ÁLGEBRA I

Profesorado

MATEMÁTICA

GUÍA PARA EL EXAMEN

A.N.E.P. CO.DI.CEN.
DIRECCIÓN DE FORMACIÓN Y PERFECCIONAMIENTO DOCENTE
Departamento de Educación a Distancia

ADMINISTRACIÓN NACIONAL DE EDUCACIÓN PÚBLICA
CONSEJO DIRECTIVO CENTRAL

Presidente:	Prof. Germán Rama
Vicepresidente:	Dr. José Claudio Williman
Vocal:	Lic. Nelly Leites de Moraes
Vocal:	Mtra. Rosa Márquez
Vocal:	Prof. Carmen Tornaría

DIRECCIÓN DE FORMACIÓN Y PERFECCIONAMIENTO DOCENTE

Directora:	Prof. Jenny Barros
Subdirector Área Magisterial:	Mtro. Milton Martorell

DEPARTAMENTO DE EDUCACIÓN A DISTANCIA

Director:	Prof. Carlos Jones Gaye
Secretaria Docente:	Mtra. Irma Paolino
Técnicos en Educación a Distancia:	Mtro. Mario Ibarra
	Prof. Graciela Rabajoli
Administrativos	Helena Schilde
	Carolina Arrascaeta

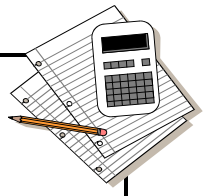
EQUIPO DOCENTE DE LA ESPECIALIDAD MATEMÁTICA

Älgebra I	Profesor Daniel Siberio
Geometría I	Profesor Sergio Peralta
Matemática Básica	Profesoras:
	María Elena Becerra
	Mónica Kacevas
	Ana María Tosetti

EDICIÓN AÑO 2000

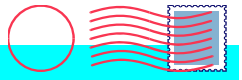
Para_volver_a_la_página_de_la_Especialidad

CONTENIDO



1. Introducción
2. Número_real
3. Número_natural
4. Completitud
5. Funciones_exponenciales
6. Divisibilidad
7. Congruencias

PORTADA: Mohammed Ibn Musa Al-Khwarizmi (789-850) conocido como el padre del álgebra. Se sabe poco de su vida, salvo que vivió en la primera mitad del Siglo IX y que trabajó en la biblioteca del califa de Bagdad. Escribió libros sobre geografía, astronomía y matemática. En su obra ***Aritmética ("Algoritmi de numero indorum")*** explica con detalle el funcionamiento del sistema decimal y del cero que usaban en la India. Obra de gran importancia pues contribuyó a la difusión del sistema de numeración indio y al conocimiento del cero.
Debe destacarse la obra de contenido algebraico ***"Hisab al abr wa´ l muqqabala"***, considerada uno de los primeros libros de álgebra.
Es el autor de uno de los métodos más antiguos que se conocen para resolver ecuaciones de segundo grado. Dicho método, geométrico, se conoce como ***de completar cuadrado.*** (Fuente: ***Gacetilla Matemática:*** **wysiwyg://principal.13/http:www.arrakis.es)**



ALGUNAS CONSIDERACIONES PREVIAS

Contenidos de la asignatura

Como se menciona en los fundamentos situados en el programa vigente *"El curso de Álgebra I gira fundamentalmente alrededor de las estructuras numéricas fundamentales; tratándolas paralelamente y dentro de las estructuras algebraicas básicas que se volverán a tratar en profundidad en los cursos posteriores"*.

Mas concretamente nos permitimos resaltar los siguientes temas:

- Número real.
- Trigonometría.
- Número Complejo.
- Divisibilidad en N y en Z.
- Polinomios sobre un anillo.

Número real.

En este punto, el más extenso de todo el programa, abarcamos no solamente un desarrollo axiomático del cuerpo totalmente ordenado y completo de los números reales sino de sus subestructuras más usuales (Naturales, Enteros y Racionales) así como un tratamiento detallado de la potenciación.

Cabe destacar que en este tema justificaremos los procedimientos que utilizamos habitualmente para la resolución de ecuaciones e inecuaciones: racionales, irracionales, exponenciales y logarítmicas en el campo de los reales así como un exhaustivo estudio de la función cuadrática (de segundo grado).

Trigonometría.

Fundamentalmente nos dedicaremos a precisar las definiciones de las funciones trigonométricas principales. No le prestaremos mayor atención a la demostración de las fórmulas ya que en su gran mayoría estas son rutinarias, y no aportan nada nuevo. Desde el punto de vista práctico nos dedicaremos fundamentalmente a la resolución de ecuaciones e inecuaciones trigonométricas.

Número complejo.

Aquí hablaremos sobre el cuerpo no ordenado de los números complejos, sus distintas formas, interpretación geométrica y algunos aspectos sobre la potenciación.

Divisibilidad en N y en Z.

Como el título lo dice trataremos en este punto cuestiones vinculadas con la división entera y exacta en los naturales y en los enteros. Temas como: división entera, divisores y múltiplos, máximo común divisor y mínimo común múltiplo, números primos y compuestos, etc. Destacamos como temas no tan vistos a las congruencias y las ecuaciones diofánticas.

Polinomios sobre un anillo.

La temática principal que se abordará en este punto es el análisis de la naturaleza dual de los polinomios como forma polinómica y como función. Así también como algunos aspectos vinculados a la divisibilidad. Cabe destacar que trabajaremos sobre un anillo cualquiera sin descuidar los casos mas utilizados, los polinomios de coeficientes reales y los de coeficientes complejos.

Otros temas del programa (por ej. conjuntos – relaciones – funciones – operaciones - estructuras algebraicas) son tratados de manera instrumental; ya que un estudio más profundo y específico se realizará en otras asignaturas; en particular en matemática básica.

Características y objetivos

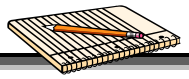
El lector habrá observado que la mayoría de los temas mencionados forman parte de los programas de secundaria. A diferencia de lo que ocurre en la universidad donde bajo el título de **Álgebra I** usualmente se tratan temas correspondientes al álgebra lineal. **Cabe destacar que la profundidad y exigencia con la que pretendemos abordar nuestra temática es muy diferente a la utilizada habitualmente en los cursos de secundaria**. Sobre todo este aspecto se pondrá de manifiesto en la **fundamentación teórica**.

Uno de los motivos por lo cual volver a estudiar y sobre todo profundizar en temas conocidos es que ellos serán entre otros los temas con los cuales deberá trabajar el futuro docente. Es innecesario destacar la necesidad de que el docente conozca profundamente y maneje con soltura la temática que desarrollará. Soltura y profundidad que no se adquieren en secundaria.

Destacamos como una de las características más salientes tanto de Álgebra I como de las otras materias específicas la pretensión de fundamentar detalladamente los distintos puntos que se tratan.

Si los comparamos con otros cursos terciarios notaremos una mayor pasión por la fundamentación teórica y por el detalle; lo cual nos lleva en contrapartida a tratar menor cantidad de temas en cada curso. Tengamos en cuenta que para nosotros **la matemática es mucho más que una herramienta con la cual resolver problemas en otras áreas.**

Algunas sugerencias



En las páginas siguientes el lector se encontrará con un desarrollo teórico de algunos de los distintos puntos del programa. Este material teórico está intercalado por ejercicios y problemas resueltos y a resolver. Además al final de cada sección se encontrará con un listado de ejercicios y de ser posible sus respuestas que coinciden con los repartidos trabajados en los cursos presenciales.

Más precisamente se encontrará con el desarrollo de **número real** y de **divisibilidad**. En el mencionado desarrollo se indica bibliografía complementaria. Con respecto a los **temas no tratados nos permitimos sugerir**: para **Número Complejo** el "Calculus" de Apostol así como otros apuntes que serán enviados a la biblioteca de cada Instituto de Formación Docente junto con la presente Guía. Respecto a **Trigonometría** le sugerimos **un trabajo del prof. R.Louro** con el mismo título, disponible donde se indicó anteriormente. (Hay dos trabajos del mismo autor, uno con el tratamiento clásico y el otro por series de potencias; nos referimos al primero). Relativo a **Polinomios** aconsejamos los apuntes titulados **"Anillo de los polinomios" del prof. R.H.Cobas**. (el enfoque tratado aquí puede resultarle muy duro en una primera lectura. Si así fuera puede leer previamente el tema en "**Matemática A para 5ª año" tomo 5-2 de A. Infantozzi**). Por supuesto que la bibliografía sugerida no implica que el lector recurra a otra, sobre todo a la indicada en el programa oficial. Es más, es recomendable que lo haga.

Le sugerimos al estudiante que re-elabore su propio teórico; sintiendo, incorporando cada definición, cada teorema, cada ejercicio en "mano propia". Así como también que amplíe cada tema con la bibliografía indicada.

También es conveniente dedicarle el tiempo necesario a realizar los ejercicios ubicados al final de cada sección antes de pasar a la siguiente; esto no significa que deban realizarse necesariamente la totalidad de los ejercicios y problemas propuestos; pero sí un porcentaje importante de los mismos.

Esta es una primera versión y seguramente aparezcan involuntariamente múltiples errores; especialmente en las respuestas de los ejercicios. Desde ya agradezco que me hagan llegar todas las discrepancias y sugerencias que permitirán mejorar esta guía. Esperando el primer contacto real o virtual les saluda atentamente:

Prof. Daniel Siberio

Les recordamos que se enviará a la Biblioteca de cada I.F.D. los siguientes materiales:

- *"Anillo de Polinomios"*, **y** *"Número Complejo"* **del profesor Raúl Cobas, y**
- *"Trigonometría"* **del profesor R. Louro.**

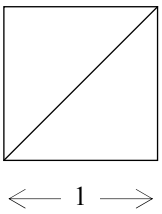
Inicio

NÚMERO REAL

Introducción

A lo largo de nuestra vida nos hemos ido encontrando con algunas estructuras numéricas. Seguramente el lector conoce desde hace mucho tiempo a los **naturales** a los **enteros** y a los **racionales**; así como también las diferencias entre ellas y las necesidades no cubiertas por una estructura que hacen necesario la creación de la siguiente.

¿Cuáles son las insuficiencias de los racionales que hacen necesario presentar una nueva estructura algebraica? Intentemos plantear una de ellas.



Consideramos un cuadrado de lado 1 (una unidad cualquiera) y pretendemos "medir" una de sus diagonales tomando al lado como unidad. Si existiese tal medida en Q (a la cual llamaremos L) por Pitágoras cumpliría:

$$L^2 = 1^2 + 1^2 \Rightarrow L^2 = 2$$

Si $L \in Q \Rightarrow L = \frac{p}{q}$ con p y q enteros primos entre si. (en otras palabras si L es un racional se puede escribir como una fracción irreducible)

$$L^2 = \left(\frac{p}{q}\right)^2 = \frac{p^2}{q^2} = 2 \Rightarrow p^2 = 2q^2 \Rightarrow p^2 \text{ es par} \Rightarrow p \text{ es par} \Rightarrow p = 2t \;; t \in Z \Rightarrow p^2 = 4t^2$$

como $p^2 = 2q^2$ sustituyendo nos queda : $2q^2 = 4t^2 \Rightarrow q^2 = 2t^2 \Rightarrow q^2$ es par $\Rightarrow$ q es par

Por lo tanto si existiese un racional $L = \frac{p}{q}$ que midiera exactamente la diagonal de un cuadrado de lado 1 tendríamos que: p es par, q es par, p y q enteros primos entre si. Lo cual es contradictorio.

En consecuencia no existe ningún racional que elevado al cuadrado sea 2 y por lo tanto los racionales no nos permiten medir la longitud de la diagonal de un cuadrado de lado uno. Es inecesario resaltar la importancia que tiene disponer de una estructura con la cual poder medir cualquier longitud u otra magnitud escalar. Hemos presentado una de las incapacidades de los racionales; no la única. Elegimos esta por ser la de mayores consecuencias desde el punto de vista histórico.

"Los Pitagóricos enamorados de los números enteros creyeron que todas las cosas podían derivarse de ellos, empezando por todos los demas números. Se produjo una crisis en esta doctrina cuando descubrieron que la raíz cuadrada de 2 (La razón entre la diagonal y el lado de un cuadrado) era irracional, es decir que $\sqrt{2}$ *no puede expresarse de modo preciso como la razón de dos enteros determinados por grandes que fueran estos números.*

Este descubrimiento se llevó a cabo utilizando irónicamente como herramienta el teorema de Pitágoras. Irracional significaba en principio que un número no podía expresarse como una razón (cociente) *Pero para los Pitagóricos llegó a suponer algo amenazador, un indicio de que su concepción del mundo podía carecer de sentido, lo cual es la otra acepción que tiene hoy la palabra irracional"* (COSMOS de Carl Sagan)

Para cubrir esta como otras carencias de los racionales presentemos a los **números reales**. Para ello existen fundamentalmente dos caminos: El constructivo; crear a los naturales, a partir de ellos a los enteros, luego a los racionales y a partir de estos últimos generar a los números reales. El otro camino consiste en crear directamente a los reales siendo los naturales, los enteros y los racionales subestructuras de los reales.

Esta última opción es la que trabajaremos en esta asignatura; la primera será vista, por lo menos parcialmente, en **"Matemática Básica"**.

Cualquiera de los dos caminos implican la utilización del método axiomático. No desarrollaremos aquí las características de este método por exceder la longitud de este trabajo y además tratarse en las otras asignaturas especiales; tanto en **"Geometría I"** como en **"Matemática Básica".** Corriendo el riesgo de caer en una simplificación excesiva diremos que: El método axiomático consiste en la aceptación de algunas proposiciones como válidas (que llamaremos **axiomas**), sin necesidad de demostración, y la deducción del resto de las proposiciones de la teoría a partir de estos.

La característica imprescindible que debe cumplir un sistema axiomático es la **consistencia**; la no contradicción de las proposiciones tomadas como axiomas (téngase en cuenta que en toda demostración por absurdo se está utilizando la consistencia del sistema). Otras propiedades como la **independencia** o la **categoricidad** no tienen porqué ser cumplidas por todos los sistemas axiomáticos.

Axioma 1 (Axioma de cuerpo)

En un conjunto que llamaremos de los ***números reales*** (al que anotamos $\Re$) en el cual están definidas dos operaciones que denominamos ***suma*** y ***producto*** (las cuales las anotamos con + y $\cdot$ respectivamente que cumplen:

S_1) **Asociativa** $a+(b+c)=(a+b)+c \quad \forall a,b,c \in \Re$

S_2) **Conmutativa** $a+b=b+a \quad \forall a,b \in \Re$

S_3) **Neutro** $\exists\, 0 \in \Re \;;\; a+0=0+a=a \quad \forall a \in \Re$

S_4) **Opuesto** $\forall a \in \Re \quad \exists\, op(a) \in \Re \;;\; a+op(a)=op(a)+a=0$

P_1) **Asociativa** $a.(b.c)=(a.b).c \quad \forall a,b,c \in \Re$

P_2) **Conmutativa** $a.b=b.a \quad \forall a,b \in \Re$

P_3) **Neutro** $\exists\, 1 \in \Re \;\; 1 \neq 0 \;;\; a.1=1.a=a \quad \forall a \in \Re$

P_4) **Inverso** $\forall a \in \Re \;\; a \neq 0 \;\; \exists\, inv(a) \in \Re \;\; ;\; a.inv(a)=inv(a).a=1$

SP) **Distributiva** $a.(b+c)=a.b+a.c \quad \forall a,b,c \in \Re$

$(b+c).a=b.a+ca \quad \forall a,b,c \in \Re$

Nota 1

En el axioma recién enunciado aparece el término "operación". ¿Qué entendemos por tal término? Antes de ir a una definición concreta de "operación" analicemos un caso más que familiar; la suma en los naturales. En el cual aparecen expresiones como:

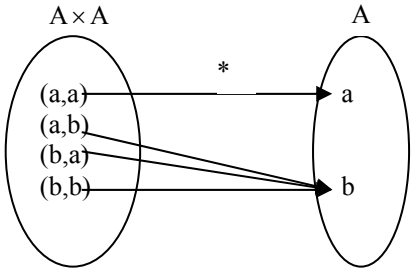
2+4=6
3+5=8
a+b=c

Cuando anotamos por ejemplo 2+4=6 aparecen en juego tres números naturales cumpliendo distintos roles (2 y 4 como sumandos y el 6 como resultado). Podemos pensar a la suma de naturales como una "correspondencia" que al par (2,4) le hace corresponder el 6, al par (3,5) el 8 .... al par de naturales (a,b) el natural c.

Y no cualquier tipo de correspondencia ya que a cada par ordenado de naturales la suma le hace corresponder un y solo un natural (el resultado de sumar ambas componentes del par). En definitiva; podemos considerar a la suma de naturales como una *función* de $N \times N$ en N.

Obsérvese que una interpretación idéntica puede hacerse con el producto de naturales; que el producto de enteros puede considerarse como una función que a pares ordenados de enteros hace corresponder un entero (o sea una función de $Z \times Z \to Z$) ; la suma de vectores como una función que a pares ordenados de vectores hace corresponder un vector;.....
Concretamente: Siendo A un conjunto no vacío llamamos **operación en A** (o ley de composición interna) a una función de $A \times A \to A$
Con esta definición podemos determinar una operación en cualquier conjunto no vacío por modesto que este sea.
Definamos una operación (llamémosla *) en el conjunto $A = \{a, b\}$

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



Solemos anotar $a * a = a$ $a * b = b$ $b * a = b$ y $b * b = b$ o también presentar una tabla de doble entrada en lugar de un diagrama de "flechas".

*	a	b
a	a	b
b	b	b

Ejercicio Definir una operación en $B = \{m, n, p\}$
Tengamos presente entonces que una operación o una ley de composición interna en un conjunto no vacío A no es otra cosa que una función de $A \times A \to A$ y por lo tanto si tenemos una correspondencia entre pares de elementos de un conjunto A y elementos del propio A para poder afirmar que dicha correspondencia es una operación debe cumplirse:
1) La imagen de cada par (el "resultado de la operación") debe pertenecer al conjunto A. 2) Y debe ser única.

Así con esta definición de operación la resta en N no es una operación pues falla la primera condición. Y tampoco es una operación el producto de un vector por un escalar pues no estamos operando elementos del mismo conjunto.

Cabe señalar que no es la única definición de operación que puede tomarse. Sino que es la mas restrictiva pues nos obliga a " operar" con elementos del mismo conjunto (lo cual deja afuera el producto de un escalar por un vector) y también nos obliga a que el resultado sea del mismo conjunto del cual son los "operandos" (con lo cual el producto interno de vectores no sería una operación) Otras definiciones mas amplias permiten "operar" elementos de distinto conjunto y también que el resultado no pertenezca al mismo conjunto que los elementos operados. Lo que se exige en casi todas las definiciones de operación que se puede encontrar en diferente bibliografía es la *unicidad* del resultado. Nosotros adoptamos esta definición pues es la elegida en "matemática básica".

Nota 2 Si leemos con atención el axioma 1 percibimos que entre las muchas cosas que este nos dice esta que el conjunto de los números reales es un conjunto no vacío que tiene al menos dos elementos: el 0 y el 1 neutros de la suma y el producto.
Nada en este axioma implica que $\Re$ tenga mas que estos dos elementos; pues si tomamos $\Re = \{0,1\}$ y la suma y el producto definidos por

+	**0**	**1**
0	0	1
1	1	0

·	**0**	**1**
0	0	0
1	0	1

El lector podrá comprobar que este modelo verifica el axioma 1 Lo cual no solamente sirve como argumento para lo dicho sino que también para corroborar la consistencia del mismo.

Nota 3 Como recién dijimos el axioma de cuerpo no lleva a que $\Re$ tenga infinitos elementos como todos esperamos. Esto será necesariamente cierto recién cuando entre en juego el segundo axioma. El lector atento también habrá notado que se indica explícitamente en el primer axioma que $0 \neq 1$. Esto se debe a que si tal proposición no es necesariamente cierta tomando $\Re = \{0\}$ y 0+0=0 , 0.0=0 tal modelo verifica toda la axiomática que veremos sobre número real; creando un modelo trivial que no es el que andamos buscando generar.

Veamos ahora algunas proposiciones que se desprenden de manera mas o menos inmediata del axioma de cuerpo.

Teorema Unicidad de los neutros

1) 0 es el único neutro de la suma. 2) 1 es el único neutro del producto

Dem2)
Supongamos que $\exists\, 1' \in \Re\,;\, a.1' = 1'.a = a \quad \forall a \in \Re$ Entonces

$$\left.\begin{array}{l} 1.1' = 1 \quad \text{por la sup osiciyn} \\ 1.1' = 1' \quad \text{por } P_3 \end{array}\right\} \Rightarrow 1 = 1'$$

Y por lo tanto 1 es el único neutro del producto de reales.

Obsérvese que en la última implicación se utilizó que el producto es una operación en $\Re$ y por lo tanto el resultado de un mismo producto es único.

Teorema Cancelativas

1) $a + b = a + c \;\Rightarrow\; b = c$ 2) $\left.\begin{array}{l} a.b = a.c \\ a \neq 0 \end{array}\right\} \;\Rightarrow\; b = c$

Dem 1) $a + b = a + c \;\Rightarrow\; op(a) + (a + b) = op(a) + (a + c) \;\Rightarrow\; [op(a) + a] + b = [op(a) + a] + c \;\Rightarrow$
$\Rightarrow\; 0 + b = 0 + c \;\Rightarrow\; b = c$

Ejercicio 1) Justifique el lector los pasos dados en la demostración anterior
2) Demuestre justificando detalladamente el punto 2)
3) ¿Por qué en la segunda proposición se exige que el factor cancelado sea distinto de cero?

Teorema Absorción

$$a.0 = 0 \quad \forall a \in \Re$$

Dem: $a + 0 = a = a.1 = a(1 + 0) = a.1 + a.0 = a + a.0 \;\Rightarrow\; a + 0 = a + a.0 \;\Rightarrow\; 0 = a.0$

Justifique el lector todos y cada uno de los pasos dados .

Teorema Ausencia de divisores de 0

$$a.b = 0 \quad \Rightarrow \quad \begin{cases} a = 0 \\ \vee \\ b = 0 \end{cases}$$

Dem: Si a=0 la proposición es verdadera

$$\underline{\text{Si } a \neq 0} \quad \left.\begin{array}{l} \text{por hipytesis } a.b = 0 \\ \text{por el teorema anterior } a.0 = 0 \end{array}\right\} \quad \Rightarrow \quad a.b = a.0 \text{ como además } a \neq 0 \quad \Rightarrow_{\text{cancelativa}} \quad b = 0$$

Teorema Existencia y unicidad de la diferencia

$$\text{H) } a, b \in \Re \qquad \text{T) } \begin{cases} 1) \exists c \in \Re \,;\, a = c + b \\ 2) \text{ c es ънico} \end{cases}$$

Dem: 1) $a = c + b \quad \Leftrightarrow \quad a + op(b) = [c + b] + op(b) \quad \Leftrightarrow \quad a + op(b) = c + [b + op(b)] \quad \Leftrightarrow \quad a + op(b) = c + 0 \quad \Leftrightarrow$
$\Leftrightarrow \quad c = a + op(b)$

Para terminar la demostración de la existencia basta tomar c=a+op(b) y realizar c+b aplicando las propiedades ya vistas el lector seguramente llegará a que c+b=a.

Dem 2) Supongamos que $\exists\, c' \in \Re \,;\, a = c' + b$ Como por lo demostrado en 1) $\exists\, c \in \Re \,;\, a = c + b$ entonces
c+b=c'+b $\Rightarrow_{\text{canc}}$ $c = c'$

Nota 1) Al número c lo denominaremos **diferencia** entre a y b. Anotamos c=a-b
2) En el teorema inmediato anterior no solamente se demostró que existe c tal que a=c+b sino que también se calculó cuanto vale; llegando a que c=a+op(b). Por lo tanto $\boxed{a - b = a + op(b)}$
3) Teniendo en cuenta el resultado anterior $0 - x = 0 + op(x) = op(x) \quad \Rightarrow \quad op(x) = 0 - x \quad \forall x \in \Re$
Lo cual justifica la notación habitual de opuesto **op(x) = -x**

Teorema Existencia y unicidad del cociente.

$$\text{H) } \begin{cases} a, b \in \Re \\ b \neq 0 \end{cases} \qquad \text{T) } \begin{cases} 1) \exists c \in \Re \,;\, a = c.b \\ 2) \text{ c es ънico} \end{cases}$$

Demostración a cargo del lector.

Nota 1) Al número c lo denominaremos **cociente** entre a y b Anotamos $c = \frac{a}{b}$
2) Cuando demostró el teorema inmediato anterior seguramente llegó a que $c = a.inv(b)$; teniendo entonces que

$$\boxed{\frac{a}{b} = a.inv(b)}$$

3) Por lo tanto $\frac{1}{x} = 1.inv(x) = inv(x) \quad \Rightarrow \quad \boxed{inv(x) = \frac{1}{x} \quad \forall x \in \Re^*} \qquad (\Re^* = \Re - \{0\})$

Ejercicios (primer repartido del curso presencial)

I) Demostrar las siguientes proposiciones en $(\Re,+,\cdot)$ donde a,b,c,d son números reales.

i) op(op(a))=a **ii)** inv(inv(a))=a **iii)** $a - b = 0 \quad \Leftrightarrow \quad a = b$ **iv)** $\frac{a}{b} = 1 \quad \Leftrightarrow \quad a = b \quad (a \neq 0 \;\; b \neq 0)$

v) op(0) = 0 **vi)** inv(1)=1 **vii)** $a \neq 0 \quad \Rightarrow \quad -a \neq 0$ **viii)** $a + b = a - (-b)$ **ix)** $-(a + b) = -a - b$

x) $-a = (-1).a$ **xi)** $-(a.b) = (-a).b = a.(-b)$ **xii)** $(-a).(-b) = a.b$ **xiii)** $a.(b-c) = ab - ac$

xiv) $\text{inv}(a.b) = \text{inv}(a).\text{inv}(b)$ **xv)** $\frac{a}{1} = a$ **xvi)** $-\frac{a}{b} = \frac{-a}{b} = \frac{a}{-b}$ **xvii)** $\text{inv}\left(\frac{a}{b}\right) = \frac{b}{a} \quad (a \neq 0\ b \neq 0)$

xviii) $\frac{a}{\frac{b}{c}} = \frac{a.c}{b} \quad (b \neq 0\ c \neq 0)$ **xix)** $\frac{a}{b} \pm \frac{c}{d} = \frac{ad \pm cb}{bd} \quad (b \neq 0\ d \neq 0)$ **xx)** $\frac{a}{b}.\frac{c}{d} = \frac{ac}{bd} \quad (b \neq 0\ d \neq 0)$

Notas 1) En la propuesta anterior utilizamos indistintamente op(a) ó –a e inv(a) ó $\frac{1}{a}$ según consideramos conveniente

A partir de este momento utilizaremos exclusivamente la notación habitual (-a y $\frac{1}{a}$).

2) Una vez culminado este ejercicio habrá demostrado muchas de las propiedades usuales del álgebra elemental de manera relativamente sencilla y transparente utilizando exclusivamente el axioma de cuerpo y sus primeras consecuencias.

II) Hallar, justificando el procedimiento, el conjunto de los números reales x que cumplen:

i) x+2=5 **ii)** 3x+1= x-3 **iii)** 5x-2=2x+4 **iv)** 0+x=x **v)** x+x=x **vi)** x.0=0

vii) x.0=2 **viii)** (x+3).(x-1)=0 **ix)** $x^3 - 2x^2 = 0$

¿Qué otro título pondría ud. al ejercicio anterior? ¿Cómo denominaría al conjunto hallado? ¿Y a cada uno de sus elementos?

Notas

1) A manera de ejemplo hagamos un par de ejercicios.

ii) $3x+1 = x-3 \Leftrightarrow_{S_4} (3x+1)+(-1) = (x-3)+(-1) \Leftrightarrow_{S_1} 3x+(1+(-1)) = x+(-3+(-1)) \Leftrightarrow$

$\Leftrightarrow_{S_4 \text{ y } (*)} 3x+0 = x-4 \Leftrightarrow_{S_3} 3x = x-4 \Leftrightarrow_{S_4} (-x)+3x = (-x)+(x-4) \Leftrightarrow_{S_1}$

$\Leftrightarrow [-1+3]x = [-x+x]-4 \Leftrightarrow_{S_4} 2x = 0-4 \Leftrightarrow_{S_3} 2x = -4 \Leftrightarrow_{P_4} (\tfrac{1}{2})(2x) = \left(\tfrac{1}{2}\right)(-4) \Leftrightarrow$

$\Leftrightarrow_{P_1} \left[\left(\tfrac{1}{2}\right)2\right]x = -2 \Leftrightarrow_{P_4} 1.x = -2 \Leftrightarrow_{P_3} x = -2$

Por lo tanto el conjunto buscado es: $S_{ii} = \{-2\}$

iv) 0+x=x Como $0 + x = x \quad \forall x \in \Re \ (S_3)$ entonces el conjunto buscado es $S_{iv} = \Re$

2) Somos conscientes que hemos utilizado números reales (2,3,-4 etc.) que no estamos autorizados a utilizar a esta altura del desarrollo teórico. A pesar de ello lo hicimos por motivos didácticos.
Por el momento entendemos: 2=1+1 , 3=2+1, 4=3+1, -4=op(4) etc. Así también $x^2 = x.x$ y $x^3 = x.x^2$
De esta forma (*) $-3+(-1) = (-1).3 + (-1).1 =_{SP} (-1).[3+1] = (-1).4 = -4$ Obsérvese que además de utilizar el axioma 1 hemos usado algunas de las propiedades demostradas en el ejercicio I).

3) Habitualmente este ejercicio lo titularíamos: Resolver justificando el procedimiento las siguientes ecuaciones en $(\Re,+,\cdot)$ Al conjunto hallado se le suele llamar conjunto solución de la ecuación y a cada uno de sus elementos raíz de la ecuación.
Nótese que la justificación no es otra cosa que la utilización de las propiedades ya vistas de los números reales. Ni definimos ecuación; ni utilizamos "metateoremas" sobre la resolución de ecuaciones. Lo cual es mas que difícil diríamos imposible de hacer correctamente.

Ejercicio Resolver y discutir según a y b en $(\Re,+,\cdot)$ la ecuación ax+b=0

ORDEN EN LOS REALES

A continuación intentaremos introducir en $(\Re,+,\cdot)$ una relación de orden estricto total ($<$) y una relación de orden amplio total compatible con la suma y el producto. En pocas palabras intentaremos ordenar al cuerpo de los reales con las características previstas. Lo cual haremos por intermedio del siguiente axioma.

Axioma 2 Axioma de orden

Existe un subconjunto de los reales a los cuales denominamos reales positivos (anot. $\Re^+$) que cumple:

1) Todo real x cumple una y solo una de las siguientes proposiciones: i) $x \in \Re^+$ ii) $x=0$ iii) $-x \in \Re^+$

2) Si $x \in \Re^+$ e $y \in \Re^+ \Rightarrow \begin{cases} x+y \in \Re^+ \\ \wedge \\ x.y \in \Re^+ \end{cases}$

Nota Cuando en el punto 1) decimos que todo real cumple una y sólo una de las siguientes proposiciones estamos diciendo que todo real necesariamente entra en uno de esos tres "casilleros" y en solamente uno. En otras palabras queremos expresar que todo real es o positivo o cero o que su opuesto es positivo; que no hay reales que no entren en una de esas tres categorías. Y además en una sola de ellas; dicho de otra forma que un mismo real no puede ser simultáneamente positivo y cero o positivo y su opuesto también o cero y su opuesto positivo.

En el segundo punto estamos diciendo que la suma y el producto de dos reales positivos da como resultado un real también positivo. Tengamos en cuenta que para nosotros por ahora ser positivo es pertenecer a ese subconjunto de los reales del cual afirmamos su existencia en el axioma 2 y que denominamos reales positivos.

Lo que primeramente demostraremos es que el mencionado subconjunto no es vacío.

Teorema

$1 \in \Re^+$

Dem Probémoslo por absurdo. Suponemos $1 \notin \Re^+$ ya que por intermedio del Ax 1 sabemos que $1 \neq 0$ aplicando la primera proposición del axioma 2 tenemos que: $-1 \in \Re^+ \Rightarrow_{Ax2\,-2)} (-1).(-1) \in \Re^+$

Como demostramos anteriormente (-a).(-b)=a.b $\Rightarrow$ $(-1).(-1) = 1.1 = 1 \Rightarrow 1 \in \Re^+$ pero habíamos supuesto que $1 \notin \Re^+$ lo cual es contradictorio.

Definición

Consideramos $a, b \in \Re$ decimos que:

1) $a < b \Leftrightarrow b - a \in \Re^+$
2) $a > b \Leftrightarrow b < a$
3) $a \leq b \Leftrightarrow \begin{cases} a < b \\ \vee \\ a = b \end{cases}$
4) $a \geq b \Leftrightarrow b \leq a$

Observación.- Notemos que definimos menor a través de los reales positivos cuya existencia está asegurada por el axioma de orden. Como ocurre habitualmente al definir la relación menor (mayor) queda definida su relación inversa mayor (menor).
Probemos ahora para nuestra tranquilidad que ser positivo es ser mayor que 0.

