coeficientes en* A al anillo $A[x]$ de expresiones polinomiales $a_0 + a_1 x + a_2 x^2 + ... + a_{n-1} x^{n-1} + a_n x^n$, $a_i \in A$, $\forall\, i = 0,1,2,\ldots,n$, dotado de un isomorfismo $\psi : A[x] \rightarrow A[b]$ tal que

$$\psi(a_0 + a_1 x + a_2 x^2 + ... + a_{n-1} x^{n-1} + a_n x^n) = a_n b^n + a_{n-1} b^{n-1} + a_{n-2} b^{n-2} + ... + a_2 b^2 + a_1 b + a_0 .$$

La estructura de anillo de $A[x]$ está unívocamente determinada por la de $A[b]$; la definición no depende del elemento b elegido, mientras sea trascendente sobre A , puesto que si c es trascendente sobre A , por el teorema anterior, tenemos que $A[x] \approx A[b] \approx A[c]$.

Anillo de polinomios A[x]

Llamaremos *polinomios en* x *con coeficientes en* A a las expresiones polinomiales en x con coeficientes en A.

Sean los polinomios $p(x) = a_0 + a_1 x + a_2 x^2 + ... + a_{n-1} x^{n-1} + a_n x^n = \sum_{i=0}^{n} a_i x^i$,

$q(x) = \sum_{i=0}^{n} b_i x^i$, por lo visto anteriormente $p(x) + q(x) = \sum_{i=0}^{n} (a_i + b_i) x^i$, y si

$t(x) = \sum_{j=0}^{m} c_j x^j$ entonces $p(x).\, t(x) = \sum_{k=0}^{n+m} d_k x^k$, donde $d_k = \sum_{i+j=k} a_i c_j$.

Además, el polinomio nulo es aquél cuyos coeficientes son todos nulos; el opuesto de $q(x)$, o sea $-\, q(x)$, es el polinomio $\sum_{i=0}^{n} -b_i x^i$.

Llamemos al algebrista…

El término álgebra surgió en España, donde la influencia árabe fue muy importante y se utilizó para referirse al arte de restituir a su lugar los huesos dislocados. Por ello, el término "algebrista" hacía referencia a la persona que sabía arreglar las dislocaciones. En Don Quijote de la Mancha podemos encontrar estos términos en muchos de sus capítulos, por ejemplo: "…donde fue ventura hallar un algebrista, con quien se curó el Sansón desgraciado…"). La obra más importante del matemático árabe Al-Khowarizmi fue "Kitab al-jabr wa al-muqabalah", título que dio nombre a toda una disciplina matemática: el álgebra. Al-jabr significa "restitución", que es lo que se intenta hacer cuando se resuelve una ecuación, restituir el valor de la incógnita.

Página del libro Kitab al-jabr wa al-muqabalah

Grado de un polinomio

***Definición*:** Sea $p(x) \in A[x]$, $p(x) \neq 0$, $p(x) = \sum_{i=0}^{n} a_i x^i$.

Como $p(x) \neq 0$ entonces $\exists\, i$, $0 \leq i \leq n$, tal que $a_i \neq 0$; sea $k = máx\{\, i \;/\; a_i \neq 0 \,\}$.
k se denomina *grado de* $p(x)$, y se lo nota $k = gr(p(x))$.

Nota: al polinomio nulo no se le define grado.

Los polinomios de grado 0 son los elementos no nulos de *A.*

De acuerdo con las definiciones de suma y producto de polinomios, observamos que si

$p(x), q(x) \in A[x] - \{\, 0 \,\}$, y $p(x) + q(x) \neq 0$ tenemos que

$$gr(p(x) + q(x)) \leq máx\{\, gr(p(x)), gr(q(x)) \}$$

y si $p(x) \,.\, q(x) \neq 0$ $gr(p(x).\, q(x)) \leq gr(p(x)) + gr(q(x))$.

Si $p(x) = \sum_{i=0}^{n} a_i x^i$ con $a_n \neq 0$, o sea, $gr(p(x)) = n$, a_n se denomina *coeficiente principal* de $p(x)$, y a a_0 *término independiente o término constante.*

Un polinomio $p(x)$ se dice *mónico* si su coeficiente principal es 1.

***Teorema*:** Sean $p(x)$, $q(x) \in A[x] - \{\, 0 \,\}$. Si A es dominio de integridad y $p(x) \,.\, q(x) \neq 0$, entonces $gr(p(x).\, q(x)) = gr(p(x)) + gr(q(x))$.
Recíprocamente, si $\forall\, p(x)$, $q(x) \in A[x]$ tales que $p(x) \,.\, q(x) \neq 0$ se verifica que $gr(p(x).\, q(x)) = gr(p(x)) + gr(q(x))$ entonces A es dominio de integridad.

***Demostración*:** Sea A dominio de integridad y sean $p(x), q(x) \in A[x]$ tales que $p(x) \,.\, q(x) \neq 0$.
Sean $p(x) = \sum_{i=0}^{n} a_i x^i$, con $a_n \neq 0$, $q(x) = \sum_{j=0}^{m} b_j x^j$, con $b_m \neq 0$,

$p(x) \,.\, q(x) = \sum_{k=0}^{n+m} d_k x^k$ con $d_k = \sum_{i+j=k} a_i b_j$; $d_{n+m} = a_n.b_m$.

Como A es dominio de integridad y $a_n \neq 0 \wedge b_m \neq 0 \Rightarrow d_{n+m} = a_n.b_m \neq 0$.

Luego $gr(p(x) \,.\, q(x)) = n + m = gr(p(x)) + gr(q(x))$.

Recíprocamente, supongamos que $\forall\, p(x)$, $q(x) \in A[x]$ tales que $p(x) \,.\, q(x) \neq 0$ se verifica que $gr(p(x).\, q(x)) = gr(p(x)) + gr(q(x))$, queremos demostrar que A es dominio de integridad.

Sean a , $b \in A - \{0\}$, y sean los polinomios $p(x) = ax + 1$, $q(x) = bx + 1$; ambos son polinomios no nulos y de grado 1, cuyo producto es $p(x).\, q(x) = abx^2 + (a+b)x + 1 \neq 0$

porque, al menos, uno de sus coeficientes es $1 \neq 0$.

Por hipótesis $gr(p(x) \,.\, q(x)) = gr(p(x)) + gr(q(x)) = 1 + 1 = 2 \Rightarrow a.b \neq 0$, como queríamos demostrar. Por lo tanto A es dominio de integridad.

Contraejemplo: Si A no es dominio de integridad , el grado del producto de dos polinomios no nulos puede ser menor que la suma de los grados.

Sean $A = \mathbb{Z}_6$, $p(x) = 2x + 1$, $q(x) = 3x + 1$; $p(x) \,.\, q(x) = 5x + 1$

$gr(p(x) \,.\, q(x)) = 1 < 2 = gr(p(x)) + gr(q(x))$.

***Teorema*:** $A[x]$ es dominio de integridad si y sólo si A lo es.

***Demostración*:** $\Rightarrow$) Sean a , $b \in A - \{0\}$ ¿ $a.b \neq 0$?

Sean $p(x) = ax \in A[x] - \{0\}$, $q(x) = bx \in A[x] - \{0\}$,

por ser $A[x]$ dominio de integridad $p(x) \,.\, q(x) \neq 0$, $p(x) \,.\, q(x) = abx^2 \Rightarrow a.b \neq 0$

$\therefore$ A es dominio de integridad

$\Leftarrow$) Sea A dominio de integridad, y sean $p(x), q(x) \in A[x] - \{0\}$

$$p(x) = \sum_{i=0}^{n} a_i x^i \quad , \quad a_n \neq 0 \,, \quad q(x) = \sum_{j=0}^{m} b_j x^j \quad , \quad b_m \neq 0$$

$p(x) \,.\, q(x) = \sum_{k=0}^{n+m} d_k x^k$ con $d_k = \sum_{i+j=k} a_i b_j$; $d_{n+m} = a_n.b_m \neq 0$ por ser A íntegro,

por lo cual $p(x) \,.\, q(x) \neq 0$ $\therefore$ $A[x]$ es dominio de integridad

Contraejemplo: Si A no es dominio de integridad , el producto de dos polinomios no nulos puede ser el polinomio nulo.

Sean $A = \mathbb{Z}_6$, $p(x) = 2x + 2$, $q(x) = 3x + 3$

$p(x) \neq 0$, $q(x) \neq 0$ y $p(x) \,.\, q(x) = 0$

Nota: También se podría obtener la implicación " $A[x]$ dominio de integridad $\Rightarrow$ A dominio de integridad" por ser A subanillo de $A[x]$, y los subanillos de dominios de integridad son también dominios de integridad.

Ejercicio: Demostrar que si $p(x) \in A[x]$, A dominio de integridad y $p(x) \neq 0$
$\Rightarrow \quad gr(p(x))^m = m.gr(p(x)) \quad \forall m \in \mathbb{N}$.

Divisibilidad en A[x]:

Definición*:** Sean $a(x), b(x) \in A[x]$, $a(x) \neq 0$, decimos que ***a(x) *divide a* ***b(x)***
(o que $a(x)$ *es factor de* $b(x)$, o que $a(x)$ *es parte de* $b(x)$, o que $a(x)$ *es divisor de* $b(x)$, o que $b(x)$ *es múltiplo de* $a(x)$) si $\exists\, c(x) \in A[x]$ tal que $b(x) = c(x).a(x)$.
Notación: $a(x) \mid b(x)$;
para indicar que $a(x)$ *no divide a* $b(x)$, escribimos $a(x) \nmid b(x)$.

***Propiedades*:** Sean $a(x), b(x), c(x) \in A[x]$, $a(x) \neq 0 \quad \wedge \quad b(x) \neq 0$

i. $a(x) \mid b(x) \ \wedge \ b(x) \mid c(x) \ \Rightarrow \ a(x) \mid c(x)$ (transitividad).
ii. $a(x) \mid b(x) \ \wedge \ a(x) \mid c(x) \ \Rightarrow \ a(x) \mid (b(x) + c(x))$ ¿Vale la recíproca?
iii. $a(x) \mid (b(x) + c(x)) \ \wedge \ a(x) \mid b(x) \ \Rightarrow \ a(x) \mid c(x)$.
iv. $a(x) \mid b(x) \ \Rightarrow \ a(x) \mid b(x) \,.\, c(x) \quad \forall\, c(x) \in A[x]$.
¿es verdadero que $a(x) \mid b(x) \,.\, c(x) \ \Rightarrow \ a(x) \mid b(x) \ \vee \ a(x) \mid c(x)$?
v. $a(x) \mid 0$, $\forall\, a(x) \in A[x]$, $a(x) \neq 0$.

***Demostración*:** Se deja como ejercicio.

Nota: Si A es dominio de integridad, cuando $a(x) \mid b(x)$ $\exists!$ (existe un único) $c(x) \in A[x]$ tal que $b(x) = c(x).a(x)$, pues si $b(x) = c(x).a(x) = c'(x).a(x)$, con $c(x)$, $c'(x) \in A[x]$
$\therefore \quad a(x)(c(x) - c'(x)) = 0$ y como $a(x) \neq 0 \quad \Rightarrow \ c(x) - c'(x) = 0 \ \therefore \ c(x) = c'(x)$.

Ejercicio: Sea A dominio de integridad, $a(x), b(x) \in A[x]$, $a(x) \neq 0$, $b(x) \neq 0$. Demostrar que $a(x) \mid b(x) \ \Rightarrow \ gr(a(x)) \leq gr(b(x))$.

Elementos inversibles en A[x] :

Sea $u(x) \in A[x]$, se dice que $u(x)$ es *inversible* si $\exists\, v(x) \in A[x]$ tal que $u(x) \,.\, v(x) = 1$.

$$(A[x])^* = \{\, u(x) \in A[x] \ / \ u(x) \text{ es inversible} \,\}$$

Si A es dominio de integridad y $u(x) \in A[x]$ es inversible entonces $\exists\, v(x) \in A[x]$ tal que $u(x) \,.\, v(x) = 1 \quad \therefore \quad gr(u(x) \,.\, v(x)) = 0$,
como $0 = gr(u(x) \,.\, v(x)) = gr(u(x) + gr(v(x)) \ \Rightarrow \ gr(u(x)) = gr(v(x)) = 0$
$\therefore \ u(x) = u \in A^* \quad \wedge \quad v(x) = v \in A^*$.

Por lo tanto, si A es dominio de integridad, las unidades de $A[x]$ son las unidades de A, o sea $(A[x])^* = A^*$.

Cuando K es cuerpo, $(K[x])^* = K^* = K - \{\, 0 \,\}$.

Ejemplos: $(\mathbb{Z}[x])^* = \{\, 1, -1 \,\}$; $(\mathbb{Q}[x])^* = \mathbb{Q} - \{\, 0 \,\}$; $(\mathbb{R}[x])^* = \mathbb{R} - \{\, 0 \,\}$;
$(\mathbb{Z}_p[x])^* = \mathbb{Z}_p - \{\, 0 \,\}$, p primo.

Contraejemplo: Si A no es dominio de integridad, existen polinomios inversibles de grado positivo.
Para $A = \mathbb{Z}_4$, $p(x) = 2x + 1$, verifica que $(p(x))^2 = 1$ $\therefore$ $p(x)$ es inversible de grado positivo, y su inverso es él mismo.

Ejercicio: Sean $a(x), b(x) \in A[x]$, $a(x) \neq 0 \wedge b(x) \neq 0$ tales que $a(x) \mid b(x) \wedge b(x) \mid a(x)$,
A dominio de integridad. Demostrar que $\exists u \in A^*$ tal que $b(x) = u.a(x)$.

***Definición*:**
Dos polinomios $a(x), b(x) \in A[x] - \{0\}$ se dicen *asociados* si $\exists u(x) \in (A[x])^*$ tal que
$b(x) = u(x).a(x)$.
Por lo tanto, $a(x)$ y $b(x)$ son asociados $\Leftrightarrow$ $a(x) \mid b(x) \wedge b(x) \mid a(x)$.
Si A es dominio de integridad y $a(x), b(x)$ son asociados entonces $gr(a(x)) = gr(b(x))$.

Ejercicios:

1) La relación en $A[x] - \{0\}$: " $a(x) \sim b(x) \Leftrightarrow a(x)$ y $b(x)$ son asociados ",
es de equivalencia.

2) Si $a(x)$ y $b(x)$ son asociados, $a(x) \mid c(x) \Leftrightarrow b(x) \mid c(x)$.

3) Si $a(x)$ y $b(x)$ son asociados, $c(x) \mid a(x) \Leftrightarrow c(x) \mid b(x)$.

4) Sea K cuerpo. Si $a(x) \neq 0$, $\exists v \in K - \{0\}$ tal que $v.a(x)$ es mónico y asociado a $a(x)$.

5) Sea K cuerpo. Si $a(x), b(x) \in K[x]$ son asociados y mónicos entonces $a(x) = b(x)$.

Por lo tanto, en cada clase de equivalencia de la relación $\sim$ definida más arriba en $K[x]$, existe un único polinomio mónico.

Elementos irreducibles en A[x] :

***Definición*:** Sea $p(x) \in A[x]$, $p(x)$ se denomina *irreducible o extremal* si:
i. $p(x) \neq 0$.
ii. $p(x) \notin (A[x])^*$.
iii. $p(x) = q(x).\ t(x) \Rightarrow q(x) \in (A[x])^* \vee t(x) \in (A[x])^*$.

Si A es dominio de integridad, la definición se puede expresar así:
$p(x)$ es *irreducible o extremal* en $A[x]$ si
i. $p(x) \neq 0$
ii. $gr(p(x)) \geq 1 \vee$ si $gr(p(x)) = 0$, $p(x) = p \notin A^*$
iii. $p(x) = q(x).\ t(x) \Rightarrow (gr(q(x)) = 0 \wedge q(x) = q \in A^*) \vee (gr(t(x)) = 0 \wedge t(x) = t \in A^*)$,
o sea, los divisores de $p(x)$ son únicamente los triviales: las unidades y sus asociados.

Si K es cuerpo, la definición significa que:
$p(x)$ es *irreducible o extremal* en $K[x]$ si
i. $p(x) \notin K$, o sea $p(x)$ tiene grado y éste es positivo

ii. $p(x) = q(x).\, t(x) \;\Rightarrow\; q(x) = q \in K - \{0\} \;\vee\; t(x) = t \in K - \{0\}$,

o sea, $\nexists\, q(x) \in K[x]$ tal que $q(x) \mid p(x) \;\wedge\; 0 < gr(q(x)) < gr(p(x))$.

Ejercicio: Sea A dominio de integridad, si $p(x) \in A[x]$ es irreducible, todos sus asociados son también irreducibles. Si $p(x) \in K[x]$ es irreducible, K es cuerpo, entonces en la clase de equivalencia de $p(x)$ (por la relación $\sim$) existe un único polinomio mónico e irreducible.

***Definición*:** Un polinomio $p(x)$ se dice *reducible* si se puede factorizar como producto de polinomios no triviales, o sea, si $\exists\, q(x), t(x) \in K[x]$ tales que $p(x) = q(x).\, t(x)$
donde $q(x) \notin (A[x])^* \;\wedge\; t(x) \notin (A[x])^*$.
Cuando K es cuerpo, $p(x) \in K[x]$ es *reducible* si $p(x) \neq 0 \;\wedge\; \exists\, q(x) \in K[x]$ tal que $q(x) \mid p(x) \;\wedge\; 0 < gr(q(x)) < gr(p(x))$.

***Teorema*:** Si K es un cuerpo, todo polinomio en $K[x]$ de grado 1 es irreducible.

***Demostración*:** Sea $p(x) \in K[x]$ tal que $gr\,(p(x)) = 1$; $p(x) = ax + b$ con $a \neq 0$.

Sea $p(x) = q(x).\, t(x)$, $q(x), t(x) \in K[x]$, $gr(p(x)) = gr(q(x)) + gr(t(x)) = 1$, y como

$gr(q(x)) \geq 0 \;\wedge\; gr(t(x)) \geq 0$, entonces

$(gr(q(x)) = 0 \;\wedge\; gr(t(x)) = 1) \;\vee\; (gr(q(x)) = 1 \;\wedge\; gr(t(x)) = 0)$

$\therefore\;\; q(x) = q \in K - \{0\} \;\vee\; t(x) = t \in K - \{0\}$ y $p(x)$ es irreducible en $K[x]$.

Nota: Si A es dominio de integridad que no es cuerpo, el teorema no se cumple, pues puede haber polinomios de grado 1 que sean reducibles:

en $\mathbb{Z}[x]$ el polinomio $p(x) = 2x + 2 = 2\,(x + 1) \;\wedge\; 2 \notin \mathbb{Z}^* \;\wedge\; x + 1 \notin \mathbb{Z}^*$, luego es reducible.

Ejercicio: Sea $p(x) = x^2 + 1$; demostrar que es irreducible en $\mathbb{R}[x]$.

***Teorema*:** Sea K cuerpo. Todo polinomio en $K[x]$, de grado positivo, es divisible por un polinomio irreducible.

***Demostración*:** Lo demostraremos por inducción sobre $n = gr(q(x))$.
Sea $q(x) \in K[x]$, $gr(q(x)) = n \geq 1$.

Si $gr(q(x)) = 1$, por el Teorema anterior $q(x)$ es irreducible $\wedge$ $q(x) \mid q(x)$,
$\therefore$ $q(x)$ es divisible por un polinomio irreducible.

HI (hipótesis inductiva): sea $n > 1$, supongamos que todo polinomio de grado k, con $k \in \mathbb{N}$ tal que $1 \leq k < n$, sea divisible por un polinomio irreducible .

Sea $q(x) \in K[x]$, tal que $gr(q(x)) = n$.
Como $gr(q(x)) = n > 1$, $q(x)$ es irreducible $\vee$ $q(x)$ es reducible.

- Si $q(x)$ es irreducible, como $q(x) \mid q(x)$, entonces $q(x)$ es divisible por un polinomio irreducible.

- Si $q(x)$ es reducible, entonces $\exists$ t$(x) \in K[x]$, tal que $t(x) \mid q(x) \;\wedge\; 1 \leq gr(t(x)) < gr(q(x)) = n$.
Por hipótesis inductiva (HI) $\exists\, p(x) \in K[x]$ irreducible tal que $p(x) \mid t(x)$, y como $t(x) \mid q(x)$ entonces $p(x) \mid q(x)$.

Luego todo polinomio de grado positivo en $K[x]$ es divisible por un polinomio irreducible.

Algoritmo de la División (AD) en A[x], A dominio de integridad :

Sean $a(x), b(x) \in A[x]$, $a(x) = \sum_{i=0}^{n} a_i x^i$, $a_n \neq 0$, $a_n \in A^*$.

$\exists!$ (existen únicos) $q(x)$, $r(x) \in A[x]$ tales que $b(x) = q(x).a(x) + r(x)$ con
$0 \leq gr(r(x)) < gr(a(x)) \ \vee \ r(x) = 0$.

***Demostración*:** Demostraremos, primero, la *existencia* de $q(x)$ y $r(x)$.

Sea $B = \{ b(x) - k(x).a(x) \ / \ k(x) \in A[x] \}$

Por ejemplo, en B están $b(x)$; $b(x) - a(x)$; $b(x) + a(x)$; $b(x) - 2a(x)$; $b(x) + 2a(x)$; etc.

- $0 \in B \Leftrightarrow a(x) \mid b(x) \Leftrightarrow \exists q(x) \in A[x]$ tal que $b(x) = q(x).a(x) = q(x).a(x) + 0$.

Luego, cuando $0 \in B$, $\exists! \, q(x), r(x) \in A[x]$ tales que $b(x) = q(x).a(x) + r(x)$ con $r(x) = 0$.

- Supongamos ahora que $0 \notin B$. Sea $r(x)$ un polinomio de grado mínimo en B.

$r(x) \in B \ \therefore \ r(x) = b(x) - q(x).a(x)$, para cierto $q(x) \in A[x] \ \therefore \ b(x) = q(x).a(x) + r(x)$, Falta ver que $gr(r(x)) < gr(a(x))$.

Supongamos que $gr(r(x)) \geq gr(a(x))$, $r(x) = \sum_{j=0}^{m} r_j x^j$ con $r_m \neq 0$, $m \geq n$;

sea $s(x) = r(x) - r_m \, . \, a_n^{-1} \, . \, x^{m-n} . a(x)$.

$s(x) = b(x) - q(x).a(x) - r_m \, . \, a_n^{-1} \, . \, x^{m-n} . a(x) = b(x) - (q(x) + r_m \, . \, a_n^{-1} \, . \, x^{m-n}).a(x) \in B$!! (absurdo!)
pues $gr(s(x)) < gr(r(x))$ y a $r(x)$ lo tomamos de grado mínimo en B

Por lo tanto, $gr(r(x)) < gr(a(x))$.

$\therefore \exists \, q(x), r(x) \in A[x]$ tales que $b(x) = q(x).a(x) + r(x)$ con $0 \leq gr(r(x)) < gr(a(x)) \ \vee \ r(x) = 0$.

Unicidad de $q(x)$ *y* $r(x)$:

Supongamos que existan $q(x), q'(x), r(x), r'(x) \in A[x]$ tales que

$$b(x) = q(x).a(x) + r(x) = q'(x).a(x) + r'(x) ,$$

con $gr(r(x)) < gr(a(x)) \ \vee \ r(x) = 0$, $gr(r'(x)) < gr(a(x)) \ \vee \ r'(x) = 0$.

Entonces $(q(x) - q'(x)).a(x) = r'(x) - r(x) \Rightarrow a(x) \mid (r(x) - r'(x))$.

Si $r'(x) - r(x) \neq 0 \Rightarrow gr(a(x)) \leq máx(gr(r(x) , gr(r'(x)) < gr(a(x))$!! (absurdo!)

$\therefore \quad r'(x) - r(x) = 0$, y así $r(x) = r'(x)$.

Por lo tanto $(q(x) - q'(x)).a(x) = 0$, y como $a(x) \neq 0 \Rightarrow q(x) - q'(x) = 0$

$\therefore \quad q(x) = q'(x).$

Luego $q(x)$ y $r(x)$ son únicos tales que $b(x) = q(x).a(x) + r(x)$, con

$0 \leq gr(r(x)) < gr(a(x)) \quad \vee \quad r(x) = 0.$

***Corolario*:** Si K es cuerpo y $a(x), b(x) \in K[x]$, $a(x) \neq 0$, $\exists!\, q(x)$, $r(x) \in K[x]$ tales que $b(x) = q(x).a(x) + r(x)$ con $0 \leq gr(r(x)) < gr(a(x)) \vee r(x) = 0$.

***Demostración*:** Si $a(x) \neq 0$ su coeficiente principal es no nulo, luego es un elemento inversible en K, que, al ser cuerpo es dominio de integridad, por lo tanto se aplica el teorema.

Nota: Si A es dominio de integridad no cuerpo, como lo es $\mathbb{Z}$, dados dos polinomios no nulos, no podemos garantizar la existencia del cociente y el resto en la división de uno por el otro, sólo cuando el coeficiente principal del divisor sea una unidad de A; si los polinomios tienen sus coeficientes en un cuerpo, esto siempre ocurre, luego dados dos polinomios siempre podemos obtener cociente y resto, y éstos son únicos, por ello decimos que el anillo $K[x]$ es un *dominio euclidiano*, donde la función $d : K[x] - \{0\} \to \mathbb{N}_0$ tal que $d(p(x)) = gr(p(x))$ satisface las condiciones correspondientes. También lo es el anillo $\mathbb{Z}$ de los números enteros, para la función $d : \mathbb{Z} - \{0\} \to \mathbb{N}_0$, $d(x) = |x|$, pero no lo es $\mathbb{Z}[x]$.

Máximo Común Divisor (MCD) en K[x], K cuerpo:

Sean $a(x), b(x) \in K[x]$, no simultáneamente nulos, K cuerpo.

Sea $D = \{ k(x) \in K[x] \ / \ k(x) \mid a(x) \wedge k(x) \mid b(x) \}$, $1 \in D \ \therefore \ D \neq \phi$.

Los grados de los polinomios de D están acotados superiormente en $\mathbb{N}$, pues si $k(x) \in D$ y $a(x) \neq 0$ entonces $gr(a(x)) \geq gr(k(x))$; análogamente si $b(x) \neq 0$.

Si $k(x) \in D$, entonces todos sus asociados también lo están, por lo tanto hay un polinomio mónico asociado a $k(x)$ que está en D.

Sea $d(x)$ mónico y de grado máximo en D.

***Definición*:** $d(x)$ se denomina un *máximo común divisor de* $a(x)$ *y* $b(x)$.

***Teorema*:** Sean $a(x), b(x) \in K[x]$, no simultáneamente nulos, $d(x) \in K[x]$ mónico, tal que $d(x) \mid a(x) \wedge d(x) \mid b(x)$.

Entonces, son equivalentes:

i. $d(x)$ es un m.c.d. de $a(x)$ y $b(x)$)

ii. $\exists\, u(x), v(x) \in K[x]$, tales que $d(x) = u(x).a(x) + v(x).b(x)$

iii. si $s(x) \in K[x]$, es tal que $s(x) \mid a(x) \wedge s(x) \mid b(x)$ entonces $s(x) \mid d(x)$.

***Demostración*:** Para demostrar la equivalencia de estas tres propiedades, nos bastará con demostrar que: i. $\Rightarrow$ ii. , ii. $\Rightarrow$ iii. , y que iii. $\Rightarrow$ i. , y por la transitividad de la implicación quedan establecidas las que restan.

i. $\Rightarrow$ ii.) Nuestra hipótesis es que $d(x) = (a(x), b(x))$; debemos probar que $\exists\, u(x), v(x) \in K[x]$ tales que $d(x) = u(x).a(x) + v(x).b(x)$.

Sea $T = \{ k(x).a(x) + h(x).b(x) \ / \ k(x),\ h(x) \in K[x] \}$, por ejemplo están en T : $a(x)$, $b(x)$, $-a(x)$, $-b(x)$, $a(x) + b(x)$, $a(x) - b(x)$, 0, $a(x) + 2b(x)$, $2a(x) - b(x)$, etc.

Sea $d'(x)$ un polinomio mónico de grado mínimo en T (obsérvese que si un polinomio está en T también lo están todos sus asociados).

Como $d'(x) \in T$ se verifica que $\exists\, u(x),\ v(x) \in K[x]$ tales que

$$d'(x) = u(x).a(x) + v(x).b(x) \ .$$

Dado que $d(x) \mid a(x) \ \wedge \ d(x) \mid b(x) \ \Rightarrow \ d(x) \mid u(x).a(x) \ \wedge \ d(x) \mid v(x).b(x)$

$\therefore \ d(x) \mid (u(x).a(x) + v(x).b(x)) = d'(x)$, y como $d(x),\ d'(x) \in K[x]$

$\Rightarrow \ gr(d(x)) \leq gr(d'(x))$.

Para ver que $gr(d'(x)) \leq gr(d(x))$ usaremos la maximalidad de $gr(d(x))$ en D.

¿ $d'(x) \mid a(x)$?

Por el Algoritmo de la División, $\exists!\, q(x),\ r(x) \in K[x]$ tales que

$$a(x) = q(x).\ d'(x) + r(x) \quad \text{con} \quad gr(r(x)) < gr(d'(x)) \quad \vee \quad r(x) = 0.$$

reemplazando $d'(x)$ tenemos que $a(x) = q(x).(u(x).a(x) + v(x).b(x)) + r(x)$,

de donde $r(x) = (1 - q(x).u(x)).a(x) - q(x).v(x).b(x) \in T$.

Como $d'(x)$ es de grado mínimo en T , si $r(x) \neq 0 \ \Rightarrow \ gr(r(x)) < gr(d'(x))$!! (absurdo!) pues $r(x) \in T \ \therefore \ r(x) = 0$, por lo tanto $d'(x) \mid a(x)$.

En forma análoga podemos demostrar que $d'(x) \mid b(x)$.

Así $d'(x) \mid a(x) \ \wedge \ d'(x) \mid b(x) \ \Rightarrow \ d'(x) \in D$ por lo que $gr(d'(x)) \leq gr(d(x))$ por definición de $d(x)$.

Luego $gr(d'(x)) = gr(d(x))$; además $d(x) \mid d'(x)$ entonces $\exists\, s(x) \in K[x]$ tal que

$d'(x) = s(x).d(x)$ con $gr(s(x)) = 0 \ \therefore \ d'(x) = s.d(x)$ con $s \in K - \{ 0 \}$.

Por lo tanto $d'(x) \ \wedge \ d(x)$ son asociados, y como ambos son mónicos, entonces $d(x) = d'(x)$

$\therefore \ \exists\, u(x)\ ,\ v(x) \in K[x]$, tales que $d(x) = u(x).a(x) + v(x).b(x)$.

ii. $\Rightarrow$ iii.) Nuestra hipótesis es

"$\exists\, u(x), v(x) \in K[x]$ tales que $d(x) = u(x).a(x) + v(x).b(x)$",

y debemos probar que :

" si $s(x) \in K[x]$ es tal que $s(x) \mid a(x) \ \wedge \ s(x) \mid b(x) \ \Rightarrow \ s(x) \mid d(x)$".

Sea entonces $s(x) \in K[x]$ tal que $s(x) \mid a(x) \ \wedge \ s(x) \mid b(x)$, luego

$s(x) \mid u(x).a(x) \ \wedge \ s(x) \mid v(x).b(x) \ \therefore \ s(x) \mid (u(x).a(x) + v(x).b(x)) = d(x)$.

iii. $\Rightarrow$ i.) La hipótesis es:

" $s(x) \in K[x]$ es tal que $s(x) \mid a(x) \wedge s(x) \mid b(x) \Rightarrow s(x) \mid d(x)$" ,

y a partir de ella debemos probar que $d(x)$ es un m.c.d. de $a(x)$ y $b(x)$.

Sabemos que $d(x) \mid a(x) \wedge d(x) \mid b(x)$, y es mónico; sólo nos queda probar que es de grado máximo con esa propiedad.

Sea $k(x) \in K[x]$ tal que $k(x) \mid a(x) \wedge k(x) \mid b(x)$, por hipótesis $k(x) \mid d(x) \Rightarrow$

$gr(k(x)) \leq gr(d(x))$, y así $d(x)$ es de grado máximo en $D \therefore d(x)$ es un m.c.d. de $a(x)$ y $b(x)$.

***Corolario*:** El máximo común divisor de $a(x)$ y $b(x)$, es único.

***Demostración*:** Si $d(x)$ y $d'(x)$ son m.c.d. de $a(x)$ y $b(x)$, ambos verifican las propiedades i. , ii. , iii. del teorema; como $d(x) \mid a(x) \wedge d(x) \mid b(x) \wedge d'(x)$ satisface iii.
$\Rightarrow d(x) \mid d'(x)$.

Como $d'(x) \mid a(x) \wedge d'(x) \mid b(x) \wedge d(x)$ satisface iii. $\Rightarrow d'(x) \mid d(x)$
Si $d'(x) \mid d(x) \wedge d(x) \mid d'(x) \Rightarrow d'(x)$ y $d(x)$ son asociados, y como ambos son mónicos $d'(x) = d(x)$.

Notación: Si $d(x)$ es el *máximo común divisor de* $a(x)$ *y* $b(x)$ se lo denota :
$d(x) = (a(x) , b(x))$.

Nota: En virtud de las definiciones, y de las propiedades de divisibilidad, se verifica que $(a(x) , b(x)) = (u.a(x) , v.b(x)) \quad \forall u, v \in K - \{0\}$.

***Definición*:** $a(x)$ y $b(x)$ se dicen *coprimos,* o *primos entre sí* si $(a(x) , b(x)) = 1$.

Observación: $a(x)$ y $b(x)$ son coprimos sii los divisores comunes son únicamente los elementos no nulos de K.

***Corolario*:** Sean $a(x), b(x) \in K[x]$ no simultáneamente nulos.
$a(x)$ y $b(x)$ son coprimos si y sólo si $\exists\, u(x), v(x) \in K[x]$ tales que
$u(x).a(x) + v(x).b(x) = 1$.

***Demostración*:** Es un caso particular del teorema

***Propiedades*:** Sean $a(x), b(x) \in K[x]$, no simultáneamente nulos, $d(x) \in K[x]$ mónico tal que $d(x) \mid a(x) \wedge d(x) \mid b(x)$.

Demostrar:

i. $d(x) = (a(x) , b(x)) \Rightarrow d(x).c(x) = (a(x).c(x) , b(x).c(x)) \quad \forall\, c(x) \in K[x]$ mónico
ii. Si $a(x) = k(x).d(x) \wedge b(x) = h(x).d(x)$, entonces $d(x) = (a(x) , b(x)) \Leftrightarrow (k(x) , h(x)) = 1$.
iii. Para $a(x) \neq 0$, $(a(x) , b(x)) = u.a(x)$ para algún $u \in K - \{0\} \Leftrightarrow a(x) \mid b(x)$.

iv. $b(x) = q(x).a(x) + r(x) \Rightarrow (a(x) , b(x)) = (a(x) , r(x))$.
En particular $(a(x) - b(x) , a(x)) = (a(x) , b(x)) = (a(x) + b(x) , a(x))$.

v. Para $c(x) \neq 0$, $c(x) \mid a(x).b(x) \wedge (a(x) , c(x)) = 1 \Rightarrow c(x) \mid b(x)$.

vi. Para $a(x) \neq 0$, $b(x) \neq 0$, $a(x) \mid c(x) \wedge b(x) \mid c(x) \wedge (a(x) , b(x)) = 1$
$\Rightarrow a(x).b(x) \mid c(x)$.

vii. Generalización: si $a_i(x) \neq 0$, $a_i(x) \mid c(x) \quad \forall i$, $i = 1,2,..n,$ y

$(a_i(x) , a_j(x)) = 1$, para $i \neq j,$ entonces $\prod_{i=1}^{n} a_i(x) \mid c(x)$.

viii. $p(x), q(x) \in K[x]$ irreducibles mónicos , $(p(x) , q(x)) = 1 \Leftrightarrow p(x) \neq q(x)$.

***Demostración*:** Se propone como ejercicio .

Ejercicios: Sea $p(x) \in K[x]$, $gr(p(x)) > 0$. Demostrar que:

1) $p(x)$ es irreducible $\Leftrightarrow \forall\, a(x) \in K[x]$ se verifica una y sólo una de estas propiedades:
$p(x) \mid a(x) \vee (p(x) , a(x)) = 1$.

2) $p(x)$ es irreducible $\Leftrightarrow$ cada vez que $p(x) \mid a(x).b(x)$, para ciertos $a(x), b(x) \in K[x]$, se verifica que $p(x) \mid a(x) \vee p(x) \mid b(x)$.

3) Sea $p(x)$ es irreducible, tal que $p(x) \mid \prod_{i=1}^{n} a_i(x)$, con los $a_i(x) \in K[x]$, entonces $\exists\, j$,
$1 \leq j \leq n,$ tal que $p(x) \mid a_j(x)$.

4) $p(x)$ es irreducible $\Leftrightarrow (p(x) , k(x)) = 1 \quad \forall\, k(x) \in K[x]$, $gr(k(x)) < gr(p(x))$.

Algoritmo de Euclides para hallar el MCD en K[x], con K cuerpo:

Veremos, de la misma manera que se hace en $\mathbb{Z}$, cómo usar el Algoritmo de la División para encontrar el MCD de dos polinomios.

Sean $a(x), b(x) \in K[x]$, no nulos, tales que $gr(a(x)) \leq gr(b(x))$.

Aplicando el Algoritmo de la División, tenemos que $\exists!\, q(x), r(x) \in K[x]$ tales que

$$b(x) = q(x).a(x) + r(x) \quad \text{con} \quad r(x) = 0 \vee gr(r(x)) < gr(a(x)).$$

Si $r(x) = 0$ entonces $a(x) \mid b(x) \wedge (a(x) , b(x)) = u.a(x)$ $(u \in K - \{0\}$ es tal que $ua(x)$ es polinomio mónico).

si $r(x) \neq 0$ entonces $gr(r(x)) < gr(a(x))$.
Aplicando el AD, dividiendo $a(x)$ por $r(x)$:

$$a(x) = q_1(x).r(x) + r_1(x) \quad \text{con} \quad r_1(x) = 0 \vee gr(r_1(x)) < gr(r(x)).$$

Si $r_1(x) = 0 \Rightarrow (a(x) , b(x)) = (a(x) , r(x)) = v.r(x)$, para algún $v \in K - \{0\}$,
si $r_1(x) \neq 0 \Rightarrow gr(r_1(x)) < gr(r(x)) < gr(a(x))$; dividiendo $r(x)$ por $r_1(x)$
$r(x) = q_2(x).\ r_1(x) + r_2(x) \quad$ con $\quad r_2(x) = 0 \vee gr(r_2(x)) < gr(r_1(x)) < gr(a(x))$

Si $r_2(x) = 0 \Rightarrow (a(x), b(x)) = (a(x), r(x)) = (r(x), r_1(x)) = t.r_1(x)$, para algún $t \in K - \{0\}$,

si $r_2(x) \neq 0 \Rightarrow gr(r_2(x)) < gr(r_1(x)) < gr(r(x)) < gr(a(x))$;

dividiendo $r_1(x)$ por $r_2(x)$, $r_1(x) = q_3(x).\ r_2(x) + r_3(x)$ con $r_3(x) = 0 \vee$

$gr(r_3(x)) < gr(r_2(x)) < gr(r_1(x)) < gr(r(x)) < gr(a(x))$.

Vemos que, continuando con este proceso, llegamos a

$$r_k(x) = q_{k+2}(x).\ r_{k+1}(x) + r_{k+2}(x) \quad \text{con} \quad r_{k+2}(x) = 0 \quad \text{para algún } k,$$

pues la sucesión $(r_i(x))_i$ con $gr(r_i(x)) < gr(r_{i-1}(x))$ no puede tener infinitos términos, dado que no hay más que finitos números naturales menores que $gr(a(x))$.

Luego, si $r_{k+2}(x) = 0$, como $r_{k-1}(x) = q_{k+1}(x).\ r_k(x) + r_{k+1}(x)$ con

$gr(r_{k+1}(x)) < gr(r_k(x)) < gr(r_{k-1}(x)) < \ldots < gr(r_1(x)) < gr(r(x)) < gr(a(x))$

tenemos que $(a(x), b(x)) = (a(x), r(x)) = (r(x), r_1(x)) = (r_1(x), r_2(x)) =$

$(r_2(x), r_3(x)) = \ldots\ldots = (r_{k-1}(x), r_k(x)) = (r_k(x), r_{k+1}(x)) = s.r_{k+1}(x)$

para algún $s \in K - \{0\}$.

Por lo tanto, el MCD de $a(x)$ y $b(x)$ es el *último resto no nulo* en este proceso, multiplicado por una unidad de K que lo haga mónico.

***Generalización del Máximo Común Divisor en K[x], con K cuerpo*:**

Sean $a_1(x), a_2(x), a_3(x), \ldots, a_n(x) \in K[x]$, no simultáneamente nulos;

Sea $D = \{ t(x) \in K[x] \ / \ t(x) \mid a_i(x) \ \ \forall i = 1, 2, \ldots, n \}$; $D \neq \phi$ y si $b(x) \in D$, $ub(x) \in D$ $\forall u \in K - \{0\}$. Como los grados de los polinomios de D están acotados superiormente por el mínimo de los grados de los polinomios $a_i(x) \neq 0$, hay en D un polinomio mónico de grado máximo $d(x)$, que se denomina un *máximo común divisor de* $a_1(x), a_2(x), a_3(x), \ldots, a_n(x)$.

Ejercicio: Sean $a_1(x), a_2(x), a_3(x), \ldots, a_n(x) \in K[x]$, no nulos, $n > 2$, $d(x) \in K[x]$ mónico tal que $d(x) \mid a_i(x) \ \ \forall i = 1, 2, \ldots, n$; demostrar que :

$d(x)$ es un m.c.d. de $a_1(x),\ a_2(x)\ , a_3(x),\ \ldots., a_n(x) \Leftrightarrow$ $d(x)$ es un m.c.d. de $d_1(x)$ y $a_n(x)$, donde $d_1(x)$ es un m.c.d. de $a_1(x), a_2(x), a_3(x),\ \ldots., a_{n-1}(x)$.

***Teorema*:** Sean $a_1(x), a_2(x), a_3(x),\ \ldots., a_n(x) \in K[x]$, no simultáneamente nulos, $n \geq 2$, $d(x) \in K[x]$ mónico tal que $d(x) \mid a_i(x)\ \ \forall i = 1, 2, ..., n$. Demostrar que son equivalentes:

i. $d(x)$ es un m.c.d. de $a_1(x), a_2(x), a_3(x),\ \ldots., a_n(x)$.

ii. $\exists u_i(x) \in K[x]\quad i = 1, 2, ..., n$, tales que $d(x) = \sum_{i=1}^{n} u_i(x)\, a_i(x)$.

iii. $t(x) \in K[x]$ tal que $t(x) \mid a_i(x)\ \ \forall i = 1, 2, ..., n \ \Rightarrow\ t(x) \mid d(x)$.

***Demostración*:** Queda como ejercicio.

Pista: usar inducción para demostrar alguna implicación.

***Corolario*:** El máximo común divisor de $a_1(x), a_2(x), a_3(x),\ \ldots., a_n(x)$ es único.

***Demostración*:** Queda como ejercicio.

Notación: Si $d(x)$ es el m.c.d. de $a_1(x), a_2(x), a_3(x),\ \ldots., a_n(x)$ se nota:

$$d(x) = (a_1(x)\ ,\ a_2(x)\ ,\ a_3(x)\ ,\ \ldots.,\ a_n(x))\ .$$

***Definición*:** Sean $a_1(x), a_2(x), a_3(x),\ \ldots., a_n(x) \in K[x]$, no simultáneamente nulos, se dicen *coprimos* si $(a_1(x)\ ,\ a_2(x)\ ,\ a_3(x)\ ,\ \ldots.,\ a_n(x)) = 1$.

Nota: no es lo mismo decir que $a_1(x), a_2(x), a_3(x),\ \ldots., a_n(x)$ son *coprimos*, que decir que *son coprimos dos a dos* , o sea $(a_i(x),\ a_j(x)) = 1$ para $i \neq j$, pues si $a_1(x), a_2(x), a_3(x),\ \ldots., a_n(x)$ son coprimos dos a dos se verifica que $a_1(x), a_2(x),\ a_3(x),\ \ldots., a_n(x)$ son coprimos , pero la recíproca no es cierta (demostrarlo).

***Corolario*:** Sean $a_1(x), a_2(x), a_3(x),\ \ldots., a_n(x) \in K[x]$, no simultáneamente nulos, $n \geq 2$,

$(a_1(x)\ ,\ a_2(x)\ ,\ a_3(x)\ ,\ \ldots.,\ a_n(x)) = 1$ si y sólo si $\exists u_i(x) \in K[x]\quad i = 1, 2, ..., n$, tales que $1 = \sum_{i=1}^{n} u_i(x)\, a_i(x)$.

***Demostración*:** Es un caso particular del teorema.

Mínimo Común Múltiplo(MCM) en K[x], K cuerpo:

Sean $a(x), b(x) \in K[x] - \{0\}$.

Sea $M = \{ t(x) \in K[x] \ / \ a(x) \mid t(x) \ \wedge \ b(x) \mid t(x) \}$; $M \neq \phi$ pues $a(x) \, . \, b(x) \in M$.

Si $t(x) \in M$ todos sus asociados están también en M, por lo tanto podemos tomar un polinomio mónico y de grado mínimo en M.

Sea $m(x)$ polinomio de grado mínimo y mónico en M; $m(x)$ verifica:

i. $m(x)$ es mónico.

ii. $a(x) \mid m(x) \ \wedge \ b(x) \mid m(x)$.

iii. $c(x) \in K[x]$ tal que $a(x) \mid c(x) \ \wedge \ b(x) \mid c(x) \ \Rightarrow \ gr(m(x)) \leq gr(c(x))$.