Teorema

$$x > 0 \quad \Leftrightarrow \quad x \in \Re^+$$

Demostración

$$x > 0 \quad \Leftrightarrow \quad 0 < x \quad \Leftrightarrow \quad x - 0 \in \Re^+ \quad \Leftrightarrow \quad x \in \Re^+$$

Definición

Llamamos conjunto de los reales negativos (anotamos $\Re^-$) al conjunto formado por los opuestos de los reales positivos. Sintéticamente:

$$\Re^- = \left\{ x \in \Re \,;\, -x \in \Re^+ \right\}$$

Con esta definición podemos enunciar de manera mas familiar la primera proposición del axioma de orden diciendo que: todo real cumple una y una sola de las siguientes proposiciones i) es positivo ii) es cero ó iii) es negativo.

Teorema

$$x < 0 \quad \Leftrightarrow \quad x \in \Re^-$$

Demostración a cargo del lector.

Probemos que las relaciones que acabamos de definir "merecen" el nombre que les dimos.

Teorema < es una relación de orden estricto total en $\Re$. O sea cumple:

1) $a \not< a \quad \forall a \in \Re$ (Inídentica)
2) $a < b \quad \Rightarrow \quad b \not< a$ (Asimétrica)
3) $\left.\begin{matrix} a < b \\ b < c \end{matrix}\right\} \quad \Rightarrow \quad a < c$ (Transitiva)
4) Todo par de reales a y b verifica una y solo uno de las siguientes proposiciones: i) a<b
ii) a=b
iii) a>b (Tricotomía)

Demostración 3)

$$\left.\begin{matrix} a < b \quad \Rightarrow \quad b - a \in \Re^+ \\ b < c \quad \Rightarrow \quad c - b \in \Re^+ \end{matrix}\right\} \Rightarrow_{Ax2} \quad (b-a)+(c-b) \in \Re^+ \quad \text{como (b-a)+(c-b)=c-a entonces}$$

$$c - a \in \Re^+ \quad \Rightarrow \quad a < c$$

Las demás demostraciones quedan a cargo del lector.

Teorema Monotonías de la suma y el producto (compatibilidad con las operaciones)

1) $a < b \Rightarrow a + c < b + c$ (Monotonía de la suma)

2) $\left.\begin{matrix} a < b \\ c < d \end{matrix}\right\} \Rightarrow a + c < b + d$ (Monotonía generalizada de la suma)

3) $\left.\begin{matrix} a < b \\ c \in \Re^+ \end{matrix}\right\} \Rightarrow a.c < b.c$ (Monotonía del producto)

4) $\left.\begin{matrix} a < b \\ c \in \Re^- \end{matrix}\right\} \Rightarrow a.c > b.c$

Dem 3) Debemos probar que: $a.c < b.c \Leftrightarrow bc - ac \in \Re^+$

Por hipótesis $\left.\begin{matrix} a < b \Rightarrow b - a \in \Re^+ \\ c \in \Re^+ \end{matrix}\right\} \Rightarrow_{Ax2} (b - a).c \in \Re^+$ Como (b-a).c = b.c - a.c

Entonces $b.c - a.c \in \Re^+ \Rightarrow a.c < b.c$

Teorema (Regla de los signos del producto)

1) $a \in \Re^+ \; b \in \Re^+ \Rightarrow a.b \in \Re^+$
2) $a \in \Re^+ \; b \in \Re^- \Rightarrow a.b \in \Re^-$
3) $a \in \Re^- \; b \in \Re^- \Rightarrow a.b \in \Re^-$

Demostración 2)

$\left.\begin{matrix} b \in \Re^- \Rightarrow -b \in \Re^+ \\ \text{como } a \in \Re^+ \end{matrix}\right\} \Rightarrow_{Ax2} a.(-b) \in \Re^+$ Por lo visto en uno de los ejercicios anteriores a.(-b) = -a.b

En consecuencia $-a.b \in \Re^+ \Rightarrow a.b \in \Re^-$ (Tengamos presente la definición adoptada de reales negativos)

Teorema Densidad

Dados dos números reales cualesquiera a y b siendo a < b se cumple que: $\exists c \in \Re \; ; a < c < b$

Demostración

$\left.\begin{matrix} a < b \Rightarrow_{\text{monot. de (+)}} a + a < a + b \\ a < b \Rightarrow_{\text{monot. de (+)}} a + b < b + b \end{matrix}\right\} \Rightarrow a + a < a + b < b + b \Rightarrow 2a < a + b < 2b \Rightarrow$

$\Rightarrow_{\text{monot. del produc.}} a < \dfrac{a + b}{2} < b$

Efectivamente $\exists c \in \Re \ \left(c = \frac{a+b}{2}\right)$ tal que $a < c < b$

Nota En la demostración anterior se utilizó que a+a = 2.a ¿Qué nos justifica tal afirmación?

$a + a = 1.a + 1.a = (1+1).a = 2.a$ Por otra parte vimos que $1 \in \Re^+ \Rightarrow 1 > 0 \Rightarrow 1+1 > 0+1 = 1$

Entonces 1+1 > 1 > 0 En consecuencia 1+1 es un real distinto del 0 y del 1, por lo tanto tenemos derecho a "bautizarlo" con un nombre diferente; lo denominamos 2.

Un razonamiento similar nos lleva a 0 , 1 , 2 , 2+1(que denominamos 3) , 3+1 (4) , 4+1 (5) ,..... son números reales necesariamente diferentes. Entonces la aceptación del axioma 1 y del axioma 2 nos lleva a que $\Re$ tiene infinitos elementos; lo cual, como vimos, no es así solamente con el primer axioma.

Ejercicios (Repartido 2 del curso regular)

I) Demostrar que en el cuerpo ordenado de los números reales se cumple:

i) $\left.\begin{matrix} a \in \Re^- \\ b \in \Re^- \end{matrix}\right\} \Rightarrow a + b \in \Re^-$ **ii)** $a \in \Re^+ \Leftrightarrow \frac{1}{a} \in \Re^+$ **iii)** $a \in \Re^- \Leftrightarrow \frac{1}{a} \in \Re^-$

iv) Si $\forall \varepsilon \in \Re^+ \ 0 \le x < \varepsilon \Rightarrow x = 0$ **v)** $a \le a \quad \forall a \in \Re$ **vi)** $\left.\begin{matrix} a \le b \\ b \le a \end{matrix}\right\} \Rightarrow a = b$

vii) $\left.\begin{matrix} a \le b \\ b \le c \end{matrix}\right\} \Rightarrow a \le c$ **viii)** $\forall a, b \in \Re \quad a \le b \ \underset{o}{y} \ b \le a$

ix) $a \le b \Rightarrow a + c \le b + c$ **x)** $\left.\begin{matrix} a \le b \\ c \le d \end{matrix}\right\} \Rightarrow a + c \le b + d$ **xi)** $\left.\begin{matrix} a \le b \\ c \in \Re^+ \end{matrix}\right\} \Rightarrow ac \le bc$

xii) $\left.\begin{matrix} a \le b \\ c \in \Re^- \end{matrix}\right\} \Rightarrow ac \ge bc$ **xiii)** $\left.\begin{matrix} 0 < a < b \\ 0 < c < d \end{matrix}\right\} \Rightarrow ac < bd$ **xiv)** $\left.\begin{matrix} a \le b \\ b < c \end{matrix}\right\} \Rightarrow a < c$

(*Las proposiciones v) vi) y vii) nos permiten afirmar que* $\le$ *es una relación de orden amplio; el cumplimiento además de la proposición viii) nos asegura que es una relación de orden amplio total.)*

II) i) Demostrar $x^2 \ge 0 \quad \forall x \in \Re$

ii) " $a^2 + b^2 = 0 \Leftrightarrow a = b = 0$

iii) Si $a, b \in \Re^+$ demostrar que $a < b \Leftrightarrow a^2 < b^2$

iv) Sin la exigencia de que a y b sean positivos ¿La proposición anterior es válida?

III) i) Probar que $x^2 + y^2 \ge 2xy \quad \forall x, y \in \Re$

ii) Sabiendo que $a, b, c \in \Re^+$ y además $a + b + c = 1$; probar:

1) $(1-a)^2 \ge 4bc$

2) $(1-a).(1-b),(1-c) \ge 8abc$

IV) Hallar el conjunto de los $x \in \Re$ tales que: **1) i)** 3x+2 < 0 **ii)** 3x+2 = 0 **iii)** 3x+2 > 0

2) i) –3x+1 <0 **ii)** –3x+1 = 0 **iv)** –3x+1 > 0

¿Qué otros nombres se le ocurren para este ejercicio?

V) Estudiar en $(\Re,+,\cdot,\leq)$ el signo de $f:\Re\to\Re\,;\,f(x)=ax+b\quad(a,b\in\Re)$

VI) Resolver en $(\Re,+,.,\leq)$ y discutir según m $(m\in\Re)$ las siguientes inecuaciones:

i) $mx>3$ **ii)** $(3-2m).x<m-1$ **iii)** $(m^2+\sqrt{2}).x<-3$

iv) $m^3x+2m<0$ **v)** $\dfrac{x}{m-1}\geq m+1\quad(m\neq 1)$ **vi)** $\dfrac{x}{m-2}>\dfrac{x}{m+2}-3\quad(m\neq -2, m\neq 2)$

Nota Pasamos ahora a la resolución de algunos ejercicios a manera de muestra.

IV) 1) i) $3x+2<0 \;\Leftrightarrow_{\text{monot.}(+)}\; (3x+2)+(-2)<0+(-2) \;\Leftrightarrow\; 3x<-2 \;\Leftrightarrow_{\text{monot}(\cdot)}\; \left(\frac{1}{3}\right)3x<\left(\frac{1}{3}\right)(-2)$

$\Leftrightarrow\quad x<-\frac{2}{3}$ Por lo tanto $S_i=\left\{x\in\Re\,;\,x<-\frac{2}{3}\right\}$

ii) $3x+2=0 \;\Leftrightarrow\; x=-\frac{2}{3}$ Entonces $S_{ii}=\left\{-\frac{2}{3}\right\}$

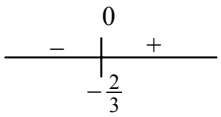
iii) $3x+2>0 \;\Leftrightarrow\; (3x+2)+(-2)>0+(-2) \;\Leftrightarrow\; 3x>-2 \;\Leftrightarrow\; \left(\frac{1}{3}\right)3x>\left(\frac{1}{3}\right)(-2) \;\Leftrightarrow\; x>-\frac{2}{3}$

En consecuencia $S_{iii}=\left\{x\in\Re\,;\,x>-\frac{2}{3}\right\}$

Este ejercicio podríamos titularlo: Resolver en $(\Re,+,\cdot,\leq)$ las siguientes inecuaciones: .....

También podríamos decir: Hallar en $(\Re,+,\cdot,\leq)$ el signo de $f:\Re\to\Re\,;\,f(x)=3x+2$ lo cual solemos esquematizar:

Sig (3x+2)



V) Entendemos por estudiar el signo de f: f(x) = ax+b en $(\Re,+,\cdot,\leq)$ a encontrar el conjunto de los x reales cuyas imágenes son positivas, el conjunto de los reales cuya imagen es 0 y el conjunto de los reales cuya imagen es negativa.

$ax+b>0 \;\Leftrightarrow_{\text{monot.}(+)}\; (ax+b)+(-b)>0+(-b) \;\Leftrightarrow\; ax>-b$

Como seguramente el lector prevé debemos ahora utilizar la monotonía del producto; para lo cual nos es necesario discutir si el factor por el cual pretendemos multiplicar la desigualdad ($\frac{1}{a}$) es positivo o negativo.

Si $a>0$ $\quad ax>-b \;\Leftrightarrow\; \left(\frac{1}{a}\right)ax>\left(\frac{1}{a}\right)(-b) \;\Leftrightarrow\; x>-\frac{b}{a}$

Si $a<0$ $\quad ax>-b \;\Leftrightarrow\; \left(\frac{1}{a}\right)ax<\left(\frac{1}{a}\right)(-b) \;\Leftrightarrow\; x<-\frac{b}{a}$

$ax+b=0 \;\Leftrightarrow\; x=-\frac{b}{a}$ (Justificación ya vista)

$ax+b<0 \;\Leftrightarrow\; (ax+b)+(-b)<0+(-b) \;\Leftrightarrow\; ax<-b$

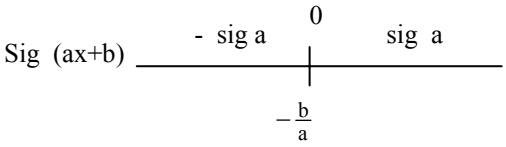
Si $a>0$ $\quad ax<-b \;\Leftrightarrow\; \left(\frac{1}{a}\right)ax<\left(\frac{1}{a}\right)(-b) \;\Leftrightarrow\; x<-\frac{b}{a}$

Si $a<0$ $\quad ax<-b \;\Leftrightarrow\; \left(\frac{1}{a}\right)ax>\left(\frac{1}{a}\right)(-b) \;\Leftrightarrow\; x>-\frac{b}{a}$

En resumen: **Si a > 0** $ax+b>0 \Leftrightarrow x>-\frac{b}{a}$ $\quad ax+b=0 \Leftrightarrow x=-\frac{b}{a}$ $\quad ax+b<0 \Leftrightarrow x<-\frac{b}{a}$

Si a < 0 $ax+b>0 \Leftrightarrow x<-\frac{b}{a}$ $\quad ax+b=0 \Leftrightarrow x=-\frac{b}{a}$ $\quad ax+b<0 \Leftrightarrow x>-\frac{b}{a}$

Resultados que esquematizamos:



Pasemos ahora a estudiar el signo de la función de segundo grado. Antes algunas proposiciones previas.

Lema

Siendo $a \in \Re$ llamamos $a^2 = a.a$ Se cumple que: 1) $(a-b).(a+b) = a^2 - b^2$

2) $a^2 = b^2 \Leftrightarrow \begin{cases} a = b \\ \vee \\ a = -b \end{cases}$

Demostración a cargo del lector.

Resolución en $(\Re,+,\cdot,\leq)$ de $ax^2+bx+c=0$ $(a \neq 0)$

$ax^2+bx+c=0 \Leftrightarrow ax^2+bx=-c \Leftrightarrow_{(*)} 4a^2x^2+4abx=-4ac \Leftrightarrow 4a^2x^2+4abx+b^2=b^2-4ac$

Llamando Δ al número real b^2-4ac como además $4a^2x^2+4abx+b^2=(2ax+b)^2$ tenemos que:

$ax^2+bx+c=0 \Leftrightarrow (2ax+b)^2=\Delta$

Si Δ>0 $(2ax+b)^2=\Delta \Leftrightarrow (3ax+b)^2=\left(\sqrt{\Delta}\right)^2 \Leftrightarrow \begin{cases} 2ax+b=\sqrt{\Delta} \Leftrightarrow x=\frac{-b+\sqrt{\Delta}}{2a} \\ 2ax+b=-\sqrt{\Delta} \Leftrightarrow x=\frac{-b-\sqrt{\Delta}}{2a} \end{cases}$

Por lo tanto en este caso $S=\left\{\frac{-b+\sqrt{b^2-4ac}}{2a}, \frac{-b-\sqrt{b^2-4ac}}{2a}\right\}$

Si Δ=0 $(2ax+b)^2=0 \Leftrightarrow 2ax+b=0 \Leftrightarrow x=-\frac{b}{2a}$

Entonces si $\Delta=0$ $S=\left\{\frac{-b}{2a}\right\}$

Si Δ< 0 Como $\forall x \in \Re\ (2ax+b)^2 \geq 0 \Rightarrow \nexists x \in \Re\,;(2ax+b)^2=\Delta \Rightarrow S=\varnothing$

Nota (*) Multiplicamos ambos miembros por 4.a (tengamos presente que $a \neq 0$) con el objetivo de completar el cuadrado de un binomio. También fue el motivo por el cual sumamos b^2 en el paso siguiente.

Nota Somos conscientes que hemos utilizado raíz cuadrada sin haberla definido y menos demostrado que todo positivo tiene una raíz cuadrada. El desarrollo teórico hecho hasta el momento no nos lo permite (Precisamos para ello el tercer axioma). A pesar de lo dicho utilizamos $\sqrt{\Delta}$ para no postergar el estudio del trinomio de segundo grado lo cual consideramos conveniente desde el punto de vista didáctico. Preferimos aquí hacer una disgreción desde el punto de vista formal con el fin de un mejor desarrollo del curso práctico.

Ejercicio Consideramos $f:\Re\to\Re\ ;\ f(x)=ax^2+bx+c \quad (a,b,c\in\Re\ ,\ a\neq 0)$ vimos que sí $\Delta=b^2-4ac>0$

la función f tiene dos raíces reales distintas; a saber $\alpha=\dfrac{-b+\sqrt{\Delta}}{2a}$ y $\beta=\dfrac{-b-\sqrt{\Delta}}{2a}$ Probar que:

1) $\alpha+\beta=-\dfrac{b}{a} \qquad \alpha.\beta=\dfrac{c}{a}$ 2) $f(x)=a.(x-\alpha).(x-\beta) \quad \forall x\in\Re$

Signo del trinomio de segundo grado

Consideramos $f:\Re\to\Re\ ;\ f(x)=ax^2+bx+c$ con $a,b,c\in\Re\ a\neq 0.$

Si Δ>0 Vimos que f acepta dos raíces reales que llamamos α y β $(\alpha<\beta)$ Además $f(x)=a.(x-\alpha).(x-\beta) \quad \forall x\in\Re$

$\forall x_1\in\Re\ ;\ x_1<\alpha<\beta \ \Rightarrow\ x_1-\alpha<0$ y $x_1-\beta<0$

Por lo tanto

Si $a>0 \ \Rightarrow\ f(x_1)=a.(x_1-\alpha).(x_1-\beta)>0$ (producto de un positivo por dos negativos)

Si $a<0 \ \Rightarrow\ f(x_1)=a.(x_1-\alpha).(x_1-\beta)>0$ (producto de tres negativos)

Análogamente se prueba que: $\forall x_2\in\Re\ ;\ \alpha<x_2<\beta$ si $a>0 \ \Rightarrow\ f(x_2)<0$

si $a<0 \ \Rightarrow\ f(x_2)>0$

Y que: $\forall x_3\in\Re\ ;\ \alpha<\beta<x_3$ si $a>0 \ \Rightarrow\ f(x_3)>0$

si $a<0 \ \Rightarrow\ f(x_3)<0$

$$f(x)=ax^2+bx+c \ \Rightarrow\ 4af(x)=4a^2x^2+4abx+4ac=\underbrace{4a^2x^2+4abx+b^2}_{(2ax+b)^2}\underbrace{-b^2+4ac}_{-\Delta} \ \Rightarrow\ 4af(x)=(2ax+b)^2-\Delta$$

Si Δ=0 $\Rightarrow\ 4af(x)=(2ax+b)^2 \ \Rightarrow\ 4af(x)\geq 0 \quad \forall x\in\Re$

Es más $4af(x)>0 \quad \forall x\in\Re\ ;\ x\neq\frac{-b}{2a}$ y $f\left(\frac{-b}{2a}\right)=0$

Por lo tanto: Si $a>0 \ \Rightarrow\ 4a>0 \ \Rightarrow\ f(x)>0 \quad \forall x\in\Re\ ;\ x\neq\frac{-b}{2a}$

Si $a<0 \ \Rightarrow\ 4a<0 \ \Rightarrow\ f(x)<0 \quad \forall x\in\Re\ ;\ x\neq\frac{-b}{2a}$

Si Δ<0 $\Rightarrow\ -\Delta>0$ como además $(2ax+b)^2\geq 0 \ \forall x\in\Re \ \Rightarrow\ 4af(x)=(2ax+b)^2-\Delta \quad \forall x\in\Re$

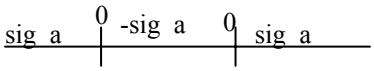
Por lo tanto: si $a>0 \ \Rightarrow\ f(x)>0 \quad \forall x\in\Re$

si $a<0 \ \Rightarrow\ f(x)<0 \quad \forall x\in\Re$

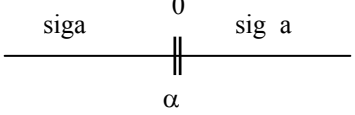
En resumen y esquemáticamente:

Consideramos $f:\Re\to\Re\,;\,f(x)=ax^2+bx+c$ con $a,b,c\in\Re$ $a\neq 0$. Denominamos $\Delta=b^2-4ac$

1) Δ>0 $\Leftrightarrow$ f acepta dos raıcesreales α y β $(\alpha<\beta)$ Sig f(x)



2) Δ=0 $\Leftrightarrow$ f acepta una sola raızreal α (doble) Sig f(x)



3) Δ<0 $\Leftrightarrow$ f no acepta raíces reales Sig f(x) sig a

Ejercicios (repartido 3 del curso habitual)

I) Resolver en $(\Re,+,.,\leq)$ los siguientes sistemas de inecuaciones:

i) $\begin{cases}(x+1)^2-(x+3)<0\\ \dfrac{2x+3}{5-3x}\geq 0\end{cases}$ **ii)** $\begin{cases}\dfrac{x^2+1}{x-3}\leq 0\\ \dfrac{1-3x}{1-x^2}>1\end{cases}$ **iii)** $x-3\leq 3x-1\leq 7-x$

II) Dada la ecuación $x^2-(m+2)x+\frac{1}{4}=0$ $(m\in\Re)$. Determinar los valores de m para que: **i)** Acepte solo una raíz real. **ii)** Acepte solo dos raíces reales.

III) Consideramos $f:\Re\to\Re$; $f(x)=x^2+px+q$ de raíces reales α y β.
Hallar en función de p y q los trinomios de segundo grado y coeficiente principal 1 que tengan las raíces:

i) $-\alpha$ y $-\beta$ **ii)** $\dfrac{1}{\alpha}$ y $\dfrac{1}{\beta}$ **iii)** α^2 y β^2

iv) $\dfrac{1}{\alpha^2+1}$ y $\dfrac{1}{\beta^2+1}$ **v)** α^3 y β^3 **vi)** $\dfrac{1}{\alpha^2+\beta}$ y $\dfrac{1}{\alpha+\beta^2}$

IV) Hallar los valores de m $(m\in\Re)$ para que las siguientes ecuaciones admiten dos raíces α y β en las condiciones indicadas.

i) $x^2+(m+1).x+2m-1=0$; α y β son de distinto signo.

ii) $x^2+(3m-3).x+m^2+2m-3=0$; $\alpha>0$ y $\beta>0$

iii) $mx^2-2(m-1).x-m^2+m=0$; $\alpha>0$, $\beta>0$ y $|\alpha|>|\beta|$

V) Hallar los valores de m $(m\in\Re)$ para que: $(2m+1)x^2+(2m+3)x+1-m>0$ $\forall x\in\Re$

VI) Hallar los valores de m $(m \in \Re)$ para que las siguientes ecuaciones admitan dos raíces reales α y β en las condiciones indicadas.

i) $mx^2 + mx - 5 = 0 \quad ; \quad \alpha < 1 < \beta$

ii) $mx^2 + 2x - m = 0 \quad ; \quad \alpha < 0 \ , \ \beta > 1$

iii) $x^2 + mx - m + 1 = 0 \quad ; \quad \alpha < \beta < 2$

iv) $(m+1)x^2 - 2(m-1)x + m + 1 = 0 \quad ; \quad \alpha < \beta < -2$

v) $(m-1)x^2 + (m-3)x + m - 1 = 0 \quad ; \quad \alpha > \beta > 3$

vi) $(m-1)x^2 - 3mx + 2m = 0 \quad ; \quad -1 < \alpha < \beta < 1$

VII) Sea $f: \Re \to \Re \quad ; \quad f(x) = ax^2 + bx + c.$ Determinar una condición necesaria y suficiente para que:

i) $f(x) = 0$ admita dos raíces reales α y β / $\alpha < j < \beta \quad (j \in \Re)$

ii) $f(x) = 0$ admita dos raíces reales α y β / $\alpha < j < k < \beta$

iii) $f(x) = 0$ admita dos raíces reales α y β / $\alpha \in (j,k)$ y $\beta \notin (j,k)$

iv) $f(x) = 0$ admita dos raíces reales α y β / $\alpha \in (j,k)$ y $\beta \in (j,k)$

v) $f(x) = 0$ admita dos raíces reales α y β / $\alpha > \beta > k$

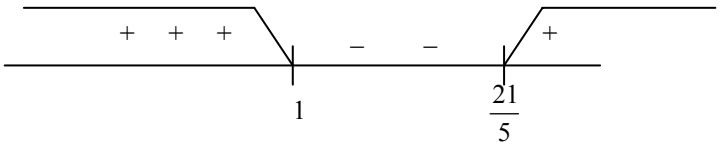
A continuación algunos ejercicios resueltos a manera de muestra.

IV) ii) La ecuación $x^2 + (3m-3)x + m^2 + 2m - 3 = 0$ acepta dos raíces reales positivas $\Leftrightarrow$

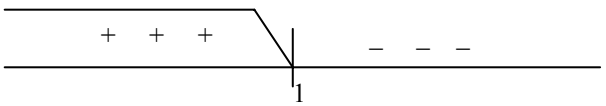
$$\Leftrightarrow \begin{cases} \Delta > 0 \\ \alpha + \beta > 0 \\ \alpha.\beta > 0 \end{cases} \Leftrightarrow \begin{cases} \Delta = b^2 - 4ac = (3m-3)^2 - 4.(1).(m^2 + 2m - 3) = 5m^2 - 26m + 21 > 0 \\ \alpha + \beta = \dfrac{-b}{a} = \dfrac{-3m+3}{1} = -3m + 3 > 0 \\ \alpha.\beta = \dfrac{c}{a} = \dfrac{m^2 + 2m - 3}{1} = m^2 + 2m - 3 > 0 \end{cases} \Leftrightarrow$$

$$\Leftrightarrow \begin{cases} 5m^2 - 26m + 21 > 0 \\ -3m + 3 > 0 \\ m^2 + 2m - 3 > 0 \end{cases}$$

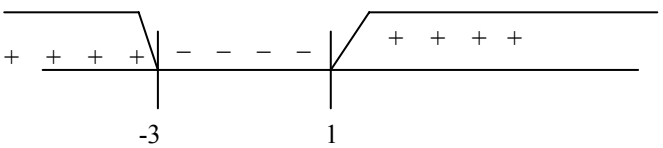
Sig $(5m^2 - 26m + 21)$



Sig (-3m+3)

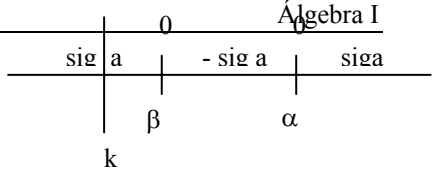


Sig $(m^2 + 2m - 3)$



La respuesta es: m < -3

VII) v) $f(x)=0$ admite dos raíces reales α y β ; $\alpha > \beta > k$ $\Leftrightarrow$ Sig $f(x)$



$$\Leftrightarrow \begin{cases} \Delta > 0 \\ a.f(k) > 0 \\ \dfrac{-b}{2a} > k \end{cases}$$

Nota

Exigimos $\Delta > 0$ con el objetivo de tener dos raíces reales. Con a.f(k)>0 obligamos a que f(k) tenga el mismo signo que a. Obsérvese que estas dos condiciones no son suficientes para lo exigido; pues puede cumplir ambas y ocurrir: $\beta < \alpha < k$ Para evitar este caso es que pedimos que el punto medio entre α y β sea mayor que k.

Téngase en cuenta que el punto medio entre α y β es $\dfrac{\alpha+\beta}{2} = \dfrac{\frac{-b}{a}}{2} = \dfrac{-b}{2a}$

Intente en el resto del ejercicio VII así como en el ejercicio VI) y en el V) buscar condiciones necesarias y suficientes que involucren valores calculables (discriminante, relaciones entre coeficientes y raíces, punto medio, etc.) lo mas "económicas" posibles.

Información mas detallada sobre el comportamiento del trinomio la puede encontrar en un trabajo titulado **"La función de segundo grado"** del prof. R.H.Cobas disponible en la Biblioteca de su Instituto de Formación Docente.

Valor absoluto

Definición

Consideramos un número real a . Denominamos **valor absoluto** de a (Anotamos $|a|$)

$$|a| = a \quad \text{si } a \geq 0 \qquad \text{y} \qquad |a| = -a \quad \text{si } a < 0$$

Ejemplos: $|4| = 4$, $|-3| = -(-3) = 3$, $|0| = 0$

Teorema

1) $|x| \geq 0 \quad \forall x \in \Re$
2) $|x| = 0 \quad \Leftrightarrow \quad x = 0$
3) $|x^2| = |x|^2 = x^2 \quad \forall x \in \Re$

4) $|x| = |y| \Leftrightarrow \begin{cases} x = y \\ \vee \\ x = -y \end{cases}$

5) $|x.y| = |x|.|y| \quad \forall x, y \in \Re$

6) $\left|\frac{x}{y}\right| = \frac{|x|}{|y|} \quad \forall x, y \in \Re$

7) $-|x| \leq x \leq |x| \quad \forall x \in \Re$

8) Siendo $r \in \Re^+$ se cumple que: i) $|x| \leq r \Leftrightarrow -r \leq x \leq r$

ii) $|x| \geq 0 \Leftrightarrow \begin{cases} x \geq r \\ \vee \\ x \leq -r \end{cases}$

(Las proposiciones anteriores son también válidas si intercambiamos $\leq$ por $<$ y $\geq$ por $>$)

9) $|x+y| \leq |x| + |y| \quad \forall x, y \in \Re$ (Desigualdad triangular)

10) $|x-y| \geq |x| - |y| \quad \forall x, y \in \Re$

Dem 7) Si $x \geq 0 \Rightarrow |x| = x$ Por otra parte $|x| \geq 0 \Rightarrow -|x| \leq 0$ como $x \geq 0 \Rightarrow -|x| \leq x$

Entonces $-|x| \leq x = |x| \Rightarrow -|x| \leq x \leq |x|$

Si $x < 0 \Rightarrow |x| = -x \Rightarrow -|x| = x \Rightarrow -|x| \leq x$

Por otra parte como $|x| \geq 0 \quad \forall x \in \Re$ y en este caso $x < 0 \Rightarrow x \leq |x|$

Entonces también en este caso $-|x| \leq x \leq |x|$

Por lo tanto $-|x| \leq x \leq |x| \quad \forall x \in \Re$

Dem 9) Por 7) $-|x| \leq x \leq |x|$

$-|y| \leq y \leq |y|$

$-|x| - |y| \leq x + y \leq |x| + |y| \Rightarrow -(|x| + |y|) \leq x + y \leq |x| + |y| \Rightarrow_{8)i} |x+y| \leq |x| + |y|$

Ejercicios (Repartido 4 del curso habitual)

I) Resolver en $(\Re, +, \bullet, \leq)$:

i) $|x-1| < 9$ **ii)** $\left|x^2 - x\right| - \frac{4x-2}{3} \geq 0$

iii) $\left|\frac{x^2-x}{x+1}\right| < x-\frac{1}{3}$ **iv)** $|x-2| \geq |3x-2|$ **v)** $\frac{3x-|x+2|}{2-2|x-1|} \geq 0$

II) Analizar el valor de verdad de las siguientes proposiciones:

i) $x<5 \Rightarrow |x|<5$ **ii)** $|x-5|<2 \Rightarrow 3<x<7$ **iii)** $|1+3x| \leq 1 \Rightarrow x \geq -\frac{2}{3}$

iv) La ecuación $|x-1|=|x-2|$ tiene solución vacía.

III) Resolver en $(\Re,+,\bullet,\leq)$ **:**

i) $\left|x^2-x\right|<6$ **ii)** $|x+1|^2-3|x+1|<0$

iii) $|2x+1|<|x-3|$ **iv)** $|x|+|3x-4|<1$

IV) Teniendo en cuenta la definición de valor absoluto y las propiedades vistas en el curso teórico; demostrar:

i) $|x-y| \geq |x|+|y| \quad (\forall x,y \in \Re)$

ii) $||x|-|y|| \leq |x-y| \quad (\forall x,y \in \Re)$

Respuestas:

I) i) $(-8,10)$ **ii)** $\left(-\infty,\frac{2}{3}\right] \cup [2,+\infty)$ **iii)** $\left(\frac{1}{2},+\infty\right)$ **iv)** $[0,1]$
v) $(-\infty,0) \cup [1,2)$

II) i) Falso **ii)** Verdadero **iii)** Verdadero **iv)** Falso

III) i) $(-2,3)$ **ii)** $(-4,-1) \cup (-1,2)$ **iii)** $\left(-4,\frac{2}{3}\right)$ **v)** $\varnothing$

Inicio

Para_volver_a_Menú

NÚMERO NATURAL

La idea en "crudo" de la generación de los números naturales ya fue presentada; recordémosla:
Como $1>0 \Rightarrow 1+1>1+0 \Rightarrow 1+1>1>0$ Por lo tanto el número real 1+1 es necesariamente distinto del 0 y del 1; mereciendo entonces un "nombre" diferente. Al real $1+1$ lo denominamos 2.
Al ser $2>1 \Rightarrow 2+1>1+1 \Rightarrow 2+1>2>1>0$ Entonces el real 2+1 es un número distinto del 0 del 1 y del 2. Lo denominamos 3. Un razonamiento idéntico nos lleva a que 3+1 es un real distinto (mayor) que el 0, que el 1, que el 2 y que el 3.
Denominamos 4 a 3+1. Y así sucesivamente.
Formalicemos esta idea.