***Definición*:** A los polinomios $m(x)$ que cumplen las condiciones *i.,ii.,iii.,* se los denomina *mínimo común múltiplo de* $a(x)$ *y* $b(x)$.

***Teorema*:** Sean $a(x), b(x) \in K[x] - \{0\}$, $m(x) \in K[x]$ mónico, tales que $a(x) \mid m(x) \ \wedge \ b(x) \mid m(x)$. Entonces, son equivalentes:

i. $m(x)$ es un mínimo común múltiplo de $a(x)$ *y* $b(x)$.

ii. $c(x) \in K[x]$ tal que $a(x) \mid c(x) \ \wedge \ b(x) \mid c(x) \ \Rightarrow \ m(x) \mid c(x)$.

***Demostración*:** i $\Rightarrow$ ii) Sea $c(x) \in K[x]$ tal que $a(x) \mid c(x) \ \wedge \ b(x) \mid c(x)$.

Aplicando AD $c(x) = q(x) \, m(x) + r(x)$ con $r(x) = 0 \ \vee \ gr(r(x)) < gr(m(x))$

$a(x) \mid m(x) \ \wedge \ b(x) \mid m(x) \ \Rightarrow \ a(x) \mid m(x) \, q(x) \ \wedge \ b(x) \mid m(x) \, q(x)$.

Además, $a(x) \mid c(x) \ \wedge \ b(x) \mid c(x) \ \Rightarrow \ a(x) \mid r(x) \ \wedge \ b(x) \mid r(x)$.

Si $r(x) \neq 0$ entonces $gr(r(x)) < gr(m(x))$!! pues $m(x)$ es de grado mínimo con esa propiedad, entonces $r(x) = 0$ y $m(x) \mid c(x)$.

ii $\Rightarrow$ i) Si $m(x)$ verifica que para todo $c(x) \in K[x]$ tal que

$$a(x) \mid c(x) \ \wedge \ b(x) \mid c(x) \ \Rightarrow \ m(x) \mid c(x) \, ,$$

veamos que es el de grado mínimo con la propiedad de ser múltiplo simultáneo de $a(x)$ y $b(x)$.

Si $c(x) \in K[x]$ es tal que $a(x) \mid c(x) \ \wedge \ b(x) \mid c(x)$, por hipótesis, tenemos que $m(x) \mid c(x)$, luego $gr(m(x)) \leq gr(c(x))$, con lo cual $m(x)$ es un mínimo común múltiplo de $a(x)$ *y* $b(x)$.

***Corolario*:** $a(x), b(x) \in K[x] - \{0\}$, el MCM de $a(x)$ y $b(x)$ es único.

***Demostración*:** Se deja como ejercicio.
(Pista: razonar en forma similar a lo realizado para la unicidad del MCD).

Nota : Como el mínimo común múltiplo de $a(x)$ y $b(x)$ es único, lo denotaremos

$$m(x) = [a(x) \, , \ b(x)] .$$

Ejercicios:

1) $\left[a(x)\,,\ b(x)\right] = \left[u.a(x)\,,\ v.b(x)\right],\quad \forall u,v \in K - \{0\}$.

2) $\left[a(x)\,,\ b(x)\right] = u.b(x)$, para algún $u \in K - \{0\}$, $\Leftrightarrow$ $a(x) \mid b(x)$.

3) Sean $a(x), b(x) \in K[x]$, $m(x) \in K[x]$ mónico, tales que $a(x) \mid m(x) \wedge b(x) \mid m(x)$. Entonces:

$$m(x) = \left[a(x)\,,\ b(x)\right] \quad \Leftrightarrow \quad \left(\frac{m(x)}{a(x)}\,,\ \frac{m(x)}{b(x)}\right) = 1.$$

4) Para $a(x), b(x) \in K[x]$, $\left[a(x)\,,\ b(x)\right] = u.a(x).b(x) \quad \Leftrightarrow \quad (a(x)\,,\ b(x)) = 1$.

Teorema Fundamental de la Aritmética (TFA) en K[x], K cuerpo:

$\forall\, a(x) \in K[x] - \{0\}$, de grado positivo, $\exists\ p_1(x), p_2(x), p_3(x) \ldots, p_n(x) \in K[x]$ irreducibles y mónicos tales que:

$a(x) = u.\prod_{i=1}^{n} p_i(x)$, donde $u \in K - \{0\} \wedge gr(p_i(x)) \le gr(p_{i+1}(x))\ \forall\, i = 1,2,\ldots..,n-1$.

Los polinomios irreducibles $p_i(x)$ *son únicos* en el sentido siguiente:

Si $p_1(x).\,p_2(x).\,p_3(x) \ldots p_k(x) = q_1(x).\,q_2(x).\,q_3(x).\,\ldots.\,q_h(x)$, con $k, h \in \mathbb{N}$,
$p_i(x)\,,\ q_j(x) \in K[x]$ irreducibles mónicos , $gr(p_i(x)) \le gr(p_{i+1}(x))$,

$gr(q_j(x)) \le gr(q_{j+1}(x))\quad \forall\, i\,,\ i = 1,2,3,\ldots,k-1\,,\ \forall j\,,\ j = 1, \ldots h-1$.
Entonces $k = h \wedge \forall\, i,\ i = 1,2,3,\ldots,k \quad \exists\, j_i\,,\ 1 \le j_i \le k$ tal que $p_i(x) = q_{j_i}(x)$, donde para $i \neq i'$ se verifica que $j_i \neq j_{i'}$.

***Demostración*:** *Existencia de la factorización en polinomios irreducibles.*

Sea $gr(a(x)) = n \in \mathbb{N}$. Demostraremos por inducción sobre n, que $a(x)$ se puede factorizar como producto de polinomios irreducibles mónicos.

Sea $a(x) \in K[x]$ tal que $gr(a(x)) = 1$; $a(x)$ es irreducible, y $\exists\, u \in K - \{0\}$ tal que
$a(x) = u.\,p(x)$, con $p(x)$ irreducible mónico.
Luego la factorización existe para todo polinomio de grado 1.
H.I. : Sea $n > 1$, supongamos que todo polinomio de grado k , $\forall\, k$, $1 \le k < n$, se pueda factorizar como producto de polinomios irreducibles mónicos y una unidad.
Sea, ahora, $a(x) \in K[x]$ tal que $gr(a(x)) = n$

$\therefore$ $a(x)$ es irreducible $\vee$ $a(x)$ es reducible

- si $a(x)$ es irreducible, entonces $a(x) \mid a(x) \;\therefore\; a(x) = u.\, p(x)$ con $p(x)$ irreducible mónico, $u \in K - \{0\}$.

  $\therefore$ la proposición es verdadera,

- si $a(x)$ es reducible, $\exists\, p(x) \in K[x]$ irreducible mónico tal que $p(x) \mid a(x)$.

  Sea $p_1(x)$ un polinomio de grado mínimo en el conjunto

$$\left\{ q(x) \in K[x] \;/\; q(x) \text{ es irreducible} \;\wedge\; q(x) \mid a(x) \right\}$$

$$\therefore \qquad a(x) = p_1(x)\, b(x)$$

con $1 \le gr(p_1(x)) < gr(a(x)) = n \;\wedge\; 1 \le gr(b(x)) < gr(a(x)) = n$

aplicando la H.I. a $b(x)$, $\exists\; p_2(x), p_3(x) \ldots, p_n(x) \in K[x]$ irreducibles y mónicos tales que

$b(x) = u. \prod_{i=2}^{n} p_i(x) \;\wedge\; gr(p_i(x)) \le gr(p_{i+1}(x))$, $\forall\, i = 2, \ldots, n-1$

$\therefore \quad a(x) = p_1(x).\, b(x) = u.\; p_1(x). \prod_{i=2}^{n} p_i(x) = u. \prod_{i=1}^{n} p_i(x)$, donde $u \in K - \{0\}$,

$\wedge \;\; gr(p_i(x)) \le gr(p_{i+1}(x)),\; \forall\, i = 1,2,\ldots,n-1.$

Unicidad de la factorización:

Si $p_1(x).\, p_2(x).\, p_3(x) \ldots p_k(x) = q_1(x).\; q_2(x).\; q_3(x). \ldots. \; q_h(x)$, con $k, h \in \mathbb{N}$,

$p_i(x)$, $q_j(x) \in K[x]$ irreducibles mónicos , $gr(p_i(x)) \le gr(p_{i+1}(x))$, $gr(q_j(x)) \le gr(q_{j+1}(x))$
$\forall\, i$, $i = 1,2,3,\ldots,k-1$; $\forall\, j$, $j = 1,2,3\ldots,h-1$;
debemos probar que $k = h \;\wedge\; \forall\, i = 1,2,\ldots,k \;\exists\, j_i$, $1 \le j_i \le k$ tal que $p_i(x) = q_{j_i}(x)$ donde si $i \neq i'$ se verifica que $j_i \neq j_{i'}$.

Lo haremos por inducción sobre k.

Si $k = 1$, supongamos que $p_1(x) = q_1(x).\; q_2(x).\; q_3(x). \ldots. \; q_h(x)$.

Si $h > 1$, $q_1(x) \mid p_1(x) \;\wedge\; q_1(x) \cdot q_2(x) \mid p_1(x)$!! (absurdo!) pues $p_1(x)$ es irreducible, entonces $h = 1 \;\wedge\; p_1(x) = q_1(x)$.

Supongamos que todo producto de k polinomios irreducibles se factorice de manera única.

Sea una producto de $k+1$ polinomios irreducibles, y supongamos que:

$$p_1(x).\, p_2(x).\, p_3(x) \ldots p_k(x)\; p_{k+1}(x) = q_1(x).\; q_2(x).\; q_3(x). \ldots. \; q_h(x), \quad \text{(I)}$$

con $p_i(x)$, $q_j(x) \in K[x]$ irreducibles mónicos , $gr(p_i(x)) \le gr(p_{i+1}(x))$,

$gr(q_j(x)) \le gr(q_{j+1}(x))$ $\forall\, i$, $i = 1,2,3,\ldots,k$; $\forall\, j$, $j = 1,2,3\ldots,h-1$;

$p_1(x) \mid q_1(x).\ q_2(x).\ q_3(x).\ \ldots.\ q_h(x)$, como $p_1(x)$ es irreducible $\Rightarrow\ \exists\ j_1\ ,\ 1 \le j_1 \le h$ tal que $p_1(x) \mid q_{j_1}(x)$, y como $q_{j_1}(x)$ también es irreducible, son asociados, o sea $p_1(x) = u.\, q_{j_1}(x)$, para algún $u \in K - \{0\}$, pero como ambos son mónicos $p_1(x) = q_{j_1}(x)$.

En la igualdad (I) cancelamos $p_1(x) \wedge q_{j_1}(x)$ respectivamente, y obtenemos

$$p_2(x)\,.\,p_3(x)\ldots p_k(x)\ p_{k+1}(x) = q_1(x).\ q_2(x).\ q_3(x).\ q_{j_1-1}(x)\ q_{j_1+1}(x)\ldots.\ q_h(x),$$

en el primer miembro de la igualdad tenemos un producto de k irreducibles mónicos que por HI, se factoriza de manera única, entonces $k = h - 1$ (el segundo miembro de la igualdad tiene $h - 1$ irreducibles) con lo cual $k + 1 = h$, además, por HI ,

$p_i(x) = q_{j_i}(x)\ \ \forall\, i = 2,\ldots., k+1$, pero como $p_1(x) = q_{j_1}(x)$, tenemos que $p_i(x) = q_{j_i}(x)$ $\forall\, i = 1,2,\ldots., k+1$.

Entonces, la proposición se verifica $\forall\, k \in \mathbb{N}$, y la factorización es única, sea cual fuere la cantidad de irreducibles mónicos que en ella intervinieren.

Especialización de polinomios

***Teorema*:** Sean A , B anillos conmutativos con identidad, $\mathcal{G}: A \to B$ un homomorfismo de anillos con identidad, $b \in B$.
Existe un único homomorfismo $\mho : A[x] \to B$ tal que $\mho\big|_A = \mathcal{G}$ ($\mho$ extiende a $\mathcal{G}$),
y tal que $\mho(x) = b$.

***Demostración*:**

Existencia:

Para demostrar la existencia de un tal homomorfismo vamos a definirlo.

Sea $\mho : A[x] \to B$ definido por: para $p(x) = \sum_{i=0}^{n} a_i x^i$

$$\mho(p(x)) = \mho\left(\sum_{i=0}^{n} a_i x^i\right) = \sum_{i=0}^{n} \mathcal{G}(a_i) b^i$$

como $p(x)$ está unívocamente determinado por sus coeficientes y los $a_i \in A$, entonces $\sum_{i=0}^{n} \mathcal{G}(a_i) b^i \in B$, luego $\mho$ está bien definida.

¿ $\mho$ es homomorfismo de anillos con identidad?

Sean $p(x)$ y $q(x)$ dos polinomios en $A[x]$, $p(x) = \sum_{i=0}^{n} a_i x^i$, $q(x) = \sum_{i=0}^{n} c_i x^i$,

entonces $p(x) + q(x) = \sum_{i=0}^{n} (a_i + c_i)\, x^i$

$$\mho(\,p(x) + q(x)) = \mho(\,\sum_{i=0}^{n} (a_i + c_i)\, x^i\,) = \sum_{i=0}^{n} \mathcal{G}(a_i + c_i)\, b^i =$$

por ser $\mathcal{G}$ un homomorfismo de anillos, $\mathcal{G}(a_i + c_i) = \mathcal{G}(a_i) + \mathcal{G}(c_i) \quad \forall i = 0,1,2,...,n$

$$= \sum_{i=0}^{n} \big(\mathcal{G}(a_i) + \mathcal{G}(c_i)\big) b^i = \sum_{i=0}^{n} \mathcal{G}(a_i) b^i + \sum_{i=0}^{n} \mathcal{G}(c_i) b^i = \mathfrak{V}(p(x)) + \mathfrak{V}(q(x)).$$

Sea ahora $p(x) = \sum_{i=0}^{n} a_i x^i$, $t(x) = \sum_{j=0}^{m} r_j x^j$, $p(x) \,.\, t(x) = \sum_{k=0}^{n+m} d_k x^k$ donde $d_k = \sum_{i+j=k} a_i . b_j$

$\mathfrak{V}(p(x) \,.\, t(x)) = \mathfrak{V}\big(\sum_{k=0}^{n+m} d_k x^k\big) = \sum_{k=0}^{n+m} \mathcal{G}(d_k) b^k$, donde $\mathcal{G}(d_k) = \sum_{i+j=k} \mathcal{G}(a_i).\mathcal{G}(c_j)$

por ser $\mathcal{G}$ un homomorfismo de anillos.

Luego $\mathfrak{V}(p(x) \,.\, t(x)) = \big(\sum_{i=0}^{n} \mathcal{G}(a_i) b^i\big).\big(\sum_{j=0}^{m} \mathcal{G}(c_j) b^j\big) = \mathfrak{V}(p(x)) \,.\, \mathfrak{V}(t(x))$

Así, $\mathfrak{V}$ es un homomorfismo de anillos.

Veamos que $\mathfrak{V}$ extiende a $\mathcal{G}$, o sea, $\mathfrak{V}(a) = \mathcal{G}(a) \quad \forall a \in A$.

Para $a \in A$, se puede pensar a a como el polinomio $a = a + 0.x$, luego

$\mathfrak{V}(a) = \mathcal{G}(a) + \mathcal{G}(0).b$, como $\mathcal{G}(0) = 0$, por ser $\mathcal{G}$ homomorfismo de anillos,

tenemos que $\mathfrak{V}(a) = \mathcal{G}(a) + 0.b = \mathcal{G}(a)$.

En particular $\mathfrak{V}(1) = \mathcal{G}(1) = 1$, por ser $\mathcal{G}$ homomorfismo de anillos con identidad.

Por lo tanto $\mathfrak{V}$ es un homomorfismo de anillos con identidad que extiende a $\mathcal{G}$.
Falta ver que $\mathfrak{V}(x) = b$.

El polinomio $x = 1.x + 0$, por definición $\mathfrak{V}(x) = \mathcal{G}(1).b + \mathcal{G}(0) = 1.b + 0 = b$.

Luego $\mathfrak{V}$ es la función buscada.

Unicidad de $\mathfrak{V}$:
Supongamos que $\exists \psi : A[x] \to B$ homomorfismo de anillos con identidad, que extiende a $\mathcal{G}$ tal que $\psi(x) = b$; $\psi \overset{?}{=} \mathfrak{V}$.

$$\psi = \mathfrak{V} \quad \Leftrightarrow \quad \psi\big(p(x)\big) = \mathfrak{V}\big(p(x)\big) \quad \forall\, p(x) \in A[x]$$

$$\psi(p(x)) = \psi\big(\sum_{i=0}^{n} a_i x^i\big) = \sum_{i=0}^{n} \psi(a_i x^i) = \sum_{i=0}^{n} \psi(a_i).\psi(x^i) = \sum_{i=0}^{n} \psi(a_i).(\psi(x))^i =$$

por ser ψ homomorfismo de anillos,

$$= \sum_{i=0}^{n} \mathcal{G}(a_i).b^i = \mathfrak{V}(p(x)) \text{ , y esto es } \forall\, p(x) \in A[x] \quad \therefore \quad \psi = \mathfrak{V}.$$

Por lo tanto $\mathfrak{V}$ es única con las propiedades que pide el teorema.

La especialización de polinomios en la búsqueda de números primos.

Los números primos sugieren todo tipo de problemas. Uno de los primeros se refiere a ¿cuántos números primos hay? Euclides (aprox. 350 a. Cristo) dio una demostración de la existencia de infinitos primos.
Otra pregunta interesante es saber ¿cuál es el n-ésimo primo? Se trataría de dar una fórmula $p_n = \ldots.$, *que exprese el n-ésimo primo* p_n *como una función de n. Esto, en algún sentido, es como la* ***piedra filosofal*** *de la Aritmética. Se conocen fórmulas, pero las mismas no son satisfactorias, pues determinan* p_n *conociendo todos los* p_k , $k<n$. *Por ejemplo, utilizando polinomios f(X), no constantes, con coeficientes enteros, ¿ es posible la existencia de un entero m tal que f(x) sea primo para todo* $x \geq m$? *Un sencillo ejercicio de Aritmética dice que esto es imposible. No obstante, existen polinomios que producen primos en número finito, para valores de X en algún intervalo finito.*

Dos ejemplos notables que dan números primos al reemplazar x por los valores señalados, son los siguientes:

Leonhard Euler
(1707-1783)

$x^2 - x + 41$ *es primo para* x=0,1,2,…..,40
Euler (1772)

Adrien Marie Legendre
(1752-1833)

$x^2 + x + 41$ *es primo para* x=0,1,2,….,39
Legendre (1798)

(“Aritmética Elemental en la formación matemática”. Enzo Gentile).

***Definición*:** La aplicación $\mho$ se denomina *especialización de x por b según* $\mathcal{G}$.

Notación: $\mho(p(x)) = p(b)$ y se lo designa como *polinomio especializado en b según* $\mathcal{G}$.

Ejemplos:

1) Si $\mathcal{G} = id_A : A \to A$, $id_A(x) = x \quad \forall\ a \in A$; $p(x) = \sum_{i=0}^{n} a_i x^i \in A[x]$, $b \in B$,

el polinomio especializa en b según la id_A , es $p(b) = \sum_{i=0}^{n} a_i\, b^i$.

2) Si A y B son anillos conmutativos con identidad, A subanillo de B,
$i : A \to B$ la aplicación inclusión, o sea $i(x) = x \quad \forall\ a \in A$, $p(x) = \sum_{i=0}^{n} a_i x^i \in A[x]$,
$p(x)$ especializado en b según i es $p(b) = \sum_{i=0}^{n} a_i\, b^i$.

3) Sea $\varphi : \mathbb{Z} \to \mathbb{Z}_n$ la proyección canónica al cociente, $\overline{\varphi} : \mathbb{Z}[x] \to \mathbb{Z}_n$, $\overline{b} \in \mathbb{Z}_n$,
la especialización de x por $\overline{b}$ según φ ; $p(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{Z}[x]$; el polinomio $p(x)$ especializado en $\overline{b}$ según φ es $p(\overline{b}) = \sum_{i=0}^{n} \overline{a_i}.\overline{b}^{\,i}$.

***Definición*:** Sean $A \underset{suba}{\subset} B$, $b \in B$, $p(x) = \sum_{i=0}^{n} a_i x^i \in A[x]$, b se dice que es *raíz* de $p(x)$, si el polinomio especializado en b (según la $id_A(x)$ o según i) es cero, o sea $p(b) = \sum_{i=0}^{n} a_i\, b^i = 0$.

> *El problema de hallar las raíces de un polinomio con coeficientes reales ocupó gran parte de la atención de los matemáticos desde los árabes en la antigüedad, quienes usaron métodos aritmético-geométricos, pasando por los griegos (especialmente los pitagóricos y euclidianos) y sus razonamientos geométricos hasta llegar al Siglo XVIII de nuestra era con la solución general de ecuaciones de tercer y cuarto grado, la imposibilidad de resolver la ecuación de quinto grado usando radicales y la demostración del teorema fundamental del álgebra.*
> ("Historia del Algebra Lineal hasta los Albores del Siglo XX". Divulgaciones Matemáticas Vol. 14 No.2 (2006))

***Teorema*:** Sea A dominio de integridad, $a \in A$, $p(x) \in A[x]$.
a es raíz de $p(x)$ si y sólo si $(x - a) \mid p(x)$.

***Demostración*:**
$\Rightarrow$) Sea a raíz de $p(x)$, queremos ver que $(x - a) \mid p(x)$.
Aplicando el Algoritmo de la División:
$$p(x) = (x - a).\, q(x) + r \quad \text{con } r \in A.$$
Especializando $p(x)$ en a tenemos que:
$$p(a) = (a - a).\, q(a) + r = 0.\, q(a) + r = r.$$
Como a es raíz de $p(x)$ tenemos que $p(a) = 0 \quad \therefore \quad r = 0$,
por tanto $(x - a) \mid p(x)$.

$\Leftarrow$) Supongamos que $(x - a) \mid p(x) \quad \therefore \quad p(x) = (x - a).\, q(x)$ para cierto $q(x) \in A[x]$;
especializando x en a, tenemos $p(a) = (a - a).\, q(a) = 0.\, q(a) = 0$.
$\therefore$ a es raíz de $p(x)$.

***Corolario* (*Teorema del Resto*):** A dominio de integridad, $a \in A$
El resto en la división de un polinomio $p(x) \in A[x]$ por $x - a$ es $p(a)$.

***Demostración*:** trivial a partir de la demostración del teorema.

***Proposición*:** Si K es cuerpo, todo polinomio de grado 1 admite una raíz en K.

***Demostración*:** Sea $p(x) = ax + b$, con $a \neq 0$, $x_0 = -b.a^{-1} \in K$ es raíz de $p(x)$.

Nota: Si A es dominio de integridad que no es cuerpo, no todo polinomio de grado 1 tiene una raíz en A.

Ejemplo: El polinomio $p(x) = 2x + 3 \in \mathbb{Z}[x]$ es grado 1 y no tiene raíces en $\mathbb{Z}$.

Ejercicios: Demostrar que si A es dominio de integridad, en $A[x]$ se verifica que:

1) $p(x) \mid q(x) \ \wedge$ a es raíz de $p(x) \ \Rightarrow$ a es raíz de $q(x)$.
En particular, dos polinomios asociados tienen las mismas raíces.

2) $p(x) = q(x) \,.\, t(x) \ \wedge$ a es raíz de $p(x) \ \Rightarrow$ a es raíz de $q(x) \ \vee$ a es raíz de $t(x)$.

3) Sea $p(x) \in A[x]$, si $gr(p(x)) > 1 \ \wedge$ $p(x)$ admite una raíz en A entonces $p(x)$ es reducible . La recíproca no se verifica.

Ejemplos: 1) $p(x) = 4x^2 + 2 \in \mathbb{Z}[x]$, es reducible en $\mathbb{Z}[x]$, pero no tiene raíces en $\mathbb{Z}$.
2) $q(x) = (x^2 + 1)(x^2 - 2) \in \mathbb{Q}[x]$, es reducible pero no tiene raíces en $\mathbb{Q}$.

***Teorema*:** Sea K es cuerpo, $p(x) \in K[x]$ tal que $2 \leq gr(p(x)) \leq 3$. Entonces $p(x)$ es irreducible en $K[x]$ si y sólo si $p(x)$ no admite raíces en K.

***Demostración*:**
$\Rightarrow$) Es lo que demuestra el ejercicio 3).

$\Leftarrow$) Sea $p(x) \in K[x]$ tal que $2 \leq gr(p(x)) \leq 3$;

si $p(x)$ es reducible, $p(x) = q(x) \,.\, t(x)$

con $1 \leq gr(q(x)) < gr(p(x)) \quad \wedge \quad 1 \leq gr(p(x)) < gr(p(x))$.

Si $gr(p(x)) = gr(q(x)) + gr(t(x)) = 2 \ \Rightarrow \ gr(q(x)) = gr(t(x)) = 1$.

Si $gr(p(x)) = gr(q(x)) + gr(t(x)) = 3 \ \Rightarrow$ ($gr(q(x)) = 1 \ \wedge \ gr(t(x)) = 2$) $\vee$

($gr(q(x)) = 2 \ \vee \ gr(t(x)) = 1$) $\therefore$ $p(x)$ es divisibles por un polinomio de grado 1, y por lo tanto es divisible por un polinomio que tiene una raíz en K $\therefore$ $p(x)$ admite una raíz en K.

Nota: Si A es dominio de integridad que no es cuerpo, el teorema no se verifica, como lo muestra el *ejemplo* 1) dado anteriormente.
Si $gr(p(x)) \geq 4$ tampoco el teorema se verifica necesariamente, como lo muestra el *ejemplo* 2) dado más arriba.

Caracterizar los polinomios irreducibles de segundo grado en K [x] en función de sus coeficientes, para K cuerpo:

Sea K un cuerpo de *característica* $\neq 2$ (esto es que $a + a \neq 0 \quad \forall a \in K, a \neq 0$),
sea $p(x) = ax^2 + bx + c \in K[x]$, $a \neq 0$; $p(x)$ es irreducible si y sólo si no admite raíces en K , o lo que es equivalente, es reducible sii admite raíces en K.

Busquemos una *condición necesaria*, relativa a sus coeficientes, para que $p(x)$ admita una raíz en K.

Sea $z \in K$ raíz de $p(x)$, $\therefore$ $p(z) = 0 = az^2 + bz + c = a(z^2 + ba^{-1}z + ca^{-1})$

por ser $a \neq 0 \Rightarrow z^2 + ba^{-1}z + ca^{-1} = 0$.

Escribiremos $ba^{-1} = \frac{b}{a} \wedge ca^{-1} = \frac{c}{a}$, $z^2 + \frac{b}{a}z + \frac{c}{a} = 0$.

Completando cuadrados: $0 = z^2 + \frac{b}{a}z + \frac{c}{a} = z^2 + \frac{b}{a}z + \frac{b^2}{4a^2} - \frac{b^2}{4a^2} + \frac{c}{a} =$

$= \left(z + \frac{b}{2a}\right)^2 - \left(\frac{b^2}{4a^2} - \frac{c}{a}\right) = \left(z + \frac{b}{2a}\right)^2 - \left(\frac{b^2 - 4ac}{4a^2}\right)$

$\therefore \left(z + \frac{b}{2a}\right)^2 = \left(\frac{b^2 - 4ac}{4a^2}\right) \Rightarrow \left[2a\left(z + \frac{b}{2a}\right)\right]^2 = b^2 - 4ac$.

Por lo tanto, si $p(x)$ admite una raíz en K demostramos que $\Delta = b^2 - 4ac$ es un cuadrado en K.
El elemento de K : $\Delta = b^2 - 4ac$ se denomina *discriminante de* $p(x)$.

Observación: el discriminante de un polinomio depende sólo de sus coeficientes.

Veamos ahora, que la *condición es suficiente*, o sea, si el discriminante Δ es un cuadrado en K entonces $p(x)$ admite una raíz en K.

Sea $\Delta = b^2 - 4ac$ un cuadrado en K $\therefore$ $\exists \omega \in K$ tal que $\Delta = \omega^2$,
sean $z_1 = \frac{-b + \omega}{2a}$, $z_2 = \frac{-b - \omega}{2a}$; veamos que son raíces de $p(x)$.

Calculemos la especialización de $p(x)$ en z_1 :

$p(z_1) = az_1^2 + bz_1 + c = a\left(\frac{-b + \omega}{2a}\right)^2 + b.\frac{-b + \omega}{2a} + c = \frac{b^2 - 2b\omega + \omega^2}{4a} + \frac{-b^2 + b\omega}{2a} + c =$

$= \frac{b^2 - 2b\omega + \omega^2 - 2b^2 + 2b\omega + 4ac}{4a} = \frac{-b^2 + 4ac + \omega^2}{4a} = \frac{-b^2 + 4ac + \Delta}{4a} =$

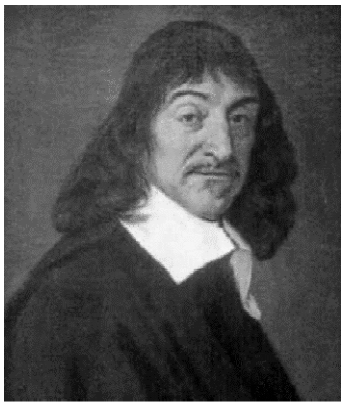
$= \frac{-b^2 + 4ac + b^2 - 4ac}{4a} = \frac{0}{4a} = 0$ $\therefore$ z_1 es raíz de $p(x)$.

De forma análoga se demuestra que z_2 es también raíz de $p(x)$.

Por lo tanto***, un polinomio de segundo grado en K [x] es irreducible si y sólo si el discriminante Δ del polinomio no es un cuadrado en K***

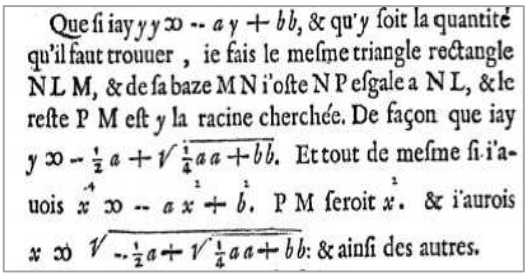
Ejemplos:

1) En $\mathbb{R}[x]$ un polinomio de segundo grado es irreducible sii $\Delta < 0$.
2) En $\mathbb{Q}[x]$ un polinomio de segundo grado es irreducible sii $\Delta < 0 \vee$ si $\Delta > 0$, Δ no es cuadrado en $\mathbb{Q}$.
3) En $\mathbb{Z}_7[x]$ un polinomio de segundo grado es irreducible sii $\Delta \notin \left\{\bar{0}, \bar{1}, \bar{2}, \bar{4}\right\}$.



René Descartes 1596-1650

En el libro primero La géométrie, Descartes plantea la resolución geométrica de ecuaciones de segundo grado. A pesar de su título, este tratado no es básicamente geométrico. Ya en el Discours, había discutido los méritos relativos del álgebra y la geometría, sin llegar a inclinarse por una o por otra. Acusaba a la geometría de apoyarse excesivamente en diagramas y figuras que llegaban a fatigar de manera innecesaria la imaginación, y acusaba al álgebra de ser un arte confuso y oscuro que desconcierta a la mente. Su método, entonces, tenía dos objetivos: el de liberar a la geometría, a través de los métodos algebraicos, del uso de las figuras y el de darle un significado concreto a las operaciones del álgebra mediante su interpretación geométrica. Convencido de que todas las ciencias matemáticas procedían de los mismos conceptos básicos, decidió utilizar lo mejor de cada rama.

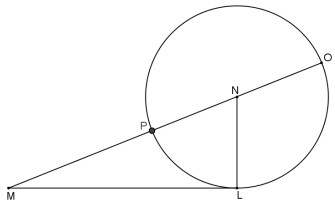


Que ſi iay $yy \propto -ay + bb$, & qu'y ſoit la quantité qu'il faut trouuer, ie fais le meſme triangle rectangle N L M, & de ſa baze M N i'oſte N P eſgale a N L, & le reſte P M eſt y la racine cherchée. De façon que iay $y \propto -\frac{1}{2}a + \sqrt{\frac{1}{4}aa + bb}$. Et tout de meſme ſi i'auois $x^4 \propto -ax^2 + b^2$. P M ſeroit x^2. & i'aurois $x \propto \sqrt{-\frac{1}{2}a + \sqrt{\frac{1}{4}aa + bb}}$: & ainſi des autres.

Texto de Descartes sobre la resolución geométrica de la ecuación $y^2 = -ay + b^2$

En español: Si $y^2 = -ay + b^2$, donde y es la cantidad que se quiere encontrar, construyo el mismo triángulo rectángulo NLM *y de la base* MN *quito* NP *igual a* NL, *y lo que resta PM es y, la raíz buscada. Así, se tiene:*

$$y = -\frac{a}{2} + \sqrt{\frac{a^2}{4} + b^2}$$

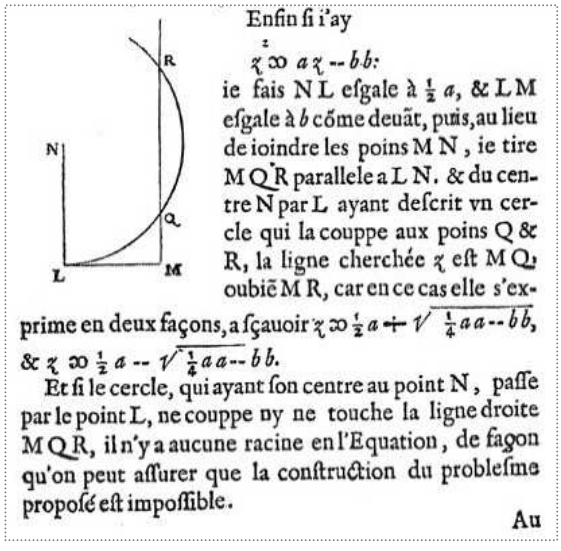


Y del mismo modo, si se tiene $x^4 = -ax^2 + b^2$, PM *será x^2 y se tendrá:*

y así $x = \sqrt{-\frac{a}{2} + \sqrt{\frac{a^2}{4} + b^2}}$ *para otros casos.*

En español: Si tenemos $z^2 = az - b^2$, hago NL *igual a a/2 y* LM *igual a b. Después, en lugar de unir los puntos* M N, *dibujo* MQR *paralela a* LN, *y con* N *como centro describo un círculo que pasa por* L *y corta a* MQR *en los puntos* Q *y* R . *La línea buscada z es* MQ *o* MR, *dado que en este caso se puede expresar de dos formas diferentes:*

$$z = \frac{a}{2} + \sqrt{\frac{a^2}{4} - b^2} \quad y \quad z = \frac{a}{2} - \sqrt{\frac{a^2}{4} - b^2}$$

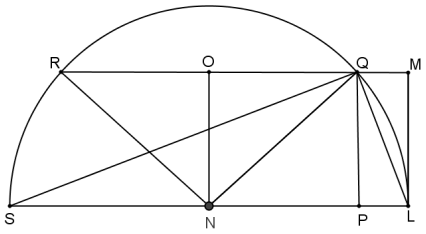


Enfin ſi i'ay $z \propto az - bb$: ie fais N L eſgale à $\frac{1}{2}a$, & L M eſgale à b cõme deuãt, puis, au lieu de ioindre les poins M N, ie tire M Q R parallele a L N. & du centre N par L ayant deſcrit vn cercle qui la couppe aux poins Q & R, la ligne cherchée z eſt M Q, oubiẽ M R, car en ce cas elle s'exprime en deux façons, a ſçauoir $z \propto \frac{1}{2}a + \sqrt{\frac{1}{4}aa - bb}$, & $z \propto \frac{1}{2}a - \sqrt{\frac{1}{4}aa - bb}$.

Et ſi le cercle, qui ayant ſon centre au point N, paſſe par le point L, ne couppe ny ne touche la ligne droite M Q R, il n'y a aucune racine en l'Equation, de façon qu'on peut aſſurer que la conſtruction du probleſme propoſé eſt impoſſible.

Au

Texto de Descartes sobre la resolución geométrica de la ecuación $z^2 = az - b^2$



Y si el círculo cuyo centro es el punto N *y pasa por* L *no corta ni toca a la recta* MQR*, la ecuación no tiene raíces, de modo que la construcción del problema propuesto es imposible.*

Para el lector entusiasta: aplique el método adecuado en cada caso para resolver las siguientes ecuaciones: $x^2-5x+4 = 0$ $x^2+3x-4 = 0$ $x^4+3x^2-4 = 0$

Ejercicio: Sea $p(x) = ax^2 + bx + c$ tal que Δ es un cuadrado en K.
Demostrar que si $z_1 \wedge z_2$ son los definidos más arriba, se verifica que

$$p(x) = a\,(x - z_1)\,(x - z_2)$$

Número de raíces de un polinomio de grado n:

***Teorema*:** Sea $p(x) \in K[x]$, K cuerpo, $gr(p(x)) = n \in \mathbb{N}$. Entonces $p(x)$ tiene, cuanto más, n raíces distintas en K.

***Demostración*:**

Sean $r_1, r_2, r_3, ..., r_k$ las raíces distintas de $p(x)$ en K; como r_i es raíz de $p(x)$
entonces $(x - r_i) \mid p(x) \quad \forall i$, $i = 1,2\ldots, k$.

Para $i \neq j$, $r_i \neq r_j$ $\therefore$ $(x - r_i, x - r_j) = 1$, por ser irreducibles mónicos distintos, entonces tenemos que $\prod_{i=1}^{k}(x-r_i) \mid p(x)$ $\therefore$ $gr(\prod_{i=1}^{k}(x-r_i)) \leq gr(p(x))$ $\therefore$ $k \leq n$, donde k es la cantidad de raíces distintas de $p(x)$.

Multiplicidad de raíces:

Sea $p(x) \in K[x]$, K cuerpo, $gr(p(x)) \geq 1$; $a \in K$ raíz de $p(x)$ $\therefore$ $(x - a) \mid p(x)$.

$$\text{Sea} \quad k = máx\left\{ i \in \mathbb{N} \,/\, (x-a)^i \mid p(x) \right\}.$$

El conjunto es no vacío porque contiene al 1, y está acotado superiormente por $gr(p(x))$, luego tiene máximo.

$\therefore$ $p(x) = (x - a)^k . q(x)$ donde $q(a) \neq 0$

k se denomina *multiplicidad de* a *como raíz de* $p(x)$.

Si $k = 1$, a se dice *raíz simple de* $p(x)$, y si $k > 1$, se dice que a es *raíz múltiple de* $p(x)$.

***Definición*:** Sea $p(x) \in K[x]$, K cuerpo, $gr(p(x)) \geq 1$, $p(x) = \sum_{i=0}^{n} a_i x^i$.

Se llama *polinomio derivado de* $p(x)$, al polinomio:

$$p'(x) = \sum_{i=0}^{n-1} (i+1) a_{i+1} x^i$$

***Propiedades*:**

1. Si $p(x) = (x-a).\, q(x) \Rightarrow p'(x) = q(x) + (x-a).q'(x)$.
2. Si $p(x) = (x-a)^k.\, q(x)$, con $k > 1 \Rightarrow p'(x) = k(x-a)^{k-1}.q(x) + (x-a)^k.q'(x)$.

***Demostración*:** Se deja como ejercicio.

***Teorema*:** Sea $p(x) \in K[x]$, K cuerpo, a raíz de $p(x)$. Entonces,
a es raíz múltiple de $p(x)$ si y sólo si es raíz de su polinomio derivado.

***Demostración*:**

$\Rightarrow$) Sea a raíz múltiple de $p(x)$, entonces $p(x) = (x-a)^k.\, q(x)$, con $k > 1$,
el polinomio derivado es $p'(x) = k(x-a)^{k-1}.q(x) + (x-a)^k.q'(x)$, como $k - 1 > 0$,
especializando $p'(x)$ en a, tenemos que $p'(a) = k(a-a)^{k-1}.q(a) + (a-a)^k q'(a) = 0$
$\therefore$ a es raíz de $p'(x)$.

$\Leftarrow$) Sea a raíz simple de $p(x)$, entonces $p(x) = (x-a).\, q(x)$, con $q(a) \neq 0$, el polinomio derivado es $p'(x) = q(x) + (x-a).q'(x)$.
Especializando $p'(x)$ en a, tenemos $p'(a) = q(a) + (a-a).q'(a) = q(a) \neq 0$
$\therefore$ a no es raíz de $p'(x)$.

***Teorema*:** Sea $p(x) \in K[x]$, K cuerpo, $gr(p(x)) = n \in \mathbb{N}$.
$p(x)$ tiene, cuanto más, n raíces en K, contando cada raíz tantas veces cuanta sea su multiplicidad.

***Demostración*:**

Sean $r_1, r_2, r_3, ..., r_s$ las raíces distintas de $p(x)$ en K, y sea k_i la multiplicidad de r_i como raíz de $p(x)$, entonces $(x-r_i)^{k_i} \mid p(x)$ $\forall i$, $i = 1,2\ldots, s$.
Para $i \neq j$, $r_i \neq r_j$ $\therefore$ $(x - r_i, x - r_j) = 1$, por ser irreducibles mónicos distintos,
$\therefore$ $((x-r_i)^{k_i}, (x-r_j)^{k_j}) = 1$ para todo $i \neq j$
$\Rightarrow$ $\prod_{i=1}^{s} (x-r_i)^{k_i} \mid p(x)$ $\therefore$ $gr(\prod_{i=1}^{s} (x-r_i)^{k_i}) \leq gr(p(x))$ $\therefore$ $\sum_{i=1}^{s} k_i \leq n$, donde $k_1 + k_2 + \ldots + k_s$ es la cantidad de raíces de $p(x)$ contando cada raíz tantas veces cuanta sea su multiplicidad.

Nota: Existe un único polinomio mónico de grado n que tiene a $x_1, x_2, x_3, ..., x_n$ como raíces : $p(x) = (x-x_1)(x-x_2)(x-x_3).....(x-x_n)$.

La familia de polinomios de grado n que tienen a $x_1, x_2, x_3, ..., x_n$ como raíces es:

$$u.\ (x-x_1)(x-x_2)(x-x_3).....(x-x_n),\quad u\in K-\{0\}.$$

***Corolario*:** Sea $p(x)\in K[x]$, K cuerpo, $gr(p(x)) = n\in \mathbb{N}$, $b\in K$. Existen cuanto más n elementos $k_i \in K$ tales que $p(k_i) = b$.

***Demostración*:** Sea $q(x) = p(x) - b$; $gr(q(x)) = gr(p(x)) = n$ $\therefore$ por el teorema, $q(x)$ tiene cuanto más, n raíces en K.

k_i es raíz de $q(x) \Leftrightarrow p(k_i) = b$

$\therefore$ existen cuanto más n elementos $k_i \in K$ tales que $p(k_i) = b$.

***Corolario*:** Sean $p(x), q(x)\in K[x]$, K cuerpo infinito, $p(k) = q(k)$ para infinitos $k \in K$ si y sólo si $p(x) = q(x)$.

***Demostración*:** Sea $h(x) = p(x) - q(x)$.

$\Rightarrow$) Si $h(x) \neq 0 \Rightarrow gr(h(x)) = n\in \mathbb{N}_0$;

para $b\in K$ $p(b) = q(b) \Leftrightarrow h(b) = 0$, y ellos pueden ser cuanto más n

$\therefore$ Si $p(k) = q(k)$ para infinitos $k \in K \Rightarrow h(x) = 0$ $\therefore$ $p(x) = q(x)$.

$\Leftarrow$) es trivial.

***Definición*:** Sea $p(x)\in K[x]$, K cuerpo. Llamamos *función polinómica asociada al polinomio* p, a la función:

$$\mathfrak{p}: K \to K \text{ tal que } \mathfrak{p}(k) = p(k)$$

o sea $\mathfrak{p}$ en cada elemento $k\in K$ es el valor del polinomio p especializado en k.

***Proposición*:** Sean $p(x)$, $q(x)\in K[x]$, K cuerpo infinito, $\mathfrak{p}$, $\mathfrak{q}$ las funciones polinómicas asociadas a los polinomios p y q respectivamente .
Entonces $\mathfrak{p} = \mathfrak{q}$ si y sólo si $p(x) = q(x)$.

***Demostración*:**

$\mathfrak{p} = \mathfrak{q}$ si y sólo si $p(k) = q(k)$ $\forall k \in K$, y como K es infinito, esto ocurre si y sólo si $p(x) = q(x)$.

Nota: La proposición no se cumple necesariamente si K es un cuerpo finito.

Contraejemplo: $K = \mathbb{Z}_p$, $p\in \mathbb{N}$ primo; $p(x) = x$, $q(x) = x^p$

Las funciones polinómicas asociadas a $p(x)$ y $q(x)$ respectivamente son $\mathfrak{p}$ y $\mathfrak{q}$,

$$\mathfrak{p}: \mathbb{Z}_p \to \mathbb{Z}_p \text{ tal que } \mathfrak{p}(\overline{a}) = \overline{a} \quad \wedge \quad \mathfrak{q}: \mathbb{Z}_p \to \mathbb{Z}_p \text{ tal que } \mathfrak{q}(\overline{a}) = (\overline{a})^p.$$

Por el Pequeño Teorema de Fermat, sabemos que $(\overline{a})^p = \overline{a}$ $\forall \overline{a} \in \mathbb{Z}_p$, entonces

$\mathfrak{p}(\overline{a}) = \mathfrak{q}(\overline{a})$ $\forall \overline{a} \in \mathbb{Z}_p$ $\therefore$ $\mathfrak{p} = \mathfrak{q}$ pero $p(x) \neq q(x)$, o sea, polinomios distintos pueden darnos funciones polinómicas asociadas coincidentes.