Definición

Consideramos: $A \subseteq \Re$ Decimos que A es un **conjunto inductivo** si y solo si se cumple:
1) $0 \in A$
2) Si $x \in A \Rightarrow x+1 \in A$

Ejemplos $\Re$ es inductivo. $\Re^+$ no lo es pues falla la primera condición. Sí es inductivo $\Re^+ \cup \{0\}$
El conjunto $B = \{-1\} \cup \Re^+$ no es inductivo pues: $-1 \in B$ pero $-1+1=0 \notin B$ fallando entonces la segunda condición.

Nota Anotamos $\Im$ a la familia de todos los conjuntos inductivos. Así $\Re \in \Im$, $\Re^+ \notin \Im$

Observación $0 \in A \ \forall A \in \Im \Rightarrow 0+1=1 \in A \ \forall A \in \Im \Rightarrow 1+1=2 \in A \ \forall A \in \Im \Rightarrow 2+1=3 \in A \ \forall A \in \Im \cdots$
Entonces $0,1,2,3,..... \in A \ \forall A \in \Im$ Los números reales que identificamos como naturales pertenecen a todos los conjuntos inductivos.

Definición

Llamamos conjunto de los **números naturales** (anotamos N) a la intersección de todos los conjuntos inductivos. Sintéticamente:

$$N = \bigcap_{A \in \Im} A$$

Observaciones:

1) $N \subseteq A \ \forall A \in \Im$ Ya que la intersección de varios conjuntos está incluido en cada uno de ellos
2) Como $0,1,2,3,... \in A \ \forall A \in \Im$ y $N \subseteq A \ \forall A \in \Im \Rightarrow 0,1,2,3,.... \in N$ (Los números que desde siempre reconocimos como naturales; con la definición que acabamos de adoptar; son efectiva y tranquilizadoramente números naturales)
3) $N \subseteq \Re$ pues $N \subseteq A \ \forall A \in \Im$ y $\Re \in \Im$ Un razonamiento similar nos lleva a:
4) $N \subseteq \Re^+ \cup \{0\}$ En otras palabras $n \geq 0 \ \forall n \in N$

Teorema

$N \in \Im$

Demostración a cargo del lector.

Teorema de inducción completa

$$H)\begin{cases} 1) H \subseteq N \\ 2)\ 0 \in H \\ 3)\ \text{Si } x \in H \ \Rightarrow\ x+1 \in H \end{cases} \qquad T)\ H = N$$

Dem

De 2) y 3) $\Rightarrow$ $H \in \Im$ $\Rightarrow$ $N \subseteq H$ como $H \subseteq N$ $\Rightarrow$ $H = N$

Observación

Al cumplirse que: $N \subseteq A \subseteq \Re \quad \forall A \in \Im$ y además N y $\Re$ ser conjuntos inductivos podemos afirmar que N es el "mínimo" y $\Re$ es el "máximo" de los conjuntos inductivos. (Para hablar de máximo y mínimo necesitamos previamente una relación de orden que en este caso es la inclusión amplia de conjuntos).

Nota

Según la teoría que venimos desarrollando los naturales son también números reales. Y por lo tanto se pueden operar como tales.

¿Las operaciones que manejamos en $\Re$ (suma, producto, resta y división) siguen siendo operaciones en N? Y en caso afirmativo que propiedades cumplen. ¿Las mismas que en $\Re$?

Antes de contestar estas preguntas analicemos la situación desde un punto de vista mas general.

Consideramos: $(A,*)$ una estructura algebraica; o sea un conjunto no vacío (A) con una operación definida en el (*)

$$B \subseteq A\ ;\ B \neq \varnothing$$

Para que $*$ sea una operación en B debe cumplirse que la restricción de $*$ sobre $B \times B$ siga siendo una función.

En otras palabras: $*$ es una operación en $B \Leftrightarrow$ $*$ es una función de $B \times B \to B \Leftrightarrow \begin{cases} 1)\ x * y \in B \\ 2)\ x * y \text{ es ъnico} \end{cases}$

Como B es un subconjunto de A y la condición 2) se cumple para todos los elementos de A tenemos entonces que: $*$ es una operación en $B \Leftrightarrow x * y \in B \ \forall x, y \in B$ ya que la condición 1) se verifica automáticamente.

Si $*$ es una operación en B decimos que $(B,*)$ es una subestructura de $(A,*)$.

Analicemos ahora siendo $(B,*)$ una subestructura de $(A,*)$ .la "transmisión" de propiedades de la estructura madre a la subestructura.

Si $(A;*)$ es conmutativa $\Rightarrow$ $x * y = y * x \quad \forall x, y \in A$

Como $\forall x, y \in B \ \Rightarrow\ x, y \in A \ \Rightarrow\ x * y = y * x \quad \forall x, y \in B \ \Rightarrow\ (B,*)$ es conmutativa.

Tenemos entonces que si una estructura es conmutativa todas sus subestructuras también. Análogamente se prueba:

Si $(A,*)$ es asociativa $\Rightarrow$ $(B,*)$ es asociativa

Si $(A,*)$ tiene neutro n entonces: $(B,*)$ tiene neutro $\Leftrightarrow$ $n \in B$

Si $(A,*)$ tiene la propiedad de inverso entonces: $(B,*)$ cumple inverso $\Leftrightarrow$ $\forall x \in B \;\; x^{-1} \in B$

Consideraciones similares pueden realizarse sobre estructuras mas complejas (que tengan por ejemplo mas de una operación).

Teorema

$$a, b \in N \;\Rightarrow\; a + b \in N$$

Dem

Consideramos $H = \{ x \in N \,;\, a + x \in N \}$

1) $H \subseteq N$ por definición de H

2) $0 \in H$ ya que $a + 0 = a \in N$ por hipótesis

3) Si $x \in H \;\Rightarrow\; x + 1 \in H$ Pues si $x \in H \Rightarrow a + x \in N \Rightarrow$
$\Rightarrow a + x + 1 \in N$ ya que N es inductivo
$\Rightarrow x + 1 \in H$

De 1) 2) y 3) aplicando el teorema de inducción completa tenemos que: N = H. Por hipótesis $b \in N \;\Rightarrow\; b \in H \;\Rightarrow$
$\Rightarrow \; a + b \in N$

Nota

Aplicando el teorema y la nota inmediata anterior podemos afirmar que + es una operación en N que cumple asociativa, conmutativa, neutro (téngase en cuenta que $0 \in N$)

También podemos afirmar que no cumple opuesto ya que: si $n \in N \,;\, n > 0 \;\Rightarrow\; -n < 0 \;\Rightarrow\; -n \notin N$

Un razonamiento similar al realizado recién nos lleva a que la diferencia no es una operación en N. Sin embargo la condición para que la resta de dos naturales sea un natural es muy sencilla y todos la conocemos (minuendo mayor o igual que el sustraendo). Verifiquemos una vez mas que la teoría que venimos desarrollando coincide con lo que ya conocemos.

Lema

$$\left.\begin{array}{l} a \in N \\ a \neq 0 \end{array}\right\} \;\Rightarrow\; a - 1 \in N$$

Dem

Consideramos $H = \{ x \in N ; x = 0 \ \text{y} \ x - 1 \in N \}$

1) $H \subseteq N$ por definición de H
2) $0 \in H$ " " " "
3) Si $x \in H \Rightarrow x + 1 \in H$ Ya que si $x \in H \Rightarrow \begin{cases} x = 0 \Rightarrow x + 1 = 1 \Rightarrow x + 1 - 1 = 0 \in N \Rightarrow x + 1 \in H \\ \text{y} \\ x - 1 \in N \Rightarrow x + 1 - 1 = x - 1 + 1 \in N \Rightarrow x + 1 \in H \end{cases}$

De 1) 2) y 3) aplicando el teorema de inducción completa tenemos que H = N En consecuencia todos los naturales son elementos de H; y por lo tanto todo natural x es 0 ó $x - 1 \in N$ Por lo tanto si $a \in N \ \text{y} \ a \neq 0 \Rightarrow a - 1 \in N$.

Teorema

$$\left.\begin{matrix} a, b \in N \\ a \geq b \end{matrix}\right\} \Rightarrow a - b \in N$$

Dem

Sea $H = \{ x \in N ; x > a \ \text{y} \ a - x \in N \}$

1) $H \subseteq N$ por definición de H
2) $0 \in H$ ya que $a - 0 = a \in N$
3) Si $x \in H \Rightarrow x + 1 \in H$ pues : si $x \in H \Rightarrow \begin{cases} x > a \Rightarrow x + 1 > a \Rightarrow x + 1 \in H \\ \text{y} \\ a - x \in N \Rightarrow \begin{cases} a - x = 0 \Rightarrow a = x \Rightarrow x + 1 > a \Rightarrow x + 1 \in H \\ \text{y} \\ a - x \neq 0 \Rightarrow_{\text{Lema}} a - x - 1 = a - (x + 1) \in N \Rightarrow x + 1 \in H \end{cases} \end{cases}$

Estamos pues en condiciones de aplicar el teorema de inducción completa sobre el conjunto H llegando a que H=N

Por lo tanto como $b \in N \Rightarrow b \in H$ al cumplir además que $b \not> a \Rightarrow a - b \in N$

Nota

Antes de encarar las dos operaciones restantes por necesidades técnicas debemos analizar el orden en N. Un razonamiento similar al realizado en la nota anterior nos lleva a que "<" y "≤" cumplen en N todas las propiedades vistas en $\Re$ a excepción de densidad. Probemos entonces que **N es discreto**.

Teorema

$\nexists\, n \in N\,;\, 0 < n < 1$

Dem

Consideramos $H = \{ x \in N\,;\, x = 0 \;\; y \;\; x \geq 1 \}$

1) $H \subseteq N$ Por definición de H
2) $0 \in H$ " " " ".
3) Si $x \in H \Rightarrow x+1 \in H$ pues: si $x \in H \Rightarrow \begin{cases} x = 0 \Rightarrow x+1 = 1 \geq 1 \Rightarrow x+1 \in H \\ \quad y \\ x \geq 1 \Rightarrow x+1 \geq 1 \Rightarrow x+1 \in H \end{cases}$

Aplicando entonces el teorema de inducción completa tenemos que H=N y por lo tanto todo natural esta en H.

O sea todo natural o vale 0 o es mayor o igual que 1. En consecuencia no existen naturales entre 0 y 1.

Teorema

H) $a \in N$ T) $\nexists n \in N\,;\, a < n < a+1$

Dem

Por absurdo. Suponemos que $\exists n \in N\,;\, a < n < a+1 \;\Rightarrow\; 0 < n-a < 1$

Como $n > a \;\Rightarrow\; n-a \in N$ Habiendo encontrado entonces un natural entre 0 y 1; lo cual contradice el teorema anterior.

Teorema

$a, b \in N$ Si $a < b \;\Rightarrow\; a+1 \leq b$

Demostración a cargo del lector.

Ejercicio

Probar que el producto es una operación en N que cumple: asociativa, conmutativa, neutro, es distributiva respecto a la suma y no cumple la propiedad de inverso. Demostrar además que la división no es una operación en N.

Continuemos con el estudio del orden en los naturales. Antes algunas definiciones de carácter general que nos son necesarias.

Definición

Consideramos $A \subseteq \Re\,;\, A \neq \varnothing$ decimos que:

1) A está **acotado superiormente** $\Leftrightarrow$ $\exists k \in \Re\,;\, k \geq a \;\; \forall a \in A$ k se dice **cota superior** de A
2) A está **acotado inferiormente** $\Leftrightarrow$ $\exists h \in \Re\,;\, h \leq a \;\; \forall a \in A$ h se dice **cota inferior** de A

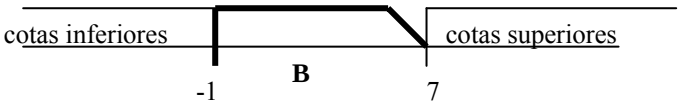
3) A está **acotado** $\Leftrightarrow$ A está acotado superior e inferiormente.

Ejemplos

Investiguemos si los siguientes conjuntos están o no acotados superior y/ó inferiormente y en caso afirmativo determinemos sus cotas.

1) $B = \{ x \in \Re ; -1 \leq x < 7 \}$ -1 es cota inferior de B pues $-1 \leq x \quad \forall x \in B$ también lo es –2 por el mismo motivo; es más $\forall h \in \Re ; h \leq -1$ h es cota inferior de B
$\forall k \in \Re ; k \geq 7$ k es cota superior de B.

Por lo tanto el conjunto B está acotado tanto superior como inferiormente. En pocas palabras B está acotado



2) $\Re^+$

$\Re^+$ está acotado inferiormente por el cero y por todos los reales negativos
$\Re^+$ no está acotado superiormente.

¿El motivo por el cual $\Re^+$ no está acotado superiormente es que es un conjunto infinito (que tiene infinitos elementos?

Definición

Consideramos: $A \subseteq \Re$, $M \in \Re$ y $m \in \Re$ Decimos que:

1) M es **máximo** de A $\Leftrightarrow$ $\begin{cases} M \geq a \quad \forall a \in A \\ M \in A \end{cases}$

2) m es **mínimo** de A $\Leftrightarrow$ $\begin{cases} m \leq a \quad \forall a \in A \\ m \in A \end{cases}$

Ejercicio

1) Demostrar que el máximo (mínimo) de un conjunto si existe es único.
Si M es máximo de A anotamos M=máxA y si m es mínimo lo hacemos: m=mínA.

2) Probar: i) –1 es el mínimo de B ii) B no tiene máximo (sugerimos. hacer una demostración por absurdo)
iii) $\Re^+$ no tiene ni máximo ni mínimo.

Observación

Los ejercicios anteriores nos llevan a que un conjunto esté acotado superior (inferiormente) no es condición suficiente para que exista máximo (mínimo).

Teorema Principio de buena ordenación

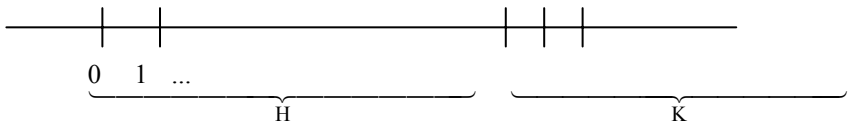
Todo conjunto de naturales no vacío tiene mínimo.

$$\left.\begin{array}{l} K \subseteq N \\ K \neq \varnothing \end{array}\right\} \Rightarrow \exists\, m \in N\ ;\ m = m_{HnA}$$

Dem

Si $0 \in K$ Como $K \subseteq N$ y $\forall n \in N\ \ n \geq 0 \ \Rightarrow\ 0 \leq k\ \ \forall k \in K$ Además teniendo en cuenta que en este caso $0 \in K \Rightarrow\ 0 = m_{HnK}$

Si $0 \notin K$ Consideramos $H = \{ x \in N\ ;\ x < k\ \ \forall k \in K \}$



La idea consiste en probar que H tiene un "último" elemento x_0 y su siguiente $x_0 + 1$ es el mínimo de K.

Es inmediato que $0 \in H$
Suponiendo que $\forall x \in H\ \ x+1 \in H$ El teorema de inducción completa nos lleva a $H = N\ \Rightarrow$

$$\left.\begin{array}{l} \Rightarrow\ K \cap H = K \cap N \\ \text{Ahora por def de H}\ \ K \cap H = \varnothing \\ \text{Por hipytesis}\ \ K \subseteq N \Rightarrow K \cap N = K \end{array}\right\} \Rightarrow\ K = \varnothing \ \text{ lo cual contradice la hipytesis}$$

En consecuencia la proposición $\forall x \in H\ \ x+1 \in H$ es falsa $\Rightarrow\ \exists x_0 \in H\ ;\ x_0 + 1 \notin H$
Probemos ahora que $x_0 + 1 = m_{HnK}$

Como $x_0 \in H\ \ \Rightarrow\ \ x_0 < k\ \ \forall k \in K\ \ \Rightarrow\ \ \underline{x_0 + 1 \leq k\ \ \forall k \in K}$
Por otra parte: $x_0 + 1 \notin H\ \ \Rightarrow\ \ x_0 + 1 \not< k\ \ \forall k \in K$ tomando en cuenta la proposición subrayada anteriormente tenemos que: $\exists\, k_0 \in K\ ;\ x_0 + 1 = k_0 \Rightarrow\ \ \underline{x_0 + 1 \in K}$
De ambas proposiciones subrayadas concluimos que $x_0 + 1$ es el mínimo de K.

Teorema

Todo conjunto de naturales no vacío y acotado superiormente tiene máximo.

Demostración a cargo del lector. Le sugerimos tomar el conjunto de las cotas superiores naturales; demostrar que este conjunto tiene mínimo y que este mínimo es el máximo que buscamos.

Método de Inducción Completa

Entendemos por inducción al proceso que nos conduce de una proposición particular a una general. Proceso inverso de la deducción que nos lleva de lo general a lo particular. Veamos algunos ejemplos:

Ejemplo 1

Observemos que:

$$1+3 = 4 = 2^2$$
$$1+3+5 = 9 = 3^2$$
$$1+3+5+7 = 16 = 4^2$$
$$1+3+5+7+9 = 25 = 5^2$$

Parece que:

$$1+3+5+7+.....+(2n-1) = n^2 \quad \forall n \in N$$

Hemos hecho una inducción. De algunos casos particulares (cuatro) hemos llegado a una proposición gral.

Ejemplo 2

Consideramos $f : N \to N ; f(x) = x^2 + x + 41$ Observemos que f(0)=41, f(1)=43, f(2)=47, f(3)=53 y 41, 43, 47 y 53 son primos.

Parece que f(n) es primo $\forall n \in N$

Calculemos ahora $f(41) = (41)^2 + 41 + 41 = 1763$ Pero 1763 no es primo ya que es divisible entre 41 y entre 43.

Por lo tanto la conclusión a la cual llegamos en el ejemplo 2 es falsa. es verdadera.

Queda claro entonces que el que una proposición sea válida para algunos casos particulares; ello no implica necesariamente que lo sea en general; pero tampoco necesariamente falsa. Veremos mas adelante que la conclusión del ejemplo 1 es válida.

Es innecesario resaltar la importancia que tendría el disponer de un procedimiento de inducción que nos lleve a conclusiones siempre verdaderas.

Ejemplo 3

Disponemos de 10.000 fichas de dominó con las cuales formar una fila. ¿Cómo debemos proceder para tener la certeza de que se caerán todas.

1 2 3 4 .....h h+1.....

Observemos que saber que se cayeron las primeras cuatro fichas no implica que necesariamente se cayeron todas. Es razonable afirmar que si:

1) Se cae la ficha 1
2) Las fichas están dispuestas de tal manera que si se cae una cualquiera necesariamente se cae la siguiente (h+1)

Entonces se caerán todas las fichas.

Téngase en cuenta que si falla cualquiera de las dos condiciones no necesariamente se caerán todas las fichas

Por otra parte observemos que si sustituimos la condición 1) por 1') Se cae la ficha 5 llegaríamos a la conclusión de que se caen todas a partir de la 5º.

En este último ejemplo entró en juego una condición (la 2)) que no lo había hecho en los ejemplos anteriores. Intentaremos a continuación formalizar esta idea.

Teorema **Principio de Inducción Completa.**

$$H)\begin{cases} P \text{ una proposiciyn referida a los naturales} \\ 1)\ P(k)\ \ V \quad \text{(La prop. P es verdadera para un natural en particular k)} \\ 2)\ \text{Si } P(h)\ V \ \Rightarrow\ P(h+1)\ V \qquad \forall h \in N\ ;\ h \geq k \end{cases}$$

$$T)\quad P(n)\ V \quad \forall n \in N\ ;\ n \geq k$$

Dem

Consideramos $H = \{ x \in N\ ;\ P(x+k)\ V \}$

1) $0 \in H$ pues $P(0+k) = P(k)\ V$

2) Si $x \in H \ \Rightarrow\ x+1 \in H$ Ya que si $x \in H \ \Rightarrow\ P(x+k)\ V \ \Rightarrow_{H)2)}\ P(x+k+1)\ V \ \Rightarrow\ x+1 \in H$

De 1) y 2) aplicando el teorema de I.C. tenemos H = N

Ahora $\forall n \in N\ ;\ n \geq k \ \Rightarrow\ n-k \in N \ \Rightarrow\ n-k \in H \ \Rightarrow\ P(n-k+k) = P(n)\ V \ \forall n \in N\ ;\ n \geq k$

Ejemplo

Demostrar que: $1+3+5+.....+2n-1 = n^2 \quad \forall n \in N\ ;\ n \leq 1$

1) La proposición es verdadera para n=1 Efectivamente pues: $1 = 1^2$

El primer miembro al ser una suma y coincidir el primer y el último termino asumimos que tiene un solo sumando;
el 1.

2) H) La proposición es verdadera para n=h $1+3+5+.....+2h-1 = h^2$

T) La proposición es verdadera para n=h+1 $\quad 1+3+5+.....+2h-1+2h+1=(h+1)^2$

$$\underbrace{1+3+5+.....+2h-1}_{=h^2}+2h+1 \;=\; h^2+2h+1 \;=\; (h+1)^2$$

De 1) y 2) por el principio de inducción completa tenemos que la proposición es verdadera para todo natural mayor o igual que 1. En otras palabras:

$$1+3+5+.....+2n-1 \;=\; n^2 \qquad \forall n\in N\,;\, n\geq 1$$

Nota

Los ejercicios correspondientes a este tema así como un desarrollo mas detallado del mismo el lector lo tendrá en el curso de matemática básica.

NÚMERO ENTERO

Definición

Denominamos conjunto de los **números enteros** (anotamos Z) al conjunto formado por los naturales y sus opuestos.

$$Z=\{x\in\Re\,;\, x\in N \;\text{ y }\; -x\in N\}$$

Teorema

$$a,b\in Z \;\Rightarrow\; \begin{cases} 1)\; a+b\in Z \\ 2)\; a.b\in Z \end{cases}$$

Dem

$$\text{Si } a\in N \text{ y } b\in N \;\Rightarrow\; \begin{cases} a+b\in N \;\Rightarrow\; a+b\in Z \\ a.b\in N \;\Rightarrow\; a.b\in Z \end{cases}$$

Si $a\in N$ y $-b\in N$ Llamemos $n=-b$ en este caso $n\in N$. $\quad a+b=a-n$

Cuando $a\geq n \;\Rightarrow\; a+b=a-n\in N \;\Rightarrow\; a+b\in Z$

Cuando $a<n \;\Rightarrow\; n-a\in N \;\Rightarrow a+b=a-n=-(n-a)\in Z$

Por otra parte: $a.b=a.(-n)=-a.n$ como $a.n\in N \;\Rightarrow\; a.b=-a.n\in Z$

Si $-a\in N$ y $b\in N$ Análogo.

Si $-a\in N$ y $-b\in N$ Denominamos $m=-a$ y $n=-b$ En este caso $m,n\in N$

$a+b=-m-n=-(m+n)$ como $m+n\in N \;\Rightarrow\; a+b\in Z$

$a.b=m.n\in N \;\Rightarrow\; a.b\in Z$

Nota

El teorema anterior junto con alguna de las observaciones realizadas en número natural nos permiten afirmar:

1) La suma es una operación en Z que cumple:

i) Asociativa

ii) Conmutativa
iii) Neutro ($0 \in N \Rightarrow 0 \in Z$)
iv) Opuesto

$$\left(\text{Si } a \in Z \Rightarrow \begin{cases} a \in N \Rightarrow -a \in Z \\ \quad y \\ -a \in N \Rightarrow -a \in Z \end{cases} \right)$$

En consecuencia la diferencia también es una operación en Z.

2) El producto es una operación en Z que verifica:

i) Asociativa
ii) Conmutativa
iii) Distributiva respecto a "+"
iv) Neutro. $(1 \in N \Rightarrow 1 \in Z)$

No cumple la propiedad de inverso. Si $a \in Z\,; a > 0 \;\Rightarrow\; a \in N \;\Rightarrow\; a \geq 1 \;\Rightarrow\; 0 < \frac{1}{a} < 1 \;\Rightarrow$

$\Rightarrow \; \frac{1}{a} \notin Z$ pues entre 0 y 1 no hay naturales ni opuestos de naturales

Un razonamiento similar nos lleva a que la división no es una operación en Z.

3) El orden en Z verifica todas las propiedades vistas en $\Re$ a excepción de la densidad.

NÚMERO RACIONAL

Definición

Llamamos conjunto de los **números racionales** (anotamos Q)

$$Q = \left\{ x \in \Re \,;\, x = \frac{p}{q} \;\text{ con } p, q \in Z \;\; q \neq 0 \right\}$$

En otras palabras llamamos racionales al conjunto de las fracciones; entendiendo por fracción el resultado obtenido de realizar el cociente entre dos enteros.

Teorema

$$a, b \in Q \;\Rightarrow\; \begin{cases} 1)\; a + b \in Q \\ 2)\; a.b \in Q \end{cases}$$

Dem

$$\left.\begin{array}{l} a \in Q \;\Rightarrow\; a = \frac{p}{q}\,; p \in Z \;\text{ y }\; q \in Z^* \\ b \in Q \;\Rightarrow\; b = \frac{p'}{q'}\,; p' \in Z \;\text{ y }\; q' \in Z^* \end{array}\right\} \Rightarrow \begin{cases} a + b = \frac{p}{q} + \frac{p'}{q'} = \frac{\overbrace{pq' + qp'}^{\in Z}}{\underbrace{qq'}_{\in Z^*}} \;\Rightarrow\; a + b \in Q \\ a.b = \left(\frac{p}{q}\right)\left(\frac{p'}{q'}\right) = \frac{\overbrace{p.p'}^{\in Z}}{\underbrace{q.q'}_{\in Z^*}} \;\Rightarrow\; a.b \in Q \end{cases}$$

Ejercicio

El teorema recién demostrado nos permite afirmar que "+" y "." son operaciones en Q.
Analizar las propiedades que estas cumplen; así como también el comportamiento de "<" y "≤".
En otras palabras: analizar $(Q,+,.,\leq)$

Inicio

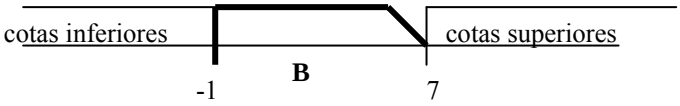
Para_volver_a_Menú

COMPLETITUD

En el ejercicio inmediato anterior seguramente el lector no encontró diferencias en cuanto a los aspectos ya estudiados entre $(\Re,+,\cdot,\leq)$ y $(Q,+,\cdot,\leq)$. Sin embargo, al comenzar el tema, planteamos un problema no resoluble en los racionales (medir la diagonal de un cuadrado de lado 1) como motivo para introducir a los números reales. Lo cual nos conduce a la conclusión de que la teoría está sin terminar.

En otras palabras; exclusivamente de los dos primeros axiomas no se desprende ninguna diferencia entre $(\Re,+,\cdot,\leq)$ y $(Q,+,\cdot,\leq)$. Nos falta un tercer axioma que marcará la diferencia entre ambas estructuras. Antes de llegar a él necesitamos algunas definiciones.

Dentro de número natural definimos conjuntos acotados, máximo y mínimo de un conjuntos de reales. Al hacerlo manejamos como uno de los ejemplos $B=\{x\in\Re;-1\leq x<7\}$



Al analizar la acotación superior del conjunto B la primera cota superior que nos viene a la mente es 7, vimos también que 7 no es máximo de B. ¿Qué diferencia al 7 de las otras cotas superiores?

Definición

Consideramos: $A\subseteq\Re, A\neq\varnothing,\ L\in\Re$ y $\ell\in\Re$. Decimos que:

1) L es **extremo superior** de A $\Leftrightarrow$ $L=\text{mín}\{k\in\Re\,;\,k \text{ es cota superior de } A\}$

2) ℓ es **extremo inferior** de A $\Leftrightarrow$ $\ell=\text{máx}\{h\in\Re\,;\,h \text{ es cota inferior de } A\}$

Nota

1) Por ser mínimo (máximo) de un conjunto el extremo superior (inferior) si existe es único. Lo cual nos permite adoptar una notación. Anotamos $L=\overline{\text{ext}}\,A$ y $\ell=\underline{\text{ext}}\,A$.

2) En otras palabras llamamos extremo superior de un conjunto a la menor de sus cotas superiores Y extremo inferior a la mayor de las cotas inferiores. El extremo superior también se denomina supremo, y el inferior ínfimo.

Ejercicios (Parte del repartido 5 del curso presencial)

I) Determinar por inspección si los siguientes conjuntos de reales están o no acotados; si tienen máximo, mínimo, extremo superior, inferior. En caso afirmativo hallarlos

.

i) $A=\{x\in\Re / x^2-2x<8\}$ **ii)** $B=\{x\in\Re / |x|.|x+1|<2\}$

iii) $C=\left\{x\in\Re / x=1-\frac{1}{n};n\in N^*\right\}$ **iv)** $C=\left\{x\in\Re / x=(-1)^n\left(2-\frac{4}{2^n}\right)\ n\in N^*\right\}$

II) Sea A un conjunto no vacío de números reales cuyo extremo superior es 3
Analizar el valor de verdad de las siguientes afirmaciones:

i) Todo número mayor que 3 es cota superior de A
ii) Todo número menor que 3 pertenece al conjunto A
iii) Existe un elemento del conjunto A mayor que 26/9.
iv) No existen elementos de A mayores que π
v) Si llamamos B al conjunto formado por los opuestos de los elementos de A. Entonces B esta acotadoinferiormente.
vi) B esta necesariamente acotado superiormente.
vii) El extremo inferior de B es -3.

III) Consideramos: $A \subseteq \Re \quad A \neq \varnothing$; L es una cota superior de A y l una cota inferior. Probar:

i) $L = \overline{ext}\, A \Leftrightarrow \forall \varepsilon \in \Re^+ \; \exists x_0 \in A \,/\, x_0 > L - \varepsilon$

ii) $l = \underline{ext}\, A \Leftrightarrow \forall \varepsilon \in \Re^+ \; \exists x_1 \in A \,/\, x_1 < l + \varepsilon$

Axioma 3 Axioma de completitud

Todo conjunto de reales no vacío y acotado superiormente tiene extremo superior

$$\left.\begin{array}{l} A \subseteq \Re \\ A \neq \varnothing \\ A \text{ acotado superiormente} \end{array}\right\} \Rightarrow \exists\, \overline{ext}\, A$$

Teorema

$(Q,+,\cdot,\leq)$ no es completo.

Dem Entendemos de que una estructura ordenada sea completa si todo subconjunto no vacío y acotado superiormente tiene extremo superior. Por lo tanto para demostrar que Q no es completo debemos encontrar un subconjunto de racionales no vacío y acotado superiormente que no tenga extremo superior.

Consideramos: $A = \left\{ x \in Q^+ \,;\, x^2 < 2 \right\}$

1) $A \subseteq Q$ Inmediato teniendo en cuenta la definición de A.

2) $A \neq \varnothing$ $\quad 1 \in Q^+$ y $1^2 = 1.1 = 1 < 2 \;\Rightarrow\; 1 \in A \;\Rightarrow\; A \neq \varnothing$

3) A acotado superiormente $\quad \forall x \in A \;\Rightarrow\; \begin{cases} x^2 < 2 < 4 \;\Rightarrow\; x^2 - 4 < 0 \;\Rightarrow\; (x-2).(x+2) < 0 \\ x \in Q^+ \;\Rightarrow\; x + 2 \in Q^+ \end{cases}$

entonces $x - 2 < 0 \;\Rightarrow\; x < 2 \quad \forall x \in A \;\Rightarrow\;$ 2 es cota superior de A

Probemos ahora que A no tiene extremo superior en Q ; lo cual haremos por absurdo. Supongamos que $\exists L \in Q \,;\, L = \overline{ext}\, A$ Como $L^2 \in Q$ ya que el orden cumple tricotomía se cumple una y solo uno de las siguientes situaciones: i) $L^2 < 2$ ii) $L^2 = 2$ iv) $L^2 > 2$

Tengamos presente que estamos realizando una demostración por absurdo. Pretendemos pues llegar a una contradicción Probemos entonces que cualquiera de las tres situaciones nos conducen a una contradicción.

i) Si $L^2 < 2$ Para generar la contradicción buscamos un elemento de A $(L+\varepsilon)$ mayor que el supuesto extremo superior.

$$L+\varepsilon \in A \quad \Leftrightarrow \quad \begin{cases} L+\varepsilon \in Q^+ \\ (L+\varepsilon)^2 < 2 \end{cases}$$

$(L+\varepsilon)^2 = L^2 + 2L\varepsilon + \varepsilon^2$ Si tomamos $0 < \varepsilon < 1 \quad \Rightarrow \quad \varepsilon^2 < \varepsilon \quad \Rightarrow \quad L^2 + 2L\varepsilon + \varepsilon^2 < L^2 + 2L\varepsilon + \varepsilon$

Si encontramos ε en las condiciones indicadas tal que $L^2 + 2L\varepsilon + \varepsilon < 2$ aplicando transitiva tendríamos que $(L+\varepsilon)^2 < 2$ como andamos buscando.

$$L^2 + 2L\varepsilon + \varepsilon < 2 \quad \Leftrightarrow \quad \varepsilon(2L+1) < 2 - L^2 \quad \Leftrightarrow \quad \varepsilon < \frac{2-L^2}{2L+1}$$

Como en este caso $L^2 < 2 \quad \Rightarrow \quad 2 - L^2 > 0 \quad \Rightarrow \quad \frac{2-L^2}{2L+1} \in Q^+ \quad \Rightarrow \quad \exists \varepsilon_0 \in Q \,;\, 0 < \varepsilon_0 < \frac{2-L^2}{2L+1}$

y además $0 < \varepsilon_0 < 1 \quad \left(\text{basta tomar} \quad 0 < \varepsilon_0 < \text{mín}\left\{ 1 \,,\, \frac{2-L^2}{2L+1} \right\} \right)$

Entonces $(L+\varepsilon_0)^2 < L^2 + 2L\varepsilon_0 + \varepsilon_0 < 2$ Como además $L+\varepsilon_0 \in Q^+ \quad \Rightarrow \quad L+\varepsilon_0 \in A$
Pero $\varepsilon_0 > 0 \Rightarrow L+\varepsilon_0 > L$ Lo cual es contradictorio ya que hemos encontrado un elemento de A mayor que el extremo superior.

ii) Si $L^2 = 2$ Ya demostramos al comienzo del tema que $\nexists L \in Q \,;\, L^2 = 2$

iii) Si $L^2 > 2$ Para generar el absurdo intentaremos hallar una cota superior de A menor que el extremo superior

$$(L-\varepsilon)^2 > 2 \quad \Leftrightarrow \quad L^2 - 2L\varepsilon + \varepsilon^2 > 2$$

$$L^2 - 2L\varepsilon + \varepsilon^2 \geq L^2 - 2L\varepsilon > 2 \quad \Leftrightarrow \quad -2L\varepsilon > 2 - L^2 \quad \Leftrightarrow \quad 2L\varepsilon < L^2 - 2 \quad \Leftrightarrow \quad \varepsilon < \frac{L^2-2}{2L}$$

Como en este caso $L^2 > 2 \quad \Rightarrow \quad \frac{L^2-2}{2L} \in Q^+ \quad \Rightarrow \quad \exists \varepsilon_1 \in Q \,;\, 0 < \varepsilon_1 < \frac{L^2-2}{2L} \quad \Rightarrow$
$\Rightarrow \quad (L-\varepsilon_1)^2 = L^2 - 2L\varepsilon_1 + \varepsilon_1^2 \geq L^2 - 2L\varepsilon_1 > 2$ como $\forall x \in A \quad x^2 < 2$ entonces
$(L-\varepsilon_1)^2 > x^2 \quad \forall x \in A \quad \Rightarrow \quad L - \varepsilon_1 > x \quad \forall x \in A$ (téngase presente que estamos trabajando con reales positivos) entonces $L - \varepsilon_1$ es una cota superior de A Pero $L - \varepsilon_1 < L$
Encontramos pues una cota superior de A $L - \varepsilon_1$ menor que el supuesto extremo superior (menor de las cotas superiores de A)

Como las tres proposiciones que necesariamente se cumplen si $\exists L \in Q \,;\, L = \overline{\text{ex}}\text{t}\, A$ Entonces A no tiene extremo superior en Q a pesar de ser un subconjunto de Q no vacío y acotado superiormente. Por lo tanto los racionales no son completos.

Podemos afirmar entonces que la diferencia entre (ℜ,+,·,<) y (Q,+,·,<) es que la primera es un cuerpo totalmente ordenado y completo en cambio la segunda es un cuerpo totalmente ordenado pero no completo

Nota Si el conjunto A del teorema anterior lo consideramos como un subconjunto de los reales (lo cual es inmediatamente cierto pues $A \subseteq Q \subseteq \Re$) tenemos que:

$$\left.\begin{array}{l} A \subseteq \Re \\ A \neq \varnothing \\ A \text{ acotado superiormente} \end{array}\right\} \Rightarrow_{Ax\,3} \quad \exists\, L \in \Re\,;\, L = \overline{ext}\, A$$

Un razonamiento idéntico al realizado nos lleva a que $L^2 \not< 2$ y $L^2 \not> 2 \;\Rightarrow\; L^2 = 2$

Probamos entonces que $\exists\, L \in \Re\,;\, L^2 = 2$ como $\nexists\, r \in Q\,;\, r^2 = 2 \;\Rightarrow\; L \notin Q$ Hemos demostrado así la existencia de un real no racional, al que usualmente denominamos $\sqrt{2}$. Al conjunto de los reales no racionales $(\Re - Q)$ los llamaremos irracionales.

Nota Es posible demostrar que el sistema axiomático presentado es ***consistente*** y ***categórico***. En otras palabras existe efectivamente un modelo que verifica los tres axiomas (consistencia) y cualquier cuerpo ordenado y completo es el de los números reales salvo isomorfismos (categoricidad).

Las mencionadas demostraciones escapan a los objetivos de este trabajo. El lector interesado las puede encontrar en el trabajo del prof. R.Louro titulado Número Real disponible en las fotocopiadoras de las cercanías del instituto; también existen trabajos publicados del mismo autor en la facultad de ingeniería.

Teorema

Todo conjunto de reales no vacío y acotado inferiormente tiene extremo inferior.

$$\left.\begin{array}{l} A \subseteq \Re \\ A \neq \varnothing \\ A \text{ acotado inferiormente} \end{array}\right\} \;\Rightarrow\; \exists\, L \in \Re\,;\, L = \underline{ext}\, A$$

Demostración a cargo del lector. Sugerimos considerar el conjunto de los opuestos de los elementos de A o sea considerar $B = \{\, x \in \Re\,;\, x = -a \;\text{ con } a \in A \,\}$ y demostrar 1) $\exists\, \overline{ext}\, B$ al que denominaremos L

2) $-L = \underline{ext}\, A$

(Realice un esquema gráfico para comprender la estrategia indicada)

Ejercicios (Resto del repartido 5)

I) Sean $A \subseteq \Re, B \subseteq \Re, A \neq \varnothing, B \neq \varnothing$. Consideramos $A + B = \{x \in \Re / x = a + b \;\; a \in A \; b \in B\}$

Demostrar:

i) Si $\exists\, \overline{ext} A$ y $\exists\, \overline{ext} B \;\Rightarrow\; \exists\, \overline{ext}(A + B)$ y $\overline{ext}(A + B) = \overline{ext} A + \overline{ext} B$

ii) Si $\exists\, \underline{ext}\, A$ y $\exists\, \underline{ext}\, B \;\Rightarrow\; \exists\, \underline{ext}\,(A + B)$ y $\underline{ext}(A + B) = \underline{ext}\, A + \underline{ext} B$

II) Idem.I) con $A.B = \{x \in \Re / x = a.b \;\; a \in A\,,\, b \in B\}$ sabiendo además que los elementos de A y de B son positivos o cero.

III) Consideramos S y T dos conjuntos de reales no vacíos.

i) Probar que si $s \leq t \;\; \forall s \in S \;\; \forall t \in T \;\Rightarrow \exists\, \underline{ext}\, T \;\; \exists \overline{ext} S$ y $\overline{ext} S \leq \underline{ext}\, T$

ii) Si con similares hipótesis pero cambiando $s \leq t$ por $s < t$ ¿ Puede afirmar que $\overline{ext} S < \underline{ext} T$? (Sugerencia: analizar $S = \left\{x \in \Re / x = -\frac{1}{n} \;\; n \in N^*\right\}$ $T = \left\{x \in \Re / x = \frac{1}{n} \;\; n \in N^*\right\}$

IV) ¿ $(N,+,\cdot,\leq)$ es completo? ¿Y $(Z,+,\cdot,\leq)$?

Teorema

El conjunto de los naturales no está acotado superiormente.

Dem Intentaremos probarlo por absurdo: Suponemos entonces que N está acotado superiormente; en otras palabras

suponemos $\exists k \in \Re\ ;\ k \geq n \quad \forall n \in N$

Tenemos entonces:

$$\left.\begin{array}{l} N \subseteq \Re \\ N \neq \varnothing \\ N \text{ acotado superiormente} \end{array}\right\} \Rightarrow_{Ax3} \quad \exists L \in \Re\ ;\ L = \overline{ext}\, N \quad \Rightarrow \quad L-1 \text{ no es cota sup. de N}$$

$\Rightarrow \quad \exists\, n_0 \in N\ ;\ n_0 > L-1 \quad \Rightarrow \quad n_0 + 1 > L$ Pero $n_0 + 1 \in N$ y es mayor que el extremo superior lo que es absurdo

Teorema de Arqúimedes

H) $a, b \in \Re^+$ T) $\exists n \in N\ ;\ n.a > b$

Dem

Como N no está acotado superiormente $\Rightarrow$ $\frac{b}{a}$ no es cota superior de N $\Rightarrow$ $\exists n \in N\ ;\ n > \frac{b}{a}$ $\Rightarrow$

$\Rightarrow \quad \exists n \in N\ ;\ n.a > b$

Ejercicios

I) Probar que Z no está acotado ni superior ni inferiormente.

II) Demostrar que $\forall \varepsilon \in \Re^+ \; \exists n_0 \in N \; ; \forall n \geq n_0 \;\; \frac{1}{n} < \varepsilon$ En otras palabras probar que $\left(\frac{1}{n}\right) \to 0$

III) Probar: $a \in \Re \;\; \Rightarrow \;\; \begin{cases} 1) \; \exists z \in Z \; ; z \leq a < z+1 \\ 2) \; z \text{ es unico} \end{cases}$

z se denomina parte entera de a y lo anotaremos $[a]$

Mas precisamente

Definición

Sea $x \in \Re$; llamamos **parte entera** de *x* (anotamos $[x]$) a un entero z tal que $z \leq x < z+1$

Ej $\left[\frac{7}{2}\right] = 3, \quad [\sqrt{2}] = 1, \quad [-\sqrt{2}] = -2$

Teorema: Densidad de Q en $\Re$

H) $a, b \in \Re \; a < b$ **T)** $\exists r \in Q / a < r < b$

Dem

$a < b \;\; \Rightarrow \;\; b - a \in \Re^+ \;\; \Rightarrow \;\; \exists n \in N \; ; \; \frac{1}{n} < b - a \;\; \Rightarrow \;\; n(b-a) = nb - na > 1$

Llamando $z = [na]$ tenemos que $z \leq na < z+1$ De donde resaltamos $\underline{na < z+1}$

Por otra parte $z \leq na \;\; \Rightarrow \;\; -z \geq -na \;\; \Rightarrow \;\; z+1-z \geq z+1-na \;\; \Rightarrow$

$\Rightarrow \left.\begin{array}{l} z+1-na \leq 1 \\ \text{como } nb - na > 1 \end{array}\right\} \;\; \Rightarrow \;\; nb - na > z+1-na \;\; \Rightarrow \;\; \underline{nb > z+1}$

De ambas desigualdades subrayadas tenemos $na < z+1 < nb \;\; \Rightarrow \;\; a < \frac{z+1}{n} < b \;\; \Rightarrow \;\; \exists r = \frac{z+1}{n} \in Q \; ; \; a < r < b$

Teorema

$\left.\begin{array}{l} x \in Q \\ y \in \Re - Q \end{array}\right\} \;\; \Rightarrow \;\; \begin{cases} 1) \; x + y \in \Re - Q \\ 2) \; x - y \in \Re - Q \\ 3) \; x.y \in \Re - Q \\ 4) \; \frac{x}{y} \in \Re - Q \end{cases}$

Dem

1) Por absurdo. Suponemos $x + y = r \; ; r \in Q \;\; \Rightarrow \;\; y = r - x \;\; \text{como } x \in Q \text{ y } r \in Q \;\; \Rightarrow \;\; y \in Q$
Lo cual contradice la hipótesis.

En el teorema anterior demostramos que el resultado de operar un racional y un irracional es irracional. ¿Qué ocurre si operamos dos irracionales?

Teorema Densidad de $\Re - Q$ en $\Re$

H) $a, b \in \Re \quad a < b$ **T)** $\exists c \in \Re - Q \ ; \ a < c < b$

Dem

$a < b \Rightarrow a + \sqrt{2} < b + \sqrt{2} \Rightarrow \exists r \in Q \ ; \ a + \sqrt{2} < r < b + \sqrt{2} \Rightarrow a < r - \sqrt{2} < b$

Como r es racional y $\sqrt{2}$ es irracional $\Rightarrow \exists \, c = r - \sqrt{2} \in \Re - Q$ tal que: $a < c < b$

Observación

Utilizando reiteradamente la densidad de Q en $\Re$ y de $\Re - Q$ en $\Re$ podemos afirmar que en un intervalo cualesquiera de reales hay infinitos racionales e irracionales.Lo cual implica que entre dos racionales hay infinitos irracionales y entre dos irracionales hay infinitos racionales.

Inicio

Para_volver_a_Menú

FUNCIONES EXPONENCIALES Y LOGARÍTMICAS

Introducción

La meta consiste en definir y estudiar propiedades de la función exponencial de base y exponente real, así como de su función inversa, la función logarítmica.

El procedimiento a seguir es constructivo; primero definiremos la potencia de base real y exponente natural, ($a^n ; a \in \Re \text{ y } n \in N$) luego la potencia de base real y exponente entero, ($a^z ; a \in \Re \text{ y } z \in Z$), posteriormente la potencia de exponente racional, ($a^r ; a \in \Re \text{ y } r \in Q$) y por último la potencia de base y exponente real ($a^b ; a \in \Re \text{ y } b \in \Re$). Se tratará en cada caso lograr una definición coherente con las anteriores desde el punto de vista de las propiedades algebraicas como las de crecimiento.

Potencia de base real y exponente natural

Definición

Sea $a \in \Re \text{ y } n \in N$ Si a=0 definimos a^n, en este caso $0^n=0 \ \forall n \in N^*$

Si $a \neq 0$ y n=0 definimos a^n en este caso $a^0=1$

Si $a \neq 0$ y $n \neq 0$ definimos $a^n = a.a^{n-1}$

Obs:

$a^1 = a.a^0 = a.1 = a$

$a^2 = a.a^1 = a.a$

$a^3 = a.a^2 = a.a.a$

También observemos que se excluye explicitamente el caso "0^0"

Teorema

Si **a** y **b** son números reales, **m** y **n** naturales excluyendo el caso " 0^0 " se cumple:

1) $a^m.a^n = a^{m+n}$
2) $\frac{a^m}{a^n} = a^{m-n} \quad (m \geq n)$
3) $a^n.b^n = (a.b)^n$
4) $\frac{a^n}{b^n} = \left(\frac{a}{b}\right)^n$
5) $\left(a^n\right)^m = a^{n.m}$

Se demostrará a modo de ejemplo una de las propiedades anteriormente enunciadas

Dem. 1) $a^m.a^n = a^{m+n}$ Intentaremos una demostración por inducción completa sobre n.

Primer paso: n=0 $a^m.a^0 = a^{m+0}$ $a^m.a^0 = a^m.1 = a^m = a^{m+0}$

Segundo paso H) n=h $a^m a^h = a^{m+h}$
T) n=h+1 $a^m.a^{h+1} = a^{m+(h+1)}$

$$a^m.a^{h+1} = a^m.a^h.a = a^{m+h}.a = a^{m+h+1}$$

Justifique el lector los pasos dados.

Del primer y del segundo paso utilizando el principio de I.C. podemos afirmar que
$a^m.a^n = a^{m+n} \quad \forall n \in N$ Como tomamos m fijo, pero puede ser cualquiera, entonces
$a^m.a^n = a^{m+n} \quad \forall n \in N$ y $\forall m \in N$

Ejercicios Probar: i) $1^n = 1 \quad \forall n \in N$

ii) $(-1)^{2n} = 1 \quad \forall n \in N$

iii) $(-1)^{2n+1} = -1 \quad \forall n \in N$

iv) $x^{2n} \geq 0 \quad \forall x \in \Re \quad \forall n \in N \quad (x^2 + n^2 \neq 0)$

v) $(-x)^{2n} = x^{2n}$ " " "

vi) $(-x)^{2n+1} = -x^{2n+1}$ " "

Teorema Desigualdad de Bernoulli

$(1+\alpha)^n \geq 1 + n\alpha \quad \forall n \in N \quad \forall \alpha \in \Re\,; \alpha \geq -1$

Dem (Por I.C.) 1er paso n=0 $(1+\alpha)^0 \geq 1 + 0.\alpha$

$$\left.\begin{array}{l}(1+\alpha)^0 = 1\\ 1 + 0.\alpha = 1\end{array}\right\} \Rightarrow (1+\alpha)^0 = 1 + 0.\alpha \Rightarrow (1+\alpha)^0 \geq 1 + 0.\alpha$$

2do paso H) $n = h \quad (1+\alpha)^h \geq 1 + h.\alpha$
T) $n = h + 1 \quad (1+\alpha)^{h+1} \geq 1 + (h+1)\alpha$

$$(1+\alpha)^{h+1} = (1+\alpha)(1+\alpha)^h \geq (1+\alpha)(1+h\alpha) = 1 + h.\alpha + \alpha + h\alpha^2 =$$
$$= 1 + (h+1)\alpha + h\alpha^2 \geq 1 + (h+1)\alpha$$

Justifique el lector los pasos dados.

Teorema Siendo a y b números reales, m y n naturales; en condiciones de existencia se cumple:

Si a>1

1) $a^n > 1 \quad \forall n \in N^*$
2) $\text{Si } n < m \Rightarrow a^n < a^m$
3) $\forall k > 0 \quad \exists n \in N \,/\, a^n > k$

Si 0<a<1

4) $a^n < 1 \quad \forall n \in N^*$

5) $\text{Si } n < m \Rightarrow a^n > a^m$

6) $\forall \varepsilon > 0 \; \exists n \in N \,/\, a^n < \varepsilon$

Haremos a continuación alguna demostración a manera de ejemplo. Las propiedades 1) y 4) aceptan una demostración por I.C. similares a las ya hechas.

Dem 2) Si n<m $\Rightarrow m - n > 0$ aplicando 1) podemos afirmar: $a^{m-n} > 1 \Rightarrow \frac{a^m}{a^n} > 1 \Rightarrow a^m > a^n$

Dem 3) Si a>1 entonces a=1+d con d>0 Ahora $a^n = (1+d)^n \geq 1 + nd$ (Bernoulli)
Queremos encontrar un n tal que $a^n > k$. Si encontramos n que cumpla 1+nd>k por transitiva se verificaría la tesis.

$1 + nd > k \Leftrightarrow nd > k - 1 \Leftrightarrow n > \frac{k-1}{d}$ Como N no esta acotado superiormente

$\exists n \in N \,/\, n > \frac{k-1}{d}$ Volviendo atrás en el razonamiento hecho $a^n > k$

Ejercicios Probar: i) $0 < a < b \Rightarrow a^n < b^n \quad \forall n \in N^*$

ii) $\text{Si } a > 1 \text{ y } a^n < a^m \Rightarrow n < m$

iii) $\text{Si } 0 < a < 1 \text{ y } a^n < a^m \Rightarrow n > m$

Obs: Consideramos f: $N \to \Re$ tal que $f(x) = a^x$. Lo demostrado anteriormente implica que:

Si a>1 f es estrictamente creciente y no acotada superiormente
Si 0<a<1 f es estrictamente decreciente y se aproxima a cero tanto como queramos.

En otras palabras: Si a>1 $\lim_{x \to +\infty} f(x) = +\infty$ Si 0<a<1 $\lim_{x \to +\infty} f(x) = 0^+$

Potencia de base real y exponente entero

Definición

Sean: $a \in \Re$, $z \in Z$ tal que $a^2 + z^2 \neq 0$ (a y z no simultaneamente nulos)

$\text{Si } z \geq 0$ entonces $z \in N$ en este caso a^z ya esta definido

Si z<0 entonces z=-n ; n∈N en este caso definimos $a^z = a^{-n} = \frac{1}{a^n} \quad (a \neq 0)$

Obs: No definimos ni "0^0" ni 0^z con z <0

Teorema

Sean a y b números reales, p y q enteros en condiciones de existencia se cumple:

1) $a^p . a^q = a^{p+q}$
2) $\frac{a^p}{a^q} = a^{p-q}$
3) $a^p . b^p = (a.b)^p$
4) $\frac{a^p}{b^p} = \left(\frac{a}{b}\right)^p$
5) $(a^p)^q = a^{p.q}$

Como ya hicimos demostraremos una propiedad a manera de ejemplo

Dem

1) Si $p \in N$ y $q \in N$ La propiedad ya fué demostrada.

Si $p \in N$ y $q = -n$; $n \in N$ $\quad a^p a^q = a^p a^{-n} = a^p \frac{1}{a^n} = \frac{a^p}{a^n}$

$$\text{Si } n \le p \text{ entonces } \frac{a^p}{a^n} = a^{p-n} = a^{p+q}$$

$$\text{Si } n > p \text{ entonces } \frac{a^p}{a^n} = \frac{1}{a^n / a^p} = \frac{1}{a^{n-p}} = a^{-(n-p)} = a^{p-n} = a^{p+q}$$

Si $p = -n$ y $q = -m$ con $n, m \in N$

$$a^p a^q = a^{-n} a^{-m} = \frac{1}{a^n} . \frac{1}{a^m} = \frac{1}{a^{m+n}} = a^{-(m+n)} = a^{-n-m} = a^{p+q}$$

Teorema

Sean: a un real ; p y q enteros; en condiciones de existencia se cumple:

Si a>1

1) $a^x > 1 \quad \forall x \in Z^+$
2) $p < q \Leftrightarrow a^p < a^q$
3) $\forall k > 0 \quad \exists x \in Z^+ \ / \ a^x > k$
4) $\forall \varepsilon > 0 \quad \exists x \in Z^- \ / \ a^x < \varepsilon$

Si 0<a<1

5) $a^x < 1 \quad \forall x \in Z^+$
6) $p < q \Leftrightarrow a^p > a^q$
7) $\forall k > 0 \quad \exists x \in Z^- \ / \ a^x > k$
8) $\forall \varepsilon > 0 \quad \exists x \in Z^+ \ / \ a^x < \varepsilon$

Dem 2)

$(\Rightarrow)$ $\quad p < q \Rightarrow q - p \in Z^+$ aplicando 1) tenemos $a^{q-p} > 1 \Rightarrow \frac{a^q}{a^p} > 1 \Rightarrow a^q > a^p$

$(\Leftarrow)$ $\quad a^p < a^q \Rightarrow \frac{a^q}{a^p} > 1 \Rightarrow a^{q-p} > 1$ como $a > 1 \Rightarrow q - p \in Z^+ \Rightarrow q - p > 0 \Rightarrow p < q$

Observemos que utilizamos en la última parte el recíproco de 1) el cual no esta enunciado, pero puede demostrarse fácilmente por absurdo.

También tengamos en cuenta que en todos los casos estamos trabajando con números positivos , lo cual nos permite realizar sin inconvenientes las transformaciones necesarias.

Potencia de base real y exponente racional

Previamente analizaremos el tema de la radicación, pues para tratar la potencia de base real y exponente racional nos resulta imprescindible.

Si $a \in \Re\ n \in N\ n \geq 2$ definir $\sqrt[n]{a} = b \Leftrightarrow b^n = a$ resulta razonable y previsible; pero antes de dar esta definición debemos asegurarnos en que condiciones existe dicho "b" y en caso de existir cuantos hay.

Lema 1 H) $\begin{cases} a, b \in \Re^+ \\ n \in N, n \neq 0 \\ b^n > a \end{cases}$ T) $\exists b' \in \Re^+ / b' < b$ y $b'^n > a$

Dem: Debemos encontrar b'<b ,entonces b'= b(1-d) con 0<d<1, que cumpla

$b'^n > a$ o sea que $b^n(1-d)^n > a$

En consecuencia la tarea consiste en hallar 0<d<1 para que $b^n(1-d)^n > a$

Como $0<d<1 \Rightarrow b^n(1-d)^n \geq b^n(1-nd)$ (Bernoulli) $b^n(1-nd) > a \Leftrightarrow 1-nd > \frac{a}{b^n} \Leftrightarrow$

$$\Leftrightarrow -nd > -1 + \frac{a}{b^n} \Leftrightarrow nd < 1 - \frac{a}{b^n} \Leftrightarrow d < \frac{1 - \frac{a}{b^n}}{n}$$

Por hipótesis $b^n > a \Rightarrow \frac{a}{b^n} < 1 \Rightarrow \frac{1 - \frac{a}{b^n}}{n} > 0$ como los reales son densos podemos afirmar que

$\exists d_0 \in \Re\ ; 0 < d_0 < 1$ tal que $0 < d_0 < \frac{1 - \frac{a}{b^n}}{n}$ volviendo atrás en el proceso anterior tenemos que $b'=b(1-d_0)$ cumple

$b'^n = b^n(1-d_0)^n \geq b^n(1-nd_0) > a$ por otra parte como $0 < d_0 < 1 \Rightarrow b' = b(1-d_0) < b$ y $b' \in \Re^+$

Lema 2 H) $\begin{cases} a, b \in \Re^+ \\ n \in N \quad n \neq 0 \\ b^n < a \end{cases}$ T) $\exists b'' \in \Re^+ / b'' > b$ y $b''^n < a$

Dem:

$a,b \in \Re^+ \Rightarrow \frac{1}{a}$ y $\frac{1}{b} \in \Re^+$ por otra parte $b^n < a \Rightarrow \left(\frac{1}{b}\right)^n = \frac{1}{b^n} > \frac{1}{a}$ aplicando el lema 1

a $\frac{1}{a}$ y $\frac{1}{b}$ tenemos que $\exists b' \in \Re^+; b' > \frac{1}{b}$ / $b'^n > \frac{1}{a} \Rightarrow \frac{1}{b'^n} < a$. Llamando $b'' = \frac{1}{b'}$ como

$b' > \frac{1}{b} \Rightarrow b'' = \frac{1}{b'} > b$ y $b''^n = \left(\frac{1}{b'}\right)^n = \frac{1}{b'^n} < a$

Teorema

H) $a \in \Re^+,\ n \in N;\ n \neq 0$ T) $\begin{cases} 1)\ \exists b \in \Re^+ \text{ / } b^n = a \\ 2)\ b \text{ es unico} \end{cases}$

Dem: 1) Consideramos $A = \left\{x \in \Re^+ \text{ / } x^n \leq a\right\}$ la idea consiste en probar:

I) $\exists\ \overline{ext}\ A$

II) $b^n = a$

I)

i) $A \subseteq \Re$ por definicion de A

ii) $A \neq \varnothing$ por hipotesis $a > 0 \Rightarrow \frac{a+1}{a} > 1$ y $n \geq 1 \Rightarrow \left(\frac{a+1}{a}\right)^n \geq \left(\frac{a+1}{a}\right)^1 = \frac{a+1}{a} = 1 + \frac{1}{a} > \frac{1}{a}$

$$\Rightarrow \left(\frac{a+1}{a}\right)^n > \frac{1}{a} \Rightarrow \left(\frac{a}{a+1}\right)^n < a \Rightarrow \frac{a}{a+1} \in A \Rightarrow A \neq \varnothing$$

iii) A acotado superiormente

Por hipotesis $a>0 \Rightarrow a+1>1$ como $n \geq 1 \Rightarrow$

$\Rightarrow (a+1)^n \geq (a+1)^1 = a+1 > a \Rightarrow (a+1)^n > a$

por otra parte $\forall x \in A, x \in \Re^+$ y $x^n < a$ juntando

ambas desigualdades tenemos $x^n < (a+1)^n \Rightarrow$

$x<a+1 \ \forall x \in A \Rightarrow a+1$ cota superior de A

De i) ii) y iii) aplicando el axioma de completitud podemos afirmar que $\exists \overline{\text{ext}}\, A$ al que llamamos “alevosamente” b .

II) Nos falta probar que $b^n = a$ lo que haremos por reducción al absurdo. Suponemos entonces que $b^n \neq a$ analizamos dos casos:

<u>Si $b^n < a$</u> Aplicando el lema 2 $\exists b'' \in \Re^+, b'' > b \,/\, b''^n < a \Rightarrow b'' \in A$ pero $b'' > b = \overline{\text{ext}}\, A$ lo cual es contradictorio.

<u>Si $b^n > a$</u> Aplicando el lema 1 podemos afirmar que $\exists\, b' \in \Re^+; b' < b \,/\, b'^n > a$ Por otra parte como $\forall x \in A \ x^n < a \Rightarrow b'^n > x^n$ teniendo en cuenta además que tanto b’ como x son positivos entonces b’>x $\forall x \in A \Rightarrow$ b’ cota superior de A
Pero $b' < b = \overline{\text{ext}}\, A$ lo cual genera el absurdo.

Por lo tanto $b^n = a$. Probemos por último la unicidad.

<u>Dem</u>: 2) Suponemos que $\exists b_1 \in \Re^+ \,/\, b_1^n = a$ Intentaremos demostrar que $b_1 = b$ por abs.
Si $b_1 < b \Rightarrow b_1^n < b^n \Rightarrow a < a$ Abs.
Si $b_1 > b \Rightarrow b_1^n > b^n \Rightarrow a > a$ Abs.
Por lo tanto $b_1 = b$ lo cual implica que b es único.

Observemos que la unicidad no se desprende de la unicidad del extremo superior de un conjunto pues se podría encontrar b ; $b^n = a$ por otro camino distinto.

<u>Observaciones</u>:

<u>Si a=0</u> $\exists 0 \in \Re \,/\, 0^n = 0 = a$ y además es el único

<u>Si a>0 y n es par</u> por el teorema anterior $\exists b \in \Re^+$ unico $/\, b^n = a$

Pero $(-b)^n = b^n = a$ por ser n par.

Si a>0 y n impar por el teorema anterior $\exists b \in \Re^+$ unico / $b^n = a$

Además $\nexists x \in \Re \; ; x \leq 0 / x^n = a$ pues $\forall x \in \Re^- \; x^n \geq 0$ por ser n impar..

Si a<0 y n par $\nexists b \in \Re / b^n = a$ pues $\forall x \in \Re \; x^n \geq 0$ por ser n par.

Si a<0 y n impar a<0 $\Rightarrow -a > 0$ aplicando el teorema anterior tenemos

$\exists b \in \Re^+$ unico / $b^n = -a \Rightarrow -b^n = a$ como $n \neq \dot{2}$ $(-b)^n = -b^n$ por lo tanto

$\exists -b \in \Re^- / (-b)^n = a$.

En resumen: Si a=0 y $n \in N$ n>0 $\exists 0 \in \Re / 0^n = 0$ y es el único

Si $a \in \Re^+$ y $n = \dot{2}$ $\exists b \in \Re^+$ y $-b \in \Re^- / b^n = (-b)^n = a$ y son los únicos dos.

Si $a \in \Re^+$ y $n \neq \dot{2}$ $\exists b \in \Re^+ / b^n = a$ y es el único.

Si $a \in \Re^-$ y $n = \dot{2}$ $\nexists x \in \Re / x^n = a$

Si $a \in \Re^-$ y $n \neq \dot{2}$ $\exists -b \in \Re^- / (-b)^n = a$ y además es el único.

Lo que nos conduce a la siguiente:

Definición $a \in \Re$ $n \in N$ $n \geq 1$

1) Si $a \geq 0$ definimos $\sqrt[n]{a} = b \Leftrightarrow \begin{cases} b^n = a \\ b \geq 0 \end{cases}$

2) Si $a < 0$ y $n \neq \dot{2}$ definimos $\sqrt[n]{a} = b \Leftrightarrow b^n = a$

Obs:

Siendo $a \in \Re, n \in N \; n \geq 1$ $\sqrt[n]{a}$ en $(\Re, +, ., \leq)$ está definida: si n es par solamente para $a \geq 0$, si n es impar para todos los a reales.

También observamos que cuando está definida $Sig\sqrt[n]{a} = Sig(a)$, en particular si n es par $\sqrt[n]{a} \geq 0$.

Teorema

Siendo a,a' números reales, n y p naturales no nulos; en condiciones de existencia se cumple:

1) $\left(\sqrt[n]{a}\right)^n = a$

2) i) $\sqrt[2n]{a^{2n}} = |a|$ ii) $\sqrt[2n+1]{a^{2n+1}} = a$

3) $\sqrt[n]{a} . \sqrt[n]{a'} = \sqrt[n]{aa'}$

4) $\frac{\sqrt[n]{a}}{\sqrt[n]{a'}} = \sqrt[n]{\frac{a}{a'}}$

5) $\left(\sqrt[n]{a}\right)^p = \sqrt[n]{a^p}$

6) $\sqrt[p]{\sqrt[n]{a}} = \sqrt[pn]{a}$

7) $\sqrt[n]{a} = \sqrt[np]{a^p}$

Dem 2) i) Como $a^{2n} \geq 0$ aplicamos la parte 1) de la definición.

Debemos probar: $\sqrt[2n]{a^{2n}} = |a| \Leftrightarrow \begin{cases} I) \ |a|^{2n} = a^{2n} \\ II) \ |a| \geq 0 \end{cases}$

I) $|a|^{2n} = \left(|a|^2\right)^n = \left(a^2\right)^n = a^{2n}$ II) ya fué demostrado en las propiedades de valor absoluto.

Ahora sí estamos en condiciones de tratar la potencia de exponente racional.

Definición

$a \in \Re \ a \geq 0 \ \ r \in Q, \Rightarrow r = \frac{p}{q}$ con $p \in Z$ y $q \in N \ \ q \geq 1$

Definimos $a^r = a^{\frac{p}{q}} = \sqrt[q]{a^p}$

.