Relación entre coeficientes y raíces de un polinomio:

François Viète (1540-1603)

François Viète estudió derecho y llegó a ser miembro del Parlamento de Bretaña y miembro del consejo real durante los reinados de Enrique III y Enrique IV. Se dedicó a la matemática sólo en sus ratos de ocio, no obstante dejó importantes contribuciones a la aritmética, al álgebra, a la trigonometría y a la geometría. Conocía algunas de las relaciones entre coeficientes y raíces de una ecuación algebraica, pero con las limitaciones obvias, al no admitir coeficientes ni raíces negativas. Por ejemplo, comprobó que si la ecuación $x^3+b = 3ax$ *tiene dos raíces positivas* x_1 *y* x_2*, entonces* $3a = x_1^2 + x_1x_2 + x_2^2$ *y* $b = x_1x_2^2 + x_2x_1^2$*, que, por supuesto, no es más que un caso particular.*

En 1629 el matemático francés Albert Girard formuló en forma clara y precisa las relaciones entre coeficientes y raíces en su obra "Invention nouvelle en l'algèbre" al permitir las raíces tanto negativas como complejas y fue, por tanto, capaz de finalizar el aún incompleto estudio de François Viète. También es posible que haya sido Girard el primero en constatar que una ecuación puede tener tantas raíces como indique su grado.

Albert Girard (1595-1632)

Sea $p(x) \in K\ [x]$ de grado positivo, sabemos que está unívocamente determinado por sus coeficientes, pero además, si tiene grado n podría tener n raíces en K; también sabemos que si conociéramos todas sus raíces, no nos bastaría para determinar el polinomio, porque, como vimos anteriormente, hay una familia de polinomios distintos que tienen las mismas raíces; ahora, si conociéramos todas las raíces y su coeficiente principal (o algún otro dato que nos conduzca a él) allí sí podríamos determinar sus coeficientes.
Analicemos el problema comenzando con un polinomio de segundo grado que tenga sus dos raíces en K.

Sea $p(x) \in K\ [x]$, $p(x) = ax^2 + bx + c$, $a \neq 0$; si $x_1 \wedge x_2$ son sus raíces,

$$p(x) = a(x - x_1)(x - x_2)\ .$$

Aplicando propiedad distributiva e igualdad de polinomios, tenemos que

$$b = -a(x_1 + x_2) \quad \wedge \quad c = a\,x_1\,x_2\ .$$

Por lo tanto $x_1 + x_2 = -\dfrac{b}{a} \quad \wedge \quad x_1\,.\,x_2 = \dfrac{c}{a}$.

Sea ahora $p(x)$ un polinomio de tercer grado, $p(x) = ax^3 + bx^2 + cx + d$, con $a \neq 0$; sean x_1 , x_2 , x_3 sus raíces , entonces $p(x) = a(x - x_1)(x - x_2)(x - x_3)$.
Aplicando propiedad distributiva obtenemos que:
$b = -a(x_1 + x_2 + x_3)$, $c = a(x_1 x_2 + x_1 x_3 + x_2 x_3)$ $\wedge$ $d = -a\, x_1 . x_2 . x_3$.
Por lo tanto $x_1 + x_2 + x_3 = -\frac{b}{a}$, $x_1 x_2 + x_1 x_3 + x_2 x_3 = \frac{c}{a}$ $\wedge$ $x_1 . x_2 . x_3 = -\frac{d}{a}$.

Ahora analicemos el caso general:

Sea $p(x) \in K[x]$, $gr(p(x)) = n$, $x_1, x_2, x_3, ..., x_n$ raíces de $p(x)$.

$$p(x) = a_n x^n + a_{n-1} x^{n-1} + ... + a_2 x^2 + a_1 x + a_0 = a_n . (x - x_1)(x - x_2)(x - x_3).....(x - x_n)$$

con $a_n \neq 0$.

$$a_{n-1} = a_n (-1)(x_1 + x_2 + x_3 + ... + x_n) \quad \boxed{\sum_{i=1}^{n} x_i = -\frac{a_{n-1}}{a_n}} \quad \Rightarrow$$

$$a_{n-2} = a_n (x_1 x_2 + x_1 x_3 + x_1 x_4 + ... + x_1 x_n + x_2 x_3 + ... + x_2 x_n + ... + x_{n-1} x_n)$$

$$\Rightarrow \quad \boxed{\sum_{i<j} x_i x_j = \frac{a_{n-2}}{a_n}}$$

$$a_{n-3} = a_n (-1)(x_1 x_2 x_3 + x_1 x_2 x_4 + ... + x_1 x_2 x_n + x_1 x_3 x_4 + ... + x_1 x_3 x_n + ... + x_{n-2} x_{n-1} x_n)$$

$$\Rightarrow \quad \boxed{\sum_{i<j<k} x_i x_j x_k = -\frac{a_{n-3}}{a_n}}$$

……..

$$a_2 = (-1)^{n-2} a_n (x_1 x_2 x_3 ... x_{n-2} + x_1 x_2 ... x_{n-3} x_{n-1} + ... + x_3 x_4 .. x_{n-1} x_n)$$

$$\Rightarrow \quad \boxed{\sum_{i_1 < i_2 < .. < i_{n-2}} x_{i_1} x_{i_2} ... x_{i_{n-2}} = (-1)^{n-2} \frac{a_2}{a_n}}$$

$$a_1 = (-1)^{n-1} a_n (x_1 x_2 ... x_{n-1} + x_1 x_2 ... x_{n-2} x_n + ... + x_2 x_3 ... x_n)$$

$$\Rightarrow \quad \boxed{\sum_{i_1 < i_2 < ... < i_{n-1}} x_{i_1} x_{i_2} ... x_{i_{n-1}} = (-1)^{n-1} \frac{a_1}{a_n}}$$

$$a_0 = (-1)^n a_n \quad x_1 x_2 .... x_n \qquad \Rightarrow \quad \boxed{\prod_{i=1}^{n} x_i = (-1)^n \frac{a_0}{a_n}}$$

Polinomios con coeficientes en $\mathbb{Z}$ **:**

- ***Lema de Gauss*:**

Sea $p(x) \in \mathbb{Z}[x]$ de grado positivo, $p(x) = \sum_{i=0}^{n} a_i x^i$, $n \in \mathbb{N}$,

$a_n \neq 0$. Si $\frac{r}{s} \in \mathbb{Q}$, con $r, s \in \mathbb{Z}$, $s \neq 0$, $(r, s) = 1$, es raíz de $p(x)$

entonces $r \mid a_0 \ \wedge \ s \mid a_n$.

***Demostración*:** Sea $\frac{r}{s}$ raíz de $p(x)$, entonces $p(\frac{r}{s}) = 0$

$$\therefore \qquad 0 = a_0 + a_1 \frac{r}{s} + a_2 \frac{r^2}{s^2} + a_3 \frac{r^3}{s^3} + ... + a_{n-1} \frac{r^{n-1}}{s^{n-1}} + a_n \frac{r^n}{s^n} \quad \text{(I)}$$

multiplicando (I) m.a.m. por s^n

$$0 = a_0 s^n + a_1 r s^{n-1} + a_2 r^2 s^{n-2} + ... + a_{n-1} r^{n-1} s + a_n r^n \quad \text{(II)}.$$

De (II) obtenemos:

$$-a_0 s^n = a_1 r s^{n-1} + a_2 r^2 s^{n-2} + ... + a_{n-1} r^{n-1} s + a_n r^n =$$

$$= r\,(a_1 s^{n-1} + a_2 r s^{n-2} + ... + a_{n-1} r^{n-2} s + a_n r^{n-1}).$$

Como $a_1 s^{n-1} + a_2 r s^{n-2} + ... + a_{n-1} r^{n-2} s + a_n r^{n-1} \in \mathbb{Z}$

tenemos que $r \mid a_0 s^n$, pero $(r, s) = 1 \ \Rightarrow \ (r, s^n) = 1 \ \therefore \ r \mid a_0$.

También de (II) tenemos que:

$$-a_n r^n = a_0 s^n + a_1 r s^{n-1} + a_2 r^2 s^{n-2} + ... + a_{n-2} r^{n-2} s^2 + a_{n-1} r^{n-1} s =$$

$$= s\,(a_0 s^{n-1} + a_1 r s^{n-2} + a_2 r^2 s^{n-3} + ... + a_{n-2} r^{n-2} s + a_{n-1} r^{n-1}).$$

Como $a_0 s^{n-1} + a_1 r s^{n-2} + a_2 r^2 s^{n-3} + ... + a_{n-2} r^{n-2} s + a_{n-1} r^{n-1} \in \mathbb{Z}$

tenemos que $s \mid a_n r^n$, pero $(r, s) = 1 \ \Rightarrow \ (r^n, s) = 1 \ \therefore \ s \mid a_n$.

Nota: El Lema de Gauss nos brinda una *condición necesaria* que deben cumplir las raíces racionales de un polinomio con coeficientes enteros, pero esta condición **no** es *suficiente*, como lo muestra el siguiente ejemplo:

Ejemplo: Sea $p(x) = 3x^2 + 4$. Si un número racional $\frac{r}{s}$ es raíz de $p(x)$, $r \mid 4 \ \wedge \ s \mid 3$;

por lo tanto, las potenciales raíces son: ± 4 ; ± 2 ; ± 1 ; $\pm\frac{1}{3}$; $\pm\frac{2}{3}$; $\pm\frac{4}{3}$, y un simple cálculo nos muestra que ninguno de estos números es raíz de $p(x)$, por lo cual $p(x)$ no admite raíces racionales; pero, además, muestra que el hecho de que un número racional verifique la condición necesaria del teorema, no implica que sea una raíz; el teorema dice que todos aquéllos que no la verifican, no son raíces, lo que nos acota las posibles raíces a una cantidad finita de números racionales.

***Corolario*:** Las raíces racionales de un polinomio mónico de $\mathbb{Z}[x]$ son enteras.

***Demostración*:** trivial.

Ejemplos:

1) $p(x) = x^5 + 3x^4 - 10x^3 + 3x^2 + 9x - 30$

Como el polinomio es mónico, si tiene raíces racionales, éstas serán enteras.
Las posibles raíces son: ± 1 ; ± 2 ; ± 3 ; ± 5 ; ± 6 ; ± 10 ; ± 15 ; ± 30 .
Probando con los distintos números, comprobamos que si dividimos $p(x)$ por $x-2$ obtenemos resto cero, con lo cual 2 es raíz.

Aplicando la regla de Ruffini:

	1	3	–10	3	9	–30
2		2	10	0	6	30
	1	5	0	3	15	0

Luego $p(x) = x^5 + 3x^4 - 10x^3 + 3x^2 + 9x - 30 = (x-2)(x^4 + 5x^3 + 3x + 15)$.

Las otras raíces de $p(x)$ son las raíces de $q(x) = x^4 + 5x^3 + 3x + 15$, que en $\mathbb{Q}$ sólo pueden ser ± 1 ; ± 3 ; ± 5 ; ± 15 ; cuando probamos con -5 , aplicando Ruffini tenemos que:

	1	5	0	3	15
–5		–5	0	0	–15
	1	0	0	3	0

Por lo tanto -5 es raíz de $p(x)$, con lo que $p(x) = (x-2)(x+5)(x^3+3)$.
Las posibles raíces racionales de x^3+3 son ± 1 ; ± 3 y ninguna lo es por lo que este polinomio es irreducible en $\mathbb{Q}[x]$ (por tener grado 3 y no tener raíces en el cuerpo).
Hemos encontrado las raíces en $\mathbb{Q}$ de $p(x)$ y su factorización en irreducibles mónicos en $\mathbb{Q}[x]$.

Paolo Ruffini (1765-1822)

***El método de Ruffini**. Este método fue publicado en* 1804 *y en su esencia coincide con el método de William G. Horner, aparecido en* 1819 *y conocido como "esquema de Horner", reservando para Ruffini el método práctico que permite determinar los coeficientes del cociente de la ecuación por sus factores lineales, procedimiento que ideó Ruffini para facilitar los cálculos. Matemáticos chinos del siglo* XIII *fueron lejanos precursores del método de Ruffini-Horner.*
("Historia de la Matemática". Vol 2. Julio Rey Pastor y José Babini).

2) $h(x) = 4x^4 + \frac{2}{5}x^3 - \frac{21}{5}x^2 - \frac{3}{10}x + \frac{9}{10}$.

$h(x) \in \mathbb{Q}[x] - \mathbb{Z}[x]$ por lo que no puede aplicarse el Lema de Gauss a este polinomio, pero sí podremos hacerlo con algún asociado a $h(x)$ que pertenezca a $\mathbb{Z}[x]$.

Sabemos que las raíces de $h(x)$ son las mismas que las de $uh(x)$ $\forall u \in \mathbb{Q} - \{0\}$, y eligiendo convenientemente a u podemos obtener que $uh(x) \in \mathbb{Z}[x]$, por ejemplo u un múltiplo del mcm de los denominadores de los coeficientes del polinomio; en nuestro caso, podemos tomar $u = 10$.

El polinomio $t(x) = 10.h(x) = 40x^4 + 4x^3 - 42x^2 - 3x + 9 \in \mathbb{Z}[x]$, y como $t(x)$ y $h(x)$ son asociados, tienen las mismas raíces, y a $t(x)$ sí podemos aplicarle el Lema de Gauss.

Si un número racional $\frac{r}{s}$ es raíz de $t(x)$ entonces $r \mid 9 \ \wedge \ s \mid 40$

$\therefore$ r puede tomar los siguientes valores : ± 1 ; ± 3 ; ± 9 ,

y s los valores: 1 ; 2 ; 4 ; 5 ; 8 ; 10 ; 20 ; 40 .

Aplicamos la regla de Ruffini para dividir por $x - \frac{1}{2}$:

	40	4	–42	–3	9
½		20	12	–15	–9
	40	24	–30	–18	0

$t(x) = 40x^4 + 4x^3 - 42x^2 - 3x + 9 = (x - \frac{1}{2})\,(40x^3 + 24x^2 - 30x - 18)$.

Dividimos el cociente por $x + \frac{3}{5}$:

	40	24	–30	–18
$-\,^3/_5$		–24	0	18
	40	0	–30	0

$t(x) = (x - \frac{1}{2}).(x + \frac{3}{5}).\,(40x^2 - 30)$.

El discriminante del polinomio de segundo grado $40x^2 - 30$ es $\Delta = 4800 = 48.100$
que no es un cuadrado en $\mathbb{Q}$ porque 48 no lo es, por lo tanto dicho polinomio es irreducible en $\mathbb{Q}[x]$.

La factorización en $\mathbb{Q}[x]$ en polinomios irreducibles mónicos de $t(x)$ es:

$$t(x) = 40\,(x - \frac{1}{2})\,(x + \frac{3}{5})\,(x^2 - \frac{3}{4})$$

$\therefore$ la de $h(x)$ es: $h(x) = 4(x - \frac{1}{2})\,(x + \frac{3}{5})\,(x^2 - \frac{3}{4})$.

- ***Criterio de irreducibilidad de Eisenstein***

Se le atribuye a Gauss la afirmación de que "ha habido sólo tres matemáticos de excepcional importancia: Arquímedes, Newton y Eisenstein". La cuestión de si Eisenstein, en el tiempo de duración de una vida normal, hubiera llegado a cumplir con predicción tan entusiasta, queda pendiente de conjetura, puesto que este joven matemático murió antes de cumplir los 30 años, siendo aun "Privatdozent". ("Historia de la Matemática" Carl B.Boyer).

***Definición*:** Sea $p(x) \in \mathbb{Z}[x]$, $p(x) = \sum_{i=0}^{n} a_i x^i$, $a_n \neq 0$. Llamamos *contenido de* $p(x)$ al máximo común divisor de los coeficientes de $p(x)$, o sea $cont(p) = (a_0, a_1, a_2, \ldots, a_n)$.

***Proposición*:** Sea $p(x) \in \mathbb{Z}[x]$ no nulo, $cont(p) = d$ si y sólo si $p(x) = d.\, t(x)$, con $t(x) \in \mathbb{Z}[x]$ $\wedge$ $cont(t) = 1$.

***Demostración*:** Sea $p(x) = \sum_{i=0}^{n} a_i x^i$, $a_n \neq 0$, $a_i \in \mathbb{Z}$ $\forall\, i = 0,1,\ldots n.$

$$d = cont(p) \Leftrightarrow d = (a_0, a_1, a_2, \ldots, a_n) \quad .$$

$\Rightarrow$) Para $d \mid a_i$ $\forall\, i = 0,1,\ldots n$, $d = (a_0, a_1, a_2, \ldots, a_n) \Leftrightarrow a_i = d.b_i$, con $b_i \in \mathbb{Z}$ $\wedge$ $(b_0, b_1, \ldots, b_n) = 1$ $\therefore$ $p(x) = dt(x)$ con $t(x) = \sum_{i=0}^{n} b_i x^i$, y $cont(t) = 1$.

$\Leftarrow$) Sea ahora $p(x) = dt(x)$, con $cont(t) = 1$.

$$t(x) = \sum_{i=0}^{n} b_i x^i \ , \ (b_0, b_1, \ldots, b_n) = 1 \quad \therefore \quad p(x) = d \sum_{i=0}^{n} b_i x^i = \sum_{i=0}^{n} d.b_i x^i$$

$$(d b_0, d b_1, \ldots, d b_n) = d.\,(b_0, b_1, \ldots, b_n) = d.1 = d$$

$\therefore$ $cont(p) = d$.

***Definición*:** Sea $q(x) \in \mathbb{Z}[x]$ se denomina *primitivo* si $cont(q) = 1$.

Por lo tanto, ***todo polinomio es producto de su contenido por un polinomio primitivo.***

***Teorema*:** Sean $f(x)$, $g(x) \in \mathbb{Z}[x]$ no nulos;
$f(x).g(x)$ es un polinomio primitivo si y sólo si $f(x)$ y $g(x)$ lo son.

***Demostración*:** $\Leftarrow$) Sean $f(x)$ $\wedge$ $g(x)$ polinomios primitivos;

$$f(x) = \sum_{j=0}^{m} a_j x^j \quad , \quad g(x) = \sum_{i=0}^{n} b_i x^i \quad , \quad f(x).g(x) = \sum_{k=0}^{m+n} d_k x^k \quad \text{con} \quad d_k = \sum_{j+i=k} a_j b_i \ .$$

Supongamos que $cont(f.g) = t > 1$ $\therefore$ $\exists\, p \in \mathbb{N}$ primo tal que $p \mid t$ $\therefore$ $p \mid d_k$
$\forall k = 0,1,\ldots n+m.$
Como $cont(f) = cont(g) = 1$ tenemos que $\exists\, i$, $0 \le i \le n$, tal que $p \nmid b_i$ $\wedge$
$\exists j$, $0 \le j \le m$, tal que $p \nmid a_j$. Sean $r = mín\{\, j \;/\; p \nmid a_j \,\}$, $s = mín\{\, i \;/\; p \nmid b_i \,\}$

$$d_{r+s} = \sum_{i+j=r+s} a_j b_i = a_r b_s + \sum_{\substack{i+j=r+s \\ j<r}} a_j b_i + \sum_{\substack{i+j=r+s \\ i<s}} a_j b_i$$

$p \mid a_j$ para $j < r$ $\Rightarrow$ $p \mid \sum_{\substack{i+j=r+s \\ j<r}} a_j b_i$;

$p \mid b_i$ para $i < s$ $\Rightarrow$ $p \mid \sum_{\substack{i+j=r+s \\ i<s}} a_j b_i$

$p \mid d_{r+s}$ $\Rightarrow$ $p \mid a_r b_s$ $\therefore$ $p \mid a_r$ $\vee$ $p \mid b_s$!! (absurdo!).

Luego $cont(f.g) = 1$, y $f(x).g(x)$ es un polinomio primitivo.

$\Rightarrow$) Supongamos que $f(x).g(x)$ es un polinomio primitivo, y sean $f(x) = d\, t(x)$,
$g(x) = e\, q(x)$ con $t(x)$ $\wedge$ $q(x)$ polinomios primitivos, $d, e \in \mathbb{N}$.
$f(x).g(x) = d.e.\, t(x).q(x)$.

Por lo visto anteriormente $t(x).q(x)$ es un polinomio primitivo $\therefore$ $1 = cont(f.g) = d.e$
con lo cual $d = e = 1$ y así $f(x)$ y $g(x)$ son polinomios primitivos.

***Corolario*:** Sean $f(x), g(x) \in \mathbb{Z}[x]$ no nulos, $cont(f.g) = cont(f).\, cont(g)$.

***Demostración*:** Inmediata a partir de lo ya demostrado.

Ejercicio: Sea $f(x) \in \mathbb{Z}[x]$ no nulo, $d \in \mathbb{N}$, demostrar que $cont(d.f) = d.cont(f)$.

- Sea $p(x) \in \mathbb{Q}[x]$, $p(x)$ $\sum_{i=0}^{n} \frac{a_i}{b_i} x^i$, $a_i, b_i \in \mathbb{Z}$. Sea $b = [\, b_0, b_1, b_2, \ldots, b_n \,]$,

$c_i = b\frac{a_i}{b_i} \in \mathbb{Z}$, $i = 0,1,\ldots,n$, luego $q(x) = b.\, p(x) \in \mathbb{Z}[x]$.
$q(x) = d.\, h(x)$, con $h(x)$ polinomio primitivo, $d = cont(q)$ $\Rightarrow$ $b.p(x) = d.h(x)$
$\therefore$ $p(x) = \frac{d}{b} h(x)$ con $h(x) \in \mathbb{Z}[x]$ primitivo.
Por lo tanto, si $p(x) \in \mathbb{Q}[x]$, $\exists r \in \mathbb{Q}$ $\wedge$ $\exists h(x) \in \mathbb{Z}[x]$ primitivo, tal que $p(x) = rh(x)$.

***Proposición*:** Sea $f(x) \in \mathbb{Z}[x]$ no nulo tal que $f(x) = h(x).\, t(x)$, con $h(x), t(x) \in \mathbb{Q}[x]$.
Entonces $\exists\, h_1(x), t_1(x) \in \mathbb{Z}[x]$ tales que $f(x) = h_1(x).\, t_1(x)$, con $gr(h_1) = gr(h)$ $\wedge$
$gr(t_1) = gr(t)$.

***Demostración*:** Por lo visto más arriba, $h(x) = r.h_1(x)$, $t(x) = s.t_1(x)$ con $r, s \in \mathbb{Q}$, $h_1(x),\ t_1(x) \in \mathbb{Z}[x]$ primitivos $\Rightarrow$ $f(x) = r.s.\ h_1(x).t_1(x)$,

$r.s \in \mathbb{Q}$ por lo tanto $r.s = \dfrac{a}{b}$, con a , $b \in \mathbb{Z}$, $(a\ ,\ b) = 1$ $\therefore$ $f(x) = \dfrac{a}{b}.h_1(x).t_1(x)$,

de donde $b.f(x) = a.h_1(x).t_1(x) \in \mathbb{Z}[x]$

$cont(b.f) = cont(a.h_1\ .t_1)$ $\therefore$ $b.cont(f) = a$ por ser $h_1(x).t_1(x)$ primitivo.

Como $cont(f) \in \mathbb{Z}$ $\Rightarrow$ $b \mid a$, por lo tanto $b = 1$ por ser $(a\ ,\ b) = 1$

$\therefore$ $f(x) = a.h_1(x).t_1(x)$; si llamamos $h_2(x) = a.h_1(x) \in \mathbb{Z}[x]$

tenemos que $f(x) = h_2(x).t_1(x)$ con $h_2(x)\ ,\ t_1(x) \in \mathbb{Z}[x]$**.**

***Corolario*:** Sea $f(x) \in \mathbb{Z}[x]$ primitivo, es irreducible en $\mathbb{Q}[x]$ si y sólo si es irreducible en $\mathbb{Z}[x]$**.**

***Demostración*:** $\Rightarrow$) Sea $f(x) \in \mathbb{Z}[x]$ reducible en $\mathbb{Z}[x]$**,** entonces $f(x) = h(x).\ t(x)$, con $h(x)\ ,\ t(x) \in \mathbb{Z}[x]$ **,** no unidades de $\mathbb{Z}$.

- Si $0 < gr(h) < gr(f)$ $\wedge$ $0 < gr(t) < gr(f)$, $h(x)\ ,\ t(x) \in \mathbb{Q}[x]$ de grado positivos $\therefore$ $h(x)\ ,\ t(x)$ no son unidades de $\mathbb{Q}$, por lo tanto $f(x)$ es reducible en $\mathbb{Q}[x]$.
- Si $gr(h) = 0$ (o $gr(t) = 0$) entonces $h(x) = c \in \mathbb{Z} - \{0, 1, -1\}$, con lo cual

  $f(x) = h(x).\ t(x) = c.\ t(x)$ $\therefore$ $1 = cont(f) = \left| c \right|.\ cont(t)$ por lo que $c \mid 1$!! (absurdo!)

  $\therefore$ $f(x)$ es reducible en $\mathbb{Q}[x]$.

$\Leftarrow$) Sea $f(x) \in \mathbb{Z}[x]$ reducible en $\mathbb{Q}[x]$, entonces $f(x) = h(x).\ t(x)$,

con $h(x)\ ,\ t(x) \in \mathbb{Q}[x]$ **,** $0 < gr(h) < gr(f)$ $\wedge$ $0 < gr(t) < gr(f)$.

Por la Proposición anterior $\exists\ h_1(x),\ t_1(x) \in \mathbb{Z}[x]$ tales que $f(x) = h_1(x).\ t_1(x)$ con $gr(h_1) = gr(h) > 0$ $\wedge$ $gr(t_1) = gr(t) > 0$ $\therefore$ $h_1(x)\ ,t_1(x)$ son polinomios de grado positivo en $\mathbb{Z}[x]$ **,** con lo cual no son unidades de $\mathbb{Z}$ $\therefore$ $f(x)$ es reducible en $\mathbb{Z}[x]$**.**

***Teorema*: (*Criterio de irreducibilidad de Eisenstein*)**

Sea $f(x) \in \mathbb{Z}[x]$**,** $gr(f) \geq 1$, $f(x) = \sum_{k=0}^{n} a_k x^k$. Supongamos que $\exists p \in \mathbb{N}$ primo tal que:

i. $p \mid a_k$ $\forall k = 0, 1, 2, ..., n-1$.

ii. $p \nmid a_n$.

iii. $p^2 \nmid a_0$.

Entonces $f(x)$ es irreducible en $\mathbb{Q}[x]$.

***Demostración*:** Supongamos $f(x)$ es reducible en $\mathbb{Q}[x]$. Entonces $f(x) = h(x).\ t(x)$ con $h(x)\ ,\ t(x) \in \mathbb{Q}[x]$ tales que $0 < gr(h) < gr(f)$ $\wedge$ $0 < gr(t) < gr(f)$.

Por la Proposición anterior $\exists\ h_1(x),\ t_1(x) \in \mathbb{Z}[x]$ tales que $f(x) = h_1(x).t_1(x)$ con $gr(h_1) = gr(h) > 0$ $\wedge$ $gr(t_1) = gr(t) > 0$.

$h_1(x) = \sum_{i=0}^{m} b_i x^i$, $t_1(x) = \sum_{j=0}^{r} c_j x^j$, $b_i , c_j \in \mathbb{Z}$, $\forall i, j$, $m + r = n$

$f(x) = h_1(x).t_1(x) \Rightarrow a_k = \sum_{i+j=k} b_i c_j \quad \forall k$, $k = 0,1,\ldots,n$

$p \mid a_0 = b_0 . c_0 \Rightarrow p \mid b_0 \vee p \mid c_0$

pero $p^2 \nmid a_0 \Rightarrow (p \mid b_0 \wedge p \nmid c_0) \vee (p \mid c_0 \wedge p \nmid b_0)$

Sin pérdida de generalidad, supongamos que $p \mid b_0 \wedge p \nmid c_0$

- $p \mid a_1 = b_1c_0 + b_0c_1 \Rightarrow p \mid b_1c_0$, y como $p \nmid c_0 \Rightarrow p \mid b_1$
- $p \mid a_2 = b_2c_0 + b_1c_1 + b_0c_2 \Rightarrow p \mid b_2c_0$, y como $p \nmid c_0 \Rightarrow p \mid b_2$
- $p \mid a_3 = b_3c_0 + b_2c_1 + b_1c_2 + b_0c_3 \Rightarrow p \mid b_3c_0$, y como $p \nmid c_0 \Rightarrow p \mid b_3$
- $p \mid a_4 = b_4c_0 + b_3c_1 + b_2c_2 + b_1c_3 + b_0c_4 \Rightarrow p \mid b_4c_0$, y como $p \nmid c_0$ $\Rightarrow p \mid b_4$

Por hipótesis, $p \nmid a_n = b_m . c_r \Rightarrow p \nmid b_m \wedge p \nmid c_r$.

Sea $h = mín\{ i / p \nmid b_i \}$ (claramente ese mínimo existe porque el conjunto es no vacío)

Por lo tanto $p \nmid b_h \wedge p \mid b_i \quad \forall i < h$

Ya que $p \mid a_h = b_hc_0 + \sum_{\substack{i+j=h \\ 0 \le i < h}} b_ic_j \wedge$ como $p \mid b_i \quad \forall i < h \Rightarrow p \mid \sum_{\substack{i+j=h \\ 0 \le i < h}} b_ic_j$

$\therefore \quad p \mid b_hc_0$, como $p \nmid c_0 \Rightarrow p \mid b_h$!! (absurdo!).

Luego $f(x)$ es irreducible en $\mathbb{Q}[x]$.

Ejemplos:

1) Los polinomios: $p(x) = 3x^3 - 2x^2 + 12x + 6$, $q(x) = 10x^4 + 6x^3 - 3x + 3$ son irreducibles en $\mathbb{Q}[x]$.

Nótese que la irreducibilidad de $p(x)$ se podría haber demostrado viendo que no tiene raíces en $\mathbb{Q}$ porque es de tercer grado (las posibles raíces serían $\pm 1; \pm 2; \pm 3; \pm 6; \pm\frac{1}{3}; \pm\frac{2}{3}$) pero es más sencillo y rápido utilizar el Criterio de Eisenstein.

En el caso de $q(x)$ no hubiera sido posible razonarlo de otra forma que no fuera por el Criterio de Eisenstein, porque aunque no tenga raíces en $\mathbb{Q}$, al tener grado 4, ello no nos permite afirmar que es irreducible.

2) $f(x) = x^n + 12$, $\forall n \in \mathbb{N}$, $n > 1$ son irreducibles en $\mathbb{Q}[x]$ por el Criterio de Eisenstein.

3) En general todo polinomio de la forma $x^n + a$, $\forall n \in \mathbb{N}$, $n > 1$, es irreducible en $\mathbb{Q}[x]$, $\forall a \in \mathbb{Z} - \{0,1,-1\}$ libre de cuadrados (*a* se dice *libre de cuadrados* si no existe ningún cuadrado mayor que 1 que divida a *a*).

Vamos a demostrar este hecho:

Si $a \in \mathbb{Z} - \{0,1,-1\}$ y es libre de cuadrados, entonces a se factoriza como $a = \pm\prod_{i=1}^{k} p_i$

con los $p_i \in \mathbb{N}$ primos distintos $\forall\, i = 1, 2,\ldots,k$, puesto que si $a = \pm\prod_{i=1}^{k} p_i^{r_i}$, p_i primos distintos, $r_i \in \mathbb{N}\ \ \forall i = 1,2...,k$, con algún $r_j > 1$ tendríamos que $p_j^2 \mid a$, y a no sería libre de cuadrados.
Aplicando el Criterio de Eisenstein con cualquiera de los primos p_i obtenemos que el polinomio $x^n + a$ es irreducible en $\mathbb{Q}[x]$.

4) En general todo polinomio de la forma $x^n + a$, $\forall n \in \mathbb{N}$, $n > 1$, es irreducible en $\mathbb{Q}[x]$ cuando $a = \pm\prod_{i=1}^{k} p_i^{r_i}$, p_i primos distintos, $r_i \in \mathbb{N}\ \ \forall i = 1,2...,k$, con algún $r_j = 1$, puesto que podemos aplicar el Criterio de Eisenstein con el primo p_j .

Polinomios ciclotómicos:

***Definición*:** Sea $p \in \mathbb{N}$ primo. Se llama *polinomio ciclotómico de orden p* al polinomio

$$f_p(x) = \frac{x^p - 1}{x - 1} = \sum_{i=0}^{p-1} x^i \ .$$

***Proposición*:** Los polinomios ciclotómicos $f_p\ (x)$ son irreducibles en $\mathbb{Q}[x]$.

***Demostración*:** Primero observemos que la especialización para $a, b \in \mathbb{Q}$, $a \neq 0$, $\psi : \mathbb{Q}[x] \to \mathbb{Q}[x]$ tal que $\psi(r) = r \quad \forall r \in \mathbb{Q} \ \wedge \ \psi(x) = ax + b$, es un isomorfismo de anillos, cuyo isomorfismo inverso es $\psi^{-1} : \mathbb{Q}[x] \to \mathbb{Q}[x]$ tal que $\psi^{-1}(r) = r \quad \forall r \in \mathbb{Q} \ \wedge$ $\psi^{-1}(x) = \dfrac{x-b}{a}$.

- $p(x)$ es irreducible en $\mathbb{Q}[x]$ si y sólo si $q(x) = p(ax+ b)$ es irreducible en $\mathbb{Q}[x]$.

Si $p(x)$ es reducible en $\mathbb{Q}[x]$, $\exists\, t(x)$, $h(x) \in \mathbb{Q}[x]$ tales que $p(x) = t(x)\ .\ h(x)$ con $0 < gr(h(x)) < gr(p(x)) \ \wedge \ 0 < gr(t(x)) < gr(p(x))$,

$$q(x) = p(ax+ b) = t(ax+ b)\ .\ h(ax+ b) = s(x)\ .\ k(x)$$

$gr(t(x)) = gr(s(x)) \ \wedge \ gr(h(x)) = gr(k(x)) \ \Rightarrow \ q(x)$ es reducible en $\mathbb{Q}[x]$.
De la misma forma se demuestra que si $q(x)$ es reducible en $\mathbb{Q}[x]$ entonces $p(x)$ es reducible en $\mathbb{Q}[x]$.

Haremos uso de la especialización $\psi : \mathbb{Q}[x] \to \mathbb{Q}[x]$ tal que $\psi(r) = r \quad \forall r \in \mathbb{Q} \ \wedge$ $\psi(x) = x + 1$. Demostraremos que $f_p\,(x+ 1)$ es irreducible en $\mathbb{Q}[x]$ y con ello obtendremos que $f_p\ (x)$ lo es.

$$g_p(x) = \ f_p(x+1) = \frac{(x+1)^p - 1}{(x+1) - 1} = \frac{(x+1)^p - 1}{x} = \sum_{k=0}^{p-1} \binom{p}{k+1} x^k$$

$$p \mid \binom{p}{k+1} \quad \forall k = 0,1,...,p-2 \quad , \quad p \nmid \binom{p}{p} = 1 \quad \wedge \quad p^2 \nmid \binom{p}{1} = p$$

Por el Criterio de Eisenstein, $g_p(x)$ es irreducible en $\mathbb{Q}[x]$ $\therefore$ $f_p(x)$ es irreducible en $\mathbb{Q}[x]$.

Otro ejemplo:

Sea el polinomio $p(x) = x^4 + x^3 - 2x + 1$. Queremos determinar si es irreducible o no en $\mathbb{Q}[x]$. Claramente no tiene raíces en $\mathbb{Q}$ pues las posibles son 1 y -1 y ninguno de ellas lo es.
Probaremos con la especialización $\theta : \mathbb{Q}[x] \to \mathbb{Q}[x]$ tal que $\theta(r) = r \quad \forall r \in \mathbb{Q} \quad \wedge$ $\theta(x) = x - 1$.
$q(x) = p(x-1) = (x-1)^4 + (x-1)^3 - 2(x-1) + 1 = x^4 - 3x^3 + 3x^2 - 3x + 3$ que es irreducible en $\mathbb{Q}[x]$ por Einsenstein aplicado al primo 3, por lo tanto $p(x)$ es también irreducible en $\mathbb{Q}[x]$.

Otro Criterio de irreducibilidad

Sea $f(x) \in \mathbb{Z}[x]$, $p \in \mathbb{N}$ primo, $f(x) = \sum_{i=0}^{n} a_i x^i$, llamaremos $\overline{f(x)} = \sum_{i=0}^{n} \overline{a}_i x^i \in \mathbb{Z}_p[x]$, donde $\overline{a}_i \in \mathbb{Z}_p$ es la clase *mód p* de a_i $\forall i = 0,1,...,n$.
Nótese que puede ocurrir que $\overline{f(x)} = 0$ siendo $f(x) \neq 0$, como lo muestra el siguiente ejemplo:

Ejemplo: $f(x) = 10x^3 + 5x^2 + 15$, en $\mathbb{Z}_5[x]$ nos da $\overline{f(x)} = 0$.

Además, si $\overline{f(x)} \neq 0$, sólo podemos afirmar que $gr(\overline{f(x)}) \leq gr(f(x))$, pues, por ejemplo, $f(x) = 7x^5 + 4x^3 + 14x^2 + 3x + 9$, $gr(f(x)) = 5$; para $p = 7$, $\overline{f(x)} = 4x^3 + 3x + 2$ en $\mathbb{Z}_7[x]$ (por abuso de notación, hemos escrito 4, 3, 2 pensándolos como las correspondientes clases *mód* 7) $\wedge$ $gr(\overline{f(x)}) = 3 < 5 = gr(f(x))$.
La aplicación $\phi : \mathbb{Z}[x] \to \mathbb{Z}_p[x]$ tal que $\phi(f(x)) = \overline{f(x)}$ es un homomorfismo de anillos con identidad que extiende a la proyección canónica al cociente $\varphi : \mathbb{Z} \to \mathbb{Z}_p$, $\varphi(a) = \overline{a} \quad \forall a \in \mathbb{Z}$, y es tal que $\phi(x) = x$.

***Teorema*:** Sean $f(x) \in \mathbb{Z}[x]$, $p \in \mathbb{N}$ primo tal que $\overline{f(x)} \in \mathbb{Z}_p[x]$ es tal que $gr(\overline{f(x)}) = gr(f(x))$. Si $f(x)$ es reducible en $\mathbb{Q}[x]$ entonces $\overline{f(x)}$ es reducible en $\mathbb{Z}_p[x]$.

***Demostración*:** Si $f(x)$ es reducible en $\mathbb{Q}[x]$ $\exists\, h(x), k(x) \in \mathbb{Q}[x]$ tales que
$0 < gr(h(x)) < gr(f(x)) \quad \wedge \quad 0 < gr(k(x)) < gr(f(x)) \quad \wedge \quad f(x) = h(x) \,.\, k(x)$.
Por lo visto anteriormente $\exists\, h_1(x), k_1(x) \in \mathbb{Z}[x]$ tales que $f(x) = h_1(x) \,.\, k_1(x)$ con
$gr(h_1(x)) = gr(h(x)) \quad \wedge \quad gr(k_1(x)) = gr(k(x))$.
Aplicando ϕ a $f(x)$ tenemos que $\overline{f(x)} = \phi(f(x)) = \phi(h_1(x)) \,.\, \phi(k_1(x)) = \overline{h_1(x)} \,.\, \overline{k_1(x)}$,
$gr(h_1(x)) + gr(k_1(x)) = gr(f(x)) = gr(\overline{f(x)}) = gr(\overline{h_1(x)}) + gr(\overline{k_1(x)})$.
Como $gr(\overline{h_1(x)}) \leq gr(h_1(x)) \quad \wedge \quad gr(\overline{k_1(x)}) \leq gr(k_1(x)) \quad \Rightarrow \quad gr(\overline{h_1(x)}) = gr(h_1(x)) > 0$

$\wedge \quad gr(\overline{k_1(x)}) = gr(k_1(x)) > 0 \quad \therefore \quad \overline{f(x)}$ es reducible en $\mathbb{Z}_p[x]$.

***Corolario*:** Sea $f(x) \in \mathbb{Z}[x]$. Supongamos que $\exists\, p \in \mathbb{N}$ primo tal que $\overline{f(x)}$ sea irreducible en $\mathbb{Z}_p[x]$, y $gr(\overline{f(x)}) = gr(f(x))$, entonces $f(x)$ es irreducible en $\mathbb{Q}[x]$.

***Demostración*:** trivial.

Ejemplos:

1) $f(x) = x^4 + 11x^3 + 6x + 7$ es irreducible en $\mathbb{Q}[x]$ porque $\overline{f(x)} = x^4 + x^3 + 1$ es irreducible en $\mathbb{Z}_2[x]$.

2) $g(x) = x^3 + 16x^2 + 9x + 56$ es irreducible en $\mathbb{Q}[x]$ porque $\overline{g(x)} = x^3 + x^2 + 2$ es irreducible en $\mathbb{Z}_3[x]$.

3) $h(x) = x^4 - 13x^3 + 16x^2 - 6x - 17$ es irreducible en $\mathbb{Q}[x]$ porque $\overline{h(x)} = x^4 + 2x^3 + x^2 + 1$ es irreducible en $\mathbb{Z}_3[x]$.

4) Sea $p(x) = x^7 + 3x^6 + 5x^5 + x^4 - 5x^3 + 4x^2 + 6x + 3$, ¿es irreducible en $\mathbb{Q}[x]$?

$p(x)$ no admite raíces en $\mathbb{Q}$. Si $p(x)$ fuera reducible $\exists h(x), q(x) \in \mathbb{Z}[x]$ tales que

$f(x) = h(x).q(x)$ con $1 < \text{gr}(h(x)) < 7 \quad \wedge \quad 1 < \text{gr}(q(x)) < 7$.

Sea $\overline{p(x)} = x^7 + x^6 + x^5 + x^4 + x^3 + 1$ en $\mathbb{Z}_2[x]$ es $\overline{p(x)} = \overline{q(x)}.\overline{h(x)}$ donde

$1 < \text{gr}(\overline{h(x)}) < 7 \quad \wedge \quad 1 < \text{gr}(\overline{q(x)}) < 7$.

Pero, además $\overline{p(x)} = x^7 + x^6 + x^5 + x^4 + x^3 + 1 = (x + 1).(x^6 + x^4 + x^2 + x + 1)$, donde ambos son irreducibles en $\mathbb{Z}_2[x]$, con lo cual $\overline{h(x)} = x + 1 \quad \vee \quad \overline{q(x)} = x + 1$, por lo que

$\text{gr}(h(x)) = 1 \quad \vee \quad \text{gr}(q(x)) = 1$!! (absurdo!) pues $p(x)$ no admite raíces en $\mathbb{Q}$.

Luego $p(x)$ es irreducible en $\mathbb{Q}[x]$.

Resumen:

Puntualizaremos los resultados más destacados a los que hemos llegado y que debemos recordar al momento de factorizar un polinomio en producto de polinomios irreducibles mónicos.
En lo que sigue K es un cuerpo.

- $p(x)$ es irreducible en $K[x] \iff up(x)$ es irreducible $\forall u \in K - \{0\}$; por lo tanto para buscar los polinomios irreducibles basta con buscar los irreducibles mónicos.
- Todo polinomio de grado 1 en $K[x]$ es irreducible y tiene una raíz en K, y sólo los de grado 1 cumplen ambas propiedades simultáneamente.

- $a \in K$ es raíz de $g(x) \Leftrightarrow (x-a) \mid g(x)$; luego si $gr(g(x)) > 1 \wedge a$ es raíz de $g(x)$ entonces $g(x)$ es reducible

- Un polinomio de grado 2 o 3 es irreducible en $K[x] \Leftrightarrow$ no admite raíces en K. Para los polinomios de mayor grado no se verifica la equivalencia pues un polinomio puede ser reducible y no tener raíces en K.

- Un polinomio de segundo grado $q(x) = ax^2 + bx + c \in K[x]$, $a \neq 0$, donde $carK \neq 2$, es irreducible si y sólo si el discriminante $\Delta = b^2 - 4ac$ del polinomio no es un cuadrado en K. Si $\exists \omega \in K$ tal que $\Delta = \omega^2$, entonces $z_1 = \dfrac{-b+\omega}{2a}$, $z_2 = \dfrac{-b-\omega}{2a}$ son las raíces de $q(x)$.

- $p(x) \in K[x]$, $a \in K$ raíz de $p(x)$. Entonces, a es raíz múltiple de $p(x)$ si y sólo si a es raíz de su polinomio derivado.

- Un polinomio de grado n en $K[x]$ puede tener, cuanto más, n raíces en K, contando cada raíz tantas veces cuanta sea su multiplicidad.

Polinomios en $\mathbb{Z}[x]$:

- ***Lema de Gauss*:** Sea $p(x) \in \mathbb{Z}[x]$ de grado positivo, $p(x) = \sum_{i=0}^{n} a_i x^i$, $n \in \mathbb{N}$,

  $a_n \neq 0$. Si $\dfrac{r}{s} \in \mathbb{Q}$, con $r, s \in \mathbb{Z}$, $s \neq 0$, $(r, s) = 1$, es raíz de $p(x)$

  entonces $r \mid a_0 \wedge s \mid a_n$.

  Por lo tanto, las raíces racionales de un polinomio mónico de $\mathbb{Z}[x]$ son enteras.

- Si $f(x) \in \mathbb{Z}[x]$ primitivo, es irrreducible en $\mathbb{Q}[x]$ si y sólo si es irreducible en $\mathbb{Z}[x]$.

- ***Criterio de irreducibilidad de Eisenstein*:** Sea $f(x) \in \mathbb{Z}[x]$, $gr(f) \geq 1$,

$f(x) = \sum_{k=0}^{n} a_k x^k$. Supongamos que $\exists p \in \mathbb{N}$ primo tal que:

i. $p \mid a_k \quad \forall k = 0,1,2,...,n-1$

ii. $p \nmid a_n$

iii. $p^2 \nmid a_0$

Entonces $f(x)$ es irreducible en $\mathbb{Q}[x]$.

- Sea $f(x) \in \mathbb{Z}[x]$. Supongamos que $\exists p \in \mathbb{N}$ primo tal que $gr(\overline{f(x)}) = gr(f(x))$ en $\mathbb{Z}_p[x]$. Si $\overline{f(x)}$ sea irreducible en $\mathbb{Z}_p[x]$, entonces $f(x)$ es irreducible en $\mathbb{Q}[x]$.

Consideraciones adicionales

Sean K , L cuerpos tales que $K \underset{subc.}{\subset} L$; sea $\alpha \in L$ algebraico sobre K , por lo tanto existe un polinomio no nulo $p(x) \in K[x]$ tal que $p(\alpha) = 0$.

Como $\{ s(x) \in K[x] \ / \ s(\alpha) = 0 \} \neq \phi$ se puede tomar un polinomio mónico de grado mínimo en dicho conjunto.

***Teorema*:** Sea K cuerpo, $\alpha \in K$ algebraico, y sea un polinomio no nulo y mónico $p(x) \in K[x]$ tal que $p(\alpha) = 0$.
$p(x)$ es un polinomio mónico de grado mínimo en $K[x]$ que tiene a α como raíz si y sólo si $p(x) \mid q(x)$, $\forall\, q(x) \in K[x]$ tal que $q(\alpha) = 0$

***Demostración*:**
$\Rightarrow$) Sea $p(x)$ es un polinomio mónico de grado mínimo en $K[x]$ que tiene a α como raíz y $q(x) \in K[x]$ tal que $q(\alpha) = 0$.
Por el Algoritmo de la División en $K[x]$:

$$q(x) = h(x) \,.\, p(x) + r(x)$$

para ciertos polinomios $h(x), r(x) \in K[x]$ con $gr(r(x)) < gr(p(x)) \ \vee \ r(x) = 0$.
Especializando en α :

$$0 = q(\alpha) = h(\alpha) \,.\, p(\alpha) + r(\alpha) = h(\alpha).0 + r(\alpha) = r(\alpha).$$

Si $r(x) \neq 0$ entonces $gr(r(x)) < gr(p(x)) \ \wedge \ r(\alpha) = 0$ pero $p(x)$ es de grado mínimo con la propiedad de tener a α como raíz !! (absurdo!) luego $r(x) = 0$ y $p(x) \mid q(x)$.

$\Leftarrow$) Si $p(x) \mid q(x) \ \ \forall\, q(x) \in K[x]$ tal que $q(\alpha) = 0$, entonces $gr(p(x)) \leq gr(q(x))$
$\forall\ q(x) \in K[x]$ tal que $q(\alpha) = 0$, luego $p(x)$ es de grado mínimo en $\{ s(x) \in K[x] \ / \ s(\alpha) = 0 \}$.

***Corolario*:** El polinomio mónico de grado mínimo que tiene a α como raíz, es único.

***Demostración*:** Queda como ejercicio.

***Proposición*:** $p(x)$ es el polinomio mónico de grado mínimo en $K[x]$ que tiene a α como raíz si y sólo si $p(x)$ es irreducible en $K[x]$.

Demostración:
$\Rightarrow$) Supongamos que $p(x)$ sea reducible en $K[x]$, entonces existe un polinomio
$q(x) \in K[x]$ tal que $q(x) \mid p(x)$ y $0 < gr(q(x)) < gr(p(x))$.
Luego $p(x) = q(x) \,.\, t(x)$ para cierto polinomio $t(x) \in K[x]$ con $0 < gr(t(x)) < gr(p(x))$.

$$0 = p(\alpha) = q(\alpha) \,.\, t(\alpha) \quad \Rightarrow \quad t(\alpha) = 0 \ \vee \ q(\alpha) = 0$$

$\therefore$ $p(x)$ no es de grado mínimo en $K[x]$ con la propiedad de tener a α como raíz.

$\Leftarrow$) Sea ahora $p(x)$ irreducible en $K[x]$ con la propiedad de tener a α como raíz, y sea $q(x) \in K[x]$ de grado mínimo tal que $q(\alpha) = 0$, $0 < gr(q(x)) \leq gr(p(x))$.
Por el teorema anterior $q(x) \mid p(x)$, pero como $p(x)$ es irreducible, $p(x) \ \wedge \ q(x)$
son asociados, luego $gr(q(x)) = gr(p(x))$ y $p(x)$ es de grado mínimo con la propiedad de tener a α como raíz.

Ejemplos:

¿Cuáles son los polinomios mónicos de grado mínimo en $\mathbb{Q}[x]$ que tienen, en cada caso, a $\sqrt[3]{13}$, $\sqrt[5]{10}$ y $\sqrt[7]{24}$ como raíz?

1) El polinomio mónico de grado mínimo en $\mathbb{Q}[x]$ que tiene a $\sqrt[3]{13}$ como raíz es $p(x) = x^3 - 13$.

¿Cómo se demuestra que es $p(x)$?: $p(x)$ tiene a $\sqrt[3]{13}$ como raíz , es mónico y es irreducible en $\mathbb{Q}[x]$, dado que es de grado 3 y no tiene raíces en $\mathbb{Q}$ (aplicando el Lema de Gauss) .

2) El polinomio mónico de grado mínimo en $\mathbb{Q}[x]$ que tiene a $\sqrt[5]{10}$ como raíz es $q(x) = x^5 - 10$. También $q(x)$ es irreducible en $\mathbb{Q}[x]$, pero la justificación no la da el hecho de no tener raíces en $\mathbb{Q}$ porque es de grado 5 , pero sí la obtengo con el Criterio de irreducibilidad de Eisenstein aplicándolo para $p = 2 \ \vee \ p = 5$.

3) El polinomio mónico de grado mínimo en $\mathbb{Q}[x]$ que tiene a $\sqrt[7]{24}$ como raíz es $h(x) = x^7 - 24$. Aquí la irreducibilidad de $h(x)$ en $\mathbb{Q}[x]$ la obtenemos por el Criterio de irreducibilidad de Eisenstein aplicado para $p = 3$.

Polinomios irreducibles de grado 4, 5 y 6 EN $\mathbb{Z}_2[x]$

- Los polinomios irreducibles de grado 4 en $\mathbb{Z}_2[x]$ son aquéllos que no tienen raíces en $\mathbb{Z}_2$ (o sea con término independiente 1 y un número impar de términos no nulos) y los que **no** son producto de irreducibles de grado 2, que en el caso de $\mathbb{Z}_2[x]$ es sólo uno.

- Los polinomios irreducibles de grado 5 en $\mathbb{Z}_2[x]$ son aquéllos que no tienen raíces en $\mathbb{Z}_2$ (o sea con término independiente 1 y un número impar de términos no nulos) y los que **no** son producto del irreducible de grado 2 por irreducibles de grado 3.

- Los polinomios irreducibles de grado 6 en $\mathbb{Z}_2[x]$ son aquéllos que no tienen raíces en $\mathbb{Z}_2$ (o sea con término independiente 1 y un número impar de términos no nulos) y los que **no** son producto del irreducible de grado 2 por irreducibles de grado 4, o irreducibles de grado 3 entre sí o el irreducible de grado 2 al cubo.

Polinomios irreducibles en $\mathbb{Z}_2[x]$		
De grado 4	De grado 5	De grado 6
$x^4 + x^3 + x^2 + x + 1$ $x^4 + x^3 + 1$ $x^4 + x + 1$	$x^5 + x^3 + x^2 + x + 1$ $x^5 + x^4 + x^2 + x + 1$ $x^5 + x^4 + x^3 + x + 1$ $x^5 + x^4 + x^3 + x^2 + 1$ $x^5 + x^2 + 1$ $x^5 + x^3 + 1$	$x^6 + x^5 + x^4 + x^3 + 1$ $x^6 + x^5 + x^4 + x + 1$ $x^6 + x^5 + x^2 + x + 1$ $x^6 + x^5 + x^3 + x^2 + 1$ $x^6 + x^5 + x^2 + x + 1$ $x^6 + x^4 + x^2 + x + 1$ $x^6 + x^5 + 1$ $x^6 + x^3 + 1$ $x^6 + x + 1$

Polinomios irreducibles de grado 4 y 5 en $\mathbb{Z}_3[x]$:

Daremos una lista de polinomios **reducibles** de $\mathbb{Z}_3[x]$ que son producto de polinomios irreducibles de menor grado pero que no tienen raíces en $\mathbb{Z}_3$.
Por ejemplo de grado 4 y mónicos hay $3^4 = 81$ polinomios, de grado 5 mónicos son $3^5 = 243$, por lo resulta muy tedioso enumerarlos a todos para descartar los reducibles; **lo que haremos es presentar la lista de los reducibles que son producto de irreducibles de menor grado y mayor o igual que 2, y luego, si un polinomio no tiene raíces en $\mathbb{Z}_3$ (término independiente no nulo tales que ni 1 ni $-1 = 2$ lo anulan en $\mathbb{Z}_3$) y no está en la lista que daremos, es irreducible.**

- Los **reducibles** de grado 4 mónicos son los que tienen a 0, 1 o $2 = -1$ como raíz, y los que son producto de irreducibles de grado 2.

- Los **reducibles** de grado 5 mónicos son los que tienen a 0, 1 o $2 = -1$ como raíz, y los que son producto de irreducibles de grado 2 por irreducibles de grado 3.

Polinomios **reducibles** de y no tienen raíces en $\mathbb{Z}_3$	$\mathbb{Z}_3[x]$ que son producto de irreducibles de menor grado	
De grado 4	De grado 5	De grado 5
x^4+2x^2+1	x^5+2x^3+1	$x^5+x^4+x^3+x^2+x+2$
x^4+1	$x^5+x^4+2x^3+2x^2+x+1$	$x^5+x^4+2x^3+x^2+2x+1$
$x^4+x^3+2x^2+2x+1$	$x^5+x^4+2x^3+x+2$	$x^5+x^4+2x^2+2x+2$
$x^4+2x^3+2x^2+x+1$	x^5+x^2+2	$x^5+2x^4+x^3+2x^2+2$
x^4+2x^3+2x+2	$x^5+2x^4+2x^3+2x^2+2x+2$	$x^5+x^3+x^2+x+1$
x^4+x^3+x+2	$x^5+x^4+2x^2+2x+1$	$x^5+2x^4+x^3+2x+1$
	x^5+2x^2+2x+2	$x^5+x^4+x^3+x^2+1$
	$x^5+x^4+x^3+1$	$x^5+x^4+x^3+2x+2$
	x^5+x^2+2x+1	$x^5+x^3+2x^2+x+2$
	$x^5+2x^4+x^3+1$	x^5+2x^2+1
	$x^5+2x^4+x^2+2x+2$	x^5+2x^3+2

***Ejercicios*:**

1.

1.1. Sean $p(x), q(x) \in \mathbb{Q}[x]$. Entonces $p^2 + q^2 = 0$ sií $p = q = 0$.

1.2. Determinar todos los $p(x) \in \mathbb{Q}$ [x] que satisfacen: $p^2(x) = x \,.\, p(x) + 1$.

2. Si $p_1, p_2, ..., p_k \in \mathbb{R}[x]$ y tienen grados $i_1, i_2, ..., i_k$ respectivamente. ¿Cuál es el grado del polinomio $(p_1 + p_2 + ... + p_k)^n$?

3. Probar que no existe $p(x) \in \mathbb{R}[x]$ de grado ≥ 1 tal que $p^2 = p$. ¿Y de grado 0?

4. Enumerar todos los polinomios de grado ≤ 5 sobre el cuerpo $\mathbb{Z}_2$. ¿Puede dar una fórmula que dé el número total de polinomios de grado $\leq n$? ¿Y de grado n?

5.

5.1. Sean $p(x) = 1 + 2x + 3x^2$, $q(x) = 1 + 2x$, $h(x) = 2 – x + x^2$ en $\mathbb{Z}_4[x]$. Calcular los grados de los polinomios: $p(x)^2$; $p(x).q(x)$; $q(x)^2$; $p(x) – h(x)$.

5.2 ¿Existen en $\mathbb{Z}_4[x]$ polinomios $t(x)$, $s(x)$ ambos no nulos tales que $t(x).s(x) = 0$?

5.3 ¿Existen en $\mathbb{Z}_4[x]$ polinomios $t(x)$ tales que $t(x)^n = 0$ para algún $n \in \mathbb{N}$?

5.4 ¿Existen en $\mathbb{Z}_4[x]$ polinomios inversibles de grado > 0?

6. Hallar en $\mathbb{Z}_2[x]$ el cociente y el resto de dividir:

6.1. $x^2 + x + 1$ por x^2 .

6.2. $x^3 + x^2 + 1$ por $x + 1$.

7. Sean $a(x), b(x), c(x) \in A[x]$, $a(x) \neq 0 \;\wedge\; b(x) \neq 0$, demostrar:

7.1. $a(x) \mid b(x) \;\wedge\; b(x) \mid c(x) \Rightarrow a(x) \mid c(x)$.

7.2. $a(x) \mid b(x) \;\wedge\; a(x) \mid c(x) \Rightarrow a(x) \mid (b(x) + c(x))$ ¿Vale la recíproca?

7.3. $a(x) \mid (b(x) + c(x)) \;\wedge\; a(x) \mid b(x) \Rightarrow a(x) \mid c(x)$.

7.4. $a(x) \mid b(x) \Rightarrow a(x) \mid b(x) \,.\, c(x) \quad \forall\, c(x) \in A[x]$.
¿es verdadero que $a(x) \mid b(x) \,.\, c(x) \Rightarrow a(x) \mid b(x) \;\vee\; a(x) \mid c(x)$?

7.5. $a(x) \mid 0$, $\forall\, a(x) \in A[x]$, $a(x) \neq 0$.

8.

8.1. Sean $a(x), b(x) \in A[x]$, $a(x) \neq 0 \wedge b(x) \neq 0$ tales que $a(x) \mid b(x) \;\wedge\; b(x) \mid a(x)$, A dominio de integridad. Demostrar que $\exists u \in A^*$ tal que $b(x) = u.a(x)$.

8.2. La relación en $A[x] - \{ 0 \}$: “ $a(x) \sim b(x) \Leftrightarrow a(x)$ y $b(x)$ son asociados ”, es de equivalencia.

8.3. Si $a(x)$ y $b(x)$ son asociados, $a(x) \mid c(x) \Leftrightarrow b(x) \mid c(x)$.

8.4. Si $a(x)$ y $b(x)$ son asociados, $c(x) \mid a(x) \Leftrightarrow c(x) \mid b(x)$.

8.5. Sea K cuerpo. Si $a(x) \neq 0$, $\exists v \in K - \{ 0 \}$ tal que $v.a(x)$ es mónico y asociado a $a(x)$.

8.6. Sea K cuerpo. Si $a(x), b(x) \in K[x]$ son asociados y mónicos entonces $a(x) = b(x)$.

9. Demostrar, utilizando la definición, que el polinomio $p(x) = x^2 + 1$ es irreducible en $\mathbb{R}[x]$.

10. Sean $a(x), b(x) \in K[x]$, no simultáneamente nulos, $d(x) \in K[x]$ mónico tal que $d(x) \mid a(x) \;\wedge\; d(x) \mid b(x)$. Demostrar:

10.1. $d(x) = (a(x) , b(x)) \Rightarrow d(x).c(x) = (a(x).c(x) , b(x).c(x)) \quad \forall\, c(x) \in K[x]$ mónico.

10.2. Si $a(x) = k(x).d(x) \ \wedge \ b(x) = h(x).d(x)$, entonces
$d(x) = (a(x) , b(x)) \ \Leftrightarrow \ (k(x) , h(x)) = 1.$

10.3. Para $a(x) \neq 0$, $(a(x) , b(x)) = u.a(x)$ para algún $u \in K - \{ 0 \} \ \Leftrightarrow \ a(x) \mid b(x).$

10.4. $b(x) = q(x).a(x) + r(x) \ \Rightarrow \ (a(x) , b(x)) = (a(x) , r(x))$.
En particular $(a(x) - b(x) , a(x)) = (a(x) , b(x)) = (a(x) + b(x) , a(x)).$

10.5. Para $c(x) \neq 0$, $c(x) \mid a(x).b(x) \ \wedge \ (a(x) , c(x)) = 1 \Rightarrow \ c(x) \mid b(x).$

10.6. Para $a(x) \neq 0$, $b(x) \neq 0$, $a(x) \mid c(x) \ \wedge \ b(x) \mid c(x) \ \wedge \ (a(x) , b(x)) = 1$
$\Rightarrow \ a(x).b(x) \mid c(x).$

10.7. Generalización: si $a_i(x) \neq 0$, $a_i(x) \mid c(x) \quad \forall i$, $i = 1,2,..n, \ \wedge$

$$(a_i(x) , a_j(x)) = 1, \text{ para } i \neq j, \quad \text{entonces } \prod_{i=1}^{n} a_i(x) \mid c(x).$$

10.8. Sean $p(x), q(x) \in K[x]$ irreducibles mónicos,
$(p(x) , q(x)) = 1 \ \Leftrightarrow \ p(x) \neq q(x)$.

11. Sea $p(x) \in K[x]$, $gr(p(x)) > 0$. Demostrar que:

11.1. $p(x)$ es irreducible $\Leftrightarrow \ \forall\, a(x) \in K[x]$ se verifica una y sólo una de estas propiedades: $p(x) \mid a(x) \ \vee \ (p(x) , a(x)) = 1.$

11.2. $p(x)$ es irreducible $\Leftrightarrow$ cada vez que $p(x) \mid a(x).b(x)$, para ciertos $a(x), b(x) \in K[x]$, se verifica que $p(x) \mid a(x) \ \vee \ p(x) \mid b(x).$

11.3. Si $p(x)$ es irreducible y es tal que $p(x) \mid \prod_{i=1}^{n} a_i(x)$, con los $a_i(x) \in K[x]$,

entonces $\exists\, j$, $1 \leq j \leq n$, tal que $p(x) \mid a_j(x)$.

11.4. $p(x)$ es irreducible $\Leftrightarrow \ (p(x) , k(x)) = 1 \quad \forall\, k(x) \in K[x]$
tal que $gr(k(x)) < gr(p(x))$.

12. Sean $a(x), b(x) \in K[x] - \{ 0 \}$, $m(x) \in K[x]$ mónico, tales que $a(x) \mid m(x) \ \wedge \ b(x) \mid m(x)$. Demostrar que son equivalentes:

i. $m(x) = [a(x) , b(x)]$.

ii. si $c(x) \in K[x]$ es tal que $a(x) \mid c(x) \ \wedge \ b(x) \mid c(x) \ \Rightarrow \ m(x) \mid c(x)$.

13. Sean $a(x), b(x) \in K[x] - \{ 0 \}$. Demostrar que el MCM de $a(x)$ y $b(x)$ es único.

14. Sean $a(x), b(x) \in K[x] - \{ 0 \}$. Demostrar que:

14.1. $[a(x) , b(x)] = [u.a(x) , v.b(x)], \quad \forall u, v \in K - \{0\}.$

14.2. $[a(x) , b(x)] = u.b(x)$, para algún $u \in K - \{ 0 \} \ \Leftrightarrow \ a(x) \mid b(x).$

14.3. Sea $m(x) \in K[x]$ mónico, tal que $a(x) \mid m(x) \ \wedge \ b(x) \mid m(x)$. Entonces:

$$m(x) = [a(x) , b(x)] \ \Leftrightarrow \ \left(\frac{m(x)}{a(x)} , \frac{m(x)}{b(x)} \right) = 1.$$

14.4. $[a(x) , b(x)] = u.a(x).b(x) \ \Leftrightarrow \ (a(x) , b(x)) = 1.$

15. Sea la aplicación $\mathfrak{V} : \mathbb{Z}[x] \to \mathbb{Z}$, la especialización de x por -1 según $\mathcal{G} = id_{\mathbb{Z}} : \mathbb{Z} \to \mathbb{Z}$.

15.1. Determinar la especialización de x por -1 en los polinomios:
$2x^2 - 1$; $(x + 1)^2$; $x^3 - x^2 + x - 1$; $x^2 - 3x + 2$.

15.2. ¿Qué polinomios $p(x)$ satisfacen que $p(-1) = 1$?
15.3. Sea, además, la especialización de x por 1. Encontrar todos los polinomios mónicos $p(x)$ tales que $p(1) = p(-1)$.

16. Probar que ninguna especialización $\mathbb{Z}[x] \to \mathbb{Z}$ puede ser inyectiva. ¿Es siempre sobreyectiva?

i) $a+b+c$ ii) $a^2+b^2+c^2$ iii) $ab+bc+ca$

17. Calcular el m.c.d de $p(x)$ y $q(x) \in \mathbb{R}[x]$:
17.1. $p(x) = 3x^2 + 2x + 1$ $q(x) = x^4 - x + 2$
17.2. $p(x) = x^3 - 1$ $q(x) = x^2 + 2x - 2$
17.3. $p(x) = x^3 - 1$ $q(x) = x^4 + 1$
17.4. En todos los casos precedentes expresar $(p(x), q(x)) = p(x).s(x) + q(x).t(x)$, $s(x), t(x) \in \mathbb{R}[x]$.

18.
18.1. ¿Para qué valores de $a \in \mathbb{Q}$ es $x^3 + ax^2 + 2x - 2a$ divisible por $x^2 + 2$?
18.2. ¿Para qué valores de $a, b \in \mathbb{Q}$ es $x^3 + ax^2 + 3x + b$ divisible por $x + 5$?
18.3 Determinar $a \in \mathbb{Q}$ para que -1 sea raíz doble del polinomio $x^5 - ax^4 - ax + 1$

19.
19.1. Sean $a, b, c, d \in K$ (cuerpo) $a \neq 0$, $c \neq 0$. Demostrar que los polinomio $ax + b$ y $cx + d$ son coprimos sii $bc - ad \neq 0$.
19.2. Deducir que $x - a$ y $x - b$ son coprimos sii $a \neq b$.
19.3. Demostrar que $(x-a)^n$ y $(x-b)^m$ son coprimos $\forall\, n, m \in \mathbb{N}$ sii $a \neq b$.

20.
20.1. Hallar el polinomio $p(x) \in \mathbb{Q}[x]$ mónico de grado mínimo que tenga a $\frac{1}{2}$, $\sqrt{2}$ y $1-\sqrt{5}$ por raíces.
20.2. Hallar el polinomio $p(x) \in \mathbb{Q}[x]$, $p(x) \neq 0$, mónico de grado mínimo tal que $\sqrt{2}$ y $\sqrt{5}$ sean raíces de $p(x)$.
20.3. Ídem 20.2 para $\sqrt{2} + \sqrt{5}$.

21.
21.1. Sea $p(x) \in \mathbb{Q}[x]$ de grado 3. Probar que $p(x)$ es reducible en $\mathbb{Q}[x]$ sii posee una raíz en $\mathbb{Q}$.
21.2. Demostrar lo análogo al anterior para un polinomio $p(x) \in \mathbb{R}[x]$ que tenga una raíz en $\mathbb{R}$.
21.3. Encontrar ejemplos de polinomios de grado 3 en $\mathbb{Q}[x]$ irreducibles.
21.4 Sea $p(x) \in \mathbb{Q}[x]$ un polinomio irreducible. Sea $a \in \mathbb{R}$ una raíz de $p(x)$; demostrar que a es raíz simple de $p(x)$. Concluir que todo polinomio irreducible en $\mathbb{Q}[x]$ admite sólo raíces simples.

22. Si las raíces de $2x^3 + 3x^2 + 4x + 2 \in \mathbb{R}[x]$ son a, b, c, calcular:

i) $a+b+c$ ii) $a^2+b^2+c^2$ iii) $ab+bc+ca$

iv) $a^{-1}+b^{-1}+c^{-1}$ v) $\dfrac{1}{a+b}+\dfrac{1}{a+c}+\dfrac{1}{b+c}$

23.

23.1. ¿Es cierto que para todo cuerpo K, y todo polinomio $p(x)\neq 0$ en $K[x]$ existe una raíz en K?

23.2 ¿Posee el cuerpo $\mathbb{Z}_p$ con $p\in\mathbb{N}$ primo, esa propiedad?

23.3. ¿Y el cuerpo real?

24. ¿Es irreducible en $\mathbb{Z}[x]$ el polinomio $4x^3+6x^2+4x+1$? Justificar.

25. Escribir el polinomio $p(x)=x^4+2x^3-3x^2-4x+1$ como expresión polinomial en $x-1$.

26. Sean a, b, c, d las raíces del polinomio $p(x)=2x^4-6x^3+5x^2-7x+1$.

Calcular: $a^2+b^2+c^2+d^2$ y $\dfrac{1}{a}+\dfrac{1}{b}+\dfrac{1}{c}+\dfrac{1}{d}$.

27. Probar que el polinomio $q(x)=\sum_{i=0}^{n}\dfrac{x^i}{i!}$ no posee raíces múltiples.

28. Expresar los siguientes polinomios como producto de irreducibles en $\mathbb{R}[x]$ y en $\mathbb{Q}[x]$:

$p_1(x)=x^2-2$ $p_2(x)=x^2-2x-3$ $p_3(x)=3x^2+1$ $p_4(x)=x^4-4$

$p_5(x)=x^3-6x^2+11x-6$ $p_6(x)=\dfrac{1}{3}x^5+\dfrac{1}{3}x^4-2x^3-\dfrac{14}{3}x^2-\dfrac{11}{3}x-1$

29. Probar que $\forall k\in\mathbb{R}$, el polinomio de $\mathbb{R}[x]$, $p(x)=x^2+(2k+2)x-k^2$ tiene raíces simples.

30. Determinar $a, b\in\mathbb{R}$ tales que $p(x)=x^3+ax^2+bx-2$ tenga a 1 como raíz doble.

31. Analizar la siguiente afirmación:
"Si $p(x)\in\mathbb{Q}[x]$ no posee ninguna raíz en $\mathbb{Q}$, es irreducible en $\mathbb{Q}[x]$".

32. Una raíz del polinomio x^4-10x^2+1 es $\sqrt{2}+\sqrt{3}$; determinar las restantes.
¿Es irreducibles este polinomio en $\mathbb{Q}[x]$?

33. Encontrar todos los polinomios irreducibles de grado 2 y 3 en $\mathbb{Z}_2[x]$, $\mathbb{Z}_3[x]$.

34. Mostrar que los siguientes polinomios son irreducibles en $\mathbb{Q}[x]$ utilizando, en cada caso, el criterio que considere más adecuado:

a) $5x^4+7x^3-x^2+x-1$

b) $x^4+11x+3$

c) x^4+5x^3+7

d) x^3+8x^2+7

e) x^3-6x^2+9x+3

f) x^4+1

g) x^4-2x^3+6

h) x^n-p (p primo)

i) x^4-3

j) $x^n-p.q$ (p, q primos distintos)

k) $2x^5+18x^3+30x^2-24$

l) x^6+12x^2-6x+3

m) $x^4+4x^3+6x^2+6x+5$

n) $x^6+x^5+x^4+x^3+x^2+x+1$

o) $3(x^2+x+1)^2-2(x-1)(x^3-x-1)$

p) x^4+x^3-2x+1

35. Dado $q(x)=x^4-3x^3-x^2+2p^2x-p^2$ determinar el o los primos positivos p para los cuales el polinomio $q(x)$ admita al menos una raíz racional positiva.

36. Factorizar el polinomio $p(x)=x^6+x^5-2x^4+3x^2-4x-6$ en producto de polinomios irreducibles sobre $\mathbb{Q}[x]$ sabiendo que $-\sqrt{2}$ es raíz.

37. Factorizar en irreducibles, si es posible, los siguientes polinomios y justificar todas las respuestas:

37.1. $p(x)=x^3-25x^2+10x-5$ en $\mathbb{Q}[x]$

37.2. $q(x)=x^5-14x^3+91x-119$ en $\mathbb{Q}[x]$

37.3. $t(x)=x^3+\sqrt{3}x^2-3x-3\sqrt{3}$ en $\mathbb{R}[x]$, sabiendo que $x_1+x_2=-2\sqrt{3}$ y $x_1=-x_3$, siendo x_1, x_2 y x_3 las raíces de $t(x)$.

38. Demostrar que si $f(x)\in\mathbb{Z}[x]$ no nulo, $d\in\mathbb{N}$, entonces $cont(d.f)=d.cont(f)$.

39. Sean $K \underset{subc.}{\subset} L$; sea $\alpha\in L$ algebraico sobre K. Demostrar que $p(x)$ es el polinomio mónico de grado mínimo en $K[x]$ que tiene a α como raíz si y sólo si $p(x) \mid q(x)$, $\forall\, q(x)\in K[x]$ tal que $q(\alpha)=0$.

40. Sean $K \underset{subc.}{\subset} L$; $car(K)=car(L)=0$; sea $\alpha\in L$ algebraico sobre K y $p(x)$ polinomio irreducible en $K[x]$ que tiene a α como raíz. Demostrar que α es raíz simple.

CAPÍTULO IX

NÚMEROS COMPLEJOS

"Los números imaginarios son un excelente y maravilloso refugio del Espíritu Santo, una especie de anfibio entre ser y no ser". Gottfried von Leibnitz (1646 – 1716).
"Estos números no son nada, ni menos que nada, lo cual necesariamente los hace imaginarios, o imposibles". Leonhard Euler (1707 – 1783):
"A los números enteros se han agregado las fracciones; a las cantidades racionales, las irracionales; a las positivas, las negativas; y a las reales, las imaginarias." Johann Carl Friedrich Gauss (1777 – 1857).

Girolamo Cardano(1501-1576)

Cardano había jugado con las raíces cuadradas de números negativos al intentar resolver el problema de dividir 10 en dos partes tales que su producto valga 40. Las reglas usuales del álgebra conducen a la solución $5+\sqrt{-15}$ *y* $5-\sqrt{-15}$ *ó, en la notación de Cardano,* 5p:Rm:15 *y* 5m:Rm:15. *Refiriéndose a estas raíces cuadradas de números negativos, las denominó Cardano como "sofísticas", concluyendo que en este caso su resultado era "tan sutil como inútil". A los matemáticos posteriores les correspondería la tarea de demostrar que tales manipulaciones eran de veras sutiles, pero que estaban muy lejos de ser inútiles. Hay que apuntar entre los méritos de Cardano el que al menos prestase cierta atención a esta situación desconcertante.*
("Historia de la Matemática", Carl B. Boyer)

Hemos estudiado los anillos de polinomios con coeficientes en un cuerpo, sus raíces, condiciones de irreducibilidad en casos específicos, pero hay muchas preguntas sin respuestas. Por ejemplo, tenemos varios criterios y propiedades que nos permiten determinar la irreducibilidad de ciertos polinomios con coeficientes en $\mathbb{Q}$, acotar la cantidad de las eventuales raíces; también sabemos que hay polinomios irreducibles en $\mathbb{Q}[x]$ de cualquier grado, pero no hemos obtenido grandes resultados para polinomios en $\mathbb{R}[x]$; quizás debamos plantearnos definir un cuerpo que extienda a $\mathbb{R}$ en el cual ciertos polinomios irreducibles en $\mathbb{R}[x]$ tengan raíces en él.

La ecuación $x^2+1=0$ no admite solución en $\mathbb{R}$ porque si $a\in\mathbb{R}$, $a^2\geq 0$, luego $a^2+1>0$.
Queremos definir un cuerpo que extienda a $\mathbb{R}$ en el cual la ecuación dada sí admita solución.

> *La solución de las ecuaciones cúbica y cuártica fue probablemente la mayor contribución al álgebra desde que los babilonios, casi cuatro milenios antes, habían aprendido a completar el cuadrado para resolver las ecuaciones cuadráticas. Los matemáticos se encontraron, sin sospecharlo, y durante más de dos siglos y medio con un problema algebraico insoluble comparable a los tres problemas geométricos clásicos de la antigüedad. El resultado de todo este trabajo iba a producir mucha y muy buena matemática, pero llevaría inevitablemente a una conclusión negativa. Una consecuencia inmediata de la solución de la cúbica fue que condujo a las primeras consideraciones significativas acerca de un nuevo tipo de número.*
> *Los algebristas habían podido hasta el momento evitar los números imaginarios diciendo sencillamente que las ecuaciones del tipo* $x^2+1=0$ *son insolubles.*

Sea A un dominio de integridad. Queremos definir en $A\times A$ dos operaciones que lo estructuren como un anillo conmutativo con identidad, y bajo ciertas condiciones, dominio de integridad, incluso un cuerpo.

Definimos: $(a\,,\,b)+(c\,,\,d)=:(a+c\,,\,b+d)$
y $(a\,,\,b)\,.\,(c\,,\,d)=:(a.c-b.d\,,\,a.d+b.c)$

Con estas operaciones $(A\times A\,,+\,,\cdot\,)$ es un anillo conmutativo con identidad (demostrarlo!) en el cual el elemento neutro de la suma es $(0\,,\,0)$, el del producto es $(1\,,\,0)$, el opuesto de $(a\,,\,b)$ es $(-a\,,-b)$ (o sea $-(a\,,\,b)=(-a\,,-b)$).

Siendo K un cuerpo, ¿es $K\times K$, con las operaciones definidas más arriba, un cuerpo?

Para serlo, todo elemento no nulo debiera ser inversible; analicemos qué condiciones necesarias y suficientes debe cumplir un $(a\ ,\ b) \neq (0\ ,\ 0)$ para tener inverso.

▪ Si $(a\ ,\ b) \in K \times K$ es inversible, $\exists (c\ ,\ d) \in K \times K$ tal que $(a\ ,\ b).\ (c\ ,\ d) = (1\ ,\ 0)$

o sea $\begin{cases} ac - bd = 1 \\ ad + bc = 0 \end{cases}$

* Si $a \neq 0 \Rightarrow d = -bca^{-1}$

reemplazando d en la primer ecuación obtenemos:

$$ac + b^2ca^{-1} = 1$$

multiplicando m.a.m. por a: $a^2c + b^2c = a$

luego $(a^2 + b^2).c = a$

con lo cual $a^2 + b^2 \neq 0$.

* Si $a = 0 \Rightarrow bc = 0$, y como $b \neq 0$, pues $(a\ ,\ b) = (0\ ,\ b) \neq (0\ ,\ 0)$, entonces $c = 0$

$\therefore$ $bd = -1$, con lo cual $d = -b^{-1}$, o sea que $(0\ ,\ b)^{-1} = (0\ ,\ -b^{-1})$, y por tanto, también se verifica que $a^2 + b^2 \neq 0$.

Luego, hemos establecido que una condición necesaria para que $(a\ ,\ b)$ tenga inverso es que $a^2 + b^2 \neq 0$ .Veamos que la condición es también suficiente.

▪ Si $(a\ ,\ b) \in K \times K$ es tal que $a^2 + b^2 \neq 0$, entonces $a \neq 0 \ \vee \ b \neq 0$, y además $a^2 + b^2$ admite inverso en K.

Definimos $(c\ ,\ d) = \left(\frac{a}{a^2+b^2}\ ,\ \frac{-b}{a^2+b^2}\right)$; queremos ver que $(c\ ,\ d)$ es el inverso de $(a\ ,\ b)$. Para ello debemos probar que su producto es $(1\ ,\ 0)$ (neutro para el producto en el anillo $K \times K$) .

$$(a\ ,\ b)\ .\ (c\ ,\ d) = \left(a.\frac{a}{a^2+b^2} - b.\frac{-b}{a^2+b^2}\ ,\ a.\frac{-b}{a^2+b^2} + b.\frac{a}{a^2+b^2}\right) =$$

$$= \left(\frac{a^2+b^2}{a^2+b^2}\ ,\ 0\right) = (1\ ,\ 0).$$

Por lo tanto $(a\ ,\ b)$ es inversible y $(a\ ,\ b)^{-1} = \left(\frac{a}{a^2+b^2}\ ,\ \frac{-b}{a^2+b^2}\right)$.

Luego, hemos demostrado que cuando K es cuerpo, $(a\ ,\ b) \in K \times K$ es inversible si y sólo si $a^2 + b^2 \neq 0$, y por tanto $K \times K$ es cuerpo si en K se verifica que:

$$a^2 + b^2 = 0 \iff a = b = 0 \ .$$

Definamos una inmersión de A en $A \times A$:

La función $j : A \to A \times A$, $j(a) = (a\ ,\ 0)$ es monomorfismo de anillos con identidad, pues

$$j(a + b) = (a + b\ ,\ 0) = (a\ ,\ 0) + (b\ ,\ 0) = j(a) + j(b)\ ,$$

$$j(a.b) = (a.b\ ,\ 0) = (a\ ,\ 0)\ .\ (b\ ,\ 0) = j(a)\ .\ j(b)$$

y $$j(1) = (1\ ,\ 0)$$

Además $Ker(j) = \{0\}$ como puede apreciarse a simple vista, con lo cual j es inyectiva y por consiguiente, monomorfismo de anillos con identidad, y es por tanto, una inmersión buscada.

Nota: También podríamos definir otra función natural $\hbar : A \to A\times A$, $\hbar(a) = (0\ ,\ a)$, que es inyectiva y verifica que $\hbar(a + b) = \hbar(a) + \hbar(b)$ pero no cumple que $\hbar(a.b) = \hbar(a)\ .\ \hbar(b)$ por lo que **no es** un monomorfismo de anillos.

Podemos *identificar* A con su imagen por $\jmath$, $A \approx \jmath(A) = A\times 0 = \{(a,0) / a\in A\}$,

y cada $a\in A$ con su imagen por $\jmath$, $a \approx \jmath(a) = (a\ ,\ 0)$.

Si llamamos $i = (0\ ,\ 1)$, tenemos que $i^2 = (0\ ,\ 1).(0\ ,\ 1) = (-1\ ,\ 0) \approx -1$

$$(0\ ,\ b) = (0\ ,\ 1)\ .\ (b\ ,\ 0) \approx b.i$$

luego $$(a\ ,\ b) = (a\ ,\ 0) + (0\ ,\ b) \approx a + b.i$$

Por lo tanto, merced a la identificación dada, escribiremos:

$$A\times A = A(i) = \{a + bi\ /\ a, b\in A \quad \wedge \quad i^2 = -1\}$$

La representación de $(a\ ,\ b)$ como $a + bi$ se denomina *forma binómica.*

Con esta inmersión consideramos a $A \underset{suba}{\subset} A(i)$ donde $a = a + 0.i$.

Las operaciones en $A(i)$ se expresan:

$$(a + b\ i) + (c + d\ i) = (a + c) + (b + d)\ i$$
$$(a + b\ i)\ .\ (c + d\ i) = (ac - bd) + (ad + bc)\ i \quad .$$

Con Euler los imaginarios se incorporan definitivamente en la Matemática. Fue el primero en simbolizar la raíz cuadrada de -1 *con la letra i, es decir* $i^2 = -1$:
"… formulam littera i …" (1777)
introduciendo de este modo la notación binómica para un número complejo.
Demostró que el conjunto de los números "imaginarios" era cerrado para las cuatro operaciones básicas, así como para la potenciación y la radicación.

Leonhard Euler (1707-1783)
Pintado por E. Handmann en 1753

Ejemplos:
1) Por lo visto anteriormente tenemos que $\mathbb{Q}(i)$ y $\mathbb{R}(i)$ son cuerpos porque en $\mathbb{Q}$ y $\mathbb{R}$ se verifica la propiedad: $a^2 + b^2 = 0 \iff a = b = 0$.
2) $\mathbb{Z}_3(i)$, $\mathbb{Z}_7(i)$, $\mathbb{Z}_{11}(i)$ son cuerpos (demostrarlo!).
3) $\mathbb{Z}_2(i)$ **no** es cuerpo pues $1 + 1 = 0$.
$\mathbb{Z}_5(i)$ **no** es cuerpo pues $2^2 + 1 = 0$.
$\mathbb{Z}_{13}(i)$ **no** es cuerpo pues $3^2 + 2^2 = 0$.

Comentario: Un teorema, que demostraremos en el Anexo I, dice que :
$\mathbb{Z}_p(i)$, con p primo, es cuerpo $\iff$ $p \equiv 3$ (*mód* 4).

Definición: Llamaremos *cuerpo de números complejos* al cuerpo $\mathbb{C} = \mathbb{R}(i)$, y *números complejos* a sus elementos $z = a + bi$, $a, b \in \mathbb{R}$;

a se denomina *parte real de* z, y b es la *parte imaginaria de* z:

$a = Re(z)$, $b = Im(z)$, ambos son números reales.

Nota: El cuerpo $\mathbb{C}$ extiende al cuerpo $\mathbb{R}$ de números reales pero no es un cuerpo ordenado, porque si lo fuera, debería verificarse una y sólo una de estas tres propiedades:

$$i = 0 \ , \quad i < 0 \ \vee \ i > 0 \ .$$

$i \neq 0$ por definición de $i \ \Rightarrow \ i < 0 \ \vee \ i > 0$.

- Si $i < 0 \ \Rightarrow \ -i > 0$

  por consistencia del orden respecto del producto por números positivos,

  $1 = (-i).\, i < (-i).0 = 0$!! (absurdo!).

- Si $i > 0$, por consistencia del orden respecto del producto por números positivos,

  $-1 = i.\, i > i.0 = 0$!! (absurdo!).

$\therefore$ no se verifica ninguna de las tres posibilidades, luego $\mathbb{C}$ no es cuerpo ordenado.

Conjugación

***Definición*:** Sea $z = a + bi$ un número complejo, llamamos *conjugado de* z, y lo notamos $\overline{z}$, al complejo $\overline{z} = a - bi$;

$$Re(\overline{z}) = Re(z) \quad \wedge \quad Im(\overline{z}) = -Im(z)$$

***Propiedades de la conjugación*:** Para z , $z' \in \mathbb{C}$.

i. $\overline{z + z'} = \overline{z} + \overline{z'}$
ii. $\overline{z.z'} = \overline{z} \,.\, \overline{z'}$
iii. $\overline{z} = 0 \ \Leftrightarrow \ z = 0$
iv. $\overline{z} = z \ \Leftrightarrow \ z \in \mathbb{R}$
v. $z + \overline{z} = 2\, Re(z)$
vi. $z - \overline{z} = 2i\, Im(z)$
vii. Si $z \neq 0$, $\overline{z}^{-1} = \overline{z^{-1}}$
viii. $\overline{\overline{z}} = z$

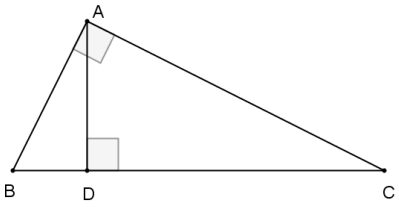
***Demostración*:** Queda como ejercicio.

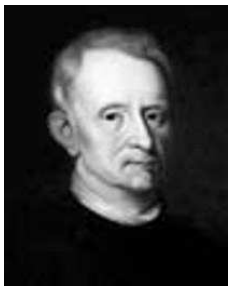
Nota: La definición de conjugación se puede extender a cualquier anillo $A(i)$, y se siguen verificando las propiedades i.-ii.-iii-viii , y en $K(i)$, K cuerpo, la vii.

Representación gráfica de un número complejo

Un poco de historia: La geometría Analítica y la representación de los números imaginarios.

En el triángulo rectángulo ABC, la perpendicular AD divide a BC en dos partes BD y DC. Así, quedan determinados dos triángulos rectángulos semejantes: ADB y ADC, por lo tanto se tiene que $\frac{AD}{BD}=\frac{DC}{AD}$ *, de donde la longitud de la perpendicular AD es* $AD=\sqrt{BD.DC}$ *, AD es denominada la media geométrica entre BD y DC.*





Jean Argand, (1768, 1822)

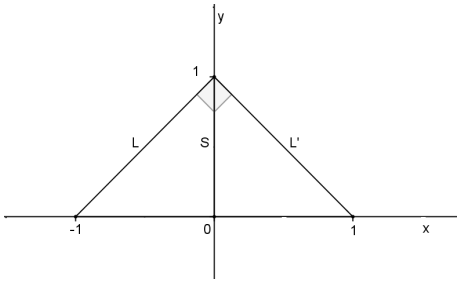
El agrimensor noruego Caspar Wessel (1745-1818) y el tenedor de libros francés Jean Argand (1768-1822), descubrieron independientemente, que los números imaginarios podían representarse aplicando este teorema.

Caspar Wessel (1745-1818)

En la figura de la derecha, la distancia S, desde el origen O *hasta* +1*, es la media geométrica del triángulo de lados L y L´, y la base formada por aquella parte del eje X que va de* -1 *a* +1.

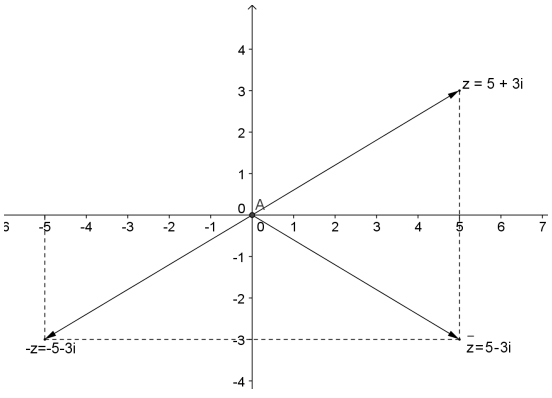
Luego $S=\sqrt{(-1).1}=\sqrt{-1}=i$.

Tenemos así la representación geométrica de un número imaginario, ya que $S=i$.



Desde la época de Girard era bien conocido el hecho de que los números reales, positivos, cero y negativos se pueden representar en correspondencia con los puntos de una recta. Incluso, el matemático inglés John Wallis (1616-1703), había llegado a sugerir que los números imaginarios puros se podrían representar por los puntos de una recta perpendicular al eje de los números reales. Gauss completó la idea al considerar las partes real e imaginaria de un número complejo a+bi como las dos coordenadas rectangulares del punto (a,b) en el plano, al cual estaría asociado un número complejo y viceversa.

Hoy suele denominarse "plano de Gauss" al plano de los números complejos.