Por ejemplo: $8^{2/3} = \sqrt[3]{8^2} = \sqrt[3]{64} = 4$

Nota: Si $\frac{p}{q} = \frac{p'}{q'} \Rightarrow a^{\frac{p}{q}} = a^{\frac{p'}{q'}}$

$a^{\frac{p}{q}} = \sqrt[q]{a^p} = \sqrt[qq']{a^{pq'}} = \sqrt[qq']{a^{p'q}} = \sqrt[q']{a^{p'}} = a^{\frac{p'}{q'}}$

(*)

(*) $\frac{p}{q} = \frac{p'}{q'} \Rightarrow pq' = qp'$

Teorema

Sean a,b $\in \Re^{+,0}$ r y r' $\in Q$ se cumple:

1) $a^r . a^{r'} = a^{r+r'}$
2) $\frac{a^r}{a^{r'}} = a^{r-r'}$
3) $a^r . b^r = (a.b)^r$
4) $\frac{a^r}{b^r} = \left(\frac{a}{b}\right)^r$
5) $\left(a^r\right)^{r'} = a^{r.r'}$

Dem 1) $r \in Q \Rightarrow r = \frac{p}{q}$ con p y $q \in Z \, ; q \geq 1$ $r' \in Q \Rightarrow r' = \frac{p'}{q'}$ con p' y $q' \in Z \, ; q' \geq 1$

$$a^r.a^{r'} = a^{\frac{p}{q}}.a^{\frac{p'}{q'}} = \sqrt[q]{a^p}.\sqrt[q']{a^{p'}} = \sqrt[qq']{a^{pq'}}.\sqrt[q'q]{a^{p'q}} = \sqrt[qq']{a^{pq'}.a^{p'q}} = \sqrt[qq']{a^{pq'+p'q}} = a^{\frac{pq'+p'q}{qq'}} = a^{\frac{p}{q}+\frac{p'}{q'}} = a^{r+r'}$$

Teorema

$a \in \Re \quad r \text{ y } r' \in Q$ **Si a>1** se cumple: 1) $a^r > 1 \ \forall r \in Q^+$

2) $r < r' \Leftrightarrow a^r < a^{r'}$

3) $\forall k > 0 \ \exists r_0 \in Q^+ / a^{r_0} > k$

4) $\forall \varepsilon > 0 \ \exists r_1 \in Q^- / a^{r_1} < \varepsilon$

Si 0<a<1

5) $a^r < 1 \ \forall r \in Q^+$

6) $r < r' \Leftrightarrow a^r > a^{r'}$

7) $\forall k > 0 \ \exists r_0 \in Q^- / a^{r_0} > k$

8) $\forall \varepsilon > 0 \ \exists r_1 \in Q^+ / a^{r_1} < \varepsilon$

Dem

1) $\forall r \in Q^+ \quad r = \frac{p}{q} \text{ con } p \text{ y } q \in Z^+ \Rightarrow a^r = a^{\frac{p}{q}} = \sqrt[q]{a^p}$

$a > 1 \text{ y } p \in Z^+ \Rightarrow a^p > 1 \Rightarrow a^r = \sqrt[q]{a^p} > 1 \quad (*)$

(*) si $\sqrt[q]{a^p} \le 1 \Rightarrow \left(\sqrt[q]{a^p}\right)^q \le 1 \Rightarrow a^p \le 1$ lo cual contradice que $a^p > 1$

Ejercicios (Repartido 6 del curso presencial)

I) Resolver en $(\Re,+,\bullet,\le)$: **i)** $x\sqrt{x+3} \le 0$ **ii)** $\sqrt{\frac{x^3}{x+1}} > 0$ **iii)** $(x+3)\sqrt{4-x} < 0$

iv) $\sqrt{x} + \sqrt{4-x} \ge 0$ **v)** $(x+2)\sqrt[3]{x^2-1} \le 0$ **vi)** $|2-x|\sqrt{\frac{3x+1}{|x|+5}} \le 0$ **vii)** $x\sqrt{x+3} - \frac{5x-1}{\sqrt{x+3}} < 0$

II) Idem.

i) $\sqrt{x+3} - 2x = 0$ **ii)** $x + \sqrt{x-1} = 13$ **iii)** $x + \sqrt{x^2-1} = \sqrt{4x^2+4x-1}$

III) Idem.

i) $\sqrt{x+1} > x-1$ **ii)** $\sqrt{x+7}+1-2x<0$ **iii)** $(1-x)\sqrt{x+1} \geq 5-3x$

iv) $\sqrt{2x+1}+\dfrac{2}{\sqrt{2x+1}} \geq 2$ **v)** $\sqrt{x+6} > \sqrt{x+1}+\sqrt{2x-5}$

IV) Ídem.

i) $\dfrac{8}{x\sqrt{x^2-4}} < 0$ **ii)** $x\sqrt{x^2+1} \geq 0$ **iii)** $\sqrt{|2x+1|-3} > 0$

iv) $\dfrac{x\sqrt[5]{x+3}}{\sqrt[6]{x^2-1}} \leq 0$ **v)** $\sqrt[3]{x(x+1)} - \dfrac{2x^2+5x+8}{3\sqrt[3]{x^2(x+1)^2}} > 0$

V) Ídem.

i) $\sqrt{x^2-1} = x+2$ **ii)** $\sqrt{x^2+1} = \sqrt{x+3}$ **iii)** $\sqrt{x+a} = x+a$

VI) Ídem.

i) $(2x-2) \leq \sqrt{x^2-4x+3}$ **ii)** $\sqrt{x^2} < 4$ **iii)** $\sqrt{x^2+1} \leq 1$

iv) $\sqrt{x^2+1} < \sqrt{x^2+2}$ **v)** $\sqrt{x^2-1} \leq \sqrt{x^2-2}$ **vi)** $\sqrt{x}+\sqrt{x-1} < \sqrt{4x-1}$

VII) Probar que $\sqrt{2}+\sqrt{3}$ es irracional. (Sug. proceder por absurdo y tener en cuenta que $\sqrt{2}$ es un irracional).

VIII) Consideramos $a,b \in \Re^+$ Probar: $\dfrac{a}{b} < \sqrt{2} \Leftrightarrow \dfrac{a+2b}{a+b} > \sqrt{2}$

Respuestas:

I) i) $[-3,0]$ **ii)** $(-\infty,-1)\cup(0,+\infty)$ **iii)** $(-\infty,-3)$ **iv)** $[0,4]$
v) $(-\infty,-2]\cup[-1,1]$ **vi)** $\left\{-\frac{1}{3},2\right\}$ **vii)** $\varnothing$

II) i) $\{1\}$ **ii)** $\{10\}$ **iii)** $\varnothing$

III) i) $[-1,3)$ **ii)** $(2,+\infty)$ **iii)** $\left[3,\dfrac{7+\sqrt{17}}{2}\right]$ **iv)** $\left(-\frac{1}{2},+\infty\right)$ **v)** $\left[\frac{5}{2},3\right]$

IV) i) $(-\infty,-2)$ **ii)** $[0,+\infty)$ **iii)** $(-\infty,-2)\cup(1,+\infty)$ **iv)** $[-3,-1)$ **v)** $(-\infty,-2)\cup(4,+\infty)$

V) i) $\left\{-\frac{5}{4}\right\}$ **ii)** $\{-1,2\}$ **iii)** $\{-a, 1-a\}$

VI) i) $(-\infty,1]$ **ii)** $(-4,4)$ **iii)** $\{0\}$ **iv)** $\Re$ **v)** $\varnothing$ **vi)** $[1,+\infty)$

Vamos a intentar ahora definir y estudiar la potencia de base y exponente real.

Potencia de base y exponente real

Teorema

$$H)\ \begin{cases} a,b \in \Re \quad a>1 \\ A=\left\{a^r \in \Re \,/\, r \in Q\,;\, r \le b\right\} \end{cases} \qquad T)\quad \exists\, \overline{ext}\, A$$

Dem: Intentaremos utilizar el axioma de completitud, para lo cual debemos probar:

i) $A \subseteq \Re$ lo cual se cumple por la propia definición del conjunto A

ii) $A \neq \varnothing \quad b-1<b$ aplicando densidad de Q en $\Re$ podemos afirmar:

$$\exists r_0 \in Q \,/\, b-1<r_0<b \Rightarrow a^{r_0} \in A \Rightarrow A \neq \varnothing$$

iii) A acotado superiormente.

$$\left.\begin{array}{l} b<b+1 \Rightarrow \exists\, r_1 \in Q \,/\, b<r_1<b+1 \\ \text{como} \quad \forall a^r \in A \quad r \le b \end{array}\right\} \Rightarrow r<r_1 \ \forall a^r \in A$$ como además a>1 tenemos que

$a^r < a^{r_1} \quad \forall a^r \in A \Rightarrow a^{r_1}$ es cota superior de A y por lo tanto A está acotado superiormente.

De i) ii) y iii) aplicando el axioma de completitud podemos afirmar que $\exists \overline{ext} A$.

Definición

Consideramos $a \in \Re^+$ y $b \in \Re$

Si a>1 definimos $a^b = \overline{ext}\left\{a^r \in \Re \,/\, r \in Q\,;\, r \le b\right\}$

Si a=1 definimos $a^b = 1^b = 1$

Si 0<a<1 definimos $a^b = \left(\frac{1}{a}\right)^{-b}$ observese que si $0<a<1 \Rightarrow \frac{1}{a}>1$

Teorema

Siendo $a, a' \in \Re^+$ b y $b' \in \Re$ se cumple:

1) $a^b . a^{b'} = a^{b+b'}$

2) $\frac{a^b}{a^{b'}} = a^{b-b'}$

3) $a^b a'^b = (aa')^b$

4) $\frac{a^b}{a'^b} = \left(\frac{a}{a'}\right)^b$

5) $\left(a^b\right)^{b'} = a^{b.b'}$

En este caso no demostraremos ninguna de las propiedades enunciadas pues las complicaciones técnicas que ello implica exceden los objetivos de este trabajo.

Teorema Consideramos: $a \in \Re^+ \quad x\ x' \in \Re$

Si a>1 se cumple: 1) $a^x > 1 \ \forall x \in \Re^+$

2) $x < x' \Leftrightarrow a^x < a^{x'}$

3) $\forall k > 0 \ \exists x \in \Re^+ \ / \ a^x > k$

4) $\forall \varepsilon > 0 \ \exists x \in \Re^- \ / \ a^x < \varepsilon$

Si 0<a<1 se cumple: 5) $a^x < 1 \ \forall x \in \Re^+$

6) $x < x' \Leftrightarrow a^x > a^{x'}$

7) $\forall k > 0 \ \exists x \in \Re^- \ / \ a^x > k$

8) $\forall \varepsilon > 0 \ \exists x \in \Re^+ \ / \ a^x < \varepsilon$

Dem

1) $\forall x \in \Re^+ \Rightarrow x > 0$ aplicando densidad de Q en $\Re$ $\exists r_0 \in Q / x > r_0 > 0$ como a>1 entonces $a^{r_0} > 1$.Por otra parte $a^x = \overline{ext}\left\{a^r \in \Re \ / \ r \in Q ; r \le x\right\}$ tenemos entonces un elemento del conjunto $\left(a^{r_0}\right)$ mayor que 1, en consecuencia el extremo superior es también mayor que uno. En definitiva $a^x > 1 \quad \forall x \in \Re^+$.

Ejercicios (Repartido 7 del curso presencial)

I) Resolver en $(\Re,+,\cdot,\le)$:

i) $3^{3x+2} = 9^x$ **ii)** $9^{2x+1} = 1$ **iii)** $2^x.16 = 4^{3x+5}$ **iv)** $3^{2x} - 5.3^x + 4 = 0$

v) $4^x - 6.2^x + 8 = 0$ **vi)** $3^{x+1} + \frac{1}{3^x} = 4$ **vii)** $(x^2 + x)\, 3^{\frac{1}{x}} = 0$ **viii)** $x^2.5^x = 5^x$

ix) $(x^2 - x)\, 7^{\frac{x}{x+1}} = 2.7^{\frac{x}{x+1}}$

II) Ídem:

i) $5^{\frac{x-1}{x}} (x^2 - 2x) \le 0$ **ii)** $(x^2 - x)\, 7^{\frac{x}{x+1}} > 2.7^{\frac{x}{x+1}}$ **iii)** $1 - 5^{x^2-4} \ge 0$ **iv)** $(0{,}2)^{x^2-2x} < 1$

v) $5^{x^2-2x} > 5^{x-4}$ **vi)** $(0{,}3)^{x^2-x} - (0{,}3)^{2x+3} \ge 0$ **vii)** $7^{x^2-1} \le 10^{x^2-1}$

III) Ídem:

i) $3^x = 9^{2x+3}$ **ii)** $\left(4^{3-x}\right)^{2-x} = 1$ **iii)** $4^{2x+1} = -4$ **iv)** $5^{3x+2} - \frac{1}{25} = 0$ **v)** $3^{\sqrt{x}} = 243$

vi) $10^{2x} - 3.10^x + 2 = 0$ **vii)** $\left(\frac{1}{9}\right)^x - 2.\left(\frac{1}{3}\right)^x - 3 = 0$ **viii)** $3^x + 3^{x-1} + 3^{x-2} + 3^{x-3} + 3^{x-4} = 363$

ix) $(x^2+x).5^x=0$ **x)** $(x^2-3)\,2^{\frac{x}{x+1}}=2x.\,2^{\frac{x}{x+1}}$ **xi)** $5^{3x+4}-7^{2x-3}=0$ **xii)** $11^{x+1}=7.6^{2x+4}$

xiii) $x^{\sqrt{x}}=\left(\sqrt{x}\right)^x$ **xiv)** $4+\frac{2}{3^x-1}=\frac{5}{3^{x-1}}$ **xv)** $2^x+2^{x+1}+2^{x+2}+2^{x+3}=3^x+3^{x+1}+3^{x+2}+3^{x+3}$

xvi) $2^x\ 4^{|x|}=8$

IV) Ídem:

i) $(x^2+x)\,5^{\frac{1}{x}}<0$ **ii)** $(x^2-2x)\,2^{\frac{x}{x+1}}\geq 3.2^{\frac{x}{x+1}}$ **iii)** $\left(\frac{1}{5}\right)^{\frac{3x+2}{x-1}}>1$ **iv)** $(0{,}72)^{x^2-7x+12}<1$

v) $27\leq 81^{5x-2}$ **vi)** $2^{\frac{x^2-1}{x-2}}\leq 256$ **vii)** $27^x\leq 81^{5x-2}$

V) Consideramos: $f_m:\Re\to\Re\ ;\quad f_m(x)=(m+3)\,x^2+2mx+m \qquad (m\in\Re)$

$g_m:\Re\to\Re\ ;\quad g_m(x)=m\,x^2+(m+1)\,x+m+1$

1) **i)** Determinar los valores de m para que $f_m(x)>1\quad\forall x\in\Re$
ii) Para m hallado en **i)** verificar que $(f_m(x))^{g_m(x)}>1\quad\forall x\in\Re$

2) Hallar los valores de m para que la ecuación $9^{g_m(x)}+3=4.3^{g_m(x)}$ tenga todas sus raíces reales menores que 1
(Parte de uno de los ejercicios propuestos en el examen del 23/7/93)

VI) Sea $f_m:\Re\to\Re\ ;\quad f_m(x)=m\,x^2+(3m+1)\,x+m$

A) **i)** Investigar si existen valores de m para los cuales $f_m(x)>0\quad\forall x\in\Re$
ii) Ídem $f_m(x)<0\quad\forall x\in\Re$

B) Hallar los valores de m para que la ecuación $2^{f_m(x)}-2^{3-f_m(x)}+2=0$ tenga dos raíces reales menores que –1.

C) Para m=-3 resolver en $(\Re,+,\cdot,\leq)$: **i)** $2^{|\,1-f_m(x)\,|}-\left(\frac{1}{4}\right)^{x-\frac{1}{2}}\leq 0$

ii) $\sqrt{1-f_m(x)}<2\,(x-1)$

(Ejercicio propuesto en el examen del 28/12/92)

Logaritmación

Definir $\log_b a = c \Leftrightarrow b^c = a$ es lo más previsible; para ello debemos investigar previamente la existencia de dicho "c" y en caso de que exista, cuantos "c" hay. Por lo tanto antes de la definición prevista tratemos las siguientes proposiciones

Lema 1

$$H)\begin{cases} a, b \text{ y } c \in \Re \\ a > 1 \\ a^b < c \end{cases} \qquad T) \quad \exists b' \in \Re\,;\, b' > b \,/\, a^{b'} < c$$

Dem:

Debemos encontrar b'>b / $a^{b'} < c$ si encontramos $n \in N$ tal que $a^{b+\frac{1}{n}} < c$ tendriamos que el b' que andamos buscando es $b + \frac{1}{n}$.

$$a^{b+\frac{1}{n}} < c \Leftrightarrow a^b a^{\frac{1}{n}} < c \Leftrightarrow a^{\frac{1}{n}} < \frac{c}{a^b} \Leftrightarrow *\left(a^{\frac{1}{n}}\right)^n < \left(\frac{c}{a^b}\right)^n \Leftrightarrow a < \left(\frac{c}{a^b}\right)^n \qquad (*)\ a > 1\ n > 0 \Rightarrow a^{\frac{1}{n}} > 1$$

Por hipótesis $a^b < c \Rightarrow \frac{c}{a^b} > 1$ aplicando una de las propiedades de la potencia de exponente natural $\exists n_0 \in N \,/\, \left(\frac{c}{a^b}\right)^{n_0} > a$ volviendo atrás en el razonamiento anterior tenemos que $a^{b+\frac{1}{n_0}} < c$.

Llamando $b' = b + \frac{1}{n_0}$ entonces b'>b y $a^{b'} < c$

Lema 2

$$H)\begin{cases} a, b, c \in \Re \\ a > 1 \\ a^b > c \end{cases} \qquad T) \quad \exists b'' \in \Re\,;\, b'' < b \,/\, a^{b''} > c$$

Demostración análoga.

Teorema

$$H)\begin{cases} a \in \Re^+ \\ b \in \Re^+ \quad b \neq 1 \end{cases} \qquad T)\begin{cases} 1)\ \exists c \in \Re \,/\, b^c = a \\ 2)\ c \text{ es unico} \end{cases}$$

Dem: Si b>1 Consideramos $A = \left\{x \in \Re \,/\, b^x \leq a\right\}$

La idea consiste en probar: I) $\exists \overline{ext} A$ al que llamaremos c

II) $b^c = a$

I) i) $A \subseteq \Re$ por la propia definición del conjunto A.

ii) $A \neq \varnothing \qquad b > 1 \ \ a \in \Re^+ \Rightarrow \exists x_0 \in \Re^- \,/\, b^{x_0} < a \Rightarrow x_0 \in A \Rightarrow A \neq \varnothing$

iii) A acotado superiormente.

$$\left.\begin{array}{l} b>1 \;\; a\in\Re^+ \Rightarrow \exists x_1 \in \Re^+ \;/\; b^{x_1} > a \\ \text{como} \quad \forall x\in A \;\; b^x \le a \end{array}\right\} \Rightarrow b^x < b^{x_1} \;\; \forall x \in A$$

además b>1 entonces $x < x_1 \;\; \forall x\in A \Rightarrow x_1$ es cota superior de A.

De i) ii) y iii) aplicando el axioma de completitud tenemos que $\exists \overline{ext}\, A$ al que denominamos c.

II) Nos falta demostrar que $b^c = a$, lo que haremos por absurdo.

<u>Si $b^c<a$</u> aplicando el lema 1 $\exists c' \in \Re\,; c' > c \,/ b^{c'} < a \Rightarrow c' \in A$ pero $c' > c = \overline{ext}A$
lo cual es absurdo.

<u>Si $b^c>a$</u> aplicando el lema 2 $\exists c'' \in \Re\,; c'' < c \,/\, b^{c''} > a$ como $\forall x \in A \;\; b^x \le a \Rightarrow$

$$\left.\begin{array}{l} \Rightarrow b^x < b^{c''} \;\; \forall x \in A \\ \text{ademas} \;\; b>1 \end{array}\right\} \Rightarrow x < c'' \;\; \forall x \in A \Rightarrow$$ c'' es cota superior de A

pero $c'' < c = \vec{\overline{ext}}\, A$ Abs.

Por lo tanto si $b^c \not< a$ y $b^c \not> a$ entonces $b^c = a$

<u>Si 0<b<1</u> $\Rightarrow \dfrac{1}{b} > 1 \Rightarrow \exists d \in \Re \,/ \left(\dfrac{1}{b}\right)^d = a \Rightarrow b^{-d} = a$ llamando c=-d tenemos que:

$\exists c \in \Re \,/\, b^c = a$

2) <u>Unicidad</u> Suponemos que: $\exists c_1 \in \Re \,/\, b^{c_1} = a$ por 1) $\exists c \in \Re \,/\, b^c = a$ entonces

$$\left.\begin{array}{l} b^{c_1} = b^c \\ \text{ademas} \;\; b \ne 1 \end{array}\right\} \Rightarrow c_1 = c$$ En consecuencia c es único.

<u>Definición</u>

Consideramos: $a \in \Re^+, b \in \Re^+ \text{y } b \ne 1$

Definimos $\log_b a = c \Leftrightarrow b^c = a$

Ejer: 1) Calcular: i) $\log_2 8$ ii) $\log_{10} 1000000$ iii) $\log_4 2$ iv) $\log_b 1$ v) $\log_a a$ vi) $\log_b b^\alpha$

2) ¿Porqué en la definición exigimos $a \ge 0 \;\; b \ge 0 \;\; \text{y } b \ne 1$?

Teorema

Siendo: $a, a' \in \Re^+$ $b, b' \in \Re^+$ $b \neq 1$ $b' \neq 1$ se cumple:

1) $b^{\log_b a} = a$
2) $\log_b a + \log_b a' = \log_b aa'$
3) $\log_b a - \log_b a' = \log_b \frac{a}{a'}$
4) $c.\log_b a = \log_b a^c \qquad (c \in \Re)$
5) $\log_b a = \frac{\log_{b'} a}{\log_{b'} b}$ (cambio de base)

Dem 1):

$$\left.\begin{array}{l} \text{Si } \log_b a = c \Rightarrow b^c = a \\ \text{como } \quad c = \log_b a \end{array}\right\} \Rightarrow b^{\log_b a} = a$$

Dem 5):

Debemos probar: $\log_b a = \frac{\log_{b'} a}{\log_{b'} b} \Leftrightarrow \log_{b'} b \,.\, \log_b a = \log_{b'} a \Leftrightarrow b'^{\log_{b'} b . \log_b a} = a$

Demostremos esta última igualdad.

$b'^{\log_{b'} b \log_b a} = \left(b'^{\log_{b'} b}\right)^{\log_b a} = (b)^{\log_b a} = a$ l.q.q.d.

Pasamos ahora al crecimiento de la función logarítmica.

Teorema

Consideramos a y b dos reales positivos.

Si b>1 se cumple: 1) i) $\log_b a > 0 \Leftrightarrow a > 1$

ii) $\log_b a < 0 \Leftrightarrow a < 1$

2) $a < a' \Leftrightarrow \log_b a < \log_b a' \qquad (a' \in \Re^+)$
3) $\forall k > 0 \;\; \exists x \in \Re \; (x > 1) \,/\, \log_b x > k$
4) $\forall k > 0 \;\; \exists x \in \Re \; (0 < x < 1) \,/\, \log_b x < -k$

Si 0<b<1 se cumple 5) i) $\log_b a > 0 \Leftrightarrow a < 1$

ii) $\log_b a < 0 \Leftrightarrow a > 1$

6) $a < a' \Leftrightarrow \log_b a > \log_b a' \qquad (a' \in \Re^+)$
7) $\forall k > 0 \;\; \exists x \in \Re \; (0 < x < 1) \,/\, \log_b x > k$
8) $\forall k > 0 \;\; \exists x \in \Re \; (x > 1) \,/\, \log_b x < -k$

Dem 1) i) $(\Rightarrow)$ $H) \begin{cases} b > 1 \\ \log_b a > 0 \end{cases}$ T) $a > 1$

$\log_b a > 0 \quad y \quad b > 1 \Rightarrow b^{\log_b a} > 1 \Rightarrow a > 1$

$(\Leftarrow) \qquad H) \begin{cases} b > 1 \\ a > 1 \end{cases} \qquad T) \quad \log_b a > 0$

por absurdo; suponemos $\log_b a \leq 0$ como b>1 entonces:
$b^{\log_b a} \leq 1 \Rightarrow a \leq 1$ lo que contradice la hipótesis.

Observación

Si b>1 y a>0

$\log_b a > 0 \Leftrightarrow a > 1 \Leftrightarrow a - 1 > 0$
$\log_b a = 0 \Leftrightarrow b^0 = a \Leftrightarrow a = 1 \Leftrightarrow a - 1 = 0$
$\log_b a < 0 \Leftrightarrow a < 1 \Leftrightarrow a - 1 < 0$

Por lo tanto: Si b>1 y a>0 $\quad Sig(\log_b a) = Sig(a-1)$

Ejercicios: Probar:

1) Si 0<b<1 y a>0 $\quad Sig(\log_b a) = Sig(1-a)$
2) En general: si b>0 a>0 y $b \neq 1 \qquad Sig(\log_b a) = Sig(a-1)(b-1)$
3) Si $b > 1 \quad a \neq 0 \quad Sig \log_b |a| = Sig(a-1)(a+1)$
4) Bosquejar las gráficas de la función exponencial ($f: f(x) = a^x$) para a>1 y para 0<a<1. También las gráficas de la función logarítmica ($f: f(x) = \log_b x$) para b>1 y para 0<b<1.

Ejercicios (Repartido 8 del curso presencial)

I) Resolver en $(\Re, +, \cdot, \leq)$:

i) $\log_3(x-2)+1 = \log_3(2x-1)$ **ii)** $2\log_4(x-8) = \log_2(3x-4) - 3$

iii) $\log_{16} x + \log_4 x + \log_2 x = 7$ **iv)** $\log_{16} x^4 + \log_8 (x+2)^3 = 3$ **v)** $\log_2 x^2 + 2\log_{x^4} 2 = 2$

vi) $\log_{2x} 2^{x^2} + \log_{2x} x^{x^2} + 3x - \frac{10}{x}\log_3 3^{-x} = x^2 \log_{\sqrt{x}} \sqrt{x^5}$

II) Sean : $f: \Re \to \Re;\ f(x) = \log_x(3x+2)$ y $g: \Re \to \Re;\ g(x) = \log_{x^2}(p-2x)$

i) Hallar p sabiendo que f(2)-g(2)=1
ii) Para p hallado estudiar dominio y signo de f y de g
iii) Resolver en $(\Re, +, \cdot, \leq)$: f(x)-g(x)=1

III) Consideramos la igualdad $\sum_{i=0}^{n} \log \frac{a\,i+b}{i+1} = \log a\,(n+b)$

i) Hallar a y b sabiendo que la igualdad anterior se cumple par n=0 y n=1
ii) Para a y b hallados probar que la igualdad se cumple $\forall n \in N$

iii) Probar que : $\sum_{i=0}^{n} \log\left(\frac{a\,i+b}{i+1}\right)^{k} = k \log a\,(n+b) \qquad \forall k \in \Re \quad \forall n \in N$

iv) Calcular:

$$\sum_{i=10}^{20} \log \sqrt{\frac{a\,i+b}{i+1}}$$

IV) Resolver en $(\Re,+,\cdot,\leq)$:

i) $\log_2(3x-1) \geq 0$ **ii)** $\log_{1/2}(5-x) \leq 0$ **iii)** $\log_{x+2}(x^2-1) \geq 0$

iv) $\log_x(4-3x) \leq 2$ **v)** $\log_{2-x}(3x+2) < \log_{2-x}(x-1)$

V) Consideramos $f:\Re \to \Re;\ f(x) = \log_{4-x}(2x+3)$

i) Estudiar dominio y signo de f.

ii) Hallar a<2 sabiendo que la ecuación $2.f(x) = 4\log_{(4-x)^2}(x^3+3x^2+ax-5)$

iii) Para a hallado resolver completamente la ecuación anterior.

iv) Para a hallado resolver en $(\Re,+,\cdot,\leq)$: $f(x) \leq 1$

VI) i) Sabiendo que la ecuación $\log_{\sqrt{x+1}}(x+a) - \log_{x+1} 2\,(x-1) = 2$ tiene raíz 3 ; hallar a

ii) Con el valor de a hallado resolver en $(\Re,+,\cdot,\leq)$: $\log_{\sqrt{x+1}}(x+a) - \log_{x+1} 2(x-1) \geq 2$

VII) Resolver en $(\Re,+,\cdot,\leq)$:

i) $\log_{x+3}(x^2-9) = 1$ **ii)** $\log_2(3-x)+4 = \log_2(x-5)$

iii) $\log 2x = 2\log(3-x) - \log(x+1)$ **iv)** $\log_{2/3}\frac{3x+1}{x-2} > -2$ **v)** $\log_{x^2-4}(x+8) \geq 1$

vi) $\log_{\frac{x+3}{4}}\frac{5-x}{7} > 1$

VIII) Resolver en $(\Re,+,\cdot,\leq)$:

i) $x^{1+\log x} = 100^{3+\log x}$ **ii)** $x + \log(1+2^x) = x\log 5 + \log 6$

iii) $\begin{cases} 7(\log_y x + \log_x y) = 50 \\ xy = 256 \end{cases}$ **iv)** $\frac{x+2}{1-\log_{x+1}(5-x)} \geq 0$ **v)** $2\log_2(x-1) + \log_{x-1} 2 - 3 \geq 0$

vi) $\log_{x2} 3x - \frac{\log_{x^4}(3x^2-2)}{\log_{9x^2}(x+2)} \leq 0$

I

IX) A) Resolver en $(\Re,+,\cdot,\leq)$:

i) $\log_{x-2}(x^2-x) = 2$ **ii)** $\log_{x-2}(x^2-x) \geq 2$

iii) $\log_{|x-2|}\sqrt{x^2-x} \geq 1$ **iv)** $\log_{|x-2|}(x^2-x) \leq 1$

B) Sea $A = \{x \in \Re / \log_{x-1}(\alpha x^2 + x + \alpha = 2)\} \quad \alpha \in \Re; \quad \alpha \neq 1$

i) Probar que si : $x_0 \in A \Rightarrow \frac{1}{x_0} \notin A$

ii) Determinar α para que $A = \phi$

(examen propuesto en julio de 1992)

Respuestas:

I) **i)** $\{5\}$ **ii)** $\{12\}$ **iii)** $\{16\}$ **iv)** $\{2\}$ **v)** $\left\{\sqrt{2}\right\}$ **vi)** $\left\{\frac{11}{4}\right\}$

II) **i)** a=1 **ii)** $D_f = \Re^+ - \left\{\frac{1}{2}\right\}$ $D_g = (-\infty,10) - \{0,1,-1\}$ **iii)** $\left\{2, \frac{7+\sqrt{65}}{2}\right\}$

III) **i)** a=1 b=2 **iv)** $\frac{1}{2}\log 2$

IV) **i)** $\left[\frac{2}{3},+\infty\right)$ **ii)** $(-\infty,4]$ **iii)** $\left[-\sqrt{2},-1\right)\cup\left[\sqrt{2},+\infty\right)$ **iv)** (0,1) **v)** (1,2)

V) **i)** $D_f = \left(\frac{-3}{2},4\right) - \{3\}$ **ii)** $a = -4$ **iii)** $\{-1,2\}$ **iv)** $\left[\frac{-1}{3},3\right)$

VI) **i)** a=11 **ii)** $[3,+\infty)$

VII) **i)** $\{4\}$ **ii)** ϕ **iii)** $\{1\}$ **iv)** $\left(-\frac{22}{3},-\frac{1}{3}\right)$ **v)** $\left[-3,-\sqrt{5}\right)\cup\left(\sqrt{5},4\right]$
vi) $\left(\frac{-1}{11},1\right)$

VIII) **i)** $\left\{1000,\frac{1}{100}\right\}$ **ii)** $\{1\}$ **iii)** x=2 e y=128 ó x=128 e y=2
iv) $(-1,0)\cup(2,5)$ **v)** $\left(2,1+\sqrt{2}\right]\cup[3,+\infty)$ **vi)** ϕ

IX) **i)** -3 **ii)** $\left(\frac{1}{2},\frac{2}{3}\right]\cup(1,2]$

X) **A)** **a)** ϕ **b)** $(3,+\infty)$ **c)** $\left(1,\frac{4}{3}\right]\cup(3,+\infty)$ **d)** $\left[-\sqrt{2},0\right)\cup\left[\sqrt{2},2\right)$

Inicio

➢ Para_volver_a_Menú

DIVISIBILIDAD

DIVISIBILIDAD EN (N,+,.,<)

Frente a la imposibilidad de realizar la división exacta en todos los casos dentro de la estructura de los naturales definiremos la división entera que seguramente como todos sospechamos una buena definición puede ser:

$$\left.\begin{matrix} a & b \\ r & q \end{matrix}\right\} \Leftrightarrow \begin{cases} a = bq + r \\ r < b \end{cases}$$

Si somos rigurosos previamente a esta definición debemos discutir en que condiciones existen q y r , y cuando ello ocurre cuantos "q" y cuantos "r" hay.