"La visualización de los números reales mediante los puntos de una recta o de los números complejos mediante los puntos del plano no solamente penetró sin gran resistencia en el análisis, sino que se puede decir con razón que, en el caso de los números complejos, esta visualización (Argand, Gauss) fue lo que hizo posible vencer la fuerte oposición de la comunidad matemática al dar carta de ciudadanía a los números complejos".

("El rincón de la pizarra: ensayos de visualización en análisis matemático". Miguel de Guzmán)

Miguel de Guzmán (1936-2004)

***Definición*:** Sea A dominio de integridad, $z \in A(i)$, llamamos *norma de z* al elemento de A: $N(z) = z \,.\, \overline{z}$.

Cuando $z = a + bi$, tenemos que $N(z) = a^2 + b^2 \in A$.

***Proposición*:** Para z , $z' \in A(i)$, $N(z.z') = N(z) \cdot N(z')$.

***Demostración*:** Queda como ejercicio.

***Teorema*:** Sea A dominio de integridad, $z \in A(i)$, z es inversible en $A(i)$ si y sólo si $N(z)$ es inversible en A.

***Demostración*:**

$\Rightarrow$**)** Sea z inversible en $A(i)$, entonces existe $z' \in A(i)$ tal que $z \,.\, z' = 1$,

$$\therefore \quad N(z.z') = 1 \ ;$$

por la proposición anterior tenemos que $N(z.z') = N(z) \cdot N(z') = 1$,

con lo cual $N(z)$ es inversible en $A \quad \wedge \quad (N(z))^{-1} = N(z^{-1})$.

$\Leftarrow$) Sea $N(z)$ inversible en $A \quad \therefore \quad \exists k \in A$ tal que $k.\, N(z) = 1$.

Sea $z' \in A(i)$ definido por $z' = k.\, \overline{z}$

$$z \,.\, z' = k.\, z.\, \overline{z} = k.\, N(z) = 1 \ ,$$

$\therefore$ z es inversible y $z^{-1} = \dfrac{\overline{z}}{N(z)}$.

***Corolario*:** Cuando K es cuerpo, $z \in K(i)$ es inversible si y sólo si $N(z) \neq 0$.

Demostración: Es un caso particular del teorema.

***Propiedades de la norma*:** Para $z \in \mathbb{C}$

i. $N(z) \geq 0$, y $N(z) = 0 \iff z = 0$
ii. $N(a) = a^2 \quad \forall a \in \mathbb{R}$
iii. $N(z) \geq (Re(z))^2 \quad \wedge \quad N(z) \geq (Im(z))^2$
iv. $N(z) = N(\overline{z})$

Demostración: Queda como ejercicio.

Módulo de un complejo

***Definición*:** Sea $z \in \mathbb{C}$, llamamos *módulo de z* al número real $|z| = \sqrt{N(z)} = \sqrt{z.\overline{z}}$

Nota: En virtud de la definición, tenemos la identidad $|z|^2 = z \,.\, \overline{z}$.

Comentario: La función *módulo* en $\mathbb{C}$ extiende a la función *valor absoluto* de $\mathbb{R}$ dado que si $a \in \mathbb{R}$, el módulo de a (como número complejo) es : $|a| = \sqrt{a^2} = |a|$ (aquí pensado como valor absoluto), razón por la cual no lleva a ninguna confusión que utilicemos la misma notación para ambas funciones.

***Propiedades del módulo* :** Para z , $z' \in \mathbb{C}$

i. $|z| \geq 0$, $|z| = 0 \iff z = 0$.

ii. $|z.z'| = |z| \,.\, |z'|$

iii. $|\overline{z}| = |z|$

iv. $|z| \geq |Re(z)| \geq Re(z) \quad \wedge \quad |z| \geq |Im(z)| \geq Im(z)$.

v. $|z|^{-1} = |z^{-1}|$ para $z \neq 0$.

vi. Cuando $z \neq 0$, $z^{-1} = \overline{z} \iff |z| = 1$.

vii. $|z + z'| \leq |z| + |z'|$ (Desigualdad Triangular o de *Minkowski*).

Demostración: Demostraremos vii**.**; el resto se deja como ejercicio.

vii. Utilizaremos la propiedad de números reales no negativos:

$x \geq 0$, $y \geq 0$, $x^2 \leq y^2 \iff x \leq y$

Por lo tanto: $|z + z'| \leq |z| + |z'| \iff |z + z'|^2 \leq (|z| + |z'|)^2$

Vamos a demostrar la desigualdad: $|z + z'|^2 \leq (|z| + |z'|)^2$

$$|z + z'|^2 = (z + z').(\overline{z + z'}) = (z + z').(\overline{z} + \overline{z'}) = z\overline{z} + z'\overline{z'} + z\overline{z'} + z'\overline{z} =$$
$$= |z|^2 + |z'|^2 + z\overline{z'} + z'\overline{z} =$$

Observemos que: $z'.\overline{z} = \overline{z\overline{z'}}$

$$= |z|^2 + |z'|^2 + z\overline{z'} + \overline{z\overline{z'}} = |z|^2 + |z'|^2 + 2Re(z\overline{z'}) \leq |z|^2 + |z'|^2 + 2|z\overline{z'}| =$$
$$= |z|^2 + |z'|^2 + 2|z|.|\overline{z'}| = |z|^2 + |z'|^2 + 2.|z|.|z'| = (|z| + |z'|)^2$$

Hemos demostrado que $|z + z'|^2 \leq (|z| + |z'|)^2$

luego se verifica que $\left| z + z' \right| \leq \left| z \right| + \left| z' \right|$

Argumento de un número complejo

Todo número complejo queda unívocamente determinado por su parte real y su parte imaginaria, pero además tenemos otra manera de caracterizarlos: por su módulo y por la medida del ángulo que determinan el eje *x* y la semirrecta que tiene origen en el origen de coordenadas y que pasa por el punto que define tal complejo. Este número real toma su valor en el intervalo $[0, 2\pi)$, y se denomina *argumento* del número complejo. Veremos que el argumento de un número complejo está unívocamente determinado por él:

Sea $z = a + bi \in \mathbb{C}$, $z \neq 0$,

$$a = Re(z) \leq \left| Re(z) \right| \leq \left| z \right| \quad \Rightarrow \quad \left| \frac{a}{|z|} \right| \leq 1 \quad \therefore \quad \frac{a}{|z|} \in [-1, 1].$$

Como la función $cos(x)$ tiene como imagen el intervalo $[-1, 1]$, entonces $\exists \alpha \in [0, 2\pi)$ tal que $cos(\alpha) = \frac{a}{|z|}$

$$b = Im(z) \leq \left| Im(z) \right| \leq \left| z \right| \quad \Rightarrow \quad \left| \frac{b}{|z|} \right| \leq 1 \quad \therefore \quad \frac{b}{|z|} \in [-1, 1]$$

Veamos si $\frac{b}{|z|} = sen(\alpha)$.

- Si $\alpha = 0 \Rightarrow cos(\alpha) = cos(0) = 1 \quad \therefore \quad a = |z| \quad \Leftrightarrow \quad z \in \mathbb{R}_{>0}$

  En este caso $b = 0 \Rightarrow \frac{b}{|z|} = 0 = sen(0) = sen(\alpha)$.

- Si $\alpha \in (0, 2\pi)$, como $|z|^2 = a^2 + b^2 \Rightarrow \frac{a^2 + b^2}{|z|^2} = 1$

  $$\therefore \quad \frac{b^2}{|z|^2} = 1 - \frac{a^2}{|z|^2} = 1 - cos^2(\alpha) = sen^2(\alpha),$$

  por la relación trigonométrica $sen^2(x) + cos^2(x) = 1$ que se verifica $\forall x \in \mathbb{R}$

  Entonces $\left| \frac{b}{|z|} \right| = \left| sen(\alpha) \right| \quad \therefore \quad \frac{b}{|z|} = sen(\alpha) \quad \vee \quad \frac{b}{|z|} = -sen(\alpha)$.

  Si $\frac{b}{|z|} = sen(\alpha)$ ya obtuvimos un α tal que

  $$cos(\alpha) = \frac{a}{|z|} \quad \wedge \quad sen(\alpha) = \frac{b}{|z|},$$

  Si $\frac{b}{|z|} \neq sen(\alpha) \Rightarrow \frac{b}{|z|} = -sen(\alpha)$; como $sen(\alpha) = -sen(2\pi - \alpha)$,

  entonces $\frac{b}{|z|} = sen(2\pi - \alpha)$.

  Además $cos(\alpha) = cos(2\pi - \alpha) \quad \wedge \quad (2\pi - \alpha) \in (0, 2\pi)$ pues $\alpha \in (0, 2\pi)$,

entonces $(2\pi - \alpha) \in (0, 2\pi)$ es tal que

$$cos(2\pi - \alpha) = \frac{a}{|z|} \quad \wedge \quad sen(2\pi - \alpha) = \frac{b}{|z|}$$

Por lo tanto, hemos demostrado que $\forall z = a + bi \neq 0 \quad \exists! \beta \in [0, 2\pi)$ tal que

$$cos(\beta) = \frac{a}{|z|} \quad \wedge \quad sen(\beta) = \frac{b}{|z|}$$

***Definición*:** El β encontrado más arriba, que existe siempre y es único para $z \in \mathbb{C}$, $z \neq 0$, se denomina *argumento de z*.

Notación : $\beta = arg(z)$.

En virtud de la definición tenemos la *representación trigonométrica* del complejo *z* :

$$z = |z| \, (cos(arg(z)) + i.sen(arg(z)))$$

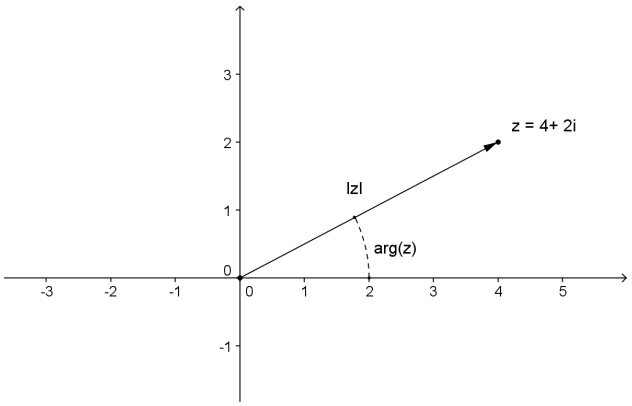
Nota: La unicidad es consecuencia de la siguiente propiedad trigonométrica:

para $\delta, \gamma \in \mathbb{R}$, $sen(\delta) = sen(\gamma) \quad \wedge \quad cos(\delta) = cos(\gamma) \quad \Leftrightarrow \quad \delta \equiv \gamma \ (mód\ 2\pi)$

donde $\delta \equiv \gamma \ (mód\ 2\pi) \ \Leftrightarrow \ \exists k \in \mathbb{Z}$ tal que $\delta - \gamma = 2k\pi$ (si los pensamos como medidas de ángulos, significa que $\delta \wedge \gamma$ difieren en un número entero de *giros*).

La *congruencia módulo* 2π es una *relación de equivalencia* en $\mathbb{R}$, en la cual el conjunto cociente $\mathbb{R}/\equiv (mód\ 2\pi)$ puede identificarse con el intervalo $[0, 2\pi)$ dado que $\forall x \in \mathbb{R}$ $\exists! y \in [0, 2\pi)$ tal que $x \equiv y \ (mód\ 2\pi)$

Ejercicio: $z \in \mathbb{C}$, $|z| = 1 \quad \Leftrightarrow \quad z = cos(\alpha) + i.\, sen(\alpha)$ para algún $\alpha \in \mathbb{R}$.



***Teorema de De Moivre*:**

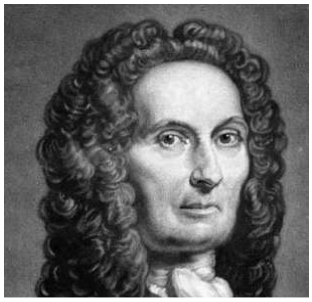
Para α, $\beta \in \mathbb{R}$, se verifica que :

$[cos(\alpha) + i.\ sen(\alpha)].[\ cos(\beta) + i.\ sen(\beta)] = cos(\alpha+\beta) + i.\ sen(\alpha+\beta)$.

***Demostración*:** Multiplicando ambos complejos, obtenemos:

$[\ cos(\alpha) + i.\ sen(\alpha)].[\ cos(\beta) + i.\ sen(\beta)] = cos(\alpha).cos(\beta) - sen(\alpha).sen(\beta) +$
$+ i.[\ cos(\alpha).sen(\beta) + sen(\alpha).cos(\beta)] = cos(\alpha+\beta) + i.\ sen(\alpha+\beta)$

en virtud de las relaciones trigonométricas conocidas.



Abraham De Moivre
(1667, Francia- 1754, Inlaterra)

Abraham de Moivre nació en Vitry-le-François, donde su padre trabajaba como cirujano. Siendo de familia protestante sufrió muchas tensiones debido a la persecución religiosa de ese momento en Francia. Estuvo prisionero por sus creencias religiosas en el priorato de San Martín debiendo emigrar finalmente a Londres donde trabajó como profesor particular de Matemáticas. De Moivre fue pionero en el desarrollo de la geometría analítica y en la teoría de la probabilidad. Estableció muchos de los elementos de los cálculos actuales y, por encima de sus muchos logros, descubrió en 1730 la relación trigonométrica:

$$(\cos q + i sen\, q)^n = \cos\, nq + i sen\, nq$$

A pesar de su eminencia científica, sus ingresos venían de sus clases particulares de matemáticas por lo que murió en la pobreza. Desesperado por conseguir una cátedra en Cambridge rogó a Johan Bernoulli que persuadiera a Leibniz para recomendarle. Ni siquiera sus influyentes amigos ingleses como Newton y Halley pudieron ayudarle a conseguir un puesto en la universidad.

***Corolario*:** $[cos(\alpha) + i.\ sen(\alpha)]^n = cos(n\alpha) + i.\ sen(n\alpha) \qquad \forall n \in \mathbb{N}$.

Demostración: Se obtiene razonando por inducción sobre n y aplicando la proposición anterior.

***Teorema*:** Para $z, w \in \mathbb{C} - \{0\}$, $\quad arg(z.w) \equiv arg(z) + arg(w) \quad (mód\ 2\pi)$.

***Demostración*:** Sean $\quad z = |z|\ [\ cos(arg(z)) + i.\ sen(arg(z))]$

$w = |w|[\ cos(arg(w)) + i.\ sen(arg(w))]$.

Multiplicando m.a.m. :

$z.w = |z|.|w|.[\ cos(arg(z)) + i.\ sen(arg(z))].\ [\ cos(arg(w)) + i.\ sen(arg(w))] =$
$= |z.w|[cos(arg(z)+ arg(w)) + i.\ sen(arg(z)+ arg(w))]$.

Por otra parte: $\quad z.w = |z.w|[\ cos(arg(z.w)) + i.\ sen(arg(z.w))]$

con lo cual:

$cos(arg(z)+ arg(w)) + i.\ sen(arg(z)+ arg(w)) = cos(arg(z.w)) + i.\ sen(arg(z.w))$

Por la igualdad de números complejos, tenemos:

$$cos(arg(z)+ arg(w)) = cos(arg(z.w))$$
$$\wedge \quad sen(arg(z)+ arg(w)) = sen(arg(z.w)).$$

De donde $arg(z)+ arg(w) \equiv arg(z.w) \pmod{2\pi}$ por la propiedad ya mencionada.

Ejemplo: $z = -\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2} i \quad ; \quad w = -i$

$$arg(z) = \frac{3\pi}{4} \quad ; \quad arg(w) = \frac{3\pi}{2}$$

$$z.w = \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2} i \quad ; \quad arg(z.w) = \frac{\pi}{4}$$

$$arg(z) + arg(w) = \frac{3\pi}{4} + \frac{3\pi}{2} = \frac{9\pi}{4} = 2\pi + \frac{\pi}{4} \equiv \frac{\pi}{4} \pmod{2\pi}.$$

***Corolario*:** $arg(z^n) \equiv n.\, arg(z) \pmod{2\pi} \quad \forall n \in \mathbb{N}, \quad \forall z \in \mathbb{C} - \{0\}$

***Demostración*:** Es inmediata, razonando por inducción sobre *n* a partir del teorema .

Ejercicios:

1) Si $z \in \mathbb{C} - \mathbb{R}_{\geq 0}$, $arg(\overline{z}) = 2\pi - arg(z)$.
2) $z \in \mathbb{C} - \{0\}$, $arg(z^{-1}) = arg(\overline{z})$.

Raíces n-ésimas de la unidad

Queremos encontrar en $\mathbb{C}$ las soluciones de la ecuación $x^n - 1 = 0 \quad \forall n \in \mathbb{N}$, o lo que es lo mismo, las raíces complejas del polinomio real $f(x) = x^n - 1$.
En $\mathbb{R}$ ya conocemos la respuesta: si *n* es impar tiene una única solución: $x = 1$; y si *n* es par admite dos: $x = 1 \quad \wedge \quad x = -1$.
También podemos establecer que no tiene raíces múltiples, porque el polinomio derivado $f'(x) = nx^{n-1}$ para $n > 1$, tiene a 0 como única raíz, que no es raíz de $f(x)$. Analicemos el problema buscando soluciones en $\mathbb{C}$ si las tuviera.

Sea $z \in \mathbb{C}$ tal que $z^n = 1 \quad \Rightarrow \quad |z^n| = 1 \quad \wedge \quad arg(z^n) = 0$

$$1 = |z^n| = |z|^n \quad \Rightarrow \quad |z| = \sqrt[n]{1} = 1$$

$$0 = arg(z^n) \equiv n.arg(z) \quad \Rightarrow \quad arg(z) = \frac{2k\pi}{n} \quad \text{para algún} \quad k \in \mathbb{Z}$$

como $arg(z) \in [0, 2\pi)$, $\quad 0 \leq \frac{2k\pi}{n} < 2\pi \quad \Leftrightarrow$

multiplicando por *n* : $\quad \Leftrightarrow \quad 0 \leq 2k\pi < 2n\pi \quad \Leftrightarrow$

dividiendo por 2π : $\Leftrightarrow \quad 0 \leq k < n$.

Hemos demostrado que si z es tal que $z^n = 1 \Rightarrow |z| = 1 \wedge arg(z) = \frac{2k\pi}{n}$ para algún k , con $0 \leq k < n$.

Veamos que esta condición es suficiente, o sea que si $z \in \mathbb{C}$ es tal que

$$|z| = 1 \wedge arg(z) = \frac{2k\pi}{n} \text{ con } 0 \leq k < n \Rightarrow z^n = 1 .$$

$$z = |z| \, [\cos(arg(z)) + i.\, sen(arg(z))] = \cos(arg(z)) + i.\, sen(arg(z)) =$$

$$= \cos\frac{2k\pi}{n} + i.\, sen\, \frac{2k\pi}{n}$$

$$z^n = \cos n\,(arg(z)) + i.\, sen\, n\,(arg(z)) = \cos n\, \frac{2k\pi}{n} + i.\, sen\, n\, \frac{2k\pi}{n} =$$

$$= \cos 2\pi + i.\, sen\, 2\pi = 1 .$$

Luego z es raíz n-ésima de la unidad.

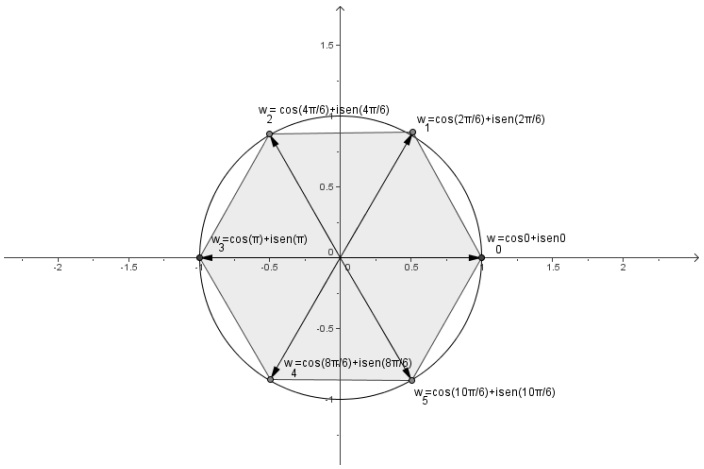
Entonces las raíces n-ésimas de la unidad son los complejos:

$$w_k = \cos(\frac{2k\pi}{n}) + i.\, sen(\frac{2k\pi}{n}) \text{ para } k = 0, 1, 2, \ldots, n-1 ,$$

que son n raíces n-ésimas distintas del complejo 1 en $\mathbb{C}$.

Representación gráfica de las raíces *n*-ésimas de 1:

$n = 6$



Raíces n-ésimas de a $\in \mathbb{R}_{>0}$

Buscamos las raíces en $\mathbb{C}$ del polinomio $g(x) = x^n - a$.

Sea $z \in \mathbb{C}$ tal que $z^n = a \Rightarrow \frac{z^n}{a} = 1$.

Como $a > 0$, $\sqrt[n]{a}$ es el único número real positivo que elevado a la n es a

$$\therefore \quad z^n = a \Leftrightarrow \left(\frac{z}{\sqrt[n]{a}}\right)^n = 1 .$$

Por lo tanto, las raíces n-ésimas de a son los z_k tales que

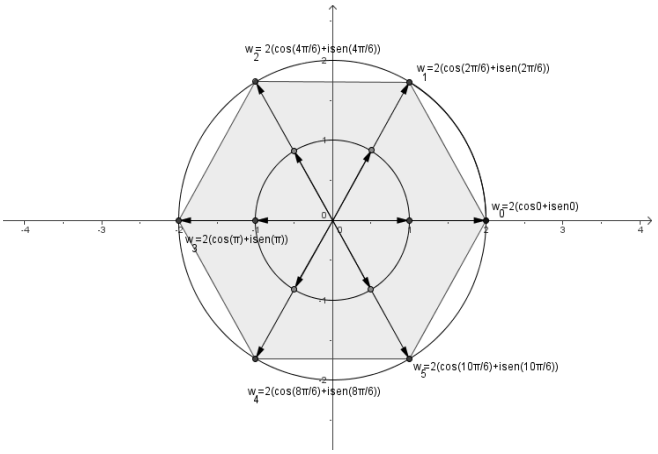
$$\frac{z_k}{\sqrt[n]{a}} = w_k = cos(\frac{2k\pi}{n}) + i.\, sen(\frac{2k\pi}{n}) \quad \text{para} \quad k = 0, 1, 2, \ldots, n-1 ,$$

con lo cual $z_k = \sqrt[n]{a}\,[cos(\frac{2k\pi}{n}) + i.\, sen(\frac{2k\pi}{n})\,]$ con $k = 0, 1, 2, \ldots, n-1$,

son las n raíces n-ésimas distintas de a.

Representación gráfica de las raíces *n*-ésimas de *a* :

$a = 64$, $n = 6$



***Raíces n-ésimas de* –1**

Buscamos en $\mathbb{C}$ las raíces del polinomio $h(x) = x^n + 1$, que sabemos que en $\mathbb{R}$, cuando n es par, no admite raíces, y cuando n es impar, admite sólo una: -1 .

Sea $z \in \mathbb{C}$ tal que $z^n = -1 \;\Rightarrow\; |z^n| = 1 \;\wedge\; arg(z^n) = \pi$.

$$1 = |z^n| = |z|^n \;\Rightarrow\; |z| = \sqrt[n]{1} = 1 .$$

$$\pi = arg(z^n) \equiv n.arg(z) \;\Rightarrow\; arg(z) = \frac{\pi}{n} + \frac{2k\pi}{n} \quad \text{para algún } k \in \mathbb{Z} ,$$

como $arg(z) \in [0, 2\pi)$, $\quad 0 \le \frac{\pi}{n} + \frac{2k\pi}{n} < 2\pi \quad \Leftrightarrow$

multiplicando por n: $\quad \Leftrightarrow \quad 0 \le \pi + 2k\pi < 2n\pi \quad \Leftrightarrow$

dividiendo por 2π: $\quad \Leftrightarrow \quad 0 \le \frac{1}{2} + k < n$

restando $\frac{1}{2}$: $\quad \Leftrightarrow \quad -\frac{1}{2} \le k < n - \frac{1}{2}$

como $k \in \mathbb{Z} \;\Rightarrow\; 0 \le k \le n-1$.

Hemos demostrado que si z es tal que $z^n = -1 \;\Rightarrow\; arg(z) = \frac{\pi}{n} + \frac{2k\pi}{n}$

para algún k, con $0 \le k \le n-1 \;\wedge\; |z| = 1$.

Veamos que esta condición es suficiente, o sea que si $z \in \mathbb{C}$ es tal que

$$|z| = 1 \quad \wedge \quad arg(z) = \frac{\pi}{n} + \frac{2k\pi}{n} \quad \text{con} \quad 0 \leq k \leq n-1 \quad \Rightarrow \quad z^n = -1 .$$

$$z = |z| \, [\, cos(arg(z)) + i.\, sen(arg(z))] = cos(arg(z)) + i.\, sen(arg(z)) =$$
$$= cos\,(\frac{\pi}{n} + \frac{2k\pi}{n}\,) + i.\, sen\,(\frac{\pi}{n} + \frac{2k\pi}{n}\,)$$

$$z^n = cos\, n(arg(z)) + i.\, sen\, n(arg(z)) = cos\, n\,(\frac{\pi}{n} + \frac{2k\pi}{n}\,) + i.\, sen\, n\,(\frac{\pi}{n} + \frac{2k\pi}{n}\,) =$$
$$= cos\,\pi + i.\, sen\,\pi = -1 .$$

Luego z es raíz n-ésima de -1.

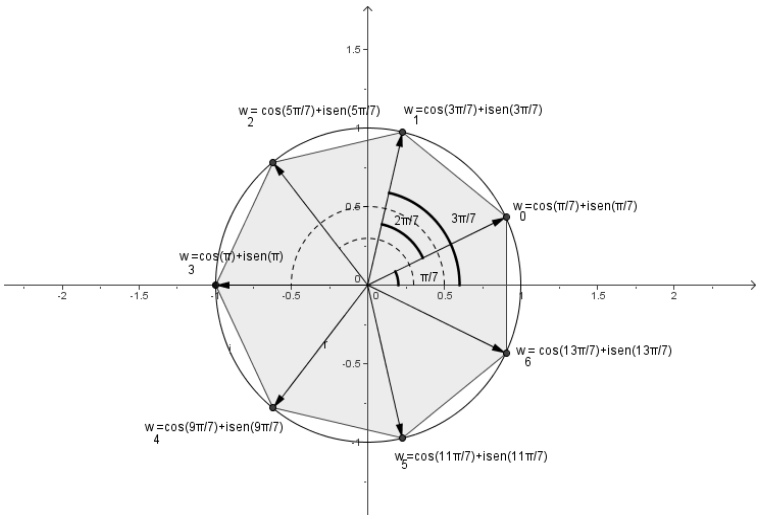
Entonces las raíces n-ésimas de -1 son los complejos:

$$v_k = cos(\frac{\pi}{n} + \frac{2k\pi}{n}\,) + i.\, sen(\frac{\pi}{n} + \frac{2k\pi}{n}\,) \quad \text{para} \quad k = 0, 1, 2, \ldots, n-1 ,$$

que son n elementos diferentes en $\mathbb{C}$.

Representación gráfica de las raíces n-ésimas de -1 :

$n = 7$



Raíces n-ésimas de $-a$, con $a \in \mathbb{R}_{>0}$

Buscamos las raíces en $\mathbb{C}$ del polinomio $p(x) = x^n + a$, $a > 0$.

Sea $z \in \mathbb{C}$ tal que $z^n = -a \quad \Rightarrow \quad \frac{z^n}{a} = -1$.

Como $a > 0$, $\sqrt[n]{a}$ es el único número real positivo que elevado a la n es a

$$\therefore \quad z^n = -a \quad \Leftrightarrow \quad \left(\frac{z}{\sqrt[n]{a}}\right)^n = -1 .$$

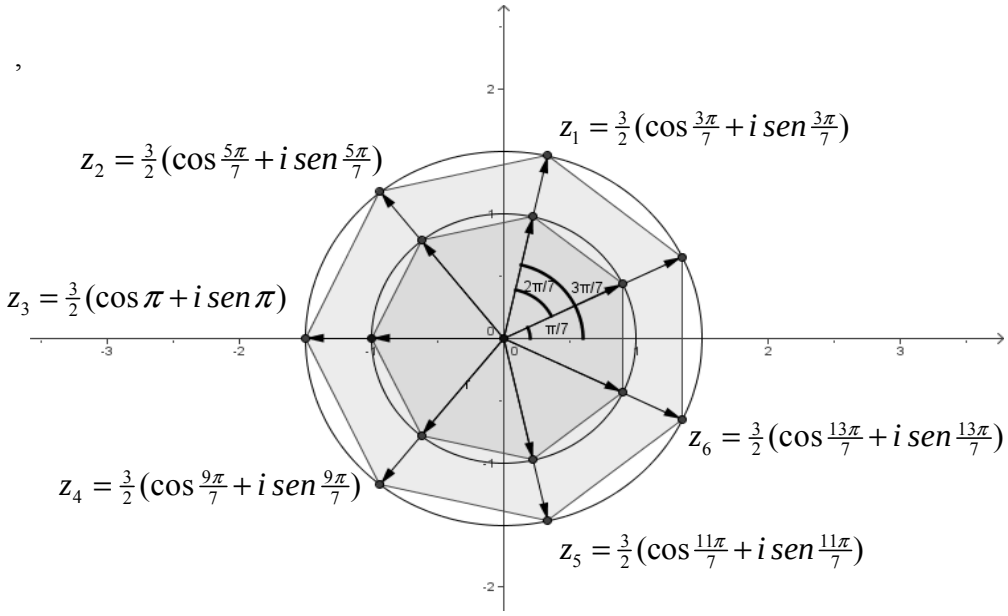
Por lo tanto, las raíces n-ésimas de $-a$ son los z_k tales que

$$\frac{z_k}{\sqrt[n]{a}} = v_k = cos(\frac{\pi}{n}+\frac{2k\pi}{n}) + i.\, sen(\frac{\pi}{n}+\frac{2k\pi}{n}) \quad \text{para} \quad k = 0, 1, 2,\ldots, n-1 ,$$

con lo cual $z_k = \sqrt[n]{a}\,[cos(\frac{\pi}{n}+\frac{2k\pi}{n}) + i.\, sen(\frac{\pi}{n}+\frac{2k\pi}{n})\,]$ con $k = 0, 1, 2,\ldots, n-1$.

Representación gráfica de las raíces *n*-ésimas de $-a$:

$a = \frac{2187}{128}$,



Raíces n-ésimas de $\omega \in \mathbb{C} - \{0\}$

Sea $z \in \mathbb{C}$ tal que $z^n = \omega \;\Rightarrow\; |z^n| = |\omega| \;\wedge\; arg(z^n) = arg(\omega)$.

$$|\omega| = |z^n| = |z|^n \quad \Rightarrow \quad |z| = \sqrt[n]{|\omega|}$$

$$arg(\omega) = arg(z^n) \equiv n.arg(z) \;\Rightarrow\; arg(z) = \frac{arg(\omega)}{n} + \frac{2k\pi}{n} \quad \text{para algún } k \in \mathbb{Z},$$

como $arg(z) \in [0, 2\pi)$, $\quad 0 \le \frac{arg(\omega)}{n} + \frac{2k\pi}{n} < 2\pi \;\Leftrightarrow$

multiplicando por n : $\quad \Leftrightarrow\; 0 \le arg(\omega) + 2k\pi < 2n\pi \;\Leftrightarrow$

dividiendo por 2π : $\quad \Leftrightarrow\; 0 \le \frac{arg(\omega)}{2\pi} + k < n$

restando $\frac{arg(\omega)}{2\pi}$: $\quad \Leftrightarrow\; -\frac{arg(\omega)}{2\pi} \le k < n - \frac{arg(\omega)}{2\pi}$

$arg(\omega) \in [0, 2\pi) \quad \Rightarrow \quad 0 \le \frac{arg(\omega)}{2\pi} < 1$

como $k \in \mathbb{Z} \quad \Rightarrow \quad 0 \le k \le n-1$.

Hemos demostrado que si z es tal que $z^n = \omega \;\Rightarrow\; arg(z) = \frac{arg(\omega)}{n} + \frac{2k\pi}{n}$

para algún k, con $0 \leq k \leq n-1 \quad \wedge \quad |z| = \sqrt[n]{|\omega|}$.

Veamos que esta condición es suficiente, o sea que si $z \in \mathbb{C}$ es tal que

$$|z| = \sqrt[n]{|\omega|} \quad \wedge \quad arg(z) = \frac{arg(\omega)}{n} + \frac{2k\pi}{n} \text{ con } 0 \leq k \leq n-1 \quad \Rightarrow \quad z^n = \omega$$

$$z = |z| \; [\, cos(arg(z)) + i.\, sen(arg(z))] =$$

$$= \sqrt[n]{|\omega|} \, [\, cos\,(\frac{arg(\omega)}{n} + \frac{2k\pi}{n}) + i.\, sen\,(\frac{arg(\omega)}{n} + \frac{2k\pi}{n})]$$

$$z^n = (\sqrt[n]{|\omega|})^n [\, cos\, n(arg(z)) + i.\, sen\, n(arg(z))] =$$

$$= |\omega| \; [\, cos\, n\,(\frac{arg(\omega)}{n} + \frac{2k\pi}{n}) + i.\, sen\, n\,(\frac{arg(\omega)}{n} + \frac{2k\pi}{n})] =$$

$$= |\omega| [cos\, arg(\omega) + i.\, sen\, arg(\omega)] = \omega.$$

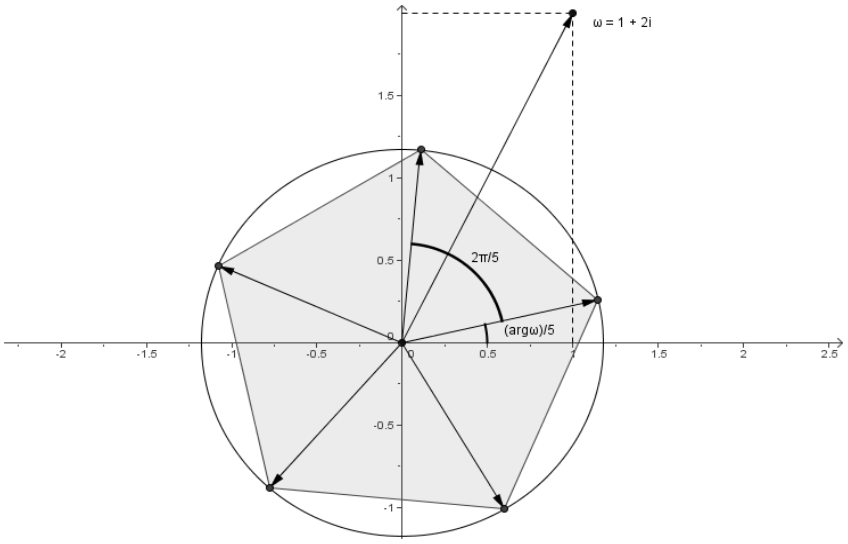
Luego z es raíz n-ésima de ω.

Entonces las raíces n-ésimas de ω son los complejos:

$$r_k = \sqrt[n]{|\omega|} \, [cos(\frac{arg(\omega)}{n} + \frac{2k\pi}{n}) + i.\, sen(\frac{arg(\omega)}{n} + \frac{2k\pi}{n})]$$

para $k = 0, 1, 2, \ldots, n-1$, que son n raíces n-ésimas de ω, distintas, en $\mathbb{C}$.

Representación gráfica de las raíces *n*-ésimas de ω : $\omega = 1 + 2i$; $n = 5$



Polinomios con coeficientes en $\mathbb{R}$

Vimos que los polinomios con coeficientes en $\mathbb{R}$ de la forma $x^n \pm a$ con $a > 0$, tienen una o dos raíces en $\mathbb{R}$, dependiendo de la paridad o no de n, y las restantes son complejas no reales, pero en $\mathbb{C}$ tienen exactamente n, lo que nos permite asegurar que la factorización en polinomios irreducibles y mónicos de dichos polinomios en $\mathbb{C}[x]$ será:

$$x^n \pm a = \prod_{i=0}^{n} (x - w_i)$$

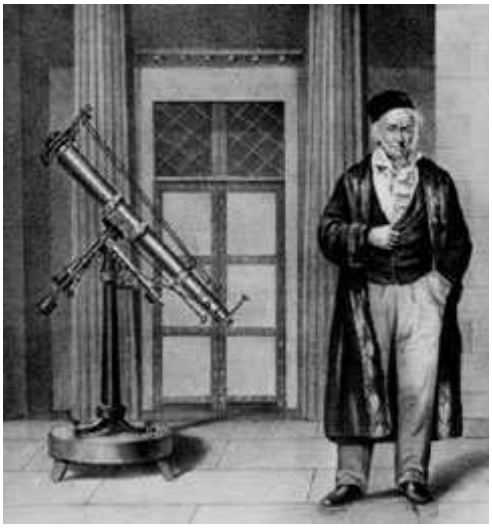
donde w_i son las raíces n-ésimas de a o $-a$ según sea uno u otro polinomio.

Lo que no sabemos aun es cuál es la factorización en irreducibles de $\mathbb{R}[x]$ de esos polinomios, y de otros, aun conociendo sus raíces en $\mathbb{C}$.

Para acercarnos a las respuestas, enunciaremos un Teorema Fundamental debido a Gauss, que no demostraremos porque requiere ahondar en otros temas de la matemática que exceden los que aquí desarrollamos, pero que utilizaremos para obtener propiedades importantes sobre los polinomios reales.

Teorema fundamental del álgebra:

Todo polinomio de $\mathbb{R}[x]$ de grado positivo admite, al menos, una raíz en $\mathbb{C}$.



Karl Friedrich Gauss (1777-1855)

El primer matemático en declarar que una ecuación polinómica de grado n había de tener n soluciones fue Albert Girard en su Nouvelle invention en Algebre publicada en 1629.

Sin embargo, Girard no dice que las soluciones puedan ser de la forma a + bi, con a y b números reales. Los matemáticos de la época aceptaron, sin demostración, la afirmación de Girard.

Es a Karl Friedrich Gauss, a quien se le concede la primera demostración del Teorema Fundamental del Algebra (TFA). En su tesis doctoral de 1799 presentó su esquema de demostración con las objeciones a todas las demostraciones anteriores (D.Alembert en 1746, Laplace en 1795…). La misma está basada en parte en consideraciones geométricas y en la idea de Wessel para representar gráficamente los números complejos.

Pugnando siempre por encontrar una demostración puramente algebraica, Gauss hizo a lo largo de su vida hasta cuatro demostraciones distintas del TFA: la primera, en su tesis doctoral de 1799, la segunda y la tercera en 1816 y la cuarta en 1849, 50 años después de la primera.

Las demostraciones dadas por Gauss están reunidas en el volumen III de sus Werke (1870-1930).

Hoy se admite que el teorema fundamental del Algebra depende esencialmente de consideraciones de tipo topológico.

A partir de este importantísimo teorema obtendremos resultados esclarecedores acerca de los polinomios reales.

***Proposición*:** Sean $f(x) \in \mathbb{R}[x]$, $gr(f(x)) > 0$, $z \in \mathbb{C}$. Entonces:
z es raíz de $f(x) \Leftrightarrow \overline{z}$ también lo es .

***Demostración*:**
$\Rightarrow$) Sea $z \in \mathbb{C}$ raíz de $f(x)$. Como $f(x) \in \mathbb{R}[x] \wedge gr(f(x)) > 0$,

$$f(x) = \sum_{i=0}^{n} a_i x^i \quad , \; a_i \in \mathbb{R} \quad \forall i = 0,1,...,n \; , \quad n \in \mathbb{N} , \quad a_n \neq 0 \; .$$

Por ser z raíz de $f(x)$ tenemos que $0 = f(z) = \sum_{i=0}^{n} a_i z^i$,

conjugando: $0 = \overline{0} = \overline{f(z)} = \overline{\sum_{i=0}^{n} a_i z^i} = \sum_{i=0}^{n} \overline{a}_i \overline{z}^i$, por propiedades de la conjugación ;

como $a_i \in \mathbb{R} \quad \forall i = 0,1,...,n$, $\overline{a}_i = a_i \quad \forall i = 0,1,...,n$

entonces $0 = \sum_{i=0}^{n} a_i \overline{z}^i = f(\overline{z}) \quad \therefore \quad \overline{z}$ es raíz de $f(x)$.

$\Leftarrow$) la recíproca es trivial a partir de lo ya demostrado y del hecho que $\overline{\overline{z}} = z$.

***Teorema*:** Todo polinomio en $\mathbb{R}[x]$ de grado impar admite, al menos, una raíz real.

***Demostración*:** Sea $f(x) \in \mathbb{R}[x]$ tal que $gr(f(x)) = 2n - 1$, $n \in \mathbb{N}$. Demostraremos por inducción sobre n que siempre admite una raíz real.

- Sea $n = 1$, entonces $f(x)$ es tal que $gr(f(x)) = 1 \quad \therefore \quad f(x) = ax + b$,
  con $a \neq 0$. En estos casos sabemos que $-\frac{b}{a} \in \mathbb{R} \quad \wedge$ es raíz de $f(x)$.

- Supongamos que todo polinomio en $\mathbb{R}[x]$ de grado $2n - 1$, admita, al menos, una raíz real (HI).

- Sea, ahora, un polinomio $g(x) \in \mathbb{R}[x]$ de $gr(g(x)) = 2n + 1$.
  Por el Teorema Fundamental del Álgebra, $\exists z \in \mathbb{C}$ tal que $g(z) = 0$; por la proposición anterior, $\overline{z}$ también es raíz de $g(x)$.

  - si $z \in \mathbb{R} \Rightarrow z = \overline{z} \quad \wedge \quad g(x)$ admite una raíz real,
  - si $z \notin \mathbb{R} \Rightarrow z \neq \overline{z}$
    $\therefore \; (x - z) \mid g(x) \quad \wedge \quad (x - \overline{z}) \mid g(x) \quad \wedge \quad (x - z \, , x - \overline{z}) = 1$
    $\Rightarrow \quad (x - z).(x - \overline{z}) \mid g(x)$
    $(x - z).(x - \overline{z}) = x^2 + 2Re(z).x + |z|^2 \in \mathbb{R}[x]$.

  Por lo tanto $\exists f(x) \in \mathbb{R}[x]$ tal que $g(x) = f(x) \, . \, (x^2 + 2Re(z).x + |z|^2)$
  con $gr(f(x)) = 2n - 1$.

Por HI $f(x)$ admite una raíz real b . Como $f(b) = 0 \quad \wedge \quad f(x) \mid g(x) \quad \Rightarrow \quad g(b) = 0$, luego $g(x)$ admite una raíz real.

Hemos demostrado que todo polinomio de grado impar admite, al menos, una raíz real.

***Corolario*:** Todo polinomio en $\mathbb{R}[x]$ de grado impar y mayor que 1 es reducible.

***Demostración*:** Es consecuencia directa del Teorema.

***Teorema*:** Los polinomios irreducibles en $\mathbb{R}[x]$ son los de grado 1 y los de grado 2 con discriminante negativo.

***Demostración*:**

- Ya demostramos que los polinomios de grado 1 son irreducibles en K[x], cualquiera sea el cuerpo K, por lo tanto el resultado se verifica para $\mathbb{R}[x]$.
- Los polinomios de grado 2 en $\mathbb{R}[x]$ son irreducibles si y sólo si su discriminante es negativo, en virtud de lo demostrado en el capítulo de polinomios.
- Sólo nos resta demostrar que ningún polinomio de grado mayor que 2 es irreducible:

  Sea $f(x) \in \mathbb{R}[x]$ tal que $gr(f(x)) > 2$. Por el Teorema Fundamental del Álgebra,

  $f(x)$ admite una raíz en $\mathbb{C}$.

  Sea $z \in \mathbb{C}$ raíz de $f(x)$.

  - Si $z \in \mathbb{R} \Rightarrow (x - z) \mid f(x)$ en $\mathbb{R}[x] \wedge 0 < gr((x - z)) = 1 < gr(f(x))$, con lo cual $f(x)$ es reducible en $\mathbb{R}[x]$.
  - Si $z \in \mathbb{C} - \mathbb{R} \Rightarrow \overline{z}$ también es raíz de $f(x) \wedge z \neq \overline{z}$

    $\therefore (x - z) \mid f(x) \wedge (x - \overline{z}) \mid f(x) \wedge (x - z, x - \overline{z}) = 1$

    $\Rightarrow (x - z).(x - \overline{z}) \mid f(x)$

    $(x - z).(x - \overline{z}) = x^2 + 2Re(z).x + |z|^2 \in \mathbb{R}[x]$,

    $(x^2 + 2Re(z).x + |z|^2) \mid f(x) \wedge$

    $0 < gr(x^2 + 2Re(z).x + |z|^2) = 2 < gr(f(x))$

    $\therefore$ $f(x)$ es reducible en $\mathbb{R}[x]$.

Por lo tanto, los polinomios irreducibles de $\mathbb{R}[x]$ son los de grado 1 y los de grado 2 con discriminante negativo.

Cuerpos algebraicamente cerrados

***Definición*:** Un cuerpo K se dice *algebraicamente cerrado* si todo polinomio en K[x], de grado positivo, admite, al menos, una raíz en K .

Ejemplos: $\mathbb{Q} \wedge \mathbb{R}$ **no** son algebraicamente cerrados pues el polinomio $p(x) = x^2 + 1$ no admite raíces en ninguno de los dos cuerpos.

***Proposición*:** Si K es algebraicamente cerrado, $f(x) \in K[x]$ es tal que $gr(f(x)) = n \in \mathbb{N}$, entonces $f(x)$ tiene n raíces en K (contando cada raíz tantas veces cuanta sea su multiplicidad) , por lo tanto, $f(x)$ se factoriza como producto de n polinomios de grado 1 en $K[x]$.