Teorema

$$\mathbf{H)} \begin{cases} a \in N, b \in N \\ b \neq 0 \end{cases} \qquad \mathbf{T)} \begin{cases} 1) \exists q, r \in N \,/\, a = bq + r \quad y \quad r < b \\ 2)\ q \text{ y } r \text{ son unicos} \end{cases}$$

Dem:

Consideramos $H=\{x \in N \,/\, bx \leq a\}$ Intentaremos demostrar que H tiene máximo y que este es el "q" de la tesis. Para ello utilizaremos el principio de buena ordenación.

i) $H \subseteq N$ por la propia definición de H.

ii) $H \neq \phi$ pues: $0.b = 0 \leq a \Rightarrow 0 \in H$

iii) H acotado superiormente. Efectivamente cualquier natural mayor o igual que $\frac{a}{b}$ es cota superior de H.

De i) ii) y iii) utilizando buena ordenación o más precisamente su consecuencia inmediata podemos afirmar que existe el máximo de H al que denominamos "alevosamente" q.

$$\left.\begin{matrix} q \in H \Rightarrow bq \leq a \\ \text{como } a, bq \in N \end{matrix}\right\} \Rightarrow a - bq \in N$$ Llamando r=a-bq tenemos que a=bq+r.

Nos falta demostrar que r<b. Hagámoslo.

$$\left.\begin{matrix} q = m\acute{a}x\, H \Rightarrow q+1 \notin H \\ \text{como } q+1 \in N \end{matrix}\right\} \Rightarrow \quad b(q+1) > a \quad \Rightarrow \quad bq + b > a = bq + r \quad \Rightarrow \quad b > r$$

Probemos ahora la unicidad.

Suponemos que existen $q' \text{ y } r' \in N \,/\, a = bq' + r' \quad y \quad r' < b$

Si $q \neq q'$; por ejemplo $q > q' \Rightarrow q - q' > 0 \Rightarrow q - q' \geq 1$ (pues estamos con naturales) $\Rightarrow$ $b(q-q') \geq b$ (recordemos que b>0 por ser un natural no nulo).

Por otra parte $\left.\begin{array}{l} a = bq + r \\ a = bq' + r' \end{array}\right\} \Rightarrow b(q - q') + r - r' = 0 \Rightarrow r' = b(q - q') + r \geq b(q - q') \geq b \Rightarrow r' \geq b$

Lo cual contradice la suposición, Por lo tanto $q = q'$.

Si $q = q' \Rightarrow \left\{\begin{array}{l} a = bq + r \\ a = bq + r' \end{array}\right\} \Rightarrow bq + r = bq + r' \Rightarrow r = r'$

Por lo tanto q y r son únicos.

Definición

Dados a y b naturales, $b \neq 0$ realizar la **división entera** de a entre b es encontrar q y r naturales tales que:

i) a=bq+r
ii) r<b

Lo cual representamos esquemáticamente

a	b
r	q

En caso de que r=0 decimos que b **divide** a a o que a es **múltiplo** de b

Anotamos b/a ó $a = \dot{b}$.

Podemos independizar la definición de divisor o de múltiplo de la definición de división entera.

$$b/a \Leftrightarrow \exists q \in N \text{ tal que } a = bq$$

Ejercicios:

1) Consideramos $R: N^* \to N^* \quad ; xRy \Leftrightarrow x / y$.
Probar que R es una relación de orden amplio (una relación que cumple idéntica, antisimétrica y transitiva

2) Probar: $\left.\begin{array}{l} x / a \\ x / b \end{array}\right\} \Rightarrow x / a \pm b$ (Si un número divide a otros dos divide a su suma y a su resta)

3) Idem. $\left.\begin{array}{l} x / a \\ c \in N \end{array}\right\} \Rightarrow x / ac$ (Si un número divide a a divide a todos sus múltiplos)

4) Idem. $\left.\begin{array}{l} x / a \wedge x / b \\ \lambda, \mu \in N \end{array}\right\} \Rightarrow x / \lambda a + \mu b$ (Si un número divide a otros dos divide a cualquier combinación lineal)

5) Probar: $\left.\begin{array}{l} x / a \wedge x / b \\ a \quad b \\ r \quad q \end{array}\right\} \Rightarrow x / r$

6) Probar: $\left.\begin{array}{l} x / y \\ y \neq 0 \end{array}\right\} \Rightarrow x \leq y$ (Los divisores de un natural no nulo son menores o iguales que el natural dado)

Ejercicios:

1) Completar de todas las formas posibles:

i) 9 ii) a a<200 iii) 60 iv) a 17 a>200
13 35 4 12 q q

2) Hallar a natural sabiendo que: a 37
q^2 q

3) Hallar todas las posibles ternas de naturales (a,b,c) tales que:

a b a+7 15
12 c b c

Nota

Siendo a un número natural anotamos d(a) al conjunto de todos sus divisores

$$d(a) = \{x \in N ; x / a\}$$

Así por ejemplo: $d(6) = \{1,2,3,6\}$ $d(0) = N^*$

Definiremos al máximo común divisor de dos naturales a y b como el máximo de los divisores comunes; o sea como el máximo del conjunto $d(a) \cap d(b)$. Para dar esta definición probemos previamente que dicho máximo existe.

Teorema

$$\left.\begin{array}{l} a \in N, b \in N \\ a^2 + b^2 \neq 0 \end{array}\right\} \Rightarrow \exists \max d(a) \cap d(b)$$

Dem: Observemos que $d(a) \cap d(b)$ es un conjunto de naturales; es pues razonable pensar en utilizar el principio buena ordenación. Para ello debemos probar:

i) $d(a) \cap d(b) \subseteq N$ Lo cual es inmediato pues por definición $d(a) \subseteq N$ y $d(b) \subseteq N$

ii) $d(a) \cap d(b) \neq \varnothing$ $1 \in d(a) \wedge 1 \in d(b) \Rightarrow 1 \in d(a) \cap d(b)$

iii) $d(a) \cap d(b)$ acotado superiormente. Como por hipótesis a y b no son simultaneamente nulos, supongamos por ej que $a \neq 0$
$\forall x \in d(a) \cap d(b) \Rightarrow x \in d(a) \Rightarrow x / a$, como $a \neq 0 \Rightarrow$
$\Rightarrow x \leq a \Rightarrow$ a es cota superior de $d(a) \cap d(b)$

De i) ii) y iii) aplicando el principio de buena ordenación estamos en condiciones de afirmar que $\exists m\acute{a}x\, d(a) \cap d(b)$.

Definición

Dados dos naturales a y b no simultáneamente nulos. Llamamos **máximo común divisor** de a y b al máx $d(a) \cap d(b)$.

Anotamos D(a.b); así por ejemplo D(10,25)=5 D(0,b)=b si $b \neq 0$

Teorema

$$\left.\begin{matrix} a & b \\ r & q \end{matrix}\right\} \Rightarrow d(a) \cap d(b) = d(b) \cap d(r)$$

Dem: Debemos probar que: i) $\forall x \in d(a) \cap d(b) \Rightarrow x \in d(b) \cap d(r)$

ii) $\forall x \in d(b) \cap d(r) \Rightarrow x \in d(a) \cap d(b)$

$$\text{i) } \forall x \in d(a) \cap d(b) \Rightarrow \left\{\begin{matrix} x \in d(a) \Rightarrow x / a \\ \wedge \\ x \in d(b) \Rightarrow x / b \Rightarrow x / bq \end{matrix}\right\} \Rightarrow x / a - bq = r \Rightarrow x \in d(r) \quad \text{como } x \in d(b) \Rightarrow$$

$$\Rightarrow x \in d(b) \cap d(r)$$

$$\text{ii) } \forall x \in d(b) \cap d(r) \Rightarrow \left\{\begin{matrix} x \in d(b) \Rightarrow x / b \Rightarrow x / bq \\ x \in d(r) \Rightarrow x / r \end{matrix}\right\} \Rightarrow x / bq + r = a \Rightarrow x \in d(a) \Rightarrow x \in d(a) \cap d(b)$$

COROLARIO

$$\left.\begin{matrix} a & b \\ r & q \end{matrix}\right\} \Rightarrow D(a,b) = D(b,r)$$

La demostración es una consecuencia inmediata del teorema anterior.

Obs. 144 50 entonces D(144,50)=D(50,44)
44 2

50 44 entonces D(50,44)=D(44,6)
6 1

44 6 entonces D(44,6)=D(6,2)
2 7

6 2 entonces D(6,2)=D(2,0)=2
0 3

Por lo tanto D(144,50)=2.La aplicación sucesiva del último corolario nos permitió calcular el máximo común divisor de 144 y 50; intentemos generalizar este procedimiento.

Algoritmo de Euclides

Consideramos $a, b \in N \quad a > b > 0$. Para hallar D(a,b) realizamos la división

$$\left.\begin{array}{cc} a & b \\ r_1 & q_1 \end{array}\right\} \Rightarrow D(a,b) = D(b,r_1)$$

Si $r_1 = 0 \Rightarrow D(a,b) = D(b,0) = b$

Si $r_1 \neq 0$ realizamos la division $\begin{array}{cc} b & r_1 \\ r_2 & q_2 \end{array} \Rightarrow D(b,r_1) = D(r_1,r_2)$

Si $r_2 = 0 \Rightarrow D(a,b) = D(b,r_1) = D(r_1,0) = r_1$

Si $r_2 \neq 0$ realizamos la division $\begin{array}{cc} r_1 & r_2 \\ r_3 & q_3 \end{array} \Rightarrow D(r_1,r_2) = D(r_2,r_3)$

Si $r_3 = 0 \Rightarrow D(a,b) = D(b,r_1) = D(r_1,r_2) = D(r_2,0) = r_2$

Si $r_3 \neq 0$ ……

……

El proceso continua hasta encontrar un resto nulo. ¿No existirá algún caso en donde esto no ocurre? (o sea que el proceso sea infinito).

Aparentemente no pues: $b > r_1 > r_2 > r_3 >$..... Probémoslo mas rigurosamente. Consideramos

H el conjunto de los restos obtenidos mediante este proceso de divisiones sucesivas; demostremos que H tiene mínimo y que este es 0.

$$\left.\begin{array}{l} H \subseteq N \\ H \neq \varnothing \quad (r_1 \in H) \end{array}\right\} \Rightarrow \exists\, r_n = m\text{ин}H$$

SI $r_n \neq 0$ realizamos la division $\begin{array}{cc} r_{n-1} & r_n \\ r_{n+1} & q_{n+1} \end{array} \Rightarrow r_{n+1} \in H$ y $r_{n+1} < r_n = \min H$ Absurdo

Por lo tanto $r_n = 0$ y en consecuencia este mecanismo de divisiones sucesivas nos conduce en todos los casos a un resto nulo siendo el último resto no nulo (r_{n-1}) el máximo común divisor buscado.

Suele utilizarse el siguiente esquema:

$$\begin{array}{cccccccccc} & q_1 & q_2 & q_3 & \ldots\ldots\ldots\ldots & q_n & & & & \\ a & b & r_1 & r_2 & \ldots\ldots\ldots\ldots & r_{n-2} & r_{n-1} & & D(a,b)= & r_{n-1} \\ r_1 & r_2 & r_3 & \ldots\ldots\ldots\ldots & 0 & & & & & \end{array}$$

Así por ejemplo para calcular D(144,100)

	1	2	3	1	2
144	100	44	12	8	4
44	12	8	4	0	

Entonces D(144,100)=4

Nota

Si en el algoritmo anterior utilizamos sucesivamente el teorema en lugar del corolario tenemos: $d(a) \cap d(b) = d(b) \cap d(r_1) = d(r_1) \cap d(r_2) = \ldots\ldots\ldots\ldots = d(r_{n-1}) \cap d(0) = d(r_{n-1})$ como $r_{n-1} = D(a,b) \Rightarrow d(a) \cap d(b) = d(d(D(a,b))$ El conjunto de los divisores comunes a a y a b es el conjunto de los divisores de su máximo común divisor.

En otras palabras: $\left.\begin{matrix} x / a \\ x / b \end{matrix}\right\} \Leftrightarrow x / D(a,b)$

Teorema

$$D(a,b) = D \quad \Leftrightarrow \quad \begin{cases} i)\ D / a \wedge D / b \\ ii)\ \text{Si } x / a \wedge x / b \Rightarrow x / D \end{cases}$$

Dem ($\Rightarrow$) Partimos de la hipótesis que $D=D(a,b)=\text{máx}\, d(a) \cap d(b) \Rightarrow D \in d(a) \cap d(b) \Rightarrow$

$\Rightarrow \begin{cases} D \in d(a) \Rightarrow D / a \\ D \in d(b) \Rightarrow D / b \end{cases}$ Quedaría por demostrar la condición ii); pero ello ya fué probado en la nota inmediata anterior.

($\Leftarrow$) Ahora debemos demostrar que $D=\text{máx}\, d(a) \cap d(b) \Leftrightarrow \begin{cases} i)\ D \in d(a) \cap d(b) \\ ii)\ D \geq x \quad \forall x \in d(a) \cap d(b) \end{cases}$

i) Por hipótesis $\left.\begin{matrix} D / a \Rightarrow D \in d(a) \\ D / b \Rightarrow D \in d(b) \end{matrix}\right\} \Rightarrow D \in d(a) \cap d(b)$

ii)

$$\left.\begin{matrix} \forall x \in d(a) \cap d(b) \Rightarrow x / a \wedge x / b \quad \text{entonces por hipotesis } x / D \\ \text{como } D \neq 0 \end{matrix}\right\} \Rightarrow x \leq D$$

De i) y ii) deducimos que $D = \max d(a) \cap d(b) = D(a,b)$

Nota: El teorema recién demostrado nos brinda una condición necesaria y suficiente para que D sea máximo común divisor de a y b .Y como tal podría sustituir a la definición dada de máximo común divisor. Es mas algunos autores toman la proposición del teorema inmediato anterior como definición; no necesitando de esta manera el "<"
.Por este motivo entre otros es la opción que se toma en Z y en polinomios.

Veamos ahora algunas otras propiedades del máximo común divisor.

Lema $\left.\begin{matrix} a & b \\ r & q \\ x \in N^* \end{matrix}\right\} \Rightarrow \begin{cases} ax & bx \\ rx & q \end{cases}$

Dem:

$\left.\begin{matrix} a & b \\ r & q \end{matrix}\right\} \Rightarrow \begin{cases} a = bq + r \Rightarrow ax = bxq + rx \\ r < b\ ; \text{como } x > 0 \Rightarrow rx < bx \end{cases}$ Entonces ax dividido bx da cociente q y resto rx.

Teorema

$$\left.\begin{array}{l} D(a,b)=D \\ x\in N^{*} \end{array}\right\} \Rightarrow D(ax,bx)=Dx$$

Dem

$$\begin{array}{cccccccc} & q_1 & q_2 & \ldots\ldots\ldots\ldots & q_{n+1} & & & q_1 \quad q_2 \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots q_{n+1} \\ a & b & r_1 \ldots\ldots\ldots\ldots & r_{n-1} & r_n & \text{Entonces} & ax & bx \quad r_1x \ldots\ldots\ldots\ldots\ldots\ldots r_{n-1}x \quad r_nx \\ r_1 & r_2 \ldots\ldots\ldots\ldots\ldots & 0 & & & & r_1x & r_2x \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots 0 \end{array}$$

Por lo tanto $D(ax,bx)= r_n x = D(a,b)x$

Corolario

$$\left.\begin{array}{l} x \,/\, a \wedge x \,/\, b \\ D(a,b)=D \end{array}\right\} \Rightarrow D\left(\frac{a}{x},\frac{b}{x}\right)=\frac{D}{x}$$

Dem: $D\left(\frac{a}{x},\frac{b}{x}\right)=D' \Rightarrow D\left(\frac{a}{x}x,\frac{b}{x}x\right)=D'x \Rightarrow D(a,b)=D'x \Rightarrow D=D'x \Rightarrow D'=\frac{D}{x}$

Definición

Consideramos a y b dos números naturales.
Decimos que a y b son **primos entre sí** $\Leftrightarrow D(a,b)=1$

Obs: a y b son primos entre si $\Leftrightarrow$ el 1 es su único divisor común

Teorema

$$D(a,b)=D \Leftrightarrow \begin{cases} a=Da' \\ b=Db' \\ D(a',b')=1 \end{cases}$$

Dem: $(\Rightarrow)\quad D(a,b)=D \Rightarrow D \,/\, a \wedge D \,/\, b \Rightarrow \begin{cases} a=Da' \\ b=Db' \end{cases} \Rightarrow MCD(Da',Db')=D \Rightarrow MCD(a',b')=1$

$(\Leftarrow)\quad D(a',b')=1 \Rightarrow D(Da',Db')=1D \Rightarrow D(a,b)=D$

Nota: Este último teorema nos permite muchas veces acortar sensiblemente los "tanteos"; veamos un ejemplo.

Hallar dos naturales a y b sabiendo que ab=9900 y D(a,b)=30

$D(a,b)=30 \Rightarrow \begin{cases} a=30a' \\ b=30b' \end{cases}$ Sustituyendo tenemos : $30a'30b'=9900 \Rightarrow a'b'=11$

obsérvese que es mucho más cómodo tantear dos números cuyo producto sea 11 y sean primos entre sí ; que dos números cuyo producto sea 9900 y su máximo común divisor 30.

a'	b'	a=30a	b=30b
1	11	30	330
11	1	330	30

Nota: Yendo a otra situación. Sabemos que si un número divide a otro divide a cualquiera de sus multiplos; si c/b entonces c/ab. ¿Es cierto el recíproco? ¿Si un número divide a un producto divide necesariamente a uno de los factores?

Teorema de Euclides

$$\left.\begin{array}{l} c \,/\, ab \\ D(a,c)=1 \end{array}\right\} \Rightarrow c \,/\, b$$

Dem: $D(a,c)=! \Rightarrow D(ab,cb)=b$

$$\left.\begin{array}{l} c \,/\, ab \ \text{por hipytesis} \\ c \,/\, cb \ \text{por definiciyn} \end{array}\right\} \Rightarrow c \,/\, D(ab,cb) \Rightarrow c \,/\, b$$

Teorema

$$\left.\begin{array}{l} c \,/\, a_1 a_2 \ldots\ldots a_{n-1} a_n \\ D(c,a_1)=D(c,a_2)=\ldots\ldots=D(c,a_{n-1})=1 \end{array}\right\} \Rightarrow c \,/\, a_n$$

Puede demostrarse por inducción completa; a cargo del lector.

Mínimo común múltiplo

Siendo $a \in N^*$ anotamos m(a) al conjunto de sus múltiplos no nulos; más precisamente:
$m(a) = \{na\,;\, n \in N^*\}$

Parecería razonable definir mínimo común múltiplo de a y b como el mín $m(a) \cap m(b)$. Para ello tenemos que demostrar previamente que dicho mínimo existe.

Teorema

$$a, b \in N^* \Rightarrow \exists \min\, m(a) \cap m(b)$$

Dem

i) $m(a) \cap m(b) \subseteq N$ por definicion
ii) $m(a) \cap m(b) \neq \varnothing$ pues $ab \in m(a) \cap m(b)$

Entonces por P.B.O. $\exists$ $\min\, m(a) \cap m(b)$

Definición

$a, b \in N^*$. Llamamos **mínimo común múltiplo de a y b** (anotamos m(a,b))

$$m(a,b) = \min\, m(a) \cap m(b)$$

Veremos a continuación un teorema que nos vincula el mínimo común múltiplo con el máximo comun divisor.

Teorema

$m(a,b).D(a,b)=ab \quad$ con $\quad a,b \in N^*$

Dem: Intentaremos escribir $m(a) \cap m(b)$ de forma que pueda hallarse su mínimo; para ello buscamos una condición necesaria y suficiente para que $x \in m(a) \cap m(b)$.

$$\text{Si } x \in m(a) \cap m(b) \Rightarrow \left.\begin{cases} x \in m(a) \Rightarrow \exists k \in N^*; x = ka \\ x \in m(b) \Rightarrow \exists h \in N^*; x = hb \end{cases}\right\} \Rightarrow ka = hb$$

$$\text{Por otra parte si } D(a,b)=D \Rightarrow \begin{cases} a = Da' \\ b = Db' \\ \text{con } D(a',b') = 1 \end{cases} \quad \text{Sustituyendo tenemos}$$

$kDa' = hDb' \Rightarrow ka' = hb'$ entonces a' / hb' como $D(a',b') = 1$ por Euclides $a' / h \Rightarrow \exists t \in N^*; h = ta'$

Además $x=hb \Rightarrow x = ta'b$ como $b = Db' \Rightarrow x = ta'b'D$

Probamos entonces que: $\forall x \in m(a) \cap m(b) \Rightarrow x = ta'b'D$. Demostremos ahora que también es cierto el recíproco.

$$\forall x \in N\,;\, x = ta'b'D \Rightarrow \left.\begin{cases} x = ta'b \Rightarrow x \in m(b) \\ x = tab' \Rightarrow x \in m(a) \end{cases}\right\} \Rightarrow x \in m(a) \cap m(b)$$

Por lo tanto: $\forall x \in N^* \text{ tal que } x = ta'b'D \Rightarrow x \in m(a) \cap m(b)$

De ambas proposiciones subrayadas podemos afirmar que:

$$m(a) \cap m(b) = \left\{x \in N\,;\, x = ta'b'D\,;\, t \in N^*\right\}$$

El mínimo del conjunto se da para t=1 Entonces: $m(a,b) = a'b'D$ con D=D(a,b) multiplicando ambos miembros por D tenemos

$$m(a,b)D(a,b)=ab$$

Ejercicios Probar: 1) $D(a,b) = 1 \Rightarrow D(a.b^n) = 1$

2) $D(a,b) = 1 \Rightarrow D(a^p, b^n) = 1$

3) $D(a,b) = 1 \Rightarrow D(a+b,b) = 1$

4) $D(a,b) = 1 \Rightarrow D(a-b,b) = 1$

5) $D(a,b) = D \Rightarrow D(a^n, b^n) = D^n$

6) $m(a,b) = m \Rightarrow m(ax,bx) = mx \quad (x \in N^*)$

7) $\left.\begin{matrix} \text{Si } x / a \wedge x / b \\ m(a,b) = m \end{matrix}\right\} \Rightarrow m\left(\frac{a}{x}, \frac{b}{x}\right) = \frac{m}{x}$

8) $m(a,b) = m \Rightarrow m(a^n, b^n) = m^n$

Números primos y compuestos

Definición

$a \in N ; a \neq 0\ a \neq 1$ Decimos que a es **primo** $\Leftrightarrow$ $d(a) = \{1, a\}$. Si a no es primo lo demominamos **compuesto**

Obs:

Como todos los naturales no nulos aceptan a 1 y si mismos como divisores podemos decir que un número es primo si y solo si acepta dos divisores.

Mediante esta definición los números naturales quedan clasificados en primos,compuestos, 0 y 1.

¿Porqué 0 y 1 no son ni primos ni compuestos? ¿Porqué los naturales distintos de 0 y de 1 que no son primos se llaman compuestos y no simplemente no primos?

Teorema

El menor de los divisores de un número compuesto distinto de 1 es primo.

Dem:

Consideramos $a \in N^* ; a \neq 1 \quad d = \min\left(d(a) - \{1\}\right)$ Debemos probar que d es primo.

Obsérvese que d existe pues $d(a) - \{1\}$ es un conjunto de naturales no vacío.

Intentaremos una demostración por absurdo; suponemos que d no es primo, como no es ni 0 ni 1 entonces es compuesto aceptando entonces un divisor distinto de 1 y de d.

$\exists d' \in N^*, d' \neq 1, d' \neq d$ tal que $d' / d \quad$ como $d / a \Rightarrow d' / a \Rightarrow d' \in d(a) - \{1\}$. Pero d' / d y $d' \neq d \Rightarrow d' < d$

Encontramos pues un elemento del conjunto menor que el mínimo lo que genera el abs.

Teorema

El conjunto de los números primos no tiene máximo

Dem:

Sea H el conjunto de todos los números primos; queremos probar que H no tiene máximo. Lo cual haremos por absurdo.

Suponemos en consecuencia que existe M=máxH. Consideramos ahora P=2.3.5.....M+1 (el producto de todos los números primos más 1)

P>M=máxH $\Rightarrow P \notin H$ como además $P \neq 0$ y $P \neq 1 \quad \Rightarrow$ P es compuesto Aplicando ahora el teorema inmediato anterior $d = \min\left[d(P) - \{1\}\right]$ es primo; pero por la definición dada de P, este dividido cualquier número primo da resto 1. Generándose así la contradicción buscada.

Teorema Euclides para primos

$$\left.\begin{array}{l} p / ab \\ p \ \text{primo} \end{array}\right\} \Rightarrow \left\{\begin{array}{l} p / a \\ \vee \\ p / b \end{array}\right. .$$

Dem:

Si p/a el teorema está demostrado.
Si $p \nmid a$ D(a,p)=1 pues p es primo; como por hipótesis p/ab aplicando Euclides tenemos que p/b.

Teorema

$$\left.\begin{array}{l} p/a_1a_2.....a_n \\ p \text{ primo} \end{array}\right\} \Rightarrow \quad p/a_i \quad \text{para algún i de 1 a n}$$

Demostración por I.C. a cargo del lector.

Definición

Consideramos a un número compuesto. Si $a = p_1p_2.....p_n$ con p_i primo decimos que a admite una **descomposición en producto de factores primos** (D.P.F.P.)

Teorema

$$a \in N \text{ ; a compuesto} \Rightarrow \begin{cases} 1) \text{ a admite una D. P. F. P:} \\ 2) \text{ Dicha D. P. F. P. es unica} \end{cases}$$

Dem 1):

$$a \text{ es compuesto} \Rightarrow \exists p_1 = \min\left(d(a) - \{1\}\right) \quad \text{siendo } p_1 \text{ primo} \Rightarrow a = p_1d_1$$

Si d_1 es primo entonces p_1d_1 es D.P.F.P. de a

Si d_1 es compuesto $\Rightarrow \exists p_2 = \min\left(d(d_1) - \{1\}\right)$ siendo p_2 primo $\Rightarrow d_1 = p_2d_2 \Rightarrow$
$\Rightarrow a = p_1p_2d_2$

Si d_2 es primo entonces $p_1p_2d_2$ es la D.P.F.P. de a
Si d_2 es compuesto .....
.....
.....

El proceso continua hasta que llegamos a un cociente d_n primo; si este mecanismo de divisiones sucesivas es siempre finito nos aseguraríamos de la existencia de la D.F.
Probemos entonces que siempre llegamos a un d_n primo.
Sea H el conjunto de los d_i , $H \subseteq N, H \neq \varnothing$ $(d_1 \in H) \Rightarrow \exists d_n = \min H$ d_n primo pues si si d_n fuese compuesto $\exists p_{n+1} = \min\left(d(d_n) - \{1\}\right)$ con p_{n+1} primo $\Rightarrow d_n = p_{n+1}d_{n+1} \Rightarrow d_{n+1} \in H$ y además $d_{n+1} < d_n = \min H$ lo cual es contradictorio; en consecuencia es proceso descrito es finito y nos conduce en todos los casos a la D.F. de a.

Dem 2) Unicidad .
$$\begin{array}{l} a = p_1p_2.....p_n \quad \text{con } p_i \text{ primo } \forall i \text{ de 1 a n} \quad p_1 \le p_2 \le ..... \le p_n \\ a = q_1q_2.....q_m \quad \text{con } q_i \text{ primo } \forall i \text{ de 1 a m} \quad q_1 \le q_2 \le ..... \le q_m \end{array}$$

Queremos demostrar que $n = m$ y $p_i = q_i$ $\forall i$ de 1 a n . Igualando nos queda

$$p_1p_2.....p_n = q_1q_2.....q_m \Rightarrow \begin{cases} p_1 / q_1q_2....q_m \text{ como } p_1 \text{ primo} \Rightarrow p_1 / q_j \text{ para algъn j de 1 a m} \Rightarrow \\ q_1 / p_1p_2....p_n \text{ como} q_1 \text{ primo} \Rightarrow q_1 / p_k \text{ para algъn k de 1 a n} \Rightarrow \end{cases}$$

$$\Rightarrow p_1 = q_j \geq q_1$$
$$\Rightarrow q_1 = p_k \geq p_1$$

Entonces $p_1 = q_1$ simplificando tenemos $p_2.....p_n = q_2.....q_m$

Reiterando el razonamiento $p_2 = q_2$, $p_3 = q_3$, ..., $p_n = q_n$ (si $n \geq m$)
Si n>m después de simplificar nos queda $q_{n+1}q_{n+2}.....q_m = 1 \Rightarrow q_{n+1} = q_{n+2} = ... = q_m = 1$
lo que contradecía que q_i es primo; por lo tanto n=m.

Ejercicios:

1) Si $a = p_1^{\alpha}p_2^{\alpha}.....p_n^{\alpha}$ con p_i primo
Probar: $x/a \Leftrightarrow x = p_1^{\beta}p_2^{\beta}.....p_n^{\beta}$ con $0 \leq \beta_i \leq \alpha_i \quad \forall i$ de 1 a n

2) Si $a = p_1^{\alpha}p_2^{\alpha}.....p_n^{\alpha}$ y $b = p_1^{\beta}p_2^{\beta}.....p_n^{\beta}$ con p_i primo
Probar: $D(a,b) = p_1^{\gamma}p_2^{\gamma}.....p_n^{\gamma}$ siendo $\gamma_i = \min\{\alpha_i, \beta_i\}$
$m(a,b) = p_1^{\delta}p_2^{\delta}.....p_n^{\delta}$ siendo $\delta_i = \max\{\alpha_i, \beta_i\}$

3)Utilizando la D.P.F.P de un número escribir todos sus divisores; describir un método práctico para obtener todos sus divisores.

4) Deducir una fórmula que permita calcular la cantidad de divisores de un número dado.

5) Probar que si $a = p_1^{\alpha}p_2^{\alpha}.....p_n^{\alpha}$ con p_i primo los divisores de a son los sumandos que se obtienen al desarrollar el producto:
$$P = (p_1^0 + p_1^1 + ... + p_1^{\alpha})(p_2^0 + p_2^1 + ... + p_2^{\alpha}).....(p_n^0 + p_n^1 + ... + p_n^{\alpha})$$

6) Utilizando 5) probar que el número de divisores de a ($\nu(a)$) es:
$$\nu(a) = (\alpha_1 + 1)(\alpha_2 + 1).....(\alpha_n + 1)$$
y que la suma de todas ellas (S_a) es:
$$S_a = \frac{p_1^{\alpha+1} - 1}{p_1 - 1} \cdot \frac{p_2^{\alpha+1} - 1}{p_2 - 1} ..... \frac{p_n^{\alpha+1} - 1}{p_n - 1}$$

Ejercicios (Repartido 11 del curso presencial)

I) Completar de todas las formas posibles los siguientes esquemas de divisiones enteras

i) $\begin{array}{r|l} __ & 9 \\ \hline & 13 \end{array}$ **ii)** $\begin{array}{r|l} a & __ \\ \hline 35 & 4 \end{array}$ a<200 **iii)** $\begin{array}{r|l} 60 & __ \\ \hline 12 & \end{array}$ **iv)** $\begin{array}{r|l} a & 17 \\ \hline q & q \end{array}$ a>200

II) En la división $\begin{array}{r|l} a & b \\ \hline r & 16 \end{array}$, r es el mayor posible y a+b=341 Hallar a,b y r.

III) Hallar a sabiendo que $\begin{array}{c|c} a & 37 \\ \hline q^2 & q \end{array}$

IV) Hallar a y b sabiendo que: $\begin{array}{c|c} a & 15 \\ \hline & q \end{array}$, $\begin{array}{c|c} b & 12 \\ \hline & q-8 \end{array}$, a+b=420

V) Hallar todas las ternas posibles de naturales (a,b,c) tales que: $\begin{array}{c|c} a & b \\ \hline 12 & c \end{array}$ y $\begin{array}{c|c} a+7 & 15 \\ \hline b & c \end{array}$

VI) Completar los siguientes esquemas de algoritmo de Euclides

	3			
	3		1	
		0		

	1	2	3
			75
		0	

VII) Hallar dos naturales a y b sabiendo que a+b=360 y D(a,b)=30

VIII) Hallar dos naturales a y b sabiendo que a,b=9900 y D(a,b)=30

IX) Hallar a y b naturales sabiendo que: a-b=48 , $\frac{a+b}{D(a,b)}=88$

X) Hallar los naturales a y b sabiendo que: $m(a,b).D(a,b)=9000,\ \frac{m(a,b)}{D(a,b)}=90$ y además $a+b<200$

XI) Ídem: sabiendo que $a.b=192,\ \frac{(m+D)^2}{4mD}=\frac{169}{48}$ siendo $m=m(a,b)$ y $D=D(a,b).$

XII) Ídem. sabiendo que: $D(a^2+ab+b^2,a^2)=36,\ \frac{a^2-b^2}{D^2}=29$ siendo $D=D(a,b)$

XIII) Ídem. sabiendo que: $a^2-b^2=6399\quad m(a,b)=4620$

XIV) Ídem sabiendo que: $m(a,b)=504,\quad a>b$ y $\begin{array}{c|c} a & b \\ \hline 20 & \end{array}$

XV) Se sabe que: $11a+8b=\dot{9}$, $3a+4b=\dot{9}$

i) Probar que: $a=\dot{9}\quad y\quad b=\dot{9}$

ii) Si además $D(a,b)=9,\ \begin{array}{c|c} a & b \\ \hline 27 & q \end{array}$, $a=2b+135$. Calcular a y b.

XVI) Sabiendo que: $D(b,c) = 3D(a,c)$ y $m(a,c) = 2m(b,c)$

i) Probar que: $a = \dot{2}$ y $b = \dot{3}$

ii) Demostrar que: $(a^3 - a)(b^3 - 9b) = \dot{\overline{162}}$

iii) Si $D(a,b) = 1$ calcular: $D(b,c)$ y $D(a,c)$.