Demostración: La haremos por inducción sobre el grado del polinomio.

- Si $gr(f(x)) = 1$, $f(x) = ax + b = a(x+\frac{b}{a})$ que es su factorización en irreducibles mónicos en $K[x]$ y donde $-\frac{b}{a} \in K$ es raíz de $f(x)$.

- Supongamos que todo polinomio de grado n se factorice en $K[x]$ como producto de n polinomios mónicos de grado 1, por una unidad, o lo que es lo mismo, que tenga n raíces en K (HI).

- Sea $f(x) \in K[x]$ tal que $gr(f(x)) = n + 1$.

  Por ser K algebraicamente cerrado, $\exists b \in K$ tal que $f(b) = 0$, por lo tanto

  $(x - b) \mid f(x) \quad \therefore \quad f(x) = (x - b).\, h(x)$ con $h(x) \in K[x]$.

  $gr(h(x)) = n$ luego, por HI $h(x) = u.(x - a_1)(x - a_2)\ldots(x - a_n)$ con $u \in K - \{0\}$,

  $a_1, a_2, ..., a_n \in K$.

  Reemplazando: $f(x) = u.(x - a_1)(x - a_2)\ldots(x - a_n)\ (x - b)$

  con lo cual $f(x)$ se factoriza en $K[x]$ como producto de $n + 1$ polinomios de grado 1, o sea, tiene $n + 1$ raíces en K.

Luego, cuando K es algebraicamente cerrado, todo polinomio de grado n en $K[x]$ tiene n raíces en K.

***Corolario*:** Si K es un cuerpo algebraicamente cerrado, los polinomios irreducibles de $K[x]$ son los de grado 1.

***Demostración*:** Los polinomios de grado 1 con coeficientes en un cuerpo son irreducibles; nos resta probar que los polinomios de grado mayor que 1 son reducibles cuando K es algebraicamente cerrado.

Sea $f(x) \in K[x]$, $gr(f(x)) = n > 1$. Por el teorema, $f(x)$ admite n raíces en K.
Si $b \in K$ es una raíz $\Rightarrow$ $(x - b) \mid f(x)$ $\wedge$ $0 < gr((x - b)) = 1 < gr(f(x))$, con lo cual $f(x)$ es reducible.

***Teorema*:** $\mathbb{C}$ es un cuerpo algebraicamente cerrado.

***Demostración*:** Debemos probar que todo polinomio en $\mathbb{C}[x]$, de grado positivo, admite una raíz en $\mathbb{C}$.

Sea $f(x) \in \mathbb{C}[x]$ tal que $gr(f(x)) > 0$,

$$f(x) = \sum_{j=0}^{n} w_j\, x^j \quad \text{con} \quad w_j \in \mathbb{C},\ n \in \mathbb{N}, \qquad w_n \neq 0$$

Definamos $\overline{f}(x) = \sum_{j=0}^{n} \overline{w}_j\, x^j \in \mathbb{C}[x]$, y calculemos el producto $h(x) = f(x).\, \overline{f}(x)$

$$h(x) = (\sum_{j=0}^{n} w_j\, x^j)(\sum_{j=0}^{n} \overline{w}_j\, x^j) = \sum_{k=0}^{2n} v_k x^k \quad \text{donde} \quad v_k = \sum_{j+\,t=k} w_j \overline{w}_t$$

Calculemos los v_k :

$$v_0 = w_0\overline{w}_0 = \left|w_0\right|^2 \in \mathbb{R}$$

$$v_1 = w_0\overline{w}_1 + w_1\overline{w}_0 = 2Re(w_0\overline{w}_1) \in \mathbb{R}$$

$$v_2 = w_0\overline{w}_2 + w_1\overline{w}_1 + w_2\overline{w}_0 = 2Re(w_0\overline{w}_2) + \left|w_1\right|^2 \in \mathbb{R}$$

$$v_3 = w_0\overline{w}_3 + w_1\overline{w}_2 + w_2\overline{w}_1 + w_3\overline{w}_0 = 2Re(w_0\overline{w}_3 + w_1\overline{w}_2) \in \mathbb{R}$$

$$v_4 = w_0\overline{w}_4 + w_1\overline{w}_3 + w_2\overline{w}_2 + w_3\overline{w}_1 + w_4\overline{w}_0 = 2Re(w_0\overline{w}_4 + w_1\overline{w}_3) + \left|w_2\right|^2 \in \mathbb{R}$$

en general, para k par tenemos:

$$v_k = w_0\overline{w}_k + w_1\overline{w}_{k-1} + w_2\overline{w}_{k-2} + \ldots + w_{\frac{k}{2}-1}\overline{w}_{\frac{k}{2}+1} + w_{\frac{k}{2}}\overline{w}_{\frac{k}{2}} +$$

$$+ w_{\frac{k}{2}+1}\overline{w}_{\frac{k}{2}-1} + \ldots. + w_{k-2}\overline{w}_2 + w_{k-1}\overline{w}_1 + w_k\overline{w}_0 =$$

$$= 2Re(w_0\overline{w}_k + w_1\overline{w}_{k-1} + w_2\overline{w}_{k-2} + \ldots + w_{\frac{k}{2}-1}\overline{w}_{\frac{k}{2}+1}) + \left|w_{\frac{k}{2}}\right|^2 \in \mathbb{R}$$

y para k impar:

$$v_k = w_0\overline{w}_k + w_1\overline{w}_{k-1} + w_2\overline{w}_{k-2} + \ldots. + w_{\frac{k-1}{2}}\overline{w}_{\frac{k+1}{2}} +$$

$$+ w_{\frac{k+1}{2}}\overline{w}_{\frac{k-1}{2}} + \ldots.. + w_{k-1}\overline{w}_2 + w_{k-1}\overline{w}_1 + w_k\overline{w}_0 =$$

$$= 2Re(w_0\overline{w}_k + w_1\overline{w}_{k-1} + w_2\overline{w}_{k-2} + \ldots. + w_{\frac{k-1}{2}}\overline{w}_{\frac{k+1}{2}}) \in \mathbb{R}$$

Luego $h(x) \in \mathbb{R}[x]$, y por el Teorema Fundamental del Álgebra admite una raíz en $\mathbb{C}$.

Sea $z \in \mathbb{C}$ raíz de $h(x) \Rightarrow h(z) = 0$.
Como $h(x) = f(x).\overline{f}(x)$ se verifica que $0 = h(z) = f(z).\overline{f}(z) \Rightarrow f(z) = 0 \vee \overline{f}(z) = 0$.

- Si $f(z) = 0$ ya encontramos en $\mathbb{C}$ una raíz para $f(x)$.
- Si $f(z) \neq 0 \Rightarrow \overline{f}(z) = 0$

$$0 = \overline{f}(z) = \sum_{j=0}^{n} \overline{w}_j\, z^j$$

$$\therefore\ 0 = \overline{0} = \overline{\overline{f}(z)} = \overline{\sum_{j=0}^{n} \overline{w}_j\, z^j} = \sum_{j=0}^{n} \overline{\overline{w}_j}\overline{z}^j = \sum_{j=0}^{n} w_j\, \overline{z}^j = f(\overline{z})$$

Por lo tanto $f(\overline{z}) = 0 \ \wedge \ \overline{z}$ es raíz en $\mathbb{C}$ de $f(x)$.

Luego $\mathbb{C}$ es algebraicamente cerrado.

***Corolario*:** Si $f(x) \in \mathbb{C}[x]$ es tal que $gr(f(x)) = n \in \mathbb{N}$, entonces $f(x)$ tiene n raíces en $\mathbb{C}$ (contando cada raíz tantas veces cuanta sea su multiplicidad) , por lo tanto, $f(x)$ se factoriza como producto de n polinomios de grado 1 en $\mathbb{C}[x]$.

En particular, los polinomios irreducibles en $\mathbb{C}[x]$ son los de grado 1.

***Demostración*:** Es consecuencia directa de lo ya demostrado.

***Resumen*:**

Hemos obtenido una caracterización de los polinomios irreducibles en $\mathbb{R}[x]$ y en $\mathbb{C}[x]$.

- En $\mathbb{R}[x]$ los polinomios irreducibles son los de grado 1 y los de grado 2 con discriminante negativo.
- En $\mathbb{C}[x]$ los polinomios irreducibles son los de grado 1.
- En $\mathbb{Q}[x]$ hay polinomios irreducibles de cualquier grado.

Ejemplos:

Factorizar los siguientes polinomios en irreducibles en $\mathbb{C}[x]$, $\mathbb{R}[x]$ y en $\mathbb{Q}[x]$.

1) $f(x) = x^6 - 1$

- en $\mathbb{C}[x]$ la factorización es:

$$f(x) = x^6 - 1 = (x-1)(x+1)\,(x-(\tfrac{1}{2}+\tfrac{\sqrt{3}}{2}i))\,(x-(-\tfrac{1}{2}+\tfrac{\sqrt{3}}{2}i))\,(x-(-\tfrac{1}{2}-\tfrac{\sqrt{3}}{2}i))\,(x-(\tfrac{1}{2}-\tfrac{\sqrt{3}}{2}i))$$

pues 1 , -1, $\frac{1}{2}\pm\frac{\sqrt{3}}{2}i$, $-\frac{1}{2}\pm\frac{\sqrt{3}}{2}i$ son las raíces sextas de la unidad en $\mathbb{C}$, y los polinomios son irreducibles porque son de grado 1 en un cuerpo.

- En $\mathbb{R}[x]$, la factorización no es la misma porque cuatro de esos polinomios no pertenecen a $\mathbb{R}[x]$; para encontrar los irreducibles en este anillo de polinomios hay que multiplicar $(x-z).(x-\overline{z})$ para cada raíz $z \in \mathbb{C}-\mathbb{R}$ del polinomio.

$(x-(\frac{1}{2}+\frac{\sqrt{3}}{2}i)).(x-(\frac{1}{2}-\frac{\sqrt{3}}{2}i)) = x^2 - x + 1$ es irreducible en $\mathbb{R}[x]$ porque es de segundo grado y no admite raíces en $\mathbb{R}$.

$(x-(-\frac{1}{2}+\frac{\sqrt{3}}{2}i)).(x-(-\frac{1}{2}-\frac{\sqrt{3}}{2}i)) = x^2 + x + 1$ es irreducible en $\mathbb{R}[x]$ porque es de segundo grado y no admite raíces en $\mathbb{R}$.

Luego la factorización en irreducibles en $\mathbb{R}[x]$ es :

$$f(x) = x^6 - 1 = (x-1)(x+1)(x^2 - x + 1)(x^2 + x + 1)$$

- En $\mathbb{Q}[x]$,

$$f(x) = x^6 - 1 = (x-1)(x+1)(x^2 - x + 1)(x^2 + x + 1)$$

y todos ellos son irreducibles en $\mathbb{Q}[x]$ porque lo son en $\mathbb{R}[x]$ y están en $\mathbb{Q}[x]$.

2) $g(x) = x^6 + 1$

Las raíces sextas de -1 en $\mathbb{C}$ son : $\pm i$; $\frac{\sqrt{3}}{2} \pm \frac{1}{2}i$; $-\frac{\sqrt{3}}{2} \pm \frac{1}{2}i$.
La factorización en irreducibles es:

- En $\mathbb{C}[x]$

$$g(x) = x^6 + 1 =$$

$$= (x-i)(x+i)\,(x-(\tfrac{\sqrt{3}}{2}+\tfrac{1}{2}i))\,(x-(\tfrac{\sqrt{3}}{2}-\tfrac{1}{2}i))\,(x-(-\tfrac{\sqrt{3}}{2}+\tfrac{1}{2}i))\,(x-(-\tfrac{\sqrt{3}}{2}-\tfrac{1}{2}i))$$

todos ellos irreducibles en $\mathbb{C}[x]$ porque son de grado 1.

- En $\mathbb{R}[x]$, para hallar los irreducibles hay que multiplicar $(x - z)\cdot(x - \overline{z})$ para cada raíz $z \in \mathbb{C} - \mathbb{R}$ del polinomio.

  - $(x-i)(x+i) = x^2 + 1$ irreducible en $\mathbb{R}[x]$ porque es de segundo grado y no admite raíces en $\mathbb{R}$.
  - $(x-(\frac{\sqrt{3}}{2}-\frac{1}{2}i))\,(x-(\frac{\sqrt{3}}{2}+\frac{1}{2}i)) = x^2 - \sqrt{3}x + 1$ irreducible en $\mathbb{R}[x]$ porque es de segundo grado y no admite raíces en $\mathbb{R}$.
  - $(x-(-\frac{\sqrt{3}}{2}+\frac{1}{2}i))\,(x-(-\frac{\sqrt{3}}{2}-\frac{1}{2}i)) = x^2 + \sqrt{3}x + 1$ irreducible en $\mathbb{R}[x]$ porque es de segundo grado y no admite raíces en $\mathbb{R}$.

- En $\mathbb{Q}[x]$

$(x^2 + \sqrt{3}x + 1)\cdot(x^2 - \sqrt{3}x + 1) = x^4 - x^2 + 1$ es irreducible en $\mathbb{Q}[x]$ porque no tiene raíces en $\mathbb{Q}$ y si fuera reducible debería factorizarse como producto de dos polinomios de grado 2 en $\mathbb{Q}[x]$, pero los polinomios de grado 2 que lo factorizan en $\mathbb{R}[x]$ no pertenecen a $\mathbb{Q}[x]$

Luego, en $\mathbb{Q}[x]$ la factorización en irreducibles es: $g(x) = x^6 + 1 = (x^2 + 1)\cdot(x^4 - x^2 + 1)$.

3) $h(x) = x^5 - 21$

- En $\mathbb{C}[x]$

Las raíces en $\mathbb{C}$ de $h(x)$ son: $\sqrt[5]{21}$; $z_1 = \sqrt[5]{21}(\cos\frac{2\pi}{5} + i\,sen\frac{2\pi}{5})$;

$$\overline{z_1} = z_4 = \sqrt[5]{21}(\cos\tfrac{8\pi}{5} + i\,sen\tfrac{8\pi}{5}) = \sqrt[5]{21}(\cos\tfrac{2\pi}{5} - i\,sen\tfrac{2\pi}{5})\ ;$$

$$z_2 = \sqrt[5]{21}(\cos\tfrac{4\pi}{5} + i\,sen\tfrac{4\pi}{5})\ ;\ \overline{z_2} = z_3 = \sqrt[5]{21}(\cos\tfrac{6\pi}{5} + i\,sen\tfrac{6\pi}{5})$$

Luego la factorización en irreducibles en $\mathbb{C}[x]$ de $h(x)$ es:

$h(x)=(x-\sqrt[5]{21})\cdot[x-\sqrt[5]{21}(\cos\frac{2\pi}{5}+i\,sen\frac{2\pi}{5})]\cdot[x-\sqrt[5]{21}(\cos\frac{2\pi}{5}-i\,sen\frac{2\pi}{5})]\cdot$
$\cdot[x-\sqrt[5]{21}(\cos\frac{4\pi}{5}+i\,sen\frac{4\pi}{5})]\cdot[x-\sqrt[5]{21}(\cos\frac{4\pi}{5}-i\,sen\frac{4\pi}{5})]$

- En $\mathbb{R}[x]$

$[x-\sqrt[5]{21}(\cos\frac{2\pi}{5}+i\,sen\frac{2\pi}{5})]\cdot[x-\sqrt[5]{21}(\cos\frac{2\pi}{5}-i\,sen\frac{2\pi}{5})] = x^2-2Re(z_1)x+|z_1|^2$

donde $Re(z_1)=\sqrt[5]{21}\cos\frac{2\pi}{5}$; $|z_1|^2=\sqrt[5]{21^2}$

$[x-\sqrt[5]{21}(\cos\frac{4\pi}{5}+i\,sen\frac{4\pi}{5})]\cdot[x-\sqrt[5]{21}(\cos\frac{4\pi}{5}-i\,sen\frac{4\pi}{5})] = x^2-2Re(z_2)x+|z_2|^2$

donde $Re(z_2)=\sqrt[5]{21}\cos\frac{4\pi}{5}$; $|z_2|^2=\sqrt[5]{21^2}$

Ambos son irreducibles en $\mathbb{R}[x]$ porque son de segundo grado sin raíces en $\mathbb{R}$.

Luego la factorización de $h(x)$ en irreducibles en $\mathbb{R}[x]$ es:

$$h(x)=(x-\sqrt[5]{21})(x^2-2Re(z_1)x+|z_1|^2)\cdot(x^2-2Re(z_2)x+|z_2|^2)=$$
$$=(x-\sqrt[5]{21})(x^2-2\sqrt[5]{21}\cos\frac{2\pi}{5}x+\sqrt[5]{21^2})\cdot(x^2-2\sqrt[5]{21}\cos\frac{4\pi}{5}x+\sqrt[5]{21^2})$$

- En $\mathbb{Q}[x]$, $h(x)=x^5-21$ es irreducible por el Criterio de Irreducibilidad de Eisenstein aplicado para el primo 3 o para el 7.

4) $t(x)=x^5-25$

- En $\mathbb{C}[x]$

Las raíces de $t(x)$ en $\mathbb{C}$ son: $\sqrt[5]{25}$; $z_k=\sqrt[5]{25}(\cos\frac{2k\pi}{5}+i\,sen\frac{2k\pi}{5})$, $k=1,..,4$
$\overline{z_1}=z_4$, $\overline{z_2}=z_3$.

Luego la factorización en irreducibles en $\mathbb{C}[x]$ de $t(x)$ es:

$t(x)=(x-\sqrt[5]{25})\cdot[x-\sqrt[5]{25}(\cos\frac{2\pi}{5}+i\,sen\frac{2\pi}{5})]\cdot[x-\sqrt[5]{25}(\cos\frac{2\pi}{5}-i\,sen\frac{2\pi}{5})]\cdot$
$\cdot[x-\sqrt[5]{25}(\cos\frac{4\pi}{5}+i\,sen\frac{4\pi}{5})]\cdot[x-\sqrt[5]{25}(\cos\frac{4\pi}{5}-i\,sen\frac{4\pi}{5})]$

- En $\mathbb{R}[x]$

$[x-\sqrt[5]{25}(\cos\frac{2\pi}{5}+i\,sen\frac{2\pi}{5})]\cdot[x-\sqrt[5]{25}(\cos\frac{2\pi}{5}-i\,sen\frac{2\pi}{5})] = x^2-2Re(z_1)x+|z_1|^2$

donde $Re(z_1)=\sqrt[5]{25}\cos\frac{2\pi}{5}$; $|z_1|^2=\sqrt[5]{5^4}$

$[x-\sqrt[5]{25}(\cos\frac{4\pi}{5}+i\,sen\frac{4\pi}{5})]\cdot[x-\sqrt[5]{25}(\cos\frac{4\pi}{5}-i\,sen\frac{4\pi}{5})] = x^2-2Re(z_2)x+|z_2|^2$

donde $Re(z_2)=\sqrt[5]{25}\cos\frac{4\pi}{5}$; $|z_2|^2=\sqrt[5]{5^4}$

Ambos son irreducibles en $\mathbb{R}[x]$ porque son de segundo grado sin raíces en $\mathbb{R}$.

Luego la factorización de $t(x)$ en irreducibles en $\mathbb{R}[x]$ es:

$$t(x) = (x-\sqrt[5]{25})(x^2 - 2\sqrt[5]{25}\cos\frac{2\pi}{5}x + \sqrt[5]{5^4})(x^2 - 2\sqrt[5]{25}\cos\frac{4\pi}{5}x + \sqrt[5]{5^4})$$

- En $\mathbb{Q}[x]$

  No podemos usar el Criterio de Irreducibilidad de Eisenstein para demostrar la irreducibilidad de $t(x)$ porque 5 es el único divisor primo de los coeficientes de $t(x)$, excepto el coeficiente principal, pero 5^2 sí divide al término independiente.

  Como $t(x)$ es un polinomio en $\mathbb{Q}[x]$ que tiene a $\sqrt[5]{25}$ como raíz, si no fuera irreducible, existiría un polinomio mónico de grado mínimo y menor que 5 que tendría a $\sqrt[5]{25}$ como raíz; él sería irreducible y dividiría a $t(x)$.

  Sea $p(x)$ tal polinomio. Obviamente $gr(p(x)) > 1$ pues $\sqrt[5]{25} \notin \mathbb{Q}$.
  Si $gr(p(x)) = 2$, como $p(x) \in \mathbb{Q}[x] \Rightarrow p(x) \in \mathbb{R}[x]$. Si z es raíz de $p(x)$,
  también lo es $\overline{z}$; como las raíces complejas de $p(x)$ son raíces complejas de $t(x) \Rightarrow$ $z = z_k$ para algún $k = 1,2,3,4$

  $\therefore \quad q(x) = (x^2 - 2\sqrt[5]{25}\cos\frac{2\pi}{5}x + \sqrt[5]{5^4}) \mid p(x) \quad \vee$

  $h(x) = (x^2 - 2\sqrt[5]{25}\cos\frac{4\pi}{5}x + \sqrt[5]{5^4}) \mid p(x)$

  además $(x-\sqrt[5]{25}) \mid p(x)$, todo en $\mathbb{R}[x]$, pero $(q(x), (x-\sqrt[5]{25})) = 1 \wedge$
  $(h(x), (x-\sqrt[5]{25})) = 1 \quad \therefore \quad q(x).(x-\sqrt[5]{25})) \mid p(x) \vee h(x).(x-\sqrt[5]{25})) \mid p(x)$ por lo cual $gr(p(x)) > 2$

  Si $gr(p(x)) = 3$ entonces $p(x) = (x-\sqrt[5]{25}).q(x) \vee p(x) = (x-\sqrt[5]{25}).h(x)$
  pero $(x-\sqrt[5]{25}).q(x) \notin \mathbb{Q}[x] \wedge (x-\sqrt[5]{25}).h(x) \notin \mathbb{Q}[x]$ (verificarlo)
  $\therefore \quad gr(p(x)) > 3.$

  Si $gr(p(x)) = 4$, como $p(x) \in \mathbb{Q}[x]$, $t(x) = x^5 - 25 \in \mathbb{Q}[x] \wedge p(x) \mid t(x)$,
  por el Algoritmo de la División en $\mathbb{Q}[x]$ el cociente $\frac{t(x)}{p(x)} \in \mathbb{Q}[x]$, pero
  $\frac{t(x)}{p(x)} = s(x)$ con $gr(s(x)) = 1 \wedge s(x) \in \mathbb{Q}[x]$!! (absurdo!) porque no hay
  ningún polinomio de grado 1 en $\mathbb{Q}[x]$ que divida a $t(x) \quad \therefore \quad gr(p(x)) > 4$.
  Por lo tanto $p(x) = t(x) = x^5 - 25$, y $t(x) = x^5 - 25$ es irreducible en $\mathbb{Q}[x]$

6) $q(x) = x^5 - 6^5$

- En $\mathbb{C}[x]$

  Las raíces de $q(x)$ en $\mathbb{C}$ son: 6, $z_k = 6\omega_k$ donde $\omega^5 = 1$.

  $\omega_k = cos\frac{2k\pi}{5} + i\, sen\frac{2k\pi}{5}$, $k = 1, 2, 3, 4$

  $q(x) = x^5 - 6^5 = (x-6)(x-z_1)(x-z_2)(x-z_3)(x-z_4)$

- En $\mathbb{R}[x]$

  $z_4 = \overline{z}_1 \ \wedge \ z_3 = \overline{z}_2$

  $q(x) = x^5 - 6^5 = (x-6)(x^2 - 2Re(z_1)x + |z_1|^2)(x^2 - 2Re(z_2)x + |z_2|^2)$

  donde los polinomios de segundo grado son irreducibles porque no tienen raíces en $\mathbb{R}$.

- En $\mathbb{Q}[x]$

  Veamos que $q(x) = x^5 - 6^5 = (x-6)(x^4 + 6x^3 + 6^2x^2 + 6^3x + 6^4)$ es el producto de irreducibles en $\mathbb{Q}[x]$.

  Las raíces de $(x^4 + 6x^3 + 6^2x^2 + 6^3x + 6^4)$ son z_1 , z_2 , z_3 , z_4 , por lo tanto en $\mathbb{R}[x]$, $(x^2 - 2Re(z_1)x + |z_1|^2) \mid q(x) \ \wedge \ (x^2 - 2Re(z_2)x + |z_2|^2) \mid q(x)$.

  $x^2 - 2Re(z_1)\, x + |z_1|^2 = x^2 - 12cos\frac{2\pi}{5}x + 36 \notin \mathbb{Q}[x]$ pues si $cos\frac{2\pi}{5} \in \mathbb{Q}$ el polinomio $x^2 - 2cos\frac{2\pi}{5}x + 1 \in \mathbb{Q}[x]$ (que tiene a $\omega_1 \ \wedge \ \omega_4$ como raíces) verifica que $(x^2 - 2cos\frac{2\pi}{5}x + 1) \mid (x^4 + x^3 + x^2 + x + 1)$!! pues $x^4 + x^3 + x^2 + x + 1$ es irreducible en $\mathbb{Q}[x]$ (polinomio ciclotómico de orden 5).

  Análogamente para $x^2 - 2Re(z_2)\, x + |z_2|^2$

  $\therefore$ la factorización en irreducibles en $\mathbb{Q}[x]$ es:

  $$q(x) = x^5 - 6^5 = (x-6)(x^4 + 6x^3 + 6^2x^2 + 6^3x + 6^4)$$

APÉNDICE

Grupo de las raíces n-ésimas de la unidad

Hemos viso que el $(\mathbb{C}-\{0\}, .)$ constituye un grupo (el grupo de unidades del cuerpo $\mathbb{C}$ de números complejos); éste es obviamente, un grupo infinito. Dentro de este grupo podemos distinguir un subgrupo $\mathbb{S}^1$ de los complejos pertenecientes a la circunferencia unidad, o sea $\mathbb{S}^1 = \{ z \in \mathbb{C} \ / \ |z| = 1 \}$.

- $\mathbb{S}^1 \underset{sg}{\subset} \mathbb{C}-\{0\}$ dado que es no vacío, puesto que $1 \in \mathbb{S}^1$; además
- si $z_1, z_2 \in \mathbb{S}^1 \Rightarrow z_1 \cdot z_2 \in \mathbb{S}^1$
  ya que si $|z_1| = |z_2| = 1$ entonces $|z_1 . z_2| = |z_1| . |z_2| = 1 . 1 = 1$;
- y si $z \in \mathbb{S}^1 \Rightarrow z^{-1} \in \mathbb{S}^1$,
  porque $|z^{-1}| = |z|^{-1} = 1^{-1} = 1$.

Este grupo también es infinito.

Para cada $n \in \mathbb{N}$ definimos el conjunto $\mathfrak{S}_n = \{ z \in \mathbb{C} \ / \ z^n = 1 \}$.

Veamos que $\mathfrak{S}_n \underset{sg}{\subset} \mathbb{S}^1 \ \forall n \in \mathbb{N}$.

- $\mathfrak{S}_n \neq \phi$ puesto que $1 \in \mathfrak{S}_n$
- si $z_1 , z_2 \in \mathfrak{S}_n \Rightarrow z_1 . z_2^{-1} \in \mathfrak{S}_n$
  pues $(z_1 . z_2^{-1})^n = z_1^n . (z_2^{-1})^n = z_1^n . (z_2^n)^{-1} = 1 . 1 = 1$.

En estos casos tenemos grupos finitos, y más precisamente cada $\mathfrak{S}_n$ es de n elementos.

Al grupo $\mathfrak{S}_n$ se lo denomina *grupo de las raíces n-ésimas de la unidad.*

Raíces n-ésimas primitivas

Sea $\mathfrak{u} \in \mathbb{C}$ para el cual $\exists m \in \mathbb{N}$ tal que $\mathfrak{u}^m = 1$. Sea $n = mín\{ h \in \mathbb{N} \ / \ \mathfrak{u}^h = 1 \}$.

Entonces, para $\mathfrak{u}$ se verifica:

***Teorema*:**

i. Para $m \in \mathbb{Z}$, $\mathfrak{u}^m = 1$ si y sólo si $n \mid m$.

ii. $\mathfrak{u}^k = \mathfrak{u}^h$ si y sólo si $k \equiv h \ (mód\ n)$.

***Demostración*:**

Observemos primero que si $z^n = 1 \Rightarrow (z^k)^n = 1 \ \forall k \in \mathbb{Z}$.

i. $\Rightarrow$) Sea $m \in \mathbb{Z}$ tal que $\mathfrak{u}^m = 1$.

Aplicando el Algoritmo de la División tenemos que $m = q.n + r$ con $0 \leq r < n$

$$1 = \mathfrak{u}^m = \mathfrak{u}^{qn+r} = (\mathfrak{u}^n)^q \mathfrak{u}^r = \mathfrak{u}^r$$

como $\mathfrak{u}^r = 1$, $r < n \ \wedge \ n = mín\{ h \in \mathbb{N} \ / \ \mathfrak{u}^h = 1 \} \ \Rightarrow \ r = 0$

$\therefore \quad n \mid m$.

$\Leftarrow$) Si $m \in \mathbb{Z}$ es tal que $n \mid m \ \Rightarrow \ \exists k \in \mathbb{Z}$ tal que $m = n.k$.
Luego $\mathfrak{u}^m = \mathfrak{u}^{q.n} = (\mathfrak{u}^n)^q = 1^q = 1$

ii. $\mathfrak{u}^k = \mathfrak{u}^h \ \Leftrightarrow \ \mathfrak{u}^{k-h} = 1 \ \Leftrightarrow \ n \mid (k-h) \ \Leftrightarrow \ k - h \equiv 0 \ \ (mód\ n) \ \Leftrightarrow$
$\Leftrightarrow \ \ k \equiv h \ \ (mód\ n)$.

***Corolario*:** $\mathfrak{S}_n$ es un grupo cíclico y $\mathfrak{u}$ es un generador.

***Demostración*:** $\mathfrak{u} \in \mathfrak{S}_n$, por lo tanto $\mathfrak{u}^k \in \mathfrak{S}_n \quad \forall k \in \mathbb{Z}$, luego $(\mathfrak{u}) \subset \mathfrak{S}_n$, pero el grupo cíclico generado por $\mathfrak{u}$ es $(\mathfrak{u}) = \{ \mathfrak{u}^0 = 1, \mathfrak{u}, \mathfrak{u}^2, \mathfrak{u}^3, \mathfrak{u}^4, ..., \mathfrak{u}^{n-1} \}$. Como ambos son finitos y de n elementos, y $(\mathfrak{u}) \subset \mathfrak{S}_n$ se verifica que $(\mathfrak{u}) = \mathfrak{S}_n$.

***Definición*:** Sean $n \in \mathbb{N}$, $n > 1$, $\mathfrak{u}$ una raíz n-ésima de la unidad, se dice que $\mathfrak{u}$ es una *raíz n-ésima primitiva* si es un generador de $\mathfrak{S}_n$, o sea, si $n = mín\{ h \in \mathbb{N} / u^h = 1 \}$.

Ejemplo:

Por lo que hemos visto oportunamente, $\omega = cos\frac{2\pi}{n} + i\, sen\frac{2\pi}{n}$, es una raíz n-ésima primitiva de la unidad, porque $\omega^n = cos\frac{2n\pi}{n} + i\, sen\frac{2n\pi}{n} = cos 2\pi + i\, sen 2\pi = 1$, y $\omega^k = cos\frac{2k\pi}{n} + i\, sen\frac{2k\pi}{n}$ es raíz n-ésima de la unidad $\forall k$, $k = 0, 1, 2, 3, \ldots, n-1$, por lo que tenemos que $\mathfrak{S}_n = \{ \omega^k \ / \ k = 0, 1, 2, ..., n-1 \}$, con lo cual $\mathfrak{S}_n$ es un grupo cíclico de orden n y ω es un generador.

Ejemplos: $\mathfrak{S}_1 = \{ 1 \}$; $\mathfrak{S}_2 = \{ 1, -1 \}$; $\mathfrak{S}_3 = \left\{ 1, -\frac{1}{2} + \frac{\sqrt{3}}{2} i, -\frac{1}{2} - \frac{\sqrt{3}}{2} i \right\}$

$\mathfrak{S}_4 = \{ 1, \ i, -1, -i \}$, $\mathfrak{S}_6 = \left\{ 1, \ \frac{1}{2} + \frac{\sqrt{3}}{2} i, \ -\frac{1}{2} + \frac{\sqrt{3}}{2} i, \ -1, \ -\frac{1}{2} - \frac{\sqrt{3}}{2} i, \ \frac{1}{2} - \frac{\sqrt{3}}{2} i \right\}$

Para cada $n \in \mathbb{N}$, $\omega = cos\frac{2\pi}{n} + i\, sen\frac{2\pi}{n}$ es una raíz n-ésima primitiva de la unidad,

Por lo tanto -1 genera $\mathfrak{S}_2$, $-\frac{1}{2} + \frac{\sqrt{3}}{2} i$ genera $\mathfrak{S}_3$, i genera $\mathfrak{S}_4$ y $\frac{1}{2} + \frac{\sqrt{3}}{2} i$ genera $\mathfrak{S}_6$.

***Teorema*:** Sea $\mathfrak{u}$ es una raíz n-ésima primitiva de 1,
$\mathfrak{u}^k$ es raíz n-ésima primitiva de 1 si y sólo si $(n, k) = 1$.

***Demostración*:**

$\Rightarrow$) Si $\mathfrak{u}^k$ es raíz *n*-ésima primitiva de 1 es un generador de $\mathfrak{S}_n$, por lo tanto todas las raíces *n*-ésimas de la unidad se pueden escribir como potencia de $\mathfrak{u}^k$, en particular $\mathfrak{u}$; luego $\exists h \in \mathbb{N}$, $0 < h < n$, $(\mathfrak{u}^k)^h = \mathfrak{u}$, por el teorema anterior eso significa que $k.h \equiv 1$ $(mód\ n)$ $\therefore$ $(k\ ,\ n) = 1$.

$\Leftarrow$) Recíprocamente, si $(k\ ,\ n) = 1$ $\exists q, v \in \mathbb{Z}$ tales que $q.k + v.n = 1$.

Por lo tanto $\mathfrak{u} = \mathfrak{u}^{qk+vn} = \mathfrak{u}^{qk}\mathfrak{u}^{vn} = (\mathfrak{u}^k)^q(\mathfrak{u}^n)^v = (\mathfrak{u}^k)^q$.

Veamos que $\mathfrak{u}^k$ es generador de $\mathfrak{S}_n$ y por tanto raíz *n*-ésima primitiva de 1.

Sea $z \in \mathfrak{S}_n$, como $\mathfrak{u}$ es raíz *n*-ésima primitiva de 1 , $\exists m \in \mathbb{N}_0$, $0 \leq m < n$ tal que $\mathfrak{u}^m = z$

$\therefore$ $z = \mathfrak{u}^m = ((\mathfrak{u}^k)^q)^m = (\mathfrak{u}^k)^{q.m}$ donde $q.m \in \mathbb{Z}$. Así todo elemento de $\mathfrak{S}_n$ se escribe como una potencia de $\mathfrak{u}^k$ lo que demuestra que es un generador de $\mathfrak{S}_n$, y por consiguiente una raíz *n*-ésima primitiva de 1.

Ejercicios:

1. Sea A un dominio de integridad. Definimos en $A\times A$ las siguientes dos operaciones
$(a\,,\,b)+(c\,,\,d) =: (a+c\,,\,b+d)$
y $(a\,,\,b)\cdot(c\,,\,d) =: (a.c-b.d\,,\,a.d+b.c)$.

Con estas operaciones, demostrar que $(A\times A\,,+\,,\cdot\,)$ es un anillo conmutativo con identidad.

2. Demostrar que $\mathbb{Z}_3(i)$, $\mathbb{Z}_7(i)$, $\mathbb{Z}_{11}(i)$ son cuerpos.

3. Calcular todos los valores posibles de : i^n , $\sum_{k=0}^{n} i^k$, $\prod_{k=0}^{n} i^k$, $n\in\mathbb{N}$. Justificar.

4. Demostrar las propiedades de la conjugación: para z , $z'\in\mathbb{C}$.
   i. $\overline{z+z'}=\overline{z}+\overline{z'}$
   ii. $\overline{z.z'}=\overline{z}.\overline{z'}$
   iii. $\overline{z}=0 \Leftrightarrow z=0$
   iv. $\overline{z}=z \Leftrightarrow z\in\mathbb{R}$
   v. $z+\overline{z}=2\,Re(z)$
   vi. $z-\overline{z}=2i\,Im(z)$
   vii. Si $z\neq 0$, $\overline{z}^{-1}=\overline{z^{-1}}$
   viii. $\overline{\overline{z}}=z$

5. Para z , $z'\in A(i)$, demostrar que $N(z.z')=N(z)\,.\,N(z')$.

6. Demostrar las propiedades de la norma: para $z\in\mathbb{C}$.
   i. $N(z)\geq 0$, y $N(z)=0 \Leftrightarrow z=0$.
   ii. $N(a)=a^2 \quad \forall a\in\mathbb{R}$.
   iii. $N(z)\geq (Re(z))^2 \;\wedge\; N(z)\geq (Im(z))^2$.
   iv. $N(z)=N(\overline{z})$.

7. Sean $z, z'\in\mathbb{C}$. Hallar una condición necesaria y suficiente para que $z+z'\in\mathbb{R}$ y para que $z.z'\in\mathbb{R}$.

8. Demostrar las propiedades del módulo : para z , $z'\in\mathbb{C}$.
   i. $|z|\geq 0$, $|z|=0 \Leftrightarrow z=0$.
   ii. $|z.z'|=|z|\,.\,|z'|$.
   iii. $|\overline{z}|=|z|$.
   iv. $|z|\geq|Re(z)|\geq Re(z) \;\wedge\; |z|\geq|Im(z)|\geq Im(z)$.
   v. $|z|^{-1}=|z^{-1}|$ para $z\neq 0$.
   vi. $z^{-1}=\overline{z} \Leftrightarrow |z|=1$.
   vii. $|z+z'|\leq|z|+|z'|$ (Desigualdad Triangular o de *Minkowski*).

9. Hallar y graficar en el plano complejo, todos los complejos $z\in\mathbb{C}$, que satisfacen:
   i. $\overline{z}=z$ ii. $z.\overline{z}=1$ iii. $\overline{z}=-z$ iv. $|z|\leq 1$
   v. $1\leq|z|\leq 2$ vi. $Re(z)=5$ vii. $Re\,(z)=-Im(z)$ viii. $|z-i|\leq 4$

ix. $|z-1| \leq 4$ x. $arg\, z \leq \frac{\pi}{4}$ xi. $z = -z$ xii. $arg\, z^2 \leq \frac{3\pi}{2}$

xiii. $z = z^{-1}$ xiv. $|z| = 1$ xv. $\frac{\pi}{2} \leq arg\, z \leq \frac{3\pi}{4}$

xvi. $\frac{\pi}{2} \leq arg\, z^2 \leq \pi$ xvii. $|Re(iz)|^2 + |Re(z)|^2 \geq 4 \quad \wedge \quad \frac{\pi}{2} \leq arg(z^2) \leq \frac{3\pi}{2}$

10. Demostrar que $[cos(\alpha) + i.\, sen(\alpha)]^n = cos(n\alpha) + i.\, sen(n\alpha) \quad \forall n \in \mathbb{N}, \ \alpha \in \mathbb{R}$.

11. Determinar y graficar todos los $z \in \mathbb{C}$ tales que:

i. $|z| = 3 \quad y \quad arg\,(-z^3) = arg((-1+i).\overline{z}^2)$ ii. $\begin{cases} z^5 = (\sqrt{3}+i)\overline{z}^3 \\ \frac{\pi}{2} \leq arg(z+iz) \leq \pi \end{cases}$

iii. $|z| = 1$ e $Im\,(\frac{1}{2} - z + 3i) \geq 2$ iv. $z^5\overline{z} + z\,\overline{z} = 9 + 9z^4$

v. $3z^{12} + 5|z|^{12} - 8 = 0$ vi. $|Re(z) + i(z - \overline{z})| \leq 3 \quad \wedge \quad \pi \leq arg\, z^2 \leq \frac{3\pi}{2}$

12. Sea $z \in \mathbb{C}$. Probar que $|Re(z) + Im(z)| \leq \sqrt{2}|z|$ y vale la igualdad sii $Re(z) = Im(z)$.

13. Sea $z = cos\frac{6}{7}\pi + i\, sen\frac{6}{7}\pi$, expresar en forma trigonométrica los complejos: z^{-1}, $\overline{z}$, z^2.

14. Encontrar todos los $z \in \mathbb{C}$, tales que:

i. $|z| - z = 1 + 2i$ ii. $|z| + z = 2 + i$

15. Calcular las raíces : i. cúbicas de : $2i$, $1 + i$, 1
ii. sextas de : -1, $(1 + i)$: $(1 + 3i)$
iii. cuartas de : 1, $1 - i$
iv. quintas de: 2, $2 + i$

16. Determinar y graficar todos los complejos z tales que:

i. $z^2 = -1$ ii. $z^2 = 2 - 3i$ iii. $z^2 = 1 + i$ iv. $z^3 = 1 - i$

v. $z^4 = -1$ vi. $z^4 + i = 0$ vii. $z^2 = (5+3i)^2$ viii. $(z^2 - 3z + 1)^4 = 1$

17. i. Sea w una raíz cuarta de $-i$. Hallar todos los $z \in \mathbb{C}$ que verifiquen:
$$z^3 = w^{12} + w^{10} - 15\, w^4 + w^2$$
ii. Sea w raíz cúbica de 1. Determinar los posibles valores de:
$(1 - w).(1 - w^2).(1 - w^4).(1 - w^5)$; de w^n y de w^{-n}, con $n \in \mathbb{N}$.

18. Calcular y expresar en forma binómica las raíces sextas de i (Calcular los valores de seno y coseno).

19. Encontrar todos los complejos z tales que:

i. $(z-1)^2 = (\overline{z}-1)^4$ ii. $(z + 1)^3 = z^3$ iii. $(z - 1)^6 = z^6$ iv. $z^5 = -3\,\overline{z}^4$

v. $|z|^6 = z^6$ vi. $|z-(1+i)|^6 = (z-(1+i))^6$ vii. $1+z^3+z^6+z^9=0$

Representar gráficamente.

20. i. Sea K un cuerpo algebraicamente cerrado, $f(x)$, $g(x) \in K[x]$. Demostrar que $(f(x)$, $g(x)) = 1$ sii $f(x)$ y $g(x)$ no admiten ninguna raíz común en K.

ii. Si $f(x)$, $g(x) \in \mathbb{Q}[x]$, demostrar que $(f(x)$, $g(x)) = 1$ sii $f(x)$ y $g(x)$ no admiten ninguna raíz común en $\mathbb{C}$.

21. Determinar todas las raíces en $\mathbb{C}$, de los siguientes polinomios:

i. $p(x) = x^5 - 32$ ii. $p(x) = i\,x^2 - x + i$

iii. $p(x) = x^2 + x - 1$ iv. $p(x) = x^2 - (1+i)\,x - 1$

v. $p(x) = 2x^4 - 3x^3 + x^2 + 4x - 2$ sabiendo que $1+i$ es raíz.

vi. $p(x) = x^5 - 3x^4 + 2x^3 - 6x^2 - 8x + 24$ sabiendo que $2i$ es raíz.

vii. $p(x) = 2x^5 + x^4 + x^3 + 21x^2 + 9x - 10$ sabiendo que $1+2i$ es raíz.

viii. $p(x) = -2ix^2 + (2-i)\,x + 1 + i$

22. Expresar los siguientes polinomios como producto de irreducibles en:

i. $\mathbb{Q}[x]$ ii. $\mathbb{R}[x]$ iii. $\mathbb{C}[x]$

a) $p(x) = x^4 + 1$ b) $p(x) = x^6 - a^6$, $a \in \mathbb{R}$

c) $p(x) = 2(x-1)^5 + (x-1)^4 + 18(x-1)^3 + 9(x-1)^2$

d) $p(x) = x^7 - x^6 - 2x^5 - 2x^4 - 2x^3 - 2x^2 - 3x - 1$, sabiendo que $1+\sqrt{2}$ es raíz.

e) $p(x) = x^5 - x^4 + 2x^3 - 2x^2 - 8x + 8$

f) $p(x) = x^9 - 6x^5 - 4x^4 + 24$

g) $p(x) = x^9 + 4x^7 - 2x^5 + 8x^4 + 32x^2 - 16$

h) $p(x) = x^8 - 3x^7 + 2x^6 + 2x^5 - 3x^4 - 3x^3 + 2x^2 + 2x - 4$ sabiendo que, al menos, una de las raíces octavas de 1 es raíz de $p(x)$.

i) $p(x) = x^5 - 16$

j) $p(x) = x^5 - 6^5$

23. Sea $p(x) = 2x^5 + ix - 3 \in \mathbb{C}[x]$. Demostrar que:

i. Si $z \in \mathbb{C}$ es raíz de $p(x)$, ¿ también lo es $\overline{z}$?

ii. $p(x)$ no admite raíces reales.

iii. Si $f(x) \in \mathbb{R}[x]$ es tal que $p(x) \mid f(x) \Rightarrow (2x^5 - ix - 3) \mid f(x)$.

24. Factorizar $f(x) = 3x^5 + 5x^4 + x^3 - x^2 - 3x + 1$ en $\mathbb{Q}[x]$, en $\mathbb{R}[x]$ y en $\mathbb{C}[x]$, sabiendo que no es coprimo con el polinomio $g(x) = x^4 + 3x - 2$. Justificar.

25. Sea $f(x) = x^{20} + 8x^{10} + 2a$. Encontrar todos los valores $a \in \mathbb{C}$ para los cuales $f(x)$ admita, al menos, una raíz múltiple. Para cada valor a hallado, determinar todas las raíces del polinomio, indicando en cada caso, su multiplicidad.