XVII) Determinar un número natural *n* compuesto de los factores primos 2,5 y 7 sabiendo que 5*n* tiene 8 divisores mas que *n*, 7*n* tiene 12 divisores mas que *n* y 8*n* tiene 18 divisores mas que *n.*

XVIII) Hallar $x = 2^a 3^b 5^c$ sabiendo que $\frac{x}{2}$ tiene 30 divisores menos que *x*, $\frac{x}{3}$ tiene 35 divisores menos que *x* y $\frac{x}{5}$ tiene 42 divisores menos que *x*.

XIX) Determinar el número mas pequeño que admite 15 divisores.

XX) i) Probar que si *m* tiene un número impar de divisores entonces $\exists n \in N\ ;\ n^2 = m$ (o sea que *m* es un cuadrado perfecto.

ii) Hallar $m \in N$ sabiendo que tiene 9 divisores y que $m - 1 = 39p$; p es primo.

XXI) Determinar todas las ternas de números naturales (a,b,c) que verifican: $D(a,b) = 3^3.5$, $m(b,c) = 2.3^4.5.7$ y $a.c = 2.3^5.5.7.13$

XXII) Hallar $n \in N \quad ; n = p^q.q^p$ con p y q primos $p \neq q$ sabiendo que en número de divisores de n es 2*p.q.*

XXIII) i) Hallar a,b y $n \in N$ sabiendo que: $n \neq 1$, $D(an,bn) = 21$, $a^2 - b^2 = \frac{21^3}{n^2}$ y $a - b = 21$

ii) Sea $N = 2^{\alpha}.a^{\beta}$ y $N' = b^{\alpha+1}.5^{\beta}$ Hallar *N* y *N'* sabiendo que 5*N* tiene 20 divisores mas que $\frac{N'}{2}$ y que $\frac{N}{N'}$ tiene dos divisores.

iii) Hallar todos los naturales *h* sabiendo que: $h^2 + 4h = \dot{7}$ $D(h+4,7) = 1$ y $m(h,70) = \sqrt[4]{N'}$

XXIV) i) ¿Qué condición deben cumplir los números naturales *a* para que tengan 12 divisores y $D(a,225) = 15$?

ii) Hallar *a* para que cumpla además que la suma de sus divisores es 168.

iii) Para el valor de *a* hallado en ii) probar que: $n^5 + 5n^2 - 6n = \dot{a}$

XXV) Probar : $D(\,a + nb, a + (n+2)b\,) = 1 \quad \forall n \in N \quad \Leftrightarrow \quad b = \dot{2}$ y $D(a,b) = 1$

XXVI) i) Hallar *a* sabiendo que: $D(a,75) = 5$ y $m(a,75) = 150$

ii) Para *a* hallado probar que: $a^{n+1} + a^n - a - 1 = \dot{\overline{99}}$

XXVII) Se realizan las divisiones enteras de un natural *n* entre dos naturales consecutivos *p* y *p*+1 Demostrar que la condición necesaria y suficiente para que los cocientes sean iguales es que el cociente de la primera división sea menor o igual que el resto de la primera división.

XXVIII) Sean *a,b* y *c* números naturales tales que: $D(a,b) = 2^3.3^2$, $m(b,c) = 2^5.3^3.7^2$ y $m(a,c) = 2^5.3^2.5.7$

i) Probar: $2^5.7 / c$, $7^2 / b$, $7^2 \nmid c$, $5 / a$ y $3^2 / b$.

ii) Si además se sabe que: $\nu(a) = 30$, $\nu(b) = 48$ y $\nu(c) = 36$. Hallar *a,b* y *c*.

XXIX) *a,b* y *c* son tres números naturales que cumplen: $D(a,b) = 2^2.3^3$, $D(a,b,c) = 3^2$ $m(a,b,c) = 2^3.3^4.5$ .7 , $5 / b$, $\nu(b) = 32$ y $\nu(c) = 9$.

Determinar *a,b* y *c* justificando el procedimiento.

XXX) i) Probar: $D(a+b, m(a,b)) = D(a,b)$

ii) Hallar dos naturales *a* y *b* para que: $m(a,b) = 630$ y $a+b = 231$

XXXI) i) Se sabe que $D(a,b) = D(c,d)$, $m(a,b) = m(c,d)$, $c.d = 2^7.3^4.5^2$ y $\nu(a) = 7$

Hallar *a* y *b*.

ii) Hallar todas las parejas (*c,d*) sabiendo además que $c = \overline{\dot{2}\dot{5}}$

DIVISIBILIDAD EN (Z,+,·,≤)

Introducción

Pretendemos en esta sección extender varios de los conceptos vistos bajo este mismo título en la estructura de los naturales ahora a los enteros. Así como también introducir otros nuevos estrechamente vinculados (Congruencias, clases residuales, ecuaciones diofánticas, etc.)

Por lo dicho parece razonable comenzar por definir división entera entre números enteros. Una posibilidad puede ser tomar textualmente la definición vista para los naturales. O sea:

$\begin{matrix} a & b \\ r & q \end{matrix} \Leftrightarrow \begin{cases} a = bq + r \\ r < b \end{cases}$ Pero tal opción nos haría perder la unicidad del cociente y del resto, ya que:

con esta definición $\begin{matrix} 14 & 3 \\ 2 & 4 \end{matrix}$ pero también $\begin{matrix} 14 & 3 \\ -1 & 5 \end{matrix}$ Como otras infinitas posibilidades .

Este inconveniente lo podemos subsanar exigiendo que el resto no sea negativo. En otras palabras nuestro proyecto de definición es:

$$\begin{matrix} a & b \\ r & q \end{matrix} \Leftrightarrow \begin{cases} a = bq + r \\ 0 \le r < b \end{cases} \qquad \text{(Estamos suponiendo que } b \in Z^+\text{)}$$

Antes de asumir tal proyecto como definición debemos demostrar el siguiente:

Teorema

$$H) \begin{cases} a, b \in Z \\ b > 0 \end{cases} \qquad T) \begin{cases} 1)\ \exists q, r \in Z\ ;\ a = bq + r\ \wedge\ 0 \le r < b \\ 2)\ q \text{ y } r \text{ son } \text{ъnicos} \end{cases}$$

Dem1)*:*

Consideramos $M = \{m \in N\ ;\ m = a - bx \text{ con } x \in Z\}$ Intentaremos probar que M tiene mínimo y que dicho mínimo es el resto que andamos buscando. Como M es un conjunto de naturales, para demostrar que tiene mínimo es mas que razonable pensar en buena ordenación. Con tal objetivo debemos verificar que:

i) $M \subseteq N$ Lo cual es cierto por la definición dada del conjunto M.

ii) $M \neq \varnothing$ Para demostrar esta proposición discutiremos dos casos.

Si $a \ge 0$ Tomando x=0 tenemos que $m = a - bx = a - b0 = a \in M$

Si $a < 0$ $\Rightarrow -a > 0$ como b>0 aplicando Arquímedes tenemos que

$\exists n \in N\ ;\ nb > -a \Rightarrow -nb < a$ Llamando $x = -n$ entonces $xb<a \Rightarrow$

$\Rightarrow a - bx \in N \Rightarrow a - bx \in M$

Aplicando buena ordenación de $\left.\begin{matrix} i) \\ ii) \end{matrix}\right\} \Rightarrow \exists$ mín M al que denominamos “alevosamente” r.

Probemos que es el "r" de la tesis. $r = \min M \Rightarrow r \in M \Rightarrow r \in N \wedge \exists q \in Z\,;\, r = a - bq \Rightarrow a = bq + r$
Falta demostrar $0 \le r < b$. Como $r \in N \Rightarrow r \ge 0$; por lo tanto lo que nos falta probar es que r < b lo que haremos por absurdo.
Supongamos que $r \ge b \Rightarrow a - bq \ge b \Rightarrow a \ge b + bq = (b+1)q \Rightarrow a - (b+1)q \in N \Rightarrow k = a - (b+1)q \in M$
Pero $k < r = a - bq = \min M$ Lo cual es contradictorio. Por lo tanto r < b .

La demostración de la unicidad queda a cargo del lector. También puede demostrarse la existencia utilizando la división entera entre naturales, discutiendo si a ≤ 0 ó si a<0.

Definición

Sean $a, b \in Z\,;\, b > 0$ Realizar la **división entera** de a entre b es encontrar $q, r \in Z$ tal que:
$a = bq + r \quad \wedge \quad 0 \le r < b$

Nota:

Puede definirse la división entera para cualquier entero b no nulo (no solamente para los positivos) sustituyendo la segunda condición por: $0 \le r < |b|$

En caso de que r=0 la división se dice exacta, ó también que a es divisible entre b, ó que **b divide a**, ó que **a es múltiplo de b**. (Anotamos b/a ó $a = \dot{b}$)

Independizando la definición de divisores (múltiplos) de la división entera tenemos:

$$b/a \quad (a = \dot{b}) \quad \Leftrightarrow \quad \exists q \in Z\,;\, a = bq$$

El lector habrá observado que no solamente utilizamos la misma notación sino también la misma definición que en naturales. De manera análoga se demuestra que:

$$x/a \;\wedge\; x/b \;\Rightarrow\; x/\alpha a + \beta b \quad \forall \alpha, \beta \in Z$$

En $(N,+,\cdot,\le)$ vimos que: $a/b \;\wedge\; b/a \;\Leftrightarrow\; a = b$ ¿Ocurrirá lo mismo en $(Z,+,\cdot,\le)$?

Teorema

$a, b \in Z$
$a/b \;\wedge\; b/a \;\Leftrightarrow\; |a| = |b|$

Dem. $(\Rightarrow)$

$$\left.\begin{array}{l} a/b \Rightarrow \exists h \in Z\,;\, b = ah \Rightarrow |b| = |a|.|h| \Rightarrow |a| / |b| \\ b/a \Rightarrow \exists k \in Z\,;\, a = bk \Rightarrow |a| = |b|.|k| \Rightarrow |b| / |a| \\ \qquad\qquad \text{como} \quad a, b \in Z \Rightarrow |a|, |b| \in N \end{array}\right\} \Rightarrow |a| = |b|$$

$(\Leftarrow)$

$$|a| = |b| \Rightarrow a = \pm b \Rightarrow \begin{cases} a = (\pm 1).b \Rightarrow b/a \\ b = (\pm 1).a \Rightarrow a/b \end{cases}$$

Definición

$a, b \in Z^*$ Decimos que a y b son **asociados** $\Leftrightarrow$ $a/b \wedge b/a$

Como consecuencia del teorema anterior los asociados de a son únicamente el propio a y su opuesto – a . En los naturales el único asociado de a es el propio a.

Máximo común divisor – mínimo común múltiplo

Antes de comenzar con el tratamiento de los temas del título necesitamos por razones técnicas recordar algunos conceptos de estructuras algebraicas, mas precisamente referidos a los anillos.

Definición

Consideramos: $(A,+,\cdot)$ un anillo conmutativo y con elemento unidad e $I \subseteq A \; ; I \neq \varnothing$

Decimos que I es un **ideal** en $(A,+,\cdot)$ $\Leftrightarrow$ $\begin{cases} 1)\ x_1 + x_2 \in I \quad \forall x_1, x_2 \in I \\ 2)\ a.x \in I \quad \forall x \in I\ , \forall a \in A \end{cases}$

Ej: El conjunto de los enteros pares es un ideal de Z. ¿El conjunto de los impares, es un ideal de Z?

Brindar otro ejemplo de ideal en Z.

Nota:

Fácilmente el lector comprobará que siendo $(A,+,\cdot)$ un anillo conmutativo y con unidad, se cumple

1) $\{0\}$ y A son ideales en $(A,+,\cdot)$ cualesquiera que sea el anillo de referencia. Por ese motivo podemos denominarlos ideales triviales en A.

2) Si $x \in I \Rightarrow -x \in I$ Siendo I un ideal en $(A,+,\cdot)$

3) Todo ideal contiene al O.

4) Si $1 \in I \Rightarrow I = A$

5) Sea: $\{I_j\}$ una familia de ideales en A $\Rightarrow \bigcap I_j$ es un ideal en A

6) Consideramos $S = \{a_1, a_2, ..., a_p\}$ un subconjunto finito de A. Denominamos I(S) al conjunto formado por todas las combinaciones lineales que pueden realizarse con los elementos de S.

O sea: $I(S) = \left\{ x \in A \; ; x = \sum_{i=1}^{p} \alpha_i a_i \quad \text{con} \quad \alpha_i \in A \right\}$

Probar que I(S) es un ideal en A al que llamaremos **ideal generado por S**.

Si un ideal está generado por un conjunto unitario decimos que es **principal**. Así por ejemplo el ideal de los pares es principal pues está generado por $\{2\}$. Si un ideal esta generado por $\{a\}$ anotamos I(a) en lugar de $I(\{a\})$ con el fin de simplificar la notación.

Teorema

En $(Z,+,\cdot,\leq)$ todo ideal es principal.

Mas precisamente: I un ideal en Z $\Rightarrow$ $I=\{0\}$ ó $I=I(c)$ siendo $c=\min I\cap Z^+$

Dem.

Si $I=\{0\}$ Se cumple la tesis.

Si $I\neq\{0\}$ Comencemos por demostrar que existe el mínimo de $I\cap Z^+$ para lo cual es mas que previsible que utilizaremos el principio de buena ordenación.

1) $I\cap Z^+\subseteq N$ $\quad I\cap Z^+\subseteq Z^+\subseteq N \Rightarrow I\cap Z^+\subseteq N$

2) $I\cap Z^+\neq\varnothing$ Como $I\neq\{0\}\Rightarrow\exists a\in I\,;a\neq 0$ Además I es un ideal $\Rightarrow$
$\Rightarrow -a\in I$
Por otra parte al ser $a\neq 0$ a ó –a es positivo.
En consecuencia a ó $-a\in I\cap Z^+$

De 1) y 2) por el P.B.O. podemos afirmar que $\exists \min I\cap Z^+$ al que denominamos c.

Probemos ahora que $M=I(c)$, para lo cual demostraremos:

i) $\forall x\in I(c)\Rightarrow x\in I$

ii) $\forall x\in I\Rightarrow x\in I(c)$

i) $\forall x\in I(c)\Rightarrow x=a.c$ con $a\in Z$. Como $c=\min I\cap Z^+\Rightarrow c\in I$ que es un ideal $\Rightarrow ac\in I\quad\forall a\in Z$

ii) $\forall x\in I$ debemos probar que $x\in I(c)$ o sea que $x=\dot{c}$. Para ello realizamos la división de x entre c demostrando que el resto es nulo.

$$\begin{array}{cc} x & c \\ r & q \end{array} \Rightarrow \begin{cases} x=cq+r \\ 0\leq r<c \end{cases}$$

Si $r\neq 0\Rightarrow r=x-cq\in Z^+$ Por otra parte como $x\in I, cq\in I$ (por i)) e I es un ideal $\Rightarrow r\in I$

Por lo tanto $r\in I\cap Z^+$ pero $r<c=\min I\cap Z^+$ Lo cual es contradictorio.

Entonces $r=0\Rightarrow x=cq\Rightarrow x\in I(c)$

Nota

En $(N,+,\cdot,\leq)$ definimos $D(a,b) = \max d(a) \cap d(b)$

Y luego demostramos $D(a,b) = D \Leftrightarrow \begin{cases} \text{i) } D/a \ \wedge \ D/b \\ \text{ii) } \forall x \in N \, ; \, x/a \wedge x/b \Rightarrow x/D \end{cases}$

En otras palabras definimos el máximo común divisor como el máximo de los divisores comunes y luego demostramos que dicha proposición es equivalente a decir que el máximo común divisor es un divisor común que es dividido por cualquier otro divisor común.

Obsérvese que la proposición tomada como definición nos obliga a trabajar en una estructura ordenada (para poder hablar de máximo de un conjunto). En cambio lo segunda proposición solamente hace referencia a divisibilidad.

En $(Z,+,\cdot,\leq)$ nos es posible en principio considerar cualquiera de las dos proposiciones como posibles definiciones de máximo común divisor. Optaremos por la segunda para allanar el camino cuando el tema sea tratado en polinomios; ya que ahí no dispondremos de una relación de orden que nos permita hablar de máximo de un conjunto.

Por lo dicho pasamos al siguiente teorema.

Teorema

$$\left.\begin{array}{l} a,b \in Z \\ a^2+b^2 \neq 0 \end{array}\right\} \Rightarrow \exists D \in Z \, ; \begin{cases} \text{i) } D/a \ \wedge \ D/b \\ \text{ii) } \forall x \in Z \, ; \, x/a \wedge x/b \Rightarrow x/D \end{cases}$$

Dem.

Consideramos I(a,b) (el ideal generado por $\{a,b\}$) $\quad I(a,b) = \{x \in Z; \, x = pa + sb \quad \text{con } p,s \in Z\}$

Como en Z todo ideal es principal $I(a,b) = I(d) \quad \text{con } d = \min I(a,b) \cap Z^+$ Intentemos demostrar que d es el D de la tesis. Para lo cual debemos probar:

i) $d/a \ \wedge \ d/b$

ii) $\forall x \in Z \, ; \, x/a \wedge x/b \ \Rightarrow x/d$

i) $a \in I(a,b) = I(d)$ (basta tomar p=1 y s=0) $\Rightarrow a = \dot{d} \Rightarrow d/a$ Análogamente se demuestra que d/b

ii) $d \in I(d) = I(a,b) \Rightarrow \exists p,s \in Z$ tal que $d = pa + sb$

Por otra parte $\forall x \in Z \, ; \, x/a \wedge x/b \Rightarrow x/pa + sb \Rightarrow x/d$

Definición

Consideramos $a,b \in Z \, ; \, a^2+b^2 \neq 0$ Decimos que D es **máximo común** divisor de a y b si y solo si:

i) $D/a \ \wedge \ D/b$

ii) $\forall x \in Z \, ; \, x/a \ \wedge \ x/b \ \Rightarrow \ x/D$

El teorema inmediato anterior nos asegura la existencia de un máximo común divisor entre dos enteros no simultáneamente nulos. Pero nada nos dice acerca de cuantos máximos aceptan.

Si $D \in Z$ es máximo común divisor de a y b $\Rightarrow \begin{cases} D/a \ \wedge \ D/b \qquad (1) \\ \forall x \in Z\,;\, x/a \ \wedge \ x/b \ \Rightarrow \ x/D \qquad (2) \end{cases}$

Si $D' \in Z$ es máximo común divisor de a y b $\Rightarrow \begin{cases} D'/a \ \wedge \ D'/b \qquad (3) \\ \forall x \in Z\,;\, x/a \ \wedge \ x/b \ \Rightarrow \ x/D' \qquad (4) \end{cases}$

De (1) y (4) se deduce que D/D' Y a partir de (2) y (3) $\Rightarrow D'/D$
Por lo tanto si a y b admiten dos máximos común divisor D y D' estos son asociados.
Es muy sencillo de probar que :

$$\left.\begin{array}{l} \text{D es M.C.D de a y b} \\ \text{D' asociado a D} \end{array}\right\} \Rightarrow \text{D' es M.C.D. de a y b}$$

En consecuencia dos enteros no simultáneamente nulos aceptan dos máximos común divisor asociados entre sí. Así por ejemplo los M.C.D. de 6 y -9 son 3 y –3.

Nota:

Si $a, b \in Z\,;\, a^2 + b^2 \neq 0$ probamos que tienen dos y solo dos M.C.D. D y D' asociados entre sí. Además por el teorema visto inmediatamente antes de la definición de M.C.D. $I(a,b) = I(D) \Rightarrow \Rightarrow D \in I(a,b) \Rightarrow \exists p, s \in Z\,;\, D = pa + sb$. Como D'=–D, D' también es C.L. de a y de b.

En definitiva podemos afirmar que los máximos común divisor de dos enteros a y b siempre pueden escribirse como combinación lineal de a y b.

Así como dimos una definición de M.C.D. independiente de la relación "<" intentaremos hacer lo propio respecto al m.c.m.

Nuestro proyecto es: m es m.c.m. de a y b $\Leftrightarrow$ $\begin{cases} 1)\ m = \overset{\bullet}{a} \ \wedge \ m = \overset{\bullet}{b} \\ 2)\ \forall x \in Z\,;\, x = \overset{\bullet}{a} \wedge x = \overset{\bullet}{b} \Rightarrow x = \overset{\bullet}{m} \end{cases}$

Por lo dicho vamos al siguiente teorema.

Teorema

H) $a, b \in Z^*$ T) $\exists m \in Z$ tal que $\begin{cases} i)\ m = \overset{\bullet}{a} \ \wedge \ m = \overset{\bullet}{b} \\ ii)\ \forall x \in Z\,;\, x = \overset{\bullet}{a} \wedge x = \overset{\bullet}{b} \Rightarrow x = \overset{\bullet}{m} \end{cases}$

Dem.

Consideramos $H = \left\{ x \in Z \,;\, x = \overset{\bullet}{a} \wedge x = \overset{\bullet}{b} \right\}$ Es inmediato verificar que H es un ideal en Z.

Por lo tanto H es principal; en otras palabras $\exists m \in Z \,;\, H = I(m)$ Probemos ahora que m cumple las proposiciones i) y ii) de la tesis.

i) $m \in I(m) = H \Rightarrow m = \overset{\bullet}{a} \wedge m = \overset{\bullet}{b}$

ii) $\forall x \in Z \,;\, x = \overset{\bullet}{a} \wedge x = \overset{\bullet}{b} \;\Rightarrow\; x \in H = I(m) \;\Rightarrow\; x = \overset{\bullet}{m}$

Definición

Sean a y b dos enteros no nulos. Decimos que m $(m \in Z)$ es **mínimo común múltiplo** de a y b si y solo si cumple:

i) $m = \overset{\bullet}{a} \;\wedge\; m = \overset{\bullet}{b}$

ii) $\forall x \in Z \,;\, x = \overset{\bullet}{a} \;\wedge x = \overset{\bullet}{b} \;\Rightarrow\; x = \overset{\bullet}{m}$

Dados dos enteros a y b no nulos el teorema inmediato anterior nos asegura la existencia de al menos un mínimo común múltiplo. Nada nos dice acerca de cuantos hay.

Probar que si a y b son dos enteros no nulos aceptan dos y solo dos m.c.m. y que además son asociados entre si.

Definición

1) $a, b \in Z$ decimos que a y b son **primos entre si** $\Leftrightarrow$ 1 es M.C.D. de a y b.
2) $p \in Z \;\; p \neq 0 \,,\, p \neq 1$ decimos que p es **primo** $\Leftrightarrow$ $d(p) = \{1, -1, p, -p\}$

Teorema de Euclides

$$\left.\begin{array}{l} c / a.b \\ a \text{ y } c \text{ primos entre si} \end{array}\right\} \Rightarrow c / b$$

Dem.

Como a y c son primos entre si 1 es M.C.D. de a y c $\Rightarrow$ $\exists p, s \in Z \,;\, 1 = pa + sc$ multiplicando ambos miembros por b tenemos que: $b = pba + sbc$ Por hipótesis c/ab y por definición c/c ; entonces $c / pba + scb$ y como pba+sbc=b $\Rightarrow$ c / b

Corolario

1) $$\left.\begin{array}{l} a \text{ y } b \text{ primos entre si} \\ a / c \;\wedge\; b / c \end{array}\right\} \Rightarrow a.b / c$$

2) $$\left.\begin{array}{l} p \in Z \;\; p \text{ primo} \\ p / ab \end{array}\right\} \Rightarrow p / a \;\vee\; p / b$$

Demostración a cargo del lector.

Ejercicios

Demostrar:

1- $\left.\begin{array}{l} a \quad b \\ r \quad q \\ D \text{ es M.C.D. de a y b} \end{array}\right\} \Rightarrow$ D es M.C.D. de b y r

2- Que el procedimiento identificado en "divisibilidad en $(N,+,\cdot,\leq)$" como algoritmo de Euclides también es válido en $(Z,+,\cdot,\leq)$

3- $D = \max d(a) \cap d(b) \Rightarrow$ D es M.C.D. de a y b.
¿Es cierto el recíproco? ¿Ocurre algo similar con el m.c.m.?

4- D es M.C.D de a y b $\Rightarrow$ Dx es M.C.D. de ax y bx

5- $\left.\begin{array}{l} D \text{ es M.C.D. de a y b} \\ x / a \\ x / b \end{array}\right\} \Rightarrow \frac{D}{x}$ es M.C.D. de $\frac{a}{x}$ y $\frac{b}{x}$

6- D es M.C.D. de a y b $\Rightarrow \begin{cases} a = Da' \\ b = Db' \\ a' \text{ y } b' \text{ primos entre si} \end{cases}$

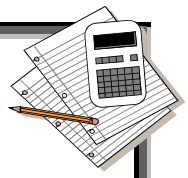
7- D es M.C.D. de a y b $\Rightarrow \begin{cases} D \text{ es M.C.D. de a y } -b \\ D \text{ es M.C.D. de } -a \text{ y } -b \end{cases}$

8- m es m.c.m. de a y b $\Rightarrow \begin{cases} m \text{ es m.c.m. de a y } -b \\ m \text{ es m.c.m. de } -a \text{ y } -b \end{cases}$

9- Si D es M.C.D. de a ,b y m es m.c.m. de a,b $\Rightarrow \left|m.D\right| = \left|a.b\right|$

10- *"Todo entero compuesto puede expresarse como el producto de* (± 1) *por factores primos positivos. Esta expresión es única, salvo el orden en que los factores se consideren."* (sic. Álgebra moderna- Birkhoff – Mc. Lane)

ANOTACIONES



Inicio

Para volver a Menú

CONGRUENCIAS

Introducción

¿ Que fecha tienen los martes del presente año? ¿Y los viernes?
Si el año de referencia es 1998, la respuesta a la primera pregunta es: 1, 8 , 15 , 22 y 29. Por otra parte los viernes de setiembre de 1998 son: 4, 11, 18 y 25.

¿Qué vinculación tienen entre si estos números?
Observemos que la diferencia entre dos cualesquiera de ellos es múltiplo de 7. También cualquiera de estos números dividido 7 da resto 1 (nos estamos refiriendo a: 1, 8 , 15 , 22 , 29) Algo similar ocurre con la fecha de los viernes.

Estos cinco números tienen algo de "igual", todos ellos representan un martes de Setiembre de 1998. Formalicemos esta idea.

Definición

Consideramos $a, b \in Z$ y $m \in Z^+$. Decimos que **a es congruente con b módulo m** si y solo si su diferencia el múltiplo de m. (Anotamos $a \equiv b\,(m)$)

$$a \equiv b\,(m) \quad \Leftrightarrow \quad a - b = \dot{m}$$

Con esta definición 1 , 8 , 15 , 22 y 29 son congruentes dos a dos módulo 7. También observamos que cualquiera de estos números dividido entre 7 da el mismo resto. Probemos que esto no es una casualidad.

Teorema

$$a, b \in Z \;\; m \in Z^+ \;\; \begin{matrix} a & m \\ r & q \end{matrix} \;\; \begin{matrix} b & m \\ r' & q' \end{matrix} \quad \text{Entonces} \quad a \equiv b\,(m) \;\Leftrightarrow\; r = r'$$

Dem

($\Rightarrow$) Por hipótesis $a \equiv b\,(m) \Rightarrow a - b = \dot{m} \Rightarrow \exists h \in Z\,;\, a - b = mh \Rightarrow a = b + mh$

Por otra parte $\left.\begin{matrix} b & m \\ r' & q' \end{matrix}\right\} \Rightarrow \begin{cases} b = mq' + r' \\ 0 \le r' < m \end{cases}$ Sustituyendo en $a = b + mh$ nos queda

$a = mq' + r' + mh = m(q' + h) + r'$ como además $0 \le r' < m \Rightarrow \begin{matrix} a & m \\ r' & q'+h \end{matrix} \Rightarrow r = r'$

($\Leftarrow$) Ahora partimos de que:

$$\left.\begin{matrix} \begin{matrix} a & m \\ r & q \end{matrix} \Rightarrow a = mq + r \\ \begin{matrix} b & m \\ r & q' \end{matrix} \Rightarrow b = mq' + r \end{matrix}\right\} \Rightarrow a - b = m(q - q') \Rightarrow a - b = \dot{m} \Rightarrow a \equiv b\,(m)$$

Al decir que 1 , 8 , 15 , 22 y 29 tienen algo de "igual" estamos insinuando la existencia de una relación de equivalencia, incluso la propia notación lo sugiere. Veamos que efectivamente es así.

Teorema

La congruencia es una relación de equivalencia

H) Consideramos $m \in Z^+$. Ahora definimos $R : Z \to Z;\ xRy \Leftrightarrow x \equiv y\ (m)$

T) R es una relación de equivalencia.

Dem.

Idéntica $xRx \ \forall x \in Z$ $\quad x - x = 0 = \overset{\bullet}{m} \ \forall x \in Z \Rightarrow x \equiv x\ (m) \ \forall x \in Z \Rightarrow xRx \ \forall x \in Z$

Recíproca Si $xRy \Rightarrow yRx$ $\quad xRy \Rightarrow x \equiv y\ (m) \Rightarrow x - y = \overset{\bullet}{m} \Rightarrow y - x = -(x-y) = \overset{\bullet}{m} \Rightarrow$
$\Rightarrow y \equiv x\ (m) \Rightarrow yRx$

Transitiva $\left.\begin{matrix} xRy \\ yRz \end{matrix}\right\} \Rightarrow xRz$

$$\left.\begin{matrix} xRy \Rightarrow x \equiv y\ (m) \Rightarrow x - y = \overset{\bullet}{m} \\ yRz \Rightarrow y \equiv z\ (m) \Rightarrow y - z = \overset{\bullet}{m} \end{matrix}\right\} \Rightarrow (x-y)+(y-z) = x - z = \overset{\bullet}{m} \Rightarrow x \equiv z\ (m) \Rightarrow xRz$$

Antes de analizar las consecuencias que trae el que la congruencia sea una relación de equivalencia veamos algunas otras propiedades que se desprenden mas o menos directamente de la definición.

Teorema

$a, b, a', b' \in Z \quad y\ m \in Z^+$

1) $\left.\begin{matrix} a \equiv b\ (m) \\ h \in Z^+ \end{matrix}\right\} \Rightarrow ah \equiv bh\ (mh)$

2) $\left.\begin{matrix} a \equiv b\ (m) \\ a \text{ y } m \text{ primos entre si} \end{matrix}\right\} \Rightarrow$ b y m primos entre si

3) $\left.\begin{matrix} a \equiv a'\ (m) \\ b \equiv b'\ (m) \end{matrix}\right\} \Rightarrow a + b \equiv a' + b'\ (m)$

4) $\left.\begin{matrix} a \equiv b\ (m) \\ h \in Z \end{matrix}\right\} \Rightarrow a + h \equiv b + h\ (m)$

5) $\left.\begin{matrix} a \equiv a'\ (m) \\ b \equiv b'\ (m) \end{matrix}\right\} \Rightarrow ab \equiv a'b'\ (m)$

6) $\left.\begin{matrix} a \equiv b\ (m) \\ h \in Z \end{matrix}\right\} \Rightarrow ah \equiv bh\ (m)$

7) Si $a \equiv b\ (m) \Rightarrow a^n \equiv b^n\ (m) \quad \forall n \in N$

8) Sea $f : Z \to Z;\ f(x) = c_n x^n + c_{n-1} x^{n-1} + \ldots\ldots c_1 x + c_0$
Si $a \equiv b\ (m) \Rightarrow f(a) \equiv f(b)\ (m)$

$$9)\ \left.\begin{array}{l} ah \equiv bh\ (m) \\ h \text{ y } m \text{ primos entre si} \end{array}\right\} \Rightarrow a \equiv b\ (m)$$

$$10)\ \left.\begin{array}{l} ah \equiv bh\ (m) \\ D \text{ M.C.D. de } h \text{ y } m \\ h = Dh' \quad m = m'D \end{array}\right\} \Rightarrow\ ah' \equiv bh'\ (m)$$

Clases residuales

Anteriormente vimos que la congruencia es una relación de equivalencia en Z. Esto nos trae como consecuencia el establecimiento de una partición en clases de equivalencia sobre dicho conjunto.

A manera de ejemplo trabajemos con la congruencia módulo 2. Si anotamos $[a]$ a la clase de equivalencia de a $(a \in Z)$ y Z_2 al conjunto cociente, tenemos:

$$[0] = \{ x \in Z ; x \equiv 0\ (2) \} = \left\{ x \in Z ; x = \dot{2} \right\}$$

$$[1] = \{ x \in Z ; x \equiv 1\ (2) \} = \left\{ x \in Z ; x - 1 = \dot{2} \right\} = \left\{ x \in Z ; x = \dot{2} + 1 \right\}$$

$$[2] = \{ x \in Z ; x \equiv 2\ (2) \} = \left\{ x \in Z ; x - 2 = \dot{2} \right\} = \left\{ x \in Z ; x = \dot{2} \right\} = [0]$$

$$[3] = \{ x \in Z ; x \equiv 3\ (2) \} = \left\{ x \in Z ; x - 3 = \dot{2} \right\} = \left\{ x \in Z ; x = \dot{2} + 3 = \dot{2} + 2 + 1 = \dot{2} + 1 \right\} = [1]$$

Parece que solo hay dos clases de equivalencia distintas; $[0]$ y $[1]$. Probemos que efectivamente es así.

$$\forall a \in Z \qquad \text{Si } \begin{array}{cc} a & 2 \\ 0 & q \end{array} \Rightarrow a = 2q \Rightarrow a = \dot{2} \Rightarrow a \equiv 0\ (2) \Rightarrow [a] = [0]$$

$$\text{Si } \begin{array}{cc} a & 2 \\ 1 & q \end{array} \Rightarrow a = 2q + 1 \Rightarrow a - 1 = \dot{2} \Rightarrow a \equiv 1\ (2) \Rightarrow [a] = [1]$$

Por lo tanto $\forall a \in Z \quad [a] = [0] \vee [a] = [1]$ y como $0 \not\equiv 1\ (2) \Rightarrow [0] \neq [1]$ En consecuencia $Z_2 = \{ [0], [1] \}$. $\left(Z_2 = Z/_R \right)$

Observemos que $[0]$ es el conjunto de los enteros pares y $[1]$ el de los impares. La partición inducida por la congruencia módulo 2 es la clasificación de los enteros en pares e impares. Clasificación que se maneja desde la mas remota antigüedad, como también las siguientes "reglas de cálculo".