26. Factorizar en $\mathbb{C}[x]$ $f(x) = x^6 + ix^5 - 2x^4 - 4ix^3 + 4x^2 + 4ix + 8$ sabiendo que tiene una raíz real múltiple.

27. Factorizar el polinomio $f(x) = \sqrt{5}x^3 + 10x^2 + 5x + 10\sqrt{5}$ en $\mathbb{R}[x]$ y en $\mathbb{C}[x]$ sabiendo que tiene una raíz que es imaginario puro.

28. i. Probar que si w es raíz n-ésima primitiva de 1, entonces para $m \in \mathbb{Z}$ $w^m = 1$ sii $n \mid m$.

ii. Probar que $w_n = cos\frac{2\pi}{n} + i\ sen\frac{2\pi}{n}$ es raíz n-ésima primitiva de 1.

iii. Probar que si w es raíz n-ésima primitiva de 1, entonces w^k, $k \in \mathbb{N}$, también lo es sii $(k, n) = 1$.

29. Encontrar las raíces n-ésimas primitivas de la unidad para $n = 2, 3, 4, 5, 6, 8, 9$.

30. Demostrar que $-1 \in \mathfrak{S}_n$ si y sólo si n es par.

31. Demostrar que si ω es una raíz n-ésima de la unidad, $\omega \neq 1$, entonces ω es raíz del polinomio $f(x) = \sum_{i=0}^{n-1} x^i$.

32. Demostrar que si ω es una raíz n-ésima primitiva de la unidad entonces:

i. $\sum_{j=0}^{n-1} \omega^j = 0$ ii. $\prod_{j=0}^{n-1} \omega^j = (-1)^{n-1}$

33. Sean $\omega, \mu \in \mathfrak{S}_5$ primitivas. Probar que $(\omega^{16} + \mu^{41})^5 \in \mathbb{R}$.

34. Toda raíz de la unidad es primitiva de algún orden, o sea, si $\omega \in \mathbb{C}$ es tal que $\omega^k = 1$ para algún $k \in \mathbb{N} \Rightarrow \exists h \in \mathbb{N}$ tal que ω es raíz h-ésima primitiva de 1.

35. Demostrar que $\mathfrak{S}_n \subsetneq \mathfrak{S}_m$ si y sólo si $n \mid m$.

36. Sean $n, m \in \mathbb{N}$. El polinomio $(x^n - 1) \mid (x^m - 1)$ sii $n \mid m$.

37. Sean $n, m \in \mathbb{N}$, $d = (n, m)$. Demostrar que $\mathfrak{S}_n \cap \mathfrak{S}_m = \mathfrak{S}_d$.

38. Demostrar que el polinomio $f(x) = \sum_{i=0}^{n-1} x^i$ es irreducible en $\mathbb{Q}[x]$ sii n es primo (cuando n es primo el polinomio es el que llamamos *polinomio ciclotómico de orden* n).

39. Sean $n, m \in \mathbb{N}$, $d = (n, m)$. Demostrar que $((x^n - 1), (x^m - 1)) = (x^d - 1)$.

40. Sea la sucesión $\{\mathfrak{S}_n\}_{n \in \mathbb{N}}$. Encontrar elementos maximales y/o minimales, si los hubiera. ¿Admite máximos y/o mínimos?
Si consideramos la sucesión $\{\mathfrak{S}_n\}_{n \in \mathbb{N} - \{1\}}$ hallar en ella los elementos minimales.

41. Sea $p \in \mathbb{N}$ primo. Demostrar que la cadena $\{\mathfrak{S}_{p^n}\}_{n \in \mathbb{N}_0}$ es estrictamente creciente,
o sea que: $\{1\} \subsetneq \mathfrak{S}_p \subsetneq \mathfrak{S}_{p^2} \subsetneq \mathfrak{S}_{p^3} \subsetneq \ldots\ldots \subsetneq \mathfrak{S}_{p^k} \subsetneq \mathfrak{S}_{p^{k+1}} \subsetneq \ldots.$

42. Decir si la cadena $\{\mathfrak{S}_{p^n}\}_{n \in \mathbb{N}_0}$ admite cotas inferiores y/o superiores en $\mathbb{S}^1$, máximos y/o mínimos ($p \in \mathbb{N}$ primo).

43. Demostrar que $\mathfrak{S}_{p^\infty} = \bigcup_{k\in\mathbb{N}} \mathfrak{S}_{p^k}$ es un subgrupo infinito de $\mathbb{S}^1$ ($p \in \mathbb{N}$ primo).

44. ¿Es el conjunto $\mathfrak{D} = \bigcup_{n\in\mathbb{N}} \mathfrak{S}_n$ un subgrupo de $\mathbb{S}^1$?

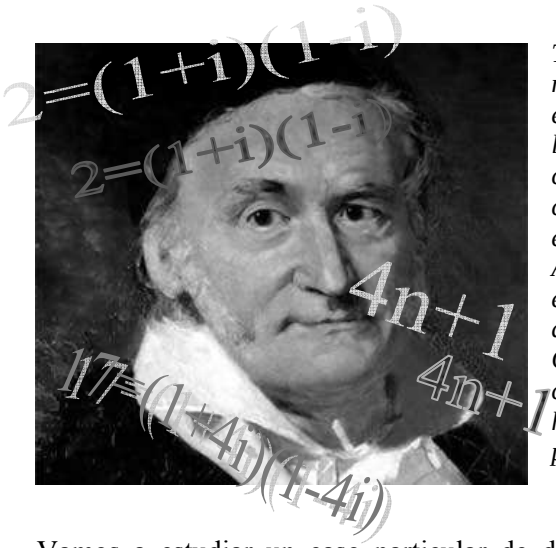
45. ¿Todo elemento de $\mathbb{S}^1$ es raíz n-ésima de la unidad para algún $n \in \mathbb{N}$?

46. Demostrar que la aplicación $\psi: \mathbb{Z}_n \to \mathfrak{S}_n$ definida por $\psi(\overline{k}) = \omega^k$ es un isomorfismo de grupos (Primero hay que demostrar que la aplicación está bien definida, o sea, que no depende del particular representante que elijamos en $\overline{k}$).

ANEXO I

Ya vimos que el cuerpo $\mathbb{Q}$ de los números racionales es el cuerpo de fracciones del anillo de enteros $\mathbb{Z}$; nos ocuparemos de dos ejemplos que constituyen parte de la generalización de los enteros racionales a enteros algebraicos. Los *enteros algebraicos* son aquéllos números complejos que son raíz de un polinomio mónico en $\mathbb{Z}[x]$. Analizaremos dos ejemplos concretos de anillo de enteros algebraicos en dos cuerpos cuadráticos particulares:
$\mathbb{Q}(i)$ y $\mathbb{Q}(\omega)$, con ω una raíz cúbica primitiva de 1, veremos sus similitudes, incluso con $\mathbb{Z}$, y sus diferencias.

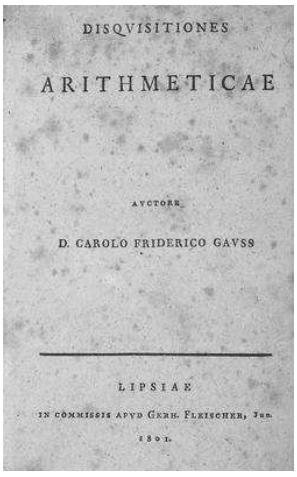
Enteros de Gauss



Tanto el conjunto de los números enteros como el de los números complejos son, a esta altura, bien conocidos. Sin embargo, cabe preguntarse qué ocurriría si "mezclamos" las definiciones de ambos. En otras palabras, ¿sería útil considerar el subconjunto de C formado por los números complejos cuyas partes real e imaginaria son números enteros?
Aunque en realidad la motivación de Gauss en 1832 fue el estudio sobre sumas de cuadrados, es posible que fuera algo así lo que pensó al introducir este conjunto.
Gauss encontró un conjunto realmente especial, actualmente conocido como el anillo de enteros de Gauss. En este anexo hablaremos sobre él y sobre sus interesantes y curiosas propiedades.

Vamos a estudiar un caso particular de dominio euclidiano, el anillo de *enteros gaussianos o enteros de Gauss*. Este ejemplo es importante, porque en este anillo se pueden demostrar propiedades de números enteros racionales en general y primos en particular.

***Definición*:** A los números complejos de la forma $z = a + bi$ con $a, b \in \mathbb{Z}$ se los denomina *enteros gaussianos* o *enteros de Gauss*.
El anillo con identidad $\mathbb{Z}[i] = \{ a + bi \ / \ a, b \in \mathbb{Z} \}$ se denomina *anillo de enteros gaussianos* o *anillo de enteros de Gauss.* Claramente este anillo tiene la propiedad de contener a $\mathbb{Z}$ y estar contenido en el cuerpo $\mathbb{C}$. Justamente por ser $\mathbb{Z}[i] \underset{suba}{\subset} \mathbb{C}$ tenemos que es un dominio de integridad.


DISQVISITIONES
ARITHMETICAE
AVCTORE
D. CAROLO FRIDERICO GAVSS
LIPSIAE
IN COMMISSIS APVD GERH. FLEISCHER, Jun.
1801.

En las Disquisitiones, incluía Gauss el Teorema Fundamental de la Aritmética, uno de los principios básicos que continúa siendo válido en el dominio de integridad de los enteros de Gauss. De hecho, a cualquier dominio de integridad con la propiedad de factorización única se le conoce hoy con el nombre de "dominio de integridad gaussiano"
("Historia de la Matemática", Carl B. Boyer).

El grupo de unidades de $\mathbb{Z}[i]$, $(\mathbb{Z}[i])^* = \{1, -1, i, -i\}$, ya que $z \in \mathbb{Z}[i]$ es inversible si y sólo si $N(z)$ es inversible en $\mathbb{Z}$, y esto es si y sólo si $N(z) = 1$ (por ser $N(z) \geq 0$).
El cuerpo de cocientes de $\mathbb{Z}[i]$ es $\mathbb{Q}(i) = \{ r + si \ / \ r, s \in \mathbb{Q} \}$ que es también subcuerpo de $\mathbb{C}$. Para demostrar que $\mathbb{Q}(i)$ es el cuerpo de cocientes de $\mathbb{Z}[i]$ veamos que todo cociente de enteros de Gauss con denominador no nulo pertenece a $\mathbb{Q}(i)$, y recíprocamente, que todo complejo en $\mathbb{Q}(i)$ puede pensarse como cociente de enteros de Gauss.

Sea $\frac{a+bi}{c+di}$ con $a, b, c, d \in \mathbb{Z}$, $c \neq 0 \ \vee \ d \neq 0$;

$$\frac{a+bi}{c+di} = \frac{a+bi}{c+di} \cdot \frac{c-di}{c-di} = \frac{ac+bd+i(bc-ad)}{c^2+d^2} \quad \text{con} \quad c^2+d^2 \neq 0$$

llamando $r = \frac{ac+bd}{c^2+d^2} \in \mathbb{Q} \ \wedge \ s = \frac{bc-ad}{c^2+d^2} \in \mathbb{Q}$,

tenemos que $\frac{a+bi}{c+di} = r + si \in \mathbb{Q}(i)$.

Recíprocamente, si $r + si \in \mathbb{Q}(i)$, $r, s \in \mathbb{Q}$ $\therefore$ $r = \frac{a}{b} \ \wedge \ s = \frac{c}{d}$ con $a, b, c, d \in \mathbb{Z}$,

$b \neq 0 \ \wedge \ d \neq 0$; $r + si = \frac{a}{b} + \frac{c}{d} i = \frac{ad+bci}{bd}$ con $ad + bci \in \mathbb{Z}[i] \ \wedge \ bd \in \mathbb{Z}[i] - \{0\}$

Por lo tanto, $\mathbb{Q}(i)$ es el cuerpo de cocientes de $\mathbb{Z}[i]$.

***Teorema*:** $\mathbb{Z}[i]$ es dominio euclidiano.

***Demostración*:** Para demostrar que $\mathbb{Z}[i]$ es un dominio euclidiano debemos ver si existe una función $d : \mathbb{Z}[i] - \{0\} \rightarrow \mathbb{N}_0$ tal que:

i. $d(z_1) \leq d(z_1 z_2) \quad \forall z_1, z_2 \in \mathbb{Z}[i] - \{0\}$.

ii. Dados $z_1, z_2 \in \mathbb{Z}[i] - \{0\}$ $\exists u, v \in \mathbb{Z}[i]$ tales que $z_2 = u z_1 + v$ con $v = 0 \ \vee \ d(v) < d(z_1)$.

Veamos que la función $d(z) = N(z) = a^2 + b^2$ para $z = a + bi$, con $a, b \in \mathbb{Z}$ satisface las condiciones pedidas.

Claramente $N(z) \in \mathbb{N} \quad \forall z \in \mathbb{Z}[i] - \{0\}$.

Para ver que esta función cumple i. : sean $z_1, z_2 \in \mathbb{Z}[i] - \{0\}$, $N(z_1), N(z_2) \in \mathbb{N}$, luego $N(z_1) \geq 1 \ \wedge \ N(z_2) \geq 1$, y como $N(z_1 z_2) = N(z_1) N(z_2) \geq N(z_1)$.

Veamos ahora que también cumple ii. :

- ✓ Analizaremos primero el caso particular en el cual $z_1 = n \in \mathbb{N} \ \wedge \ z_2 = a + bi \in \mathbb{Z}[i]$

Por el Algoritmo de la División en $\mathbb{Z}$, $\exists \ q_1, q_2, r_1, r_2 \in \mathbb{Z}$ tales que $a = q_1 n + r_1$, $b = q_2 n + r_2$ con $0 \leq r_1 < n \ \wedge \ 0 \leq r_2 < n$. Si $\frac{n}{2} < r_1 < n$, entonces $0 < n - r_1 \leq \frac{n}{2}$ y $a = (q_1 + 1)n + r_1 - n$,

en este caso llamando $l_1 = q_1 + 1 \ \wedge \ t_1 = r_1 - n$, tenemos que siempre existen $l_1, t_1 \in \mathbb{Z}$ tales que $a = l_1 n + t_1$ con $|t_1| \leq \frac{n}{2}$. Análogamente para *b.*

Sean entonces $q_1, q_2, r_1, r_2 \in \mathbb{Z}$ tales que $a = q_1 n + r_1$, $b = q_2 n + r_2$ con $|r_1| \leq \frac{n}{2} \ \wedge \ |r_2| \leq \frac{n}{2}$. Entonces $z_2 = a + bi = (q_1 + q_2 i)n + r_1 + r_2 i = un + v$ con $u = q_1 + q_2 i \in \mathbb{Z}[i] \ \wedge \ v = r_1 + r_2 i \in \mathbb{Z}[i] \ \wedge \ N(v) = r_1^2 + r_2^2 \leq \frac{n^2}{4} + \frac{n^2}{4} < n^2 = N(n)$.

Luego, hemos demostrado que $\forall z \in \mathbb{Z}[i] \ \wedge \ \forall n \in \mathbb{N}, \ \exists u, v \in \mathbb{Z}[i]$ tales que $z = un + v$ con $v = 0 \ \vee \ d(v) < d(n)$.

✓ Sea ahora el caso general, $z_1, z_2 \in \mathbb{Z}[i] - \{0\}$. $z_1 \overline{z}_1 = |z_1|^2 = n \in \mathbb{N}$; aplicando el resultado anterior a n y a $z_2 \overline{z}_1$, vemos que $\exists u, v \in \mathbb{Z}[i]$ tales que $z_2 \overline{z}_1 = un + v$ con $v = 0 \ \vee \ d(v) < d(n)$.

Como $v = z_2 \overline{z}_1 - u z_1 \overline{z}_1 \ \wedge \ d(v) = N(v) = N(z_2 \overline{z}_1 - u z_1 \overline{z}_1) < d(n) = N(z_1 \overline{z}_1)$, tenemos que $N(z_2 \overline{z}_1 - u z_1 \overline{z}_1) = N[\overline{z}_1 (z_2 - u z_1)] = N(\overline{z}_1) N(z_2 - u z_1) < N(z_1) N(\overline{z}_1)$, y como $z_1 \neq 0$, entonces $N(z_1) \in \mathbb{N}$, con lo cual $N(z_2 - u z_1) < N(z_1)$. Llamando $w = z_2 - u z_1 \in \mathbb{Z}[i]$, tenemos que $z_2 = u z_1 + w$ con $w = 0 \ \vee \ d(w) = N(w) < N(z_1) = d(z_1)$, lo que prueba el teorema.

Ejemplo: Encontrar el cociente y el resto en la división de $z_2 = 8 + 7i$ por $z_1 = 3 + 4i$

$z_2 \overline{z}_1 = 52 - 11i$, $N(z_1) = 25$, $52 = 2 \times 25 + 2$, $-11 = 0 \times 25 - 11$.

$z_2 \overline{z}_1 = 52 - 11i = 2 \times 25 + 2 + i(0 \times 25 - 11) = 2 \times 25 + (2 - 11i)$ con $N(2 - 11i) < N(25)$

Sea $w = z_2 - 2 z_1 = 2 - i$ con $N(w) = N(2 - i) < N(z_1)$, entonces

$$z_2 = 8 + 7i = 2(3 + 4i) + (2 - i) \text{ donde } N(2 - i) < N(z_1).$$

***Corolario*:** $\mathbb{Z}[i]$ es dominio principal.

***Corolario*:** $\mathbb{Z}[i]$ es dominio factorial.

***Proposición*:** Sea $p \in \mathbb{N}$ primo y supongamos que $\exists c \in \mathbb{Z}$, $(p \ , \ c) = 1$ tal que $pc = x^2 + y^2$ para ciertos $x, y \in \mathbb{Z}$. Entonces $\exists a, b \in \mathbb{Z}$ tales que $p = a^2 + b^2$.

***Demostración*:** $\mathbb{Z} \underset{suba}{\subset} \mathbb{Z}[i]$, supongamos que p es también primo en $\mathbb{Z}[i]$.

Como $pc = x^2 + y^2 = (x + iy)(x - yi)$ entonces $p \mid (x + iy) \ \vee \ p \mid (x - iy)$.

Si $(x + iy) = p\,(n + mi)$ entonces $x = pn \ \wedge \ y = pm$ con lo cual p también divide a $(x - iy)$ y así $p^2 \mid pc$ con lo cual $p \mid c$!! (absurdo) pues $(p \ , c) = 1$. Luego p no es primo en $\mathbb{Z}[i]$. Análogamente si suponemos que $p \mid (x - iy)$.

Por lo tanto $p = (d + ei)(k + hi)$ con $d, e, k, h \in \mathbb{Z}$, y ninguno de los enteros de Gauss es una unidad en $\mathbb{Z}[i]$, o sea $d^2 + e^2 \neq 1 \ \wedge \ k^2 + h^2 \neq 1$. Como $p \in \mathbb{Z}$, $p = (d + ei)(k + hi) \Rightarrow p = (d - ei)(k - hi) \ \therefore \ p^2 = (d + ei)\,(k + hi)\,(d - ei)\,(k - hi) = (d^2 + e^2)\,(k^2 + h^2)$, así $(d^2 + e^2) \mid p^2 \ \wedge \ (k^2 + h^2) \mid p^2$, como esta divisibilidad es en $\mathbb{Z}$, esto ocurre si

$\left(d^2+e^2=1 \wedge k^2+h^2=p^2\right) \vee \left(d^2+e^2=p^2 \wedge k^2+h^2=1\right) \vee \left(d^2+e^2=p \wedge k^2+h^2=p\right)$;
como $d^2+e^2 \neq 1 \wedge k^2+h^2 \neq 1$ entonces la única posibilidad es $d^2+e^2=p$.

Nota: Los primos impares en $\mathbb{Z}$ son de dos tipos, aquéllos de la forma $4k + 1$ o los de la forma $4k + 3$, con $k \in \mathbb{Z}$, esto es $p \equiv 1 \ (mód\ 4) \ \vee \ p \equiv 3 \ (mód\ 4)$. (Recordemos que hay un único primo par positivo que es el 2) . Veremos que estas dos clases de primos impares tienen propiedades muy diferentes entre sí.

***Proposición*:** Si $p \in \mathbb{N}$ primo tal que $p \equiv 1 \ (mód\ 4)$ entonces la ecuación $x^2 \equiv -1 \ (mód\ p)$ admite solución.

***Demostración*:** Por el Teorema de Wilson, se tiene que $(p-1)! \equiv -1 \ \ (mód\ p)$.

$$(p-1)! = 1 \cdot 2 \cdot 3 \cdot 4 \cdots \frac{p-1}{2} \cdot \frac{p+1}{2} \cdots (p-2)(p-1) \ ;$$

observemos que $p-1 \equiv -1$, $p-2 \equiv -2$,...., $\frac{p+1}{2} \equiv -\frac{p-1}{2} \ \ (mód\ p)$,

con lo cual $(p-1)! = 1 \cdot 2 \cdot 3 \cdot 4 \cdots \frac{p-1}{2} \cdot \frac{p+1}{2} \cdots (p-2)(p-1) \equiv (-1)^{\frac{p-1}{2}} (1 \cdot 2 \cdot 3 \cdots \frac{p-1}{2})^2$

como $p = 4k + 1$ para cierto $k \in \mathbb{Z}$, se tiene que $\frac{p-1}{2}$ es par, tenemos que

$x = 1 \cdot 2 \cdot 3 \cdots \frac{p-1}{2}$ satisface la ecuación $x^2 \equiv -1 \ (mód\ p)$.

***Comentario*:** Queremos demostrar la recíproca de la proposición anterior, para lo cual debemos hacer unas consideraciones previas adicionales:
Por el Pequeño Teorema de Fermat, tenemos que si p es un natural primo, $a \in \mathbb{Z}$, tal que $p \nmid a$ se verifica que $a^{p-1} \equiv 1 \ \ (mód\ p)$.
Sea entonces $n = mín\left\{ k \in \mathbb{N} \ / \ \ a^k \equiv 1 \ \ (mód\ p) \right\}$

- Veamos primero que $a^0 = 1$, $a^1 = a$, a^2 , a^3 ,...., a^{n-1} son no congruentes dos a dos, o sea para $0 \leq i \leq j \leq n-1$, $a^i \equiv a^j \ \ (mód\ p) \ \Leftrightarrow \ i = j$
  Demostración:
  $\Leftarrow$) trivial.
  $\Rightarrow$) Si $a^i \equiv a^j \ \ (mód\ p) \Rightarrow \ a^j - a^i \equiv 0 \ \ (mód\ p)$,
  luego $a^i(a^{j-i} - 1) \equiv 0 \ \ (mód\ p)$, como $p \nmid a$, entonces $p \nmid a^i$, por lo que $a^{j-i} - 1 \equiv 0 \ \ (mód\ p)$ con lo cual $a^{j-i} \equiv 1 \ \ (mód\ p)$. Como $0 \leq j - i \leq j < n$, esto significa que $j - i = 0$, o sea, que $j = i$.
- En segundo término veremos que son los únicos no congruentes, o sea que $\forall m \in \mathbb{N}$ $\exists k \in \mathbb{N}_0$, $0 \leq k < n$, tal que $a^m \equiv a^k \ \ (mód\ p)$. Además, por lo visto anteriormente, ese k es único.
  Demostración:
  Sea $m \in \mathbb{N}$, por el Algoritmo de la División en $\mathbb{Z}$, $\exists q, r \in \mathbb{Z}$ tal que $m = qn + r$ con $0 \leq r < n$, entonces $a^m = (a^n)^q a^r \equiv 1^q a^r = a^r$.
- En tercer lugar demostraremos que para $m \in \mathbb{N}$: $a^m \equiv 1 \ \ (mód\ p) \ \Leftrightarrow \ n \mid m$.
  En particular $n \mid (p-1)$.

Demostración:

$\Leftarrow$) trivial

$\Rightarrow$) Sea $m = qn + r$, con $0 \le r < n$, $q, r \in \mathbb{Z}$, $1 \equiv a^m = (a^n)^q a^r \equiv 1^q a^r = a^r$, como $0 \le r < n$, se tiene que $r = 0$, con lo que $n \mid m$.

Claramente $n \mid (p-1)$.

- Para $k, h \in \mathbb{N}_0$, $a^k \equiv a^h \ (mód\ p) \iff k \equiv h \ (mód\ n)$.

  Demostración:

  Sin pérdida de generalidad, supongamos $k \le h$,

  $a^k \equiv a^h \ (mód\ p) \iff a^{h-k} \equiv 1 \ (mód\ p) \iff n \mid (h-k) \iff k \equiv h \ (mód\ n)$.

***Definición*:** Para p es un natural primo, $a \in \mathbb{Z}$, llamamos *orden de a respecto de* p, y lo simbolizamos $ord_p(a)$, al número natural $ord_p(a) = mín\{ k \in \mathbb{N} \ / \ a^k \equiv 1 \ (mód\ p) \}$.

***Teorema*:** Si $p \in \mathbb{N}$ primo, la ecuación $x^2 \equiv -1 \ (mód\ p)$ admite solución si y sólo si $p \equiv 1 \ (mód\ 4)$.

***Demostración*:**

$\Leftarrow$) Está demostrado en la proposición anterior.

$\Rightarrow$) Sea $x \in \mathbb{Z}$ tal que $x^2 \equiv -1 \ (mód\ p)$, entonces $x^4 \equiv 1 \ (mód\ p)$; además 4 es el menor natural con esa propiedad ya que 1, 2 y 3 no la verifican, por lo tanto $4 \mid (p-1)$ y así $p \equiv 1 \ (mód\ 4)$.

Comentario: Hemos demostrado que -1 es RC (mód p) si y sólo si $p \equiv 1 \ (mód\ 4)$, cuando p es primo positivo impar. Por consiguiente obtenemos la identidad: $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$

Caractericemos, ahora, los primos que se escriben como suma de cuadrados en $\mathbb{Z}$.

***Teorema* (*Fermat*):** Sea $p \in \mathbb{N}$ primo impar, $p \equiv 1 \ (mód\ 4)$ si y sólo si $\exists a, b \in \mathbb{Z}$ tales que $p = a^2 + b^2$.

***Demostración*:**

$\Rightarrow$) Sea $p \in \mathbb{N}$ primo tal que $p \equiv 1 \ (mód\ 4)$, por lo demostrado anteriormente $\exists x \in \mathbb{Z}$ tal que $x^2 \equiv -1 \ (mód\ p)$. Tomemos un tal x que además verifique $0 < x < p$ (esto siempre es posible eligiendo el resto en la división por p de cualquier entero que satisfaga aquélla propiedad). Podemos, además, elegir x tal que $0 < x \le \frac{p-1}{2}$, dado que $x^2 = (-x)^2 \equiv -1 \ (mód\ p)$ y si $\frac{p+1}{2} \le x \le p-1$ entonces $\exists y \in \mathbb{Z}$ tal que $y \equiv -x \ (mód\ p) \ \wedge \ 1 \le y \le \frac{p-1}{2}$ (Ese y es: $y = p - x$).

Sea entonces x, $0 < x \le \frac{p-1}{2} < \frac{p}{2}$, tal que $x^2 + 1 = cp$ para cierto $c \in \mathbb{Z}$; $cp = x^2 + 1 < \frac{p^2}{4} + 1 < p^2$ con lo cual $c < p$ y por tanto $p \nmid c \ \wedge \ (p, c) = 1$. Por la proposición demostrada anteriormente $\exists a, b \in \mathbb{Z}$ tal que $p = a^2 + b^2$.

$\Leftarrow$) Si $p = a^2 + b^2$, como $p \nmid a$ por ser p primo $\exists c \in \mathbb{Z}$ tal que $ac \equiv 1 \ (mód \ p)$ con $(c \ , \ p) = 1 \ \therefore \ pc^2 = a^2c^2 + b^2c^2 \ \Rightarrow \ 1 + (bc)^2 \equiv 0 \ (mód \ p)$, y así la ecuación $x^2 \equiv -1 \ (mód \ p)$ admite solución en $\mathbb{Z}$. Por lo demostrado anteriormente, esto significa que $p \equiv 1 \ (mód \ 4)$.

***Corolario*:** $\mathbb{Z}_p(i)$ es cuerpo si y sólo si p es primo positivo tal que $p \equiv 3 \ (mód \ 4)$.

***Demostración*:**
$\mathbb{Z}_p(i)$ es cuerpo si y sólo si la ecuación $a^2 + b^2 = 0$ no admite soluciones no triviales en $\mathbb{Z}_p$.
Si $p = 2$, se tiene que 1 + 1 = 0 en $\mathbb{Z}_2$, con lo cual $\mathbb{Z}_2(i)$ no es cuerpo, y si $p \equiv 1 \ (mód \ 4)$ tenemos que $a^2 + b^2 = 0$ para algunos $a \neq 0 \ \wedge \ b \neq 0$ en $\mathbb{Z}_p$, con lo cual, tampoco en estos casos, $\mathbb{Z}_p(i)$ es cuerpo.
Sea $p \equiv 3 \ (mód \ 4)$. Si $p \mid (k^2 + h^2) \ \wedge \ p \nmid k$ entonces $\exists t \in \mathbb{Z}$ tal que $tk \equiv 1 \ (mód \ p)$ $\therefore \ k^2 + h^2 \equiv 0 \ \Rightarrow \ (kt)^2 + (ht)^2 \equiv 0 \ (mód \ p)$ o sea $1 + (ht)^2 \equiv 0 \ (mód \ p)$ con lo que la ecuación $x^2 \equiv -1 \ (mód \ p)$ admite solución !! (absurdo) pues $p \not\equiv 1 \ (mód \ 4)$ y es impar. Análogamente si suponemos que $p \nmid h$.
Si $p \mid k$ entonces $p \mid k^2$ y como $p \mid (k^2 + h^2)$, se verifica que $p \mid h$.
Análogamente si suponemos que $p \mid h$. Así $p \mid k \ \wedge \ p \mid h$.
Por lo tanto la ecuación $a^2 + b^2 = 0$ en $\mathbb{Z}_p$ admite sólo la solución trivial $a = b = 0$. Luego $\mathbb{Z}_p(i)$ es cuerpo .

***Corolario*:** Sea $p \in \mathbb{N}$ primo impar, $p \equiv 3 \ (mód \ 4)$ si y sólo si se verifica:

$$p \mid (a^2 + b^2), \text{ con } a, b \in \mathbb{Z}, \Leftrightarrow \ p \mid a \ \wedge \ p \mid b.$$

***Demostración*:**

- Sea $p \in \mathbb{N}$ primo , $p \equiv 3 \ (mód \ 4)$,

$\Rightarrow$) sean $a, b \in \mathbb{Z}$ tales que $p \mid (a^2 + b^2)$
$\therefore \ a^2 + b^2 \equiv 0 \ (mód \ p)$, por lo visto anteriormente $a \equiv 0 \ \wedge \ b \equiv 0 \ (mód \ p)$.

$\Leftarrow$) Claramente si $p \mid a \ \wedge \ p \mid b$ también se cumple que $p \mid (a^2 + b^2)$.

- Recíprocamente, si $p \equiv 1 \ (mód \ 4)$, $\exists x \in \mathbb{Z}$ tal que $x^2 \equiv -1 \ (mód \ p)$, claramente se tiene que $p \nmid x \ \wedge \ p \mid (x^2 + 1)$.

***Proposición*:** Si $p \in \mathbb{N}$ es primo tal que $p = a^2 + b^2$, los cuadrados están unívocamente determinados, excepto por el orden, o sea, si $p = a^2 + b^2 = c^2 + d^2$ con $a, b, c, d \in \mathbb{N}$, entonces $(a = c \wedge b = d) \vee (a = d \wedge b = c)$.

***Demostración*:** Sea p primo positivo tal que $p = a^2 + b^2 = c^2 + d^2$ con $a, b, c, d \in \mathbb{N}$.

$p^2 = (a^2 + b^2)(c^2 + d^2) = (a + bi)(a - bi)(c + di)(c - di) = (ac - bd)^2 + (ad + bc)^2$ (I)

$(ad - bc)(ad + bc) = a^2d^2 - b^2c^2 = a^2d^2 + b^2d^2 - b^2d^2 - b^2c^2 = d^2(a^2 + b^2) - b^2(c^2 + d^2) =$

$= p(d^2 - b^2)$ entonces $p \mid (ad - bc) \vee p \mid (ad + bc)$, por ser p primo.

- Si $p \mid (ad + bc)$ entonces $p \mid (ac - bd)$ por (I). Sean $ad + bc = kp \wedge ac - bd = hp$

$\therefore \quad p^2 = h^2p^2 + k^2p^2 = p^2(k^2 + h^2)$ con lo cual $k^2 + h^2 = 1$; como $ad + bc = kp > 0$

entonces $k = 1 \wedge h = 0$, así $ac = bd \wedge ad + bc = p$

luego $pa = (a^2 + b^2)d = pd \Rightarrow a = d \wedge c = b$.

- Si $p \mid (ad - bc)$ como $p^2 = (a + bi)(c - di)(a - bi)(c + di) = (ac + bd)^2 + (ad - bc)^2$, se tiene que $p \mid (ac + bd)$, razonando como antes se tiene que $a = c \wedge b = d$.

Primos de Gauss

***Teorema*:** Los primos de $\mathbb{Z}[i]$ son los primos de $\mathbb{N}$ tales que $p \equiv 3 \pmod 4$ y sus asociados, los $z = a + bi$ tales que $N(z) = p \equiv 1 \pmod 4$, primo, y los $z = a + bi$ tales que $N(z) = 2$.

> ***¡¡¿5 no es primo pero 7 sí lo es?!!***
> *"los problemas de divisibilidad se hacen aquí más complicados ya que, por ejemplo 5 es factorizable en producto de dos "primos": 1+2i y 1-2i. De hecho, ningún primo natural de la forma 4n+1 es un primo de Gauss, mientras que los primos naturales de la forma 4n-1 siguen siendo primos en el sentido generalizado".*("Historia de la Matemática", Carl B. Boyer)

***Demostración*:**

- ✓ Sea $p \in \mathbb{N}$, $p \equiv 3 \pmod 4$ primo ; veamos que es primo en $\mathbb{Z}[i]$.

Sea $p = (a + bi)(c + di)$ con $a, b, c, d \in \mathbb{Z}$, $N(p) = p^2 = (a^2 + b^2)(c^2 + d^2)$

luego hay dos posibilidades:

i. $a^2 + b^2 = 1 \vee c^2 + d^2 = 1$ ó ii. $a^2 + b^2 = c^2 + d^2 = p$

$a^2 + b^2 = c^2 + d^2 = p$ es absurdo pues $p \equiv 3 \pmod 4$, y la suma de dos cuadrados módulo 4 puede dar 0, 1 o 2 , nunca 3 , entonces la única posibilidad es que $a^2 + b^2 = 1 \vee c^2 + d^2 = 1$, con lo cual $a + bi \in (\mathbb{Z}[i])^* \vee c + di \in (\mathbb{Z}[i])^*$, así los únicos divisores de p son las unidades y sus asociados, luego es primo en $\mathbb{Z}[i]$.

Los asociados de p son: p , $-p$, pi , $-pi$, todos ellos primos en $\mathbb{Z}[i]$ cuando $p \equiv 3 \pmod 4$.

- ✓ Sea $p \in \mathbb{N}$ primo, tal que $p = 2 \vee p \equiv 1 \pmod 4$. ¿$p$ no es primo en $\mathbb{Z}[i]$?

$2 = (1 + i)(1 - i)$ y $1 + i \notin (\mathbb{Z}[i])^* \wedge 1 - i \notin (\mathbb{Z}[i])^* \quad \therefore$ 2 no es primo en $\mathbb{Z}[i]$.

Si $p \equiv 1 \pmod 4$ $\exists a, b \in \mathbb{Z}$ tales que $p = a^2 + b^2 \quad \therefore \quad p = (a + bi)(a - bi)$ con

$a+bi \notin (\mathbb{Z}[i])^* \wedge a-bi \notin (\mathbb{Z}[i])^* \quad \therefore \quad p$ no es primo en $\mathbb{Z}[i]$.

✓ Sea $z=a+bi$ tal que $N(z)=p$ primo, con $p=2 \vee p \equiv 1 \pmod 4$.

Si $z=a+bi=(c+di)(e+fi)$, $N(z)=p=N(c+di)N(e+fi)=(c^2+d^2)(e^2+f^2)$, como $c^2+d^2 \geq 1 \wedge e^2+f^2 \geq 1$ y p es primo en $\mathbb{Z}$, entonces

$$(c^2+d^2=p \wedge e^2+f^2=1) \vee (e^2+f^2=p \wedge c^2+d^2=1) .$$

Luego $c+di \in (\mathbb{Z}[i])^* \vee e+fi \in (\mathbb{Z}[i])^*$ con lo cual z es primo en $\mathbb{Z}[i]$.

Observación: Notemos que $a+bi \wedge a-bi$ son primos porque tienen la misma norma, y cuando $p \equiv 1 \pmod 4$ no son asociados; a cada uno de ellos se le agregan sus tres asociados, todos ellos también primos.

Caractericemos los $z=a+bi$ tal que $N(z) = 2$. $a^2+b^2=2 \Leftrightarrow |a|=|b|=1$, luego los enteros de Gauss en cuestión son: $1+i, 1-i, -1+i, -1-i$. En este caso éstos son todos asociados entre sí.

✓ $\nexists z \in \mathbb{Z}[i]$ tal que $N(z)=p \equiv 3 \pmod 4$ y p primo

✓ Sea $z \in \mathbb{Z}[i]$ tal que z es primo. $z=a+bi \wedge N(z)=a^2+b^2=n>1$.

Si $\exists\, p \equiv 3 \pmod 4$ primo, tal que $p \mid n$ entonces $p \mid a \wedge p \mid b \therefore p \mid z$. Luego $z=p \cdot w$ con $w \in \mathbb{Z}[i]$. Como z es primo entonces $w \in (\mathbb{Z}[i])^*$, y así z es un asociado a p, ya considerado en un caso anterior.

Si $\forall p \in \mathbb{N}$ primo tal que $p \mid n$ se tiene que $p \equiv 1 \pmod 4 \vee p=2$; para un tal p, $n=pm$ con $p=k^2+h^2$. Si $z=a+bi$, $N(z)=a^2+b^2=n=pm=(k^2+h^2)m$.

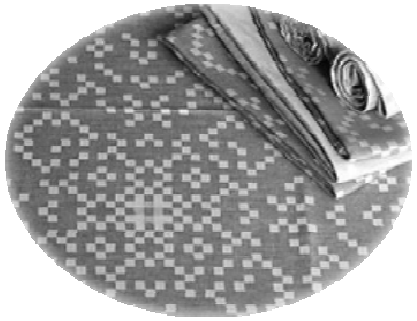
Supongamos $m>1$ pues el caso $m = 1$ ya fue analizado anteriormente.
$\exists q \in \mathbb{N}$ primo tal que $q \mid m$ y $q \equiv 1 \pmod 4 \vee q=2$, luego $m=qt \wedge q=u^2+v^2$,
así $N(z)=a^2+b^2=n=(k^2+h^2)m=(k^2+h^2)(u^2+v^2)t$
con lo que $(a+bi)(a-bi)=(k+hi)(k-hi)(u+vi)(u-vi)t$; $z=a+bi$ es primo $\wedge$ $z \nmid (k+hi)$ pues $N(z)>N(k+hi)$, análogamente para $k-hi$, $u+vi$, $u-vi$, entonces $z \mid t$ con lo que $t>1$.

Por el TFA en $\mathbb{Z}$ podemos escribir a $t=\prod_{j=1}^{s} p_j$ con $p_j \in \mathbb{N}$ primos y $p_j \equiv 1 \pmod 4 \vee p_j=2 \quad \forall j=1,...,s$; cada $p_j=(c_j^2+d_j^2)=(c_j+d_j i)(c_j-d_j i)$, entonces

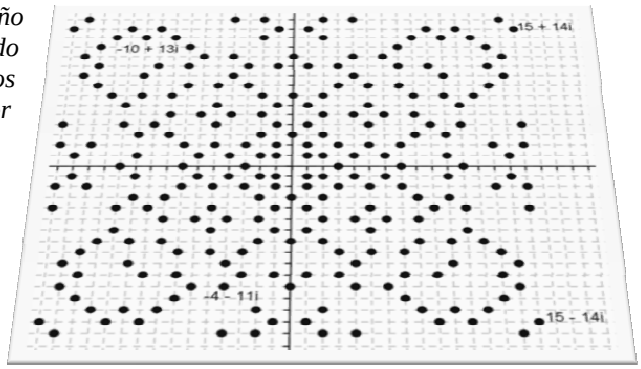
$$(a+bi)(a-bi)=(k+hi)(k-hi)(u+vi)(u-vi)\prod_{j=1}^{s}(c_j+d_j i)(c_j-d_j i)$$

donde cada factor es un primo en $\mathbb{Z}[i]$ de norma menor que n, por lo que no puede ser múltiplo de z, ni z divisible por él, porque z es primo, lo que contradice la factorización única en primos en $\mathbb{Z}[i]$!! (absurdo). Luego, si $z \in \mathbb{Z}[i]$ es tal que $N(z)$ no es primo en $\mathbb{Z}$ ni el cuadrado de un primo p tal que $p \equiv 3 \pmod 4$, no es primo en $\mathbb{Z}[i]$.

"Los primos de Gauss y la mantelería"*: En la década de los años 50, el diseño que muestra la imagen fue de gran aceptación en la industria textil. De hecho, es muy posible que el lector lo tenga visto en alguna servilleta o mantel familiar. Si bien el diseño parece haber sido creado en forma aleatoria, no es así sino que fue realizado por el físico holandés Balthasar van der Pol y llevado a la industria textil por el holandés Van Dissel. La posición de los cuadraditos es nada menos que la que corresponde a los números "Primos de Gauss" representados en el plano Complejo o Plano de Gauss, ubicando el centro de la "flor" en el origen y extendiéndose el dibujo hasta el número 39 de los ejes real e imaginario.*



A la derecha se muestra un fragmento del diseño hasta el número 15 de los ejes, realizado mediante GeoGebra y en el que se colocaron los valores a algunos de los puntos para una mejor interpretación.



Observación: Si $a,b,c \in \mathbb{Z}$ son tales que $a = b \cdot c$,

$$a \equiv -1 \ (4) \ \Rightarrow \ b \equiv -1 \ \vee \ c \equiv -1 \ (4).$$

Luego si $a = \prod_{j=1}^{n} p_j$ con $p_j \in \mathbb{N}$ primos, si $a \equiv -1 \ (4)$ entonces $\exists k \ \ 1 \le k \le n$ tal que $p_k \equiv -1 \equiv 3 \ \ (4)$.

***Proposición*:** En $\mathbb{Z}$ existen infinitos primos de la forma $4k+3$.

***Demostración*:** Supongamos que el conjunto $P = \{ \ p \in \mathbb{N} \ / \ p \ es \ primo \ \wedge \ p \equiv 3 \ (4) \ \}$ sea finito.

Sea $P = \{ \ p_1 , p_2 , p_3 , ... , p_n \ \}$; por ejemplo tenemos que $3, 7, 11 \in P$.

Sea $a = 4\prod_{j=1}^{n} p_j - 1$ con $p_j \in P$; claramente $a > 1 \ \wedge \ a \equiv -1 \ \ (4)$, luego $\exists q \in \mathbb{N}$ primo tal que $q \mid a \ \wedge \ q \equiv 3 \ (4)$, entonces $q \in P$ con lo cual $q \mid \prod_{j=1}^{n} p_j$ de donde $q \mid 1$!! (absurdo) por lo tanto P es infinito, lo que completa la prueba.

***Proposición*:** En $\mathbb{Z}$ existen infinitos primos de la forma $4k+1$.

***Demostración*:**

Supongamos que el conjunto $R = \{ \ p \in \mathbb{N} \ / \ p \ es \ primo \ \wedge \ p \equiv 1 \ (4) \ \}$ sea finito.

Sea $R = \{ p_1, p_2, p_3, ..., p_n \}$ y sea $a = 2\prod_{j=1}^{n} p_j$. Consideremos el número natural $b = a^2 + 1 > 1$ y sea $q \in \mathbb{N}$ primo tal que $q \mid b$; claramente q es impar porque b lo es; además $a^2 \equiv -1 \ (q)$ con lo que $a^4 \equiv 1 \ (q)$; $ord_q(a) = 4$, puesto que a, a^2, a^3 no son congruentes con 1 módulo q. Por lo visto anteriormente, esto significa que $4 \mid (q-1)$ o sea, $q \equiv 1 \ (4)$, de donde $q \in R$. Como $q \mid b \ \wedge \ q \mid a \Rightarrow q \mid 1$!! absurdo que provino de suponer que R es finito $\therefore$ R es infinito.

***Corolario*:** Existen infinitos primos en $\mathbb{Z}[i]$.

Ejercicios:

1. Demostrar que el producto de dos números que se pueden escribir como suma de dos cuadrados también se puede escribir como suma de dos cuadrados (consideramos a los cuadrados dentro de los números que pueden escribirse como suma de cuadrados). Generalizar este resultado al producto de cualquier familia finita de números que puedan escribirse como suma de dos cuadrados.
2. Demostrar que todo número natural m, o es un cuadrado o se puede escribir como $m = n^2 k$ con k *libre de cuadrados* (que no es divisible por ningún cuadrado mayor que 1).

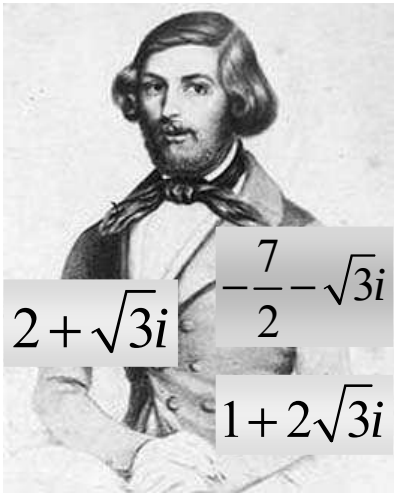
***Teorema*:** Un número natural n es suma de dos cuadrados si y sólo si los primos p, $p \equiv 3 \ (4)$, que aparecen en su factorización en primos (si existieran) lo hacen con exponente par.

***Demostración*:** $\Leftarrow$) trivial a partir del ejercicio 1.

$\Rightarrow$) Sea $n = m^2 k$ con $k = 1 \ \vee \ k$ libre de cuadrados, tal que n puede escribirse como suma de cuadrados. Si $k = 1$ no hay nada que demostrar pues es un cuadrado, por lo tanto todos los primos que aparecen en su factorización lo hacen con exponente par.
Supongamos que $k > 1$, $k = p_1 \cdot p_2 \cdot p_3 \cdots p_t$ con $p_i \in \mathbb{N}$ primos y distintos dos a dos.
Si $\exists j, \ 1 \le j \le t$ tal que $p_j \equiv 3 \ (4)$, se tiene que $p_j \mid m$ y si $m = a^2 + b^2$ entonces $p_j \mid a \ \wedge \ p_j \mid b$. Sea $a = p_j^r c \ \wedge \ b = p_j^s d$, con $r, s, c, d \in \mathbb{N}$, $(p_j, cd) = 1$, y supongamos que $r \le s$, $m = a^2 + b^2 = p_j^{2r}(c^2 + p_j^{2(s-r)} d^2) = p_j^{2r} m_1$. Si $p_j \mid m_1$ entonces $p_j \mid c$!!, luego $p_j \nmid m_1 \ \wedge \ m = p_j^{2r} m_1$ con $(p_j, m_1) = 1$, por lo cual p_j aparece en la factorización de m con exponente par !!. Por lo tanto $p_i \equiv 1 \ (4) \ \vee \ p_i = 2 \quad \forall i = 1, 2, ...t$.

Ejemplos: Algunos de los primos en $\mathbb{Z}$ que son primos de Gauss: 3, 7, 11, 19, 23, 31, 43, 47, 59, 67,…
Algunos de los primos de Gauss no reales: $1 + i$, $2 + i$, $3 + 2i$, $4 + i$, $5 + 2i$, $7 + 2i$, $4 + 5i$, …. ; además, cada uno de ellos multiplicado por las unidades y los conjugados nos dan más primos.

Enteros de Eisenstein



Nacido en Berlín en 1823, ***Ferdinand Gotthold Einsenstein*** *desde muy temprana edad demostró talento en las matemáticas. Sufrió muchos problemas de salud durante toda su vida, incluyendo meningitis, enfermedad que terminó con la vida de sus cinco hermanos. A los 15 años ya había superado los conocimientos que podía obtener en la escuela y comenzó a estudiar cálculo diferencial de obras de Euler y Lagrange. A los 17, estando aún en la escuela, comenzó a asistir a las clases de Dirichlet y otros matemáticos en la Universidad de Berlín. En 1843, en Dublín, Hamilton le dio una copia de una obra suya sobre el trabajo de Abel acerca de la imposibilidad de resolver ecuaciones quínticas, lo que estimuló notablemente el interés del joven Eisenstein en la investigación matemática.*
Murió de tuberculosis en 1852, a los 29 años de edad. En su corta vida, Eisenstein realizó numerosas contribuciones en varios campos de las matemáticas. Las tres áreas principales en las que realizó aportes fundamentales fueron la teoría de formas, generalizando los resultados obtenidos por Gauss respecto de las formas cuadráticas; las leyes de reciprocidad, con el objetivo de generalizar los resultados de Gauss sobre reciprocidad cuadrática; y las funciones elípticas.

Vamos a estudiar ahora otro dominio euclidiano, el *anillo de enteros de Eisenstein.*
Este anillo es $\mathbb{Z}[\omega]=\{\, z\in\mathbb{C} \;/\; z=a+b\omega,\ a,b\in\mathbb{Z}\,\}$, donde ω es una raíz cúbica primitiva de la unidad, por ejemplo $\omega=\dfrac{-1+\sqrt{3}\,i}{2}$. Los elementos de $\mathbb{Z}[\omega]$ se denominan *enteros de Eisenstein.*

Para $z=a+b\omega\in\mathbb{Z}[\omega]$, la norma de z es $N(z)=(a+b\omega)(a+b\bar{\omega})=a^2-ab+b^2\in\mathbb{N}_0$.
El cuerpo de cocientes de $\mathbb{Z}[\omega]$ es $\mathbb{Q}\left(\sqrt{3}\,i\right)=\left\{\, w=r+s\sqrt{3}\,i \;/\; r,s\in\mathbb{Q}\,\right\}$, pues si K es el cuerpo de fracciones de $\mathbb{Z}[\omega]$, como $\sqrt{3}\,i\in\mathbb{Z}[\omega] \;\wedge\; \mathbb{Z}\subset\mathbb{Z}[\omega] \Rightarrow \sqrt{3}\,i\in K \;\wedge\; \mathbb{Q}\subset K$ $\therefore\ \mathbb{Q}\left(\sqrt{3}\,i\right)\subset K$, pero además, $\omega\in\mathbb{Q}\left(\sqrt{3}\,i\right) \;\wedge\; \mathbb{Z}\subset\mathbb{Q}\left(\sqrt{3}\,i\right)$ con lo cual $\mathbb{Z}[\omega]\subset\mathbb{Q}\left(\sqrt{3}\,i\right)$ así $K\subset\mathbb{Q}\left(\sqrt{3}\,i\right)$.
Ejercicio: Si $z\in\mathbb{Z}[\omega]$, $z=a+b\omega=c+d\omega$, con $a,b,c,d\in\mathbb{Z}$, si y sólo si $a=c \;\wedge\; b=d$.

Observación:
El anillo de enteros de $\mathbb{Q}\left(\sqrt{3}\,i\right)$ no es $\mathbb{Z}\left[\sqrt{3}\,i\right]=\mathbb{Z}\left[\sqrt{-3}\right]=\left\{\, a+b\sqrt{3}\,i \;/\; a,b\in\mathbb{Z}\,\right\}$, dado que ω es un entero en $\mathbb{Q}\left(\sqrt{3}\,i\right)$, porque es raíz del polinomio mónico $f_3(x)=x^2+x+1$, pero $\omega\notin\mathbb{Z}\left[\sqrt{3}\,i\right]$, por lo tanto $\mathbb{Z}\left[\sqrt{3}\,i\right]\subsetneq\mathbb{Z}[\omega]$.

Unidades en $\mathbb{Z}[\omega]$:
$z=a+b\omega\in\mathbb{Z}[\omega]$ es inversible si y sólo si $N(z)=a^2-ab+b^2$ es inversible en $\mathbb{Z}$, o sea si y sólo si $N(z)=a^2-ab+b^2=1$.

- ✓ Para $a=0$, se debe verificar que $b=1 \vee b=-1$, con lo cual se obtienen las unidades: $\omega \wedge -\omega$.
- ✓ Para $b=0 \Rightarrow a=1 \vee a=-1$, de donde se obtienen las unidades $1 \wedge -1$
- ✓ Para $ab<0 \Rightarrow ab\leq -1$ con lo cual $a^2+b^2\leq 0$!!
- ✓ Para $ab>0 \Rightarrow ab\geq 1 \therefore a^2+b^2=1+ab\geq 2$
  - Si $a=1$ entonces $b^2=b \Rightarrow b=1$, con lo cual se tiene la unidad $1+\omega$
  - Si $a=-1$ entonces $b^2=-b \Rightarrow b=-1$, y la unidad es $-1-\omega$
  - Si $b=1$ entonces $a^2=a \Rightarrow a=1$ (ya está)
  - Si $b=-1$ entonces $a^2=-a \Rightarrow a=-1$, (ya está)
  - Si $|a|>1 \wedge |b|>1$ entonces $ab\geq 4$, luego
    $1=a^2+b^2-ab=(a-b)^2+ab$ lo que implica que $(a-b)^2\leq -3$!!

Luego las unidades de $\mathbb{Z}[\omega]$ son: $(\mathbb{Z}[\omega])^*=\{1,-1,\omega,-\omega,1+\omega,-1-\omega\}$.

Observemos que $1+\omega+\omega^2=0$ pues ω es raíz cúbica primitiva de la unidad, luego es raíz del polinomio ciclotómico de orden 3, con lo cual $\bar{\omega}=\omega^2=-(1+\omega)=-1-\omega$ y así $1+\omega=-\bar{\omega}$.

***Teorema*:** $\mathbb{Z}[\omega]$ es dominio euclidiano.

***Demostración*:** La demostración de que $\mathbb{Z}[\omega]$ es dominio euclidiano es análoga a la realizada para ver que $\mathbb{Z}[i]$ es euclidiano. También en este anillo la función

$d:\mathbb{Z}[\omega]-\{0\}\rightarrow \mathbb{N}_0$ es $d(z)=N(z)=z\cdot\bar{z}=a^2+b^2-ab$ para $z=a+b\omega$ con $a,b\in\mathbb{Z}$. Claramente la función d cumple:

i. $d(z_1)\leq d(z_1z_2)$ $\forall z_1,z_2\in\mathbb{Z}[\omega]-\{0\}$ por ser la norma una función multiplicativa y positiva para complejos no nulos.

También cumple:

ii. Dados $z_1,z_2\in\mathbb{Z}[\omega]-\{0\}$ $\exists u,v\in\mathbb{Z}[\omega]$ tales que $z_2=uz_1+v$ con $v=0 \vee d(v)<d(z_1)$

y la demostración de ello es similar a la realizada para enteros de Gauss.

- ✓ Analizaremos primero el caso particular en el cual $z_1=n\in\mathbb{N} \wedge z_2=a+b\omega\in\mathbb{Z}[\omega]$

Por el Algoritmo de la División en $\mathbb{Z}$, $\exists q_1,q_2,r_1,r_2\in\mathbb{Z}$ tales que $a=q_1n+r_1$, $b=q_2n+r_2$ con $|r_1|\leq\frac{n}{2} \wedge |r_2|\leq\frac{n}{2}$.

Entonces $z_2=a+b\omega=(q_1+q_2\omega)n+r_1+r_2\omega=un+v$ con $u=q_1+q_2\omega\in\mathbb{Z}[\omega]$ $\wedge$ $v=r_1+r_2\omega\in\mathbb{Z}[\omega]$ $\wedge$ $N(v)=r_1^2+r_2^2-r_1r_2\leq\frac{n^2}{4}+\frac{n^2}{4}+\frac{n^2}{4}<n^2=N(n)$.

Luego, hemos demostrado que $\forall z\in\mathbb{Z}[\omega] \wedge \forall n\in\mathbb{N}$, $\exists u,v\in\mathbb{Z}[\omega]$ tales que $z=un+v$ con $v=0 \vee d(v)<d(n)$.

✓ Sea ahora el caso general, $z_1, z_2 \in \mathbb{Z}[\omega]-\{0\}$. $z_1\overline{z}_1 = |z_1|^2 = n \in \mathbb{N}$; aplicando el resultado anterior a n y a $z_2\overline{z}_1$, vemos que $\exists u, v \in \mathbb{Z}[\omega]$ tales que $z_2\overline{z}_1 = un+v$ con $v=0 \ \vee \ d(v)<d(n)$.

Como $v = z_2\overline{z}_1 - uz_1\overline{z}_1 \ \wedge \ d(v)=N(v)=N(z_2\overline{z}_1-uz_1\overline{z}_1)<d(n)=N(z_1\overline{z}_1)$, tenemos que $N(z_2\overline{z}_1-uz_1\overline{z}_1)=N[\overline{z}_1(z_2-uz_1)]=N(\overline{z}_1)N(z_2-uz_1)<N(z_1)N(\overline{z}_1)$, y como $z_1 \neq 0$, entonces $N(z_1)\in\mathbb{N}$, con lo cual $N(z_2-uz_1)<N(z_1)$. Llamando $w=z_2-uz_1\in\mathbb{Z}[\omega]$, tenemos que $z_2=uz_1+w$ con $w=0 \ \vee \ d(w)=N(w)<N(z_1)=d(z_1)$, lo que prueba el teorema.

***Corolario*:** $\mathbb{Z}[\omega]$ es dominio principal.

***Corolario*:** $\mathbb{Z}[\omega]$ es dominio factorial.

Primos de Eisenstein

***Proposición*:** Si $z\in\mathbb{Z}[\omega]$ es tal que $N(z)=p$, con p primo de $\mathbb{N}$, entonces z es primo en $\mathbb{Z}[\omega]$.

***Demostración*:**
Sea $z\in\mathbb{Z}[\omega]$ tal que $N(z)=p$, con p primo de $\mathbb{N}$, y supongamos que $z=z_1z_2$ con $z_1, z_2 \in \mathbb{Z}[\omega]$, $p=N(z)=N(z_1z_2)=N(z_1)N(z_2)$,
como p es primo $N(z_1)=p \ \wedge \ N(z_2)=1$ o bien $N(z_2)=p \ \wedge \ N(z_1)=1$,
por lo cual $z_1\in(\mathbb{Z}[\omega])^* \ \vee \ z_2\in(\mathbb{Z}[\omega])^*$, luego z es primo en $\mathbb{Z}[\omega]$.

Adrien Marie Legendre nació en Tolouse Francia en 1752 y murió en París en 1833. A los 18 años ya había concluido sus estudios sobre matemática y física. En lo que respecta a la aritmética publicó (1797-1798) una obra en dos volúmenes, "Essai sur la Théorie des nombres" que es a la vez el primer tratado dedicado exclusivamente a la Teoría de Números. En él recopiló todo lo que se conocía en la época sobre el tema, especialmente los resultados aportados por Euler y Lagrange a las afirmaciones de Fermat y agregó sus investigaciones y descubrimientos originales, como una demostración, aunque no completa, de la Ley de Reciprocidad cuadrática. Fue quien introdujo la notación $\left(\frac{a}{p}\right)$ *para* **p** *primo positivo impar y* **a** *cualquier entero coprimo con* **p,** *para designar a la función* $\left(\frac{a}{p}\right)=\begin{cases}1 \ si \quad x^2\equiv a\,(mód\ p)\ tiene\ solución\ en\ \mathbb{Z}\\ -1\ si \quad x^2\equiv a\,(mód\ p)\ no\ tiene\ solución\ en\ \mathbb{Z}\end{cases}$

Adrien Marie Legendre
(1752-1833)

Enunciaremos una importante ley de la Aritmética, demostrada por Gauss en 1796, que nos será de gran utilidad en lo que sigue.

***Ley de reciprocidad cuadrática*:** Si p y q son primos positivos, impares y distintos, se tiene que

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=(-1)^{\frac{(p-1)}{2}\cdot\frac{(q-1)}{2}}$$

***Proposición*:** Si $p\in\mathbb{N}$ es primo tal que $p\equiv 1\ (mód\ 3)$ entonces $\exists z\in\mathbb{Z}[\omega]$ tal que $N(z)=p$.

***Demostración*:** Si $p\in\mathbb{N}$ primo es tal que $p\equiv 1\ (mód\ 3)$ entonces p es un residuo *cuadrático módulo* 3, usando el símbolo de Legendre, decimos que $\left(\frac{p}{3}\right)=1$. Por la *Ley de Reciprocidad Cuadrática,* se tiene que $\left(\frac{3}{p}\right)\left(\frac{p}{3}\right)=(-1)^{\frac{(p-1)}{2}\frac{(3-1)}{2}}=(-1)^{\frac{p-1}{2}}$ o sea que $\left(\frac{3}{p}\right)=(-1)^{\frac{p-1}{2}}$, entonces $\left(\frac{-3}{p}\right)=\left(\frac{-1}{p}\right)\left(\frac{3}{p}\right)=(-1)^{\frac{p-1}{2}}(-1)^{\frac{p-1}{2}}=(-1)^{p-1}=1$, por ser p primo impar. Quiere decir que –3 es residuo cuadrático (*mód p*) , por lo tanto $\exists y\in\mathbb{Z}$ tal que $y^2\equiv -3\ (p)$. Tomando x tal que $y=x+1$ tenemos que $p\mid\left[(x+1)^2+3\right]=(x^2+2x+4)$

$$x^2+2x+4=(x-2\omega)(x-2\bar{\omega}).$$

Si p es primo en $\mathbb{Z}[\omega]$ entonces $p\mid(x-2\omega)\ \vee\ p\mid(x-2\bar{\omega})$; si $p\mid(x-2\omega)\ \exists a,b\in\mathbb{Z}$ tales que $p(a+b\omega)=x-2\omega$, pero $p\nmid 2$!! , análogamente si suponemos que $p\mid(x-2\bar{\omega})\ \therefore\ p$ no es primo en $\mathbb{Z}[\omega]$ y $\exists z_1,z_2\in\mathbb{Z}[\omega]$ tales que $p=z_1z_2\ \wedge\ z_1,z_2\notin(\mathbb{Z}[\omega])^*$, con lo cual $N(z_1)=N(z_2)=p$.

Ejercicio: $z\in\mathbb{Z}[\omega]$ es primo si y sólo si $\bar{z}$ es primo.

***Teorema*:** Los primos de Eisenstein son:

i. Los $p\in\mathbb{N}$ primos tales que $p\equiv -1\ (mód\ 3)$ y sus asociados.

ii. Los $z\in\mathbb{Z}[\omega]$ tales que $N(z)=3$.

iii. Los $z\in\mathbb{Z}[\omega]$ tales que $N(z)=p$, con p primo tal que $p\equiv 1\ (mód\ 3)$.

***Demostración*:**

i. Sea $p\in\mathbb{N}$ primo tal que $p\equiv -1\ (mód\ 3)$, y tal que $p=z_1z_2$ con $z_1,z_2\in\mathbb{Z}[\omega]$.

$p^2=N(z_1z_2)=N(z_1)N(z_2)$; si $z_1,z_2\notin(\mathbb{Z}[\omega])^*$ entonces $N(z_1)>1\ \wedge\ N(z_2)>1$ con lo cual $N(z_1)=p\ \wedge\ N(z_2)=p$.

Si $z_1=a+b\omega$, con $a,b\in\mathbb{Z}$, $N(z_1)=a^2+b^2-ab=p\equiv -1\ (mód\ 3)$ entonces $a\not\equiv 0\ (3)\ \wedge\ b\not\equiv 0\ (3)$ pues los cuadrados módulo 3 son 0 y 1.

Si $a\equiv 1\ (3)$ entonces $b^2-b+2\equiv 0\ (3)$, pero esta ecuación no admite soluciones *mód* 3 pues su discriminante $\Delta=1-8=-7\equiv -1\ (3)$ no es un cuadrado *mód* 3 . Análogamente si suponemos que $b\equiv 1\ (3)$. Por lo tanto, la única posibilidad es que $a\equiv -1\ (3)\ \wedge\ b\equiv -1\ (3)$, con lo cual $N(z_1)=a^2+b^2-ab\equiv 1\ (mód\ 3)$!!

Luego si $p\equiv -1\ (mód\ 3)\ \nexists z\in\mathbb{Z}[\omega]$ tal que $N(z)=p$, por lo tanto p es primo en $\mathbb{Z}[\omega]$.

ii. Los $z \in \mathbb{Z}[\omega]$ tales que $N(z) = 3$, son primos en $\mathbb{Z}[\omega]$. Veamos cuáles son:

Sea $z = a + b\omega$, con $a, b \in \mathbb{Z}$, y $N(z) = a^2 + b^2 - ab = 3$, claramente $a \neq 0 \wedge b \neq 0$ pues 3 es primo.

- Si $a = 1$ entonces $b^2 - b = b(b-1) = 2$ con lo cual $b = 2 \vee b = -1$, y así tenemos los primos: $1 + 2\omega$ y $1 - \omega$.
- Si $b = 1$ entonces $a = 2 \vee a = -1$, y así tenemos los primos: $2 + \omega$ y $-1 + \omega$.
- Si $a = -1$ entonces $b = -2 \vee b = 1$, con lo que incorporamos un nuevo primo $-1 - 2\omega$
- Si $b = -1$ entonces $a = -2 \vee a = 1$, que nos da otro primo: $-2 - \omega$

Veamos que $\nexists z \in \mathbb{Z}[\omega]$ tal que $N(z) = 3$ y $|a| > 1 \wedge |b| > 1$. Supongamos, primero que $ab < 0$. $N(z) = a^2 + b^2 - ab = 3 \geq 4 + 4 + 4 = 12$!! . Entonces $ab > 0$; si $N(z) = 3$ entonces $N(-z) = 3$, así que podemos suponer $a > 0 \wedge b > 0$. $N(z\omega) = N(z\omega^2) = 3$, $z\omega = -b + (a-b)\omega$ y $z\omega^2 = (b-a) - a\omega$ donde $a - b > 0 \vee b - a > 0$. Si $a - b = 1$ entonces $b = a - 1$, y la ecuación $a^2 + b^2 - ab = 3 \Rightarrow a^2 - a - 2 = 0$, que tiene como solución $a = 2 \vee a = -1$; como $a > 1$ se deduce que $b = 1$!!. De la misma manera podemos demostrar que $b - a \neq 1$. Por lo tanto tenemos que $a - b > 1 \vee b - a > 1$; $a - b > 1 \wedge -b < -1$ vimos que es imposible, igual que $-a < -1 \wedge b - a > 1$.

Luego los $z \in \mathbb{Z}[\omega]$ tales que $N(z) = 3$, son: $1 + 2\omega$, $1 - \omega$, $2 + \omega$, $-1 + \omega$, $-1 - 2\omega$, $-2 - \omega$, que son asociados entre sí.

iii. trivial a partir de lo ya visto.

Falta demostrar que $\nexists z \in \mathbb{Z}[\omega]$ primo tal que $N(z) = n$ con $n \neq p^2$, para p primo $p \equiv -1 \pmod 3$, $n \neq 3 \wedge n$ no es primo $\equiv 1 \pmod 3$.

Supongamos que $\exists z \in \mathbb{Z}[\omega]$ primo tal que $N(z) = n$, $z = a + b\omega$, $a, b \in \mathbb{Z}$, con n no primo y $n \neq p^2$, para p primo $p \equiv -1 \pmod 3$. Como $n > 1$ $\exists p \in \mathbb{N}$ primo tal que $p \mid n$. Si $p \equiv -1 \pmod 3$, entonces p es primo en $\mathbb{Z}[\omega] \wedge n = (a + b\omega)(a + b\bar{\omega})$ entonces $p \mid (a + b\omega) \vee p \mid (a + b\bar{\omega})$, además $p \neq a + b\omega \wedge p \neq a + b\bar{\omega}$ pues $n \neq p^2$!!
por ser ambos primos. Entonces $\forall p \in \mathbb{N}$ primo tal que $p \mid n$ se verifica que $p \equiv 1 \pmod 3$ $\vee$ $p = 3$; en ambos casos $p = (c + d\omega)(c + d\bar{\omega})$, con $c + d\omega \wedge c + d\bar{\omega}$ primos; entonces $(c + d\omega) \mid (a + b\omega) \vee (c + d\bar{\omega}) \mid (a + b\omega)$, con $c + d\omega \wedge c + d\bar{\omega}$ no asociados a $a + b\omega$ pues tienen distintas normas, absurdo !! pues éste es primo.

Ejemplo: Algunos primos de $\mathbb{Z}$ que son primos de Eisenstein: 2 , 5 , 11 , 17 , 23 , 29 , 41 , 47 , 53, 59 , ….., 101, …
Primos de Eisenstein no reales: $2 + \omega$, $3 + \omega$, $5 + 2\omega$, $4 + \omega$, $6 + \omega$, $7 + \omega$, $7 + 3\omega$

Nota: Los primos de norma 3 son: $\omega-1=-\frac{3}{2}+\frac{\sqrt{3}}{2}i$; $(-1)(\omega-1)=1-\omega=\frac{3}{2}-\frac{\sqrt{3}}{2}i$; $\omega(\omega-1)=-1-2\omega=-\sqrt{3}\,i$; $(-\omega)(\omega-1)=1+2\omega=\sqrt{3}\,i$; $\omega^2(\omega-1)=2+\omega=\frac{3}{2}+\frac{\sqrt{3}}{2}i$; $-\omega^2(\omega-1)=-2-\omega=-\frac{3}{2}-\frac{\sqrt{3}}{2}i$

***Proposición*:** Sea $n\in\mathbb{N}$ para el cual $\exists x,y\in\mathbb{Z}$ tales que $n=x^2-xy+y^2$. Sea $p\in\mathbb{N}$ primo, $p\equiv -1 \ (mód\ 3)$, tal que $p\mid n$. Si $r=máx\{\, j\in\mathbb{N} \ / \ p^j\mid n\,\}$, entonces r es par.

***Demostración*:** Sea $n=p^r m$ con $(m\,,p)=1$ **.**
Tenemos que $n=(x+\omega y)(x+\overline{\omega}\,y)$, como $p\mid n$ y p es primo en $\mathbb{Z}[\omega]$ se verifica que $p\mid(x+\omega y) \ \vee \ p\mid(x+\overline{\omega}y)$. Supongamos que $x+\omega y=p^s z$ con $z\in\mathbb{Z}[\omega]$, $s\in\mathbb{N}$ $\wedge$ $p\nmid z$, entonces $x+\overline{\omega}y=p^s\overline{z}$, con lo cual $p\mid(x+\omega y) \ \wedge \ p\mid(x+\overline{\omega}y)$: Análogamente si suponemos que $p\mid(x+\overline{\omega}y)$. Como $x+\omega y=p^s z \ \wedge \ x+\overline{\omega}y=p^s\overline{z}$, con $p\nmid z$, entonces $n=p^{2s}z\cdot\overline{z}$, con $\wedge$ $p\nmid z\cdot\overline{z}$, y así $r=2s$, como queríamos demostrar.

***Teorema*:** Sea $n\in\mathbb{N}$, $\exists x,y\in\mathbb{Z}$ tales que $n=x^2-xy+y^2$ si y sólo si los primos $p\in\mathbb{N}$ con $p\equiv -1 \ (mód\ 3)$ que aparecen en la factorización en primos de n , lo hacen con exponente par.

***Demostración*:** $\Rightarrow$) está demostrado en la proposición precedente.
$\Leftarrow$) Sea $n\in\mathbb{N}$ tal que $n=p_1^{2r_1}p_2^{2r_2}....p_k^{2r_k}p_{k+1}^{r_{k+1}}p_{k+2}^{r_{k+2}}....p_s^{r_s}$ donde $r_j\in\mathbb{N}$, $\forall j=1,2,...,s$ $p_j\equiv -1 \ (3) \quad \forall j=1,2,...,k$, $p_j=3 \ \vee \ p_j\equiv 1 \ (3) \quad \forall j=k+1,...,s$, $p_i\neq p_j$ para $i\neq j$
Sea $p_j=(a_j+b_j\omega)(a_j+b_j\overline{\omega}) \quad \forall j=k+1,k+2,...,s$ y sea
$x+y\omega=\prod_{t=1}^{k}p_t^{r_t}\cdot\prod_{j=k+1}^{s}(a_j+b_j\omega)^{r_j}$ entonces $x+y\overline{\omega}=\prod_{t=1}^{k}p_t^{r_t}\cdot\prod_{j=k+1}^{s}(a_j+b_j\overline{\omega})^{r_j}$ con lo cual $n=x^2-xy+y^2$

Problemas:

1. Para cada $n\in\mathbb{N}$, el número de soluciones enteras de la ecuación $x^2-xy+y^2=n$ es finito y múltiplo de seis.
Tenemos que ver que existen finitos, y su número es múltiplo de seis, $x+\omega y$, con $x,y\in\mathbb{Z}$ que satisfacen la ecuación $N(x+\omega y)=n$;
   - ✓ si $n=1$, ya vimos que tenemos seis soluciones: $1,\ -1,\ \omega,-\omega,\ 1+\omega,-1-\omega$;
   - ✓ si $n=p$ primo, y $p\equiv -1 \ (mód\ 3)$ ya vimos que $\nexists\, z\in\mathbb{Z}[\omega]$ tal que $N(z)=p$;
   - ✓ si $n=3$, ya vimos cuáles son las soluciones : $1+2\omega$, $1-\omega$, $2+\omega$, $-1+\omega$, $-1-2\omega$, $-2-\omega$;
   - ✓ si $n=p$ primo, $p\equiv 1 \ (mód\ 3)$, la ecuación $x^2-xy+y^2=p$ implica $z\cdot\overline{z}=p$ donde $N(z)=N(\overline{z})=p$, por lo que $z \ \wedge \ \overline{z}$ son primos en $\mathbb{Z}[\omega]$. Por la unicidad de

la factorización en primos en $\mathbb{Z}[\omega]$ (es un dominio de factorización única) los únicos primos que pueden aparecer son z , $\overline{z}$ o sus asociados, que en cada caso suman seis, luego son finitos y múltiplos de seis.

- ✓ Por el teorema precedente, la ecuación $n = x^2 - xy + y^2$ admite solución sii los primos $p \in \mathbb{N}$, $p \equiv -1 \ (mód\ 3)$, que aparecen en la factorización de n , lo hacen con exponente par. Sea un tal n . Si $n = (x^2 - xy + y^2) = (u^2 - uv + v^2)$, $x + y\omega = z_1 z_2 z_3 ... z_k \ \wedge$ $u + v\omega = w_1 w_2 ... w_h$, con z_j, w_t primos , entonces:
  $n = z_1\overline{z}_1 z_2\overline{z}_2 .... z_k\overline{z}_k = w_1\overline{w}_1 w_2\overline{w}_2 ... w_h\overline{w}_h$, por la unicidad en la factorización en primos, excepto el orden y asociados, tenemos que $k = h$ y cada z_i es asociado a algún $w_{j_i} \vee \overline{w}_{j_i}$ y por tanto $\overline{z}_i$ es asociado a $\overline{w}_{j_i} \vee w_{j_i}$, respectivamente. Como en cada caso hay seis asociados, el número de soluciones es un múltiplo de seis.

Ejercicio: Sea p primo positivo, $p \equiv 1 \ (mód\ 3)$, demostrar que si $z = a + b\omega$ es tal que $N(z) = p$ entonces $\overline{z}$ no es asociado a z.

Ejemplo: Soluciones de $x^2 - xy + y^2 = 7$.
Observemos que si (x , y) es solución, también lo será (y , x) , pero los enteros de Eisenstein $x + y\omega \ \wedge \ y + x\omega$ son distintos, pero ambos de norma 7.
Las soluciones de $N(z) = 7$ en $\mathbb{Z}[\omega]$ son:
$1 + 3\omega$ y sus asociados: $1 + 3\omega , -1 - 3\omega , -3 - 2\omega , 3 + 2\omega , 2 - \omega , -2 + \omega$, y
$1 - 2\omega = 3 + 2\overline{\omega}$ y sus asociados: $1 - 2\omega , -1 + 2\omega , 2 + 3\omega , -2 - 3\omega , 3 + \omega , -3 - \omega$
Entonces en $\mathbb{Z} \times \mathbb{Z}$ las soluciones son: $(1 , 3) , (3 , 1) , (-1 , -3) , (-3 , -1) , (3 , 2) , (-3 , -2) ,$ $(2 , 3) , (-2 , -3) , (2 , -1) , (-2 , 1) , (1 , -2) , (-1 , 2)$.

ANEXO II

Existencia de anillos de polinomios

En el capítulo VIII, relativo a anillo de polinomios con coeficientes en un anillo conmutativo con identidad A, hemos:

- definido elementos trascendentes b sobre un tal anillo A,
- construido el anillo $A[b]$ de expresiones polinomiales en b con coeficientes en A,
- demostrado que dos de estos anillos son isomorfos, independientemente de los eventuales anillos que contengan a A donde se encontraren dichos elementos trascendentes.

De esta manera hemos definido al anillo de polinomios en una indeterminada con coeficientes en A como un representante en la clase de equivalencia de $A[b]$. No hemos demostrado que *siempre* tenemos un elemento trascendente sobre A, con lo cual, *siempre* existe el anillo de polinomios $A[x]$.

Anillo de las series enteras

Sea A un anillo conmutativo con identidad, y sea $A^{\mathbb{N}_0}$ el conjunto de las sucesiones en A.
Por sucesión en A entenderemos una función $f:\mathbb{N}_0 \to A$, donde $f(n)=a_n \in A$
Usaremos la notación clásica de sucesiones $(a_n)_{n\in\mathbb{N}_0}$ en vez de la general para funciones f.

Vamos a definir una suma y un producto en $A^{\mathbb{N}_0}$.
Para $\mathfrak{a}=(a_i)_{i\in\mathbb{N}_0}$, $\mathfrak{b}=(b_j)_{j\in\mathbb{N}_0}$ dos sucesiones en A, definimos:
$\mathfrak{a}+\mathfrak{b}=(a_i+b_i)_{i\in\mathbb{N}_0}$ $\wedge$ $\mathfrak{a}\cdot\mathfrak{b}=(d_k)_{k\in\mathbb{N}_0}$ donde $d_k=\sum_{i+j=k} a_i b_j$ $\forall k\in\mathbb{N}_0$.

Obsérvese que el producto está bien definido ya que la suma que define cada d_k es finita.
De esta manera $(A^{\mathbb{N}_0},+,\cdot)$ es un anillo conmutativo con identidad (demostrarlo!), en el cual el elemento neutro de la suma es la sucesión idénticamente nula: $(a_i)_{i\in\mathbb{N}_0}$ donde $a_i=0$ $\forall i\in\mathbb{N}_0$, el elemento neutro del producto es la sucesión $(b_i)_{i\in\mathbb{N}_0}$, donde $b_0=1$ $\wedge$ $b_i=0$ $\forall i\in\mathbb{N}$, y el opuesto de cada $\mathfrak{c}=(c_i)_{i\in\mathbb{N}_0}$ es la sucesión $-\mathfrak{c}=(-c_i)_{i\in\mathbb{N}_0}$.

Sea ahora la sucesión $(u_i)_{i\in\mathbb{N}_0}$ tal que $u_i=\begin{cases}1 & si\ \ i=1\\ 0 & si\ \ i\neq 1\end{cases}$, a la que llamaremos X.

Entonces $X=(0,1,0,0,.....,0,0,....)$; calculemos X^2
$X^2=(0,1,0,0,....,0,0,....)(0,1,0,0,...,0,0,....)=(d_k)_{k\in\mathbb{N}_0}$ con $d_k=\sum_{i+j=k} u_i u_j$.

$d_0=u_0^2=0$, $d_1=2u_0u_1=0$, $d_2=2u_0u_2+u_1^2=1$, y para $k>2$, los únicos sumandos en d_k eventualmente no nulos son los dos u_1u_{k-1}, pero como $k-1>1$, se tienen $u_{k-1}=0$, luego $d_k=0$ $\forall k\neq 2$. Por lo tanto $X^2=(0,0,1,0,0,....,0,....)$.
De la misma manera podemos demostrar que $X^n=(\delta_i^n)_{i\in\mathbb{N}_0}$, donde δ_i^n es la *delta de Kronecker*

$\delta_i^n=\begin{cases}1 & si\ \ i=n\\ 0 & si\ \ i\neq n\end{cases}$, o sea $X^n=(\underbrace{0,0,....,0}_{n},1,0,0....)$

Vamos a definir una inmersión de A en el anillo $A^{\mathbb{N}_0}$. Sea $\mathfrak{h}:A\to A^{\mathbb{N}_0}$ tal que $\mathfrak{h}(a)=(a_i)_{i\in\mathbb{N}_0}$
con $a_i=\begin{cases}a & si\ \ i=0\\ 0 & si\ \ i\neq 0\end{cases}$, $\forall a\in A$.

Claramente η es un monomorfismo de anillos con identidad, que nos permite identificar el elemento a de A con las sucesión $(a,0,0,...,0,0...)$; además el producto de una sucesión del tipo $(a,0,0,...,0,0...)$ por X^n es la sucesión $aX^n = (\underbrace{0,0,....,0}_{n},a,0,0....) \quad \forall a \in A, \forall n \in \mathbb{N}_0$.

Por esta construcción al anillo $A^{\mathbb{N}_0}$ lo notaremos como $A[\![X]\!]$, y a las sucesiones $(a_i)_{i\in\mathbb{N}_0}$ como $\sum_{i\geq 0} a_i X^i$.

Cada $\sum_{i\geq 0} a_i X^i$ se denomina *serie formal* y el anillo $A[\![X]\!]$ se denomina *anillo de series formales en una indeterminada con coeficientes en* A.

***Proposición*:** X es un elemento trascendente sobre A.

***Demostración*:** Para demostrar que X es trascendente sobre A debemos probar que si

$$a_0 + a_1X + a_2X^2 + ... + a_nX^n = 0 \quad \text{con} \quad a_i \in A \quad \forall i = 0,1,2,...,n$$

entonces $a_i = 0 \quad \forall i = 0,1,...,n$.

$$a_0 + a_1X + a_2X^2 + ... + a_nX^n = (a_0,0,0,...,0,...) + (0,a_1 0,0,...,0,...) + (0,0,a_2,0,...,0,...) + ... +$$
$$+ (\underbrace{0,0,0,...0}_{n},a_n,0,0,...0,...) = (a_0,a_1,a_2,....,a_n,0,0,...,0,...) = (0,0,0,.....,0,.....)$$

por igualdad entre funciones en general, y de sucesiones en particular,

$$a_i = 0 \quad \forall i = 0,1,...,n.$$

Luego X es trascendente sobre A.

Sea $B = \left\{ \sum_{i\geq 0} a_i X^i \in A[\![X]\!] \ / \ a_i = 0 \quad \forall i \in \mathbb{N}_0 - C, \ \textit{donde } C \textit{ es algún conjunto finito} \right\}$,

o sea B es el conjunto de sucesiones para las cuales sus términos son todos nulos excepto, quizás, para algún subconjunto finito de $\mathbb{N}_0$.

Sea $p(X) \in B - \{0\}$, $p(X) = \sum_{i\geq 0} a_i X^i$, con $a_i = 0$ para casi todo $i \in \mathbb{N}_0$ (todos nulos excepto finitos) y sea $n = máx\{ i \in \mathbb{N}_0 \ / \ a_i \neq 0 \}$, entonces $p(x) = \sum_{i=0}^{n} a_i X^i$

B es un subanillo con identidad de $A[\![X]\!]$, llamado *anillo de polinomios en una indeterminada con coeficientes en* A y sus elementos $p(X)$ son *polinomios en una indeterminada con coeficientes en* A, y el n definido más arriba es lo que llamamos *grado* del *polinomio no nulo* $p(X)$. Al anillo B lo notaremos $A[X]$.

Nota: Obsérvese que la suma y el producto definidos para series enteras, cuando las restringimos a polinomios (o sea, series enteras con sólo un número finito de términos no nulos), coincide con las definiciones dadas en el capítulo de polinomios.

La inmersión η restringida al codominio $A[X]$ aplica cada $a \in A$ en el polinomio nulo, si $a = 0$, y en el polinomio de grado cero $a = aX^0$, cuando $a \neq 0$

Conclusión: Hemos demostrado que, dado un anillo conmutativo con identidad A, *siempre* podemos obtener un elemento trascendente sobre A y por consiguiente, *siempre* está definido el anillo de polinomios en una indeterminada con coeficientes en A, el anillo $A[X]$, que es infinito, independientemente de cuántos elementos tenga A y que tiene polinomios de grado $n \quad \forall n \in \mathbb{N}_0$.

Ejercicios:

1. Demostrar que $(A^{\mathbb{N}_0}, +, \cdot)$ es un anillo conmutativo con identidad, donde las operaciones $+$ y $\cdot$ están definidas por: $\mathfrak{a}+\mathfrak{b}=(a_i+b_i)_{i\in\mathbb{N}_0}$; $\mathfrak{a}\cdot\mathfrak{b}=(d_k)_{k\in\mathbb{N}_0}$ con $d_k=\sum_{i+j=k} a_i b_j \quad \forall k\in\mathbb{N}_0$.

2. Para $X=(0,1,0,0,.....,0,0,....)$, demostrar que:

i. $X^n=(\delta_i^n)_{i\in\mathbb{N}_0} \ \forall n\in\mathbb{N}_0$, donde $\delta_i^n=\begin{cases}1 & si \ \ i=n\\ 0 & si \ \ i\neq n\end{cases}$.

ii. $aX^n=(\underbrace{0,0,....,0}_{n},a,0,0....) \quad \forall a\in A, \forall n\in\mathbb{N}_0$.

3. Demostrar que la aplicación $\mathfrak{h}: A\to A^{\mathbb{N}_0}$ tal que $\mathfrak{h}(a)=(a_i)_{i\in\mathbb{N}_0}$ donde

$a_i=\begin{cases}a & si \ \ i=0\\ 0 & si \ \ i\neq 0\end{cases}$ es un monomorfismo de anillos con identidad .

4. Demostrar que el conjunto B definido más arriba, es un subanillo con identidad de $A[\![X]\!]$.

BIBLIOGRAFÍA

Alvarez, E.; Oliver, M.I.; Vecino, S. (2001). *Los Números. Su Representación en distintas bases*. Mar del Plata: Ediciones Suarez.

Babini, J. (1980). *Historia de las ideas modernas en matemática*. Washington, D.C: Secretaría General de la Organización de los Estados Americanos. Programa Regional de Desarrollo Científico y Tecnológico.

Becker, M.E.; Pietrocola, N.; Sanchez, S. (2001). *Aritmética*. Buenos Aires: Red Olímpica.

Birkhoff, G. y MacLane, S.(1963). *Álgebra Moderna.* Barcelona:Vincens Vives.

Bosch, Jorge (1965). *Introducción al simbolismo lógico*. Buenos Aires: EUDEBA.

Boyer, Carl B. (1994). *Historia de la Matemática* Madrid: Alianza Universidad Textos.

Courant, R. Y Robbins, H. (1954). *Qué es la matemática?*. Buenos Aires: Editorial Alda.

Eves, Howard (1997). *Introdução à Historia da Matemática*. Campinas: Editora Da Unicamp.

Ferrater Mora, J. (1969). *Diccionario de Filosofía*, *Tomos I y II*. Buenos Aires: Editorial Sudamericana.

Gentile, Enzo R. (1967). *Estructuras Algebraicas I*. Serie de Matematica. Monografía Nro. 3. Washington, D.C: Secretaría General de la Organización de los Estados Americanos. Programa Regional de Desarrollo Científico y Tecnológico.

Gentile, Enzo R. (1976). *Notas de Álgebra I* . Buenos Aires: EUDEBA.

Gentile, Enzo R. (1991). *Aritmética Elemental en la Formación Matemática.* Buenos Aires: Red Olímpica.

Godement, R. (1971). *Álgebra*. Madrid: Editorial Tecnos.

Guzmán, Miguel de (1988). *Aventuras Matemáticas.* Barcelona: Editorial Labor.

Guzman, Miguel de (1996). *El rincón de la pizarra : ensayos de visualización en análisis matemático : elementos básicos del análisis***.** Madrid**:** Pirámide.

Halmos, P. (1965). *Teoría Intuitiva de los Conjuntos.* México: CECSA.

Herstein, I.N. (1973). *Álgebra Moderna*. México: Editorial Trillas.

Kasner E. & Newman J. (1985). *Matemáticas e Imaginación*. Buenos Aires: Hispamerica Ediciones.

Lang, Serge (1971). *Álgebra*. Madrid: Editorial Aguilar.

Luzardo, D.; Peña, A.(2006). Historia del Algebra Lineal hasta los Albores del Siglo XX . *Divulgaciones Matemáticas*, 14(2), 153-170.

Miller, Ch.; Heeren, V.; Hornsby, E Jr. (1999). *Matemática: Razonamiento y Aplicaciones*- México: Addison Wesley Longman.

Oubiña, L. (1965). *Introducción a la Teoría de Conjuntos*. Buenos Aires: EUDEBA.

Perelman, Yakov (1975). *Álgebra Recreativa*. Moscú: Editorial Mir.

Polya, G. (1979). *Cómo plantear y resolver problemas.* México: Editorial Trillas.

Polya, G. (1981). *Mathematical Discovery*: *On Understanding, Learning and Teaching Problem Solving* (combined edition)- New York: Wiley.

Rey Pastor, J. Y Babini, J. (2000). *Historia de la Matemática*, vol 2. Barcelona: Gedisa.

Stewart, Ian (2012). *Historia de la Matemática en los últimos 10.000 años.* Barcelona: Editorial Crítica.

AUTORAS

Lic. Estella Maris Alvarez: Licenciada en Matemática, egresada de la Universidad Nacional de La Plata. Profesora Adjunta con dedicación exclusiva en el área Algebra, en la Facultad de Ciencias Exactas y Naturales de la Universidad Nacional de Mar del Plata. Responsable, durante más de treinta años, de la asignatura Algebra, actualmente denominada Introducción al Álgebra según el nuevo plan de estudios, para las carreras de Profesorado en Matemática y Licenciatura en Ciencias Matemáticas.

Mg. María Susana Vecino: Profesora en Matemática, egresada de la Universidad Nacional de Mar del Plata. Master en Informática Educativa, título otorgado por la UNED. Se desempeña como docente con dedicación parcial en el área Algebra, en la en la Facultad de Ciencias Exactas y Naturales de la Universidad Nacional de Mar del Plata y es integrante del grupo "Investigación Educativa".

Prof. María Isabel Oliver: Profesora en Matemática, egresada de la Universidad Nacional de Mar del Plata. Se desempeña como Jefe de Trabajos Prácticos con dedicación exclusiva en el área Algebra, en la Facultad de Ciencias Exactas y Naturales de la Universidad Nacional de Mar del Plata y es integrante del grupo "Investigación Educativa". Durante más de treinta años ha estado a cargo de la práctica de la asignatura Algebra, para las carreras de Profesorado en Matemática y Licenciatura en Ciencias Matemáticas.

Las tres docentes son coautoras de los libros *"Los Números. Su Representación en distintas bases"* (Ediciones Suarez-2001) y "*Temas de Algebra-Primera parte: R, N, Z, Q"* (Ed. Red Olímpica-2011) y han dictado numerosos cursos de capacitación para docentes de distintos niveles, varios de ellos en forma conjunta.


eudem