"par +par = par" "par + impar = impar" "impar + impar = par" "par x par =par" "par x impar = par","impar x impar = impar".

Esto podemos formalizarlo definiendo en Z_2 dos operaciones que anotaremos $\oplus$ y $\otimes$ definidas por:

$$\begin{array}{c|cc} \oplus & [0] & [1] \\ \hline [0] & [0] & [1] \\ [1] & [1] & [0] \end{array} \qquad \begin{array}{c|cc} \otimes & [0] & [1] \\ \hline [0] & [0] & [0] \\ [1] & [0] & [1] \end{array}$$

En general si utilizamos la congruencia módulo m $(m \in Z^+)$ inducimos en Z una partición en m clases de equivalencia, llamadas **clases residuales**. Siendo $Z_m = \{[0],[1],.....,[m-1]\}$; pues:

$$\forall a \in Z \quad \text{si} \quad \begin{array}{cc} a & m \\ r & q \end{array} \Rightarrow \begin{cases} a = mq + r \Rightarrow a - r = \dot{m} \Rightarrow a \equiv r\,(m) \Rightarrow [a] = [r] \\ 0 \le r < m \end{cases}$$

(motivo por el cual se denominan clases residuales)

Además si $0 \le h < k < m \Rightarrow 0 < k - h < m \Rightarrow k - h \neq \dot{m} \Rightarrow k \not\equiv h\,(m) \Rightarrow [k] \neq [h]$

Ahora en Z_m definimos $\oplus$ y $\otimes$ de la siguiente forma:

$$[a] \oplus [b] = [a + b] \quad \text{y} \quad [a] \otimes [b] = [a.b]$$

Es inmediato que $\oplus$ y $\otimes$ son operaciones en Z_m ; parece entonces razonable estudiar que tipo de estructura algebraica es $(Z_m, \oplus, \otimes)$. Antes de hacerlo sugerimos analizar los casos particulares $(Z_2, \oplus, \otimes)$, $(Z_3, \oplus, \otimes)$ y $(Z_4, \oplus, \otimes)$.

El lector habrá observado que en todos los casos estamos frente a un anillo conmutativo y con elemento unidad. Que las dos primeras estructuras son además cuerpos; no así Z_4 ya que $[2]$ no tiene inverso.

Es mas $(Z_4, \oplus, \otimes)$ tiene divisores de 0 (no cumple "Hankeliana") pues $[2] \otimes [2] = [0]$ siendo $[0]$ el neutro de $"\oplus"$ y $[2] \neq [0]$.

Teorema

$(Z_m, \oplus, \otimes)$ es un anillo conmutativo y con elemento unidad.

Dem:

Asociativa $([a] \oplus [b]) \oplus [c] = [a] \oplus ([b] \oplus [c]) \quad \forall [a],[b],[c] \in Z_m$

$$\left.\begin{array}{l} ([a] \oplus [b]) \oplus [c] = [a + b] \oplus [c] = [(a + b) + c] \\ [a] \oplus ([b] \oplus [c]) = [a] \oplus [b + c] = [a + (b + c)] \\ (a + b) + c = a + (b + c) \ \text{ por asociativa de } (Z,+) \Rightarrow [(a + b) + c] = [a + (b + c)] \end{array}\right\} \Rightarrow$$

$$\Rightarrow ([a] \oplus [b]) \oplus [c] = [a] \oplus ([b] \oplus [c])$$

Conmutativa $[a] \oplus [b] = [b] \oplus [a] \quad \forall [a],[b] \in Z_m$

$$\left.\begin{array}{l} [a] \oplus [b] = [a + b] \\ [b] \oplus [a] = [b + a] \\ a + b = b + a \ \text{ por conmutativa de } (Z,+) \Rightarrow [a + b] = [b + a] \end{array}\right\} \Rightarrow [a] \oplus [b] = [b] \oplus [a]$$

Neutro $\exists [0] \in Z_m \; ; [a] \oplus [0] = [a] \quad \forall [a] \in Z_m$

$$[a] \oplus [0] = [a+0] = [a]$$

Opuesto $\forall [a] \in Z_m \; \exists -[a] \in Z_m \; ; [a] \oplus (-[a]) = [0]$

$$\forall [a] \in Z_m \; \exists [m-a] \in Z_m \; ; \; [a] \oplus [m-a] = [m] = [0]$$

Análogamente se demuestra que $\otimes$ es asociativa, conmutativa, distributiva respecto a $\oplus$ y tiene neutro ($[1]$).

Teorema

$(Z_m, \oplus, \otimes)$ es un cuerpo $\Leftrightarrow$ m es primo

Dem. $(\Rightarrow)$ Por absurdo. Suponemos que m no es primo, al sobrentender que $m \neq 1 \Rightarrow$ m es compuesto

$$\Rightarrow \exists p, q \in Z \text{ con } 1 < p < m \; \wedge \; 1 < q < m \quad \text{tal que } p.q = m$$

Entonces $\exists [p], [q] \in Z_m$ con $[p] \neq [0] \wedge [q] \neq 0$ tal que $[p] \otimes [q] = [p.q] = [m] = [0]$

Por lo tanto hay divisores de 0; en consecuencia $(Z_m, \oplus, \otimes)$ no es cuerpo. (recordemos que en todo cuerpo hay ausencia de divisores de 0).

$(\Leftarrow)$ Al ser $(Z_m, \oplus, \otimes)$ un anillo conmutativo y con unidad, nos falta por demostrar que se cumple: $\forall [a] \in Z_m \; ; [a] \neq [0] \; \exists [x] \in Z_m \; ; [a] \otimes [x] = [1]$

$$\left. \begin{array}{l} \forall [a] \in Z_m \; ; [a] \neq [0] \Rightarrow a \not\equiv 0 \; (m) \Rightarrow a \neq \dot{m} \\ \text{como m es primo} \end{array} \right\} \Rightarrow \text{a y m son primos entre sí} \Rightarrow$$

$$\Rightarrow 1 \text{ es M.C.D. de a y m} \Rightarrow \exists p, s \in Z \; ; pa + sm = 1 \Rightarrow pa - 1 = \dot{m} \Rightarrow pa \equiv 1 \; (m) \Rightarrow$$
$$\Rightarrow [pa] = [1]$$

Por lo tanto $\forall [a] \in Z_m \; ; [a] \neq [0] \; \exists [p] \in Z_m \; ; [a] \otimes [p] = [ap] = [1]$ l.q.q.d.

Ecuaciones en congruencias – ecuaciones diofánticas

Resolución en (Z,+,·,≤) de $ax \equiv b \; (m)$

Dados $a, b, m \in Z \quad m > 0$, pretendemos hallar $S = \{ x \in Z \; ; ax \equiv b \; (m) \}$.

Observemos que si $\exists x_0 \in Z \; ; ax_0 \equiv b \; (m) \Rightarrow ax_0 - b = \dot{m} \Rightarrow b = ax_0 - \dot{m}$ En consecuencia todo divisor común de a y de m lo es de b. Por lo tanto <u>si el M.C.D. de a y m no divide a b $\Rightarrow$ S=∅</u>

Analicemos ahora que ocurre cuando el M.C.D. de a y m si divide a b. Empecemos por un caso particular; cuando a y m son primos entre sí.

Si 1 es M.C.D. de a y m $\Rightarrow \exists p,s \in Z\,;\, 1 = pa + sm$ multiplicando a ambos miembros por b nos queda:

$$b = pab + smb \;\Rightarrow\; a(pb) - b = -smb = \dot{m} \;\Rightarrow\; a(pb) \equiv b\,(m) \;\Rightarrow\; \exists x_0 = pb\,;\, ax_0 \equiv b\,(m) \;\Rightarrow\; x_0 \in S$$

En consecuencia <u>si a y m son primos entre sí $\Rightarrow$ S≠∅</u> Veamos ahora si existen mas soluciones y en caso afirmativo cuales son.

$$\forall x \in S \;\Rightarrow\; ax \equiv b\,(m) \;\text{ como }\; ax_0 \equiv b\,(m) \;\Rightarrow\; ax \equiv ax_0\,(m) \;\Rightarrow\; \left.\begin{array}{l} ax - ax_0 = \dot{m} \;\Rightarrow\; m / a(x - x_0) \\ \text{además m y a primos entre sí} \end{array}\right\} \Rightarrow$$

$$\Rightarrow\; m/(x - x_0) \;\Rightarrow\; \exists t \in Z\,;\, x - x_0 = mt \;\Rightarrow\; x = x_0 + mt$$

Entonces $\forall x \in S \;\Rightarrow\; x = x_0 + mt \quad \text{con } t \in Z$.

Basta operar para demostrar que $\forall x \in Z\,;\, x = x_0 + mt \;\text{ con } t \in Z \;\Rightarrow\; x \in S$

En consecuencia $\underline{\text{si a y m son primos entre sí} \Rightarrow\; S = \{x \in Z\,;\, x = x_0 + mt \quad \text{con } t \in Z\}}$

siendo x_0 una solución particular de $ax \equiv b\,(m)$

Por último analicemos que ocurre si a y m no son primos entre sí pero el M.C.D. de a y m divide a b

Si D es M.C.D. de a y m $\Rightarrow\; a = Da' \quad m = Dm' \quad$ siendo a' y m' primos entre sí.

Por otra parte como D/b $\Rightarrow\; b = Db'$

Ahora $ax \equiv b\,(m) \Leftrightarrow Da'x \equiv Db'\,(Dm') \Leftrightarrow a'x \equiv b'\,(m')$ con a' y m' primos entre sí. (Observemos que la simplificación realizada es válida; en caso de duda sugerimos revisar las propiedades de la congruencia puestas a consideración como ejercicio).

Entonces este caso lo reducimos al inmediato anterior, el cual fue resuelto completamente.

<u>Nota</u>

Si en lugar de resolver $ax \equiv b\,(m)$ en $(Z,+,\cdot)$ lo hacemos en $(Z_m,\oplus,\otimes)$ puede demostrarse que en el caso de que a y m sean primos entre sí la solución es única y si no lo son pero si D/b siendo D M.C.D. de a y m (D>0); entonces la ecuación $ax \equiv b\,(m)$ tiene exactamente D raíces en $(Z_m,\oplus,\otimes)$

<u>Ejemplo 1</u> Resolver en $(Z,+,\cdot)$ $35x \equiv 14\,(182)$

Observemos que D(35,182)=7 y 7/14 por lo tanto la ecuación tiene solución no vacía. Primero que nada comenzamos por simplificar entre 7 quedándonos $5x \equiv 2\,(26)$

Para resolver esta última ecuación podemos utilizar distintas estrategias; una de ellas consiste en reiterar en este caso particular el procedimiento realizado en general para determinar el conjunto solución. Nos referimos a escribir 1 como C.L. de 5 y 26, luego multiplicar ambos miembros por 2 y de esa forma determinar una solución

particular. Recordemos que una vez obtenida una solución particular x_0 el problema esta resuelto, ya que $S = \{ x \in Z ; x = x_0 + mt \text{ con } t \in Z \}$.

Es inmediato que
$1 = -5.(5) + 1.(26) \Rightarrow 2 = -10.(5) + 2.(26) \Rightarrow 5.(-10) \equiv 2\,(26) \Rightarrow x_0 = -10$ es una solución particular $\Rightarrow S = \{ x \in Z ; x = -10 + 26t ; t \in Z \}$

Otra posible estrategia consiste en utilizar propiedades de la congruencia con el objetivo de "despejar" x

$$\left.\begin{array}{l} 5x \equiv 2\,(26) \Rightarrow 25x \equiv 10\,(26) \\ \text{como } \ 26x \equiv 0\,(26) \end{array}\right\} \Rightarrow x \equiv -10\,(26) \Rightarrow x = -10 + 26t \Rightarrow S = \{ x \in Z ; x = -10 + 26t \quad t \in Z \}$$

Ejemplo 2 Resolver en (Z,+,·) $243x + 17 \equiv 101\,(725)$

$243x + 17 \equiv 101\,(725) \Leftrightarrow 243x \equiv 84\,(725)$ (¿Qué justifica esta "transposición" de términos?) Como 243 y725 son primos entre sí tenemos la certeza de que la ecuación a resolver tiene solución no vacía. Si queremos resolver esta última ecuación utilizando la primera de las estrategias descrita en el primer ejemplo debemos escribir 1 como C.L. de 243 y 725, lo cual no es inmediato como ocurría en el ejemplo anterior. Un procedimiento sistemático para tal fin consiste en utilizar el algoritmo de Euclides; veámoslo.

	2	1	59	1
725	243	239	4	3
239	4	3	1	

Aplicando la definición en las distintas divisiones del algoritmo tenemos:

$$\left.\begin{array}{l} 725 = 2.(243) + 239 \Rightarrow 239 = 725 - 2.(243) \\ 243 = 1.(239) + 4 \Rightarrow 4 = 243 - 239 \\ 239 = 59.(4) + 3 \Rightarrow 3 = 239 - 59.(4) \\ 4 = 1.(3) + 1 \Rightarrow 1 = 4 - 3 \end{array}\right] \Rightarrow 1 = 4 - (239 - 59.(4)) = 60.(4) - 239 \Bigg] \Rightarrow 1 = 60.(243 - 239) - 239 \Rightarrow$$

$$\left.\begin{array}{l} 1 = 60.(243) - 61.(239) \\ \text{como } \ 239 = 725 - 2.(243) \end{array}\right] \Rightarrow 1 = 60.(243) - 61.(725 - 2.(243)) = 182.(243) - 61.(725)$$

Tenemos entonces $1=182.(243) - 61.(725) \Rightarrow 84 = 243.(15288) - 725.(5124) \Rightarrow 243.(15288) \equiv 84\,(725)$
$x_0 = 15288$ es una solución particular. Si queremos una solución particular mas pequeña podemos proceder como sigue:

$$\left.\begin{array}{cc} 15288 & 725 \\ 63 & 21 \end{array}\right\} \Rightarrow 15288 \equiv 63\,(725) \Rightarrow \left.\begin{array}{l} 243.(15288) \equiv 243.(63)\,(725) \\ \text{como } \ 243.(15288) \equiv 84\,(725) \end{array}\right\} \Rightarrow$$

$243.(63) \equiv 84\,(725) \Rightarrow x_1 = 63$ también es una solución particular de la ecuación. Por lo tanto
$S = \{ x \in Z ; x = 63 + 725t \quad \text{con } t \in Z \}$

(No hicimos otra cosa que probar en particular que si x_0 es solución particular de $ax \equiv b\,(m)$ y $x_1 \equiv x_0\,(m) \Rightarrow x_1$ también es solución particular de la ecuación)

Como seguramente habrá observado la estrategia utilizada en este caso particular es larga y tediosa. Veamos si el segundo procedimiento utilizado en el ejemplo 1 nos resulta mas conveniente.

$$\left.\begin{array}{l} 243x \equiv 84\ (725) \Leftrightarrow 729x \equiv 252\ (725) \\ \text{como} \quad 725x \equiv 0\ (725) \end{array}\right\} \Rightarrow 4x \equiv 252\ (725) \Rightarrow \left.\begin{array}{l} 724x \equiv 45612\ (725) \\ \text{como} \quad 725x \equiv 45675\ (725) \end{array}\right\} \Rightarrow x \equiv 63\ (725)$$

$$\Rightarrow S = \{ x \in Z\ ;\ x = 63 + 725t \quad t \in Z \}$$

Ecuaciones diofánticas

Consideramos $a, b, c \in Z$; queremos hallar $S = \{(x, y) \in Z^2\ ;\ ax + by = c\}$ Lo que usualmente se denomina resolver en Z la ecuación ax+by=c.

Observemos que si $\exists (x_0, y_0) \in Z \times Z\ ;\ ax_0 + by_0 = c$ todo divisor común de a y b también lo es de c

Por lo tanto si D es M.C.D. de a , b y D no divide a c $\Rightarrow S = \varnothing$

Analicemos ahora que ocurre cuando D/c. Comencemos por el caso particular de que a y b sean primos entre sí.

Si 1 es M.C.D. de a y b $\Rightarrow \exists p, s \in Z\ ;\ 1 = pa + sb$ multiplicando a ambos miembros por c nos queda: $a.(pc) + b.(sc) = c \Rightarrow \exists (x_0, y_0) \in Z^2\ (x_0 = pc\ ,\ y_0 = sc)$ tal que $ax_0 + by_0 = c$
En consecuencia si a y b son primos entre sí $S \neq \varnothing$ Intentemos hallar todos los elementos de S.

$$\left.\begin{array}{l} \forall (x, y) \in S \Rightarrow ax + by = c \\ \text{como} \quad ax_0 + by_0 = c \end{array}\right\} \Rightarrow a.(x - x_0) + b.(y - y_0) = 0 \Rightarrow a.(x - x_0) = b(y_0 - y) \Rightarrow a / b(y_0 - y)$$

Al saber además que a y b son primos entre sí podemos aplicar Euclides llegando a que $a / y_0 - y \Rightarrow \Rightarrow \exists\, t \in Z\ ;\ y_0 - y = at \Rightarrow y = y_0 - at$ Sustituyendo en $a.(x - x_0) = b.(y_0 - y)$ nos queda:

$a.(x - x_0) = bat \Rightarrow x - x_0 = bt \Rightarrow x = x_0 + bt$

Probamos entonces que $\forall (x, y) \in S \Rightarrow x = x_0 + bt \wedge y = y_0 - at$ con (x_0, y_0) una solución particular de la ecuación. Si demostramos la validez de la proposición recíproca tendríamos al conjunto S

$\forall (x, y) \in Z\ ;\ x = x_0 + bt \wedge y = y_0 - at \Rightarrow ax + by = a(x_0 + bt) + b(y_0 - at) = ax_0 + abt + by_0 - abt =$
$ax_0 + by_0 = c \Rightarrow (x, y) \in S$

Por lo tanto:

Si a y b son primos entre sн $S = \{(x, y) \in Z^2\ ;\ x = x_0 + bt \wedge y = y_0 - at\}$ con (x_0, y_0)

una soluciyn particular de la ecuaciyn

En caso de que a y b no sean primos entre sí pero D/c (D es M.C.D. de a y b) basta simplificar para reducirlo al caso recién tratado. Pues si D es M.C.D. de a y b $\Rightarrow a = Da' \wedge b = Db'$ con a' y b' primos entre sí, como además $D / c \Rightarrow c = Dc'$ Entonces:

$$ax + by = c \Leftrightarrow Da'x + Db'y = Dc' \Leftrightarrow a'x + b'y = c'$$

Ejemplo 1 Consideramos: $126x + 105y = c$

i) Hallar $c \in Z\,;\, 60 < c < 70$ para que la ecuación anterior tenga solución no vacía.

ii) Para el valor de c hallado resolver la mencionada ecuación.

i) Para que la ecuación tenga solución no vacía es condición necesaria y suficiente que el M.C.D. de 126 y 105 (que es 21) debe dividir a c; como además
$60 < c < 70 \quad \Rightarrow \quad c = 63$

ii) $126x + 105y = 63 \quad \Leftrightarrow \quad 6x + 5y = 3$

Una posible estrategia para resolver esta ecuación consiste en hallar una solución particular de la mismo escribiendo 1 como C.L. de 6 y 5; luego multiplicar a ambos miembros por 3. Una vez encontrada una solución particular basta utilizar las fórmulas recién vistas.

$1 = 6 - 5 \quad \Rightarrow \quad 3 = 6.(3) + 5.(-3) \quad \Rightarrow \quad (3,-3)$ es una solución particular $\Rightarrow$

$\Rightarrow \quad S = \left\{(x, y) \in Z^2 \,;\, x = 3 + 5t \;\wedge\; y = -3 - 6t \quad \text{con } t \in Z\right\}$

Otra posibilidad es trasformar la ecuación a resolver en una ecuación en congruencias.

$6x + 5y = 3 \quad \Leftrightarrow \quad 6x - 3 = -5y \quad \Leftrightarrow \quad 6x - 3 = \dot{5} \quad \Leftrightarrow \quad 6x \equiv 3\,(5)$

$\left.\begin{array}{r} 6x \equiv 3\,(5) \\ \text{como } 5x \equiv 0\,(5) \end{array}\right\} \Rightarrow x \equiv 3\,(5) \quad \Rightarrow \quad x = 3 + 5t$ sustituyendo en la ecuación original nos queda:

$6(3 + 5t) + 5y = 3 \quad \Rightarrow \quad 18 + 30t + 5y = 3 \quad \Rightarrow \quad 5y = -15 - 30t \quad \Rightarrow \quad y = -3 - 6t$

Ejemplo 2 Resolver el siguiente sistema: $\left\{\begin{array}{l} 3x \equiv 2\ (5) \\ 2x \equiv 1\ (3) \end{array}\right.$

Debemos hallar los enteros que verifican simultáneamente ambas congruencias. Por lo visto anteriormente estamos en condiciones de hallar aquellos números que verifican cada una de las congruencias independientemente. Hagámoslo y luego veremos como determinar aquellos enteros que verifican las dos ecuaciones al mismo tiempo.

(1) $3x \equiv 2\,(5) \quad \Rightarrow \quad \left.\begin{array}{l} 6x \equiv 4\,(5) \\ 5x \equiv 0\,(5) \end{array}\right\} \quad \Rightarrow \quad x \equiv 4\,(5) \quad \Rightarrow \quad x = 4 + 5t$

(2) $\left.\begin{array}{l} 2x \equiv 1\,(3) \\ 3x \equiv 0\,(3) \end{array}\right\} \Rightarrow \quad x \equiv -1\,(3) \quad \Rightarrow \quad x = -1 + 3k$

Como buscamos los enteros "x" que cumplan ambas congruencias los valores hallados en (1) y (2) deben ser iguales.

$4 + 5t = -1 + 3k \quad \Leftrightarrow \quad 3k - 5t = 5 \quad \Leftrightarrow \quad 3k - 5 = 5t \quad \Leftrightarrow \quad 3k - 5 = \dot{5} \quad \Leftrightarrow \quad 3k \equiv 5\,(5) \quad \Leftrightarrow$

$$\Leftrightarrow \left.\begin{array}{l} 6k \equiv 10\,(5) \\ 5k \equiv 10\,(5) \end{array}\right\} \Leftrightarrow \quad k \equiv 0\,(5) \quad \Leftrightarrow \quad k = 5h \quad \text{como} \quad x = -1+3k \quad \Rightarrow \quad x = -1+15h$$

Por lo tanto la solución del sistema es: $S = \{ x \in Z ; x = -1+15h \quad \text{con} \quad h \in Z \}$

Nota

Tengamos presente cuando resolvemos una ecuación en congruencias como una ecuación diofántica así como un sistema, estamos trabajando con ecuaciones o sistemas y en consecuencia podemos verificar.

Congruencias de Fermat y de Euler

Teorema

H) $\begin{cases} a_1, a_2, ..., a_n, b, c \in Z \quad m \in Z^+ \\ a_1, a_2, ..., a_n \quad \text{incongruentes dos a dos mydulo m} \\ b \text{ y m primos entre sн} \end{cases}$

T) $ba_1 + c\,,\ ba_2 + c\,, ..., ba_n + c$ son incongruentes dos a dos módulo m

Dem.

Intentaremos hacer una demostración por absurdo.

Suponemos $\exists\, ba_i + c$ y $ba_j + c$ con $1 \le i < n \quad 1 \le j < n \quad i \ne j$ tal que $ba_i + c \equiv ba_j + c\,(m) \Rightarrow$

$$\Rightarrow \quad (ba_i + c) - (ba_j + c) = b(a_i - a_j) = \overset{\bullet}{m} \quad \Rightarrow \quad m / b(a_i - a_j) \left.\begin{array}{l} \\ \text{como b y m primos entre sн} \end{array}\right\} \Rightarrow m/(a_i - a_j) \quad \Rightarrow \quad a_i - a_j = \overset{\bullet}{m} \quad \Rightarrow$$

$\Rightarrow \quad a_i \equiv a_j\,(m)$ lo cual contradice la hipytesis

Teorema Congruencia de Fermat

H) $\begin{cases} a, p \in Z^+ \\ a \ne \overset{\bullet}{p} \\ p \text{ primo} \end{cases}$ **T)** $a^{p-1} \equiv 1\,(p)$

Dem.

Comencemos por observar que: 1, 2 ,....., p-1 son enteros incongruentes dos a dos módulo p (La diferencia entre dos cualesquiera de ellos es distinto de cero y en valor absoluto menor que p; por lo tanto dicha diferencia no es múltiplo de p)

De la hipótesis se desprende que a y p son primos entre sí; estamos pues en condiciones de aplicar el teorema inmediato anterior llegando a que: $a\,, 2a\,, ..., (p-1)a$ son incongruentes dos a dos módulo p

Al haber solamente hay p clases de equivalencia en Z_p tanto en $\{1, 2, ..., p-1\}$ como en $\{a, 2a, ..., (p-1)a\}$ hay un representante de cada clase de Z_p excepto de $[0]$. (En el caso del segundo conjunto como p es primo y a no es múltiplo de p ninguno de los elementos de $\{a, 2a, ..., (p-1)a\}$ es congruente con 0 módulo m).

Por lo dicho cada elemento de $\{1, 2, ..., p-1\}$ es congruente módulo p a uno de $\{a, 2a, ..., (p-1)a\}$

Entonces:

$1.2.....(p-1) \equiv a.2a.....(p-1)a \ (p)$ como p es primo podemos simplificar quedándonos:

$$1 \equiv \underbrace{a.a.....a}_{p-1 \text{ factores}} \ (p) \quad \Rightarrow \quad a^{p-1} \equiv 1 \ (p)$$

Definición

Llamamos **indicador de a** $(a \in N)$ al cardinal del conjunto $\{n \in N \ ; \ n \le a \wedge D(n, a) = 1\}$

Al indicador de a lo anotamos $\varphi(a)$.

Ej. $\varphi(6) = 2$ pues de los naturales menores o iguales que 6 (1,2,3,4,5 y 6) solo 1 y 5 son primos con 6

Nota

Si p $(p \in N)$ es primo $\varphi(p) = p - 1$ ya que todos los naturales menores que p a excepción de 0 son primos con él. Calculemos ahora $\varphi(p^\alpha)$; para ello debemos saber cuántos naturales menores que p^α son primos con él. Al ser p un número primo los únicos naturales que no son primos con p^α son los múltiplos de p menores que dicho número. A saber: $p, 2p, 3p, ..., (p^{\alpha-1} - 1).p \ , \underbrace{p^{\alpha-1}.p}_{p^\alpha}$

Por lo tanto tenemos $p^{\alpha-1}$ números naturales menores o iguales que p^α no primos con él.

Entonces $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^{\alpha-1}(p-1)$

Al disponer de esta última fórmula podríamos hallar el indicador de un número compuesto recurriendo a su descomposición factorial.

Demostrando previamente que si m y n son naturales primos entre sí entonces $\varphi(m.n) = \varphi(m).\varphi(n)$ tenemos que: Si $n \in N$ y $p_1^\alpha.p_2^\beta.....p_h^\lambda$ su D.P.F.P. entonces $\varphi(n) = \varphi(p_1^\alpha.p_2^\beta.....p_h^\lambda) =$

$$= \varphi(p_1^\alpha).\varphi(p_2^\beta).....\varphi(p_h^\lambda) = p_1^{\alpha-1}(p_1 - 1).p_2^{\beta-1}(p_2 - 1).....p_h^{\lambda-1}(p_h - 1)$$

En resumen: $\varphi(n) = p_1^{\alpha-1}.p_2^{\beta-1}.....p_h^{\lambda-1}.(p_1 - 1).(p_2 - 1).....(p_h - 1)$

Así como $60 = 2^2.3.5 \quad \Rightarrow \quad \varphi(60) = 2^1.3^0.5^0.(2-1).(3-1).(5-1) = 16$

Teorema Congruencia de Euler

$$\textbf{H)} \begin{cases} b, m \in N \\ D(b,m)=1 \end{cases} \qquad \textbf{T)} \quad b^{\varphi(m)} \equiv 1\,(m)$$

Dem

Consideremos $a_1, a_2, ..., a_{\varphi(m)}$ naturales menores o iguales que m primos con él. Observemos que además son incongruentes dos a dos módulo m.

Al ser b y m primos entre sí podemos aplicar el teorema anterior a la congruencia de Fermat llegando a que $ba_1, ba_2, ..., ba_{\varphi(m)}$ son incongruentes dos a dos módulo m y además primos con él.

Probemos que cada elemento de $\{ba_1, ba_2, ..., ba_{\varphi(m)}\}$ es congruente con uno de $\{a_1, a_2, ..., a_{\varphi(m)}\}$

Realicemos la siguiente división $\begin{matrix} ba_i & m \\ r_i & q \end{matrix} \Rightarrow \begin{cases} ba_i \equiv r_i\ (m) \\ 0 \le r_i < m \end{cases}$ Si logramos demostrar que

$D(r_i, m) = d \Rightarrow r_i \in \{a_1, a_2, ..., a_{\varphi(m)}\}$

$D(r_i, m) = d \Rightarrow \begin{cases} d/m \\ d/r_i \end{cases} \Rightarrow d/mq + r_i \Rightarrow d/ba_i$ como D(d,b)=1 (*) $\Rightarrow \left.\begin{matrix} d/a_i \\ \text{como además } d/m \end{matrix}\right\} \Rightarrow$

$\Rightarrow d/D(a_i, m) = 1 \Rightarrow d = \pm 1$

(*) D(d,b)=h $\Rightarrow \left[\begin{cases} h/d \text{ como } d/m \Rightarrow h/m \\ h/b \end{cases}\right] \Rightarrow h/D(b,m) = 1 \Rightarrow h = 1$

Tenemos entonces que cada elemento de $\{ba_1, ba_2, ..., ba_{\varphi(m)}\}$ es congruente módulo m a uno del conjunto $\{a_1, a_2, ..., a_{\varphi(m)}\}$. Además como los elementos de ambos conjuntos son incongruentes dos a dos y hay la misma cantidad de elementos; cada elemento del primer conjunto es congruente con uno y solo uno del segundo y recíprocamente. Multiplicando miembro a miembro las mencionadas congruencias nos queda:

$$a_1.a_2.....a_{\varphi(m)} \equiv ba_1.ba_2.....ba_{\varphi(m)}\ (m)$$

Al ser $a_1, a_2, ..., a_{\varphi(m)}$ primos con m podemos simplificar quedándonos:

$$1 \equiv \underbrace{b.b.....b}_{\varphi(m) \text{ factores}}\ (m) \Rightarrow b^{\varphi(m)} \equiv 1\,(m)$$

Veamos ahora algunos ejemplos de aplicación tanto de la congruencia de Fermat como la de Euler.

Ejemplo 1

Hallar el resto de dividir 3^{85} entre 7

Observemos que si $\begin{matrix} 3^{85} & 7 \\ r & q \end{matrix} \Leftrightarrow 3^{85} \equiv r\ (7)$ Por lo tanto debemos hallar a quien es congruente 3^{85} módulo 7.

Como 7 es primo podemos aplicar Fermat $\Rightarrow 3^6 \equiv 1\,(7)$ Por otra parte $\begin{matrix} 85 & 6 \\ 1 & 14 \end{matrix}$

$3^6 \equiv 1\,(7) \Rightarrow \left(3^6\right)^{14} \equiv 1^{14}\,(7) \Rightarrow 3^{6.14} \equiv 1\,(7) \Rightarrow 3^{6.14}.3 \equiv 1.3\,(7) \Rightarrow 3^{85} \equiv 3\,(7)$

En consecuencia el resto de dividir 3^{85} entre 7 es 3.

Ejemplo 2

Determinar las últimas dos cifras de 3^{85}.

Observemos las últimas dos cifras de 3^{85} coinciden con el resto de dividir dicho número entre 100

$$\begin{matrix} 3^{85} & 100 \\ r & q \end{matrix} \Leftrightarrow 3^{85} \equiv r\,(100)$$

Si intentamos proceder como en el primer ejemplo deberíamos encontrar una potencia de 3 de exponente próximo a 85 congruente con 1 módulo 100. Para ello en esta caso nos es imposible utilizar Fermat ya que 100 no es primo. Veamos si podemos utilizar la congruencia de Euler.

$$\left.\begin{array}{l} 3 \text{ es primo con } 100 \\ 100 = 2^2.5^2 \Rightarrow \varphi(100) = 2^1.5^1.(2-1).(5-1) = 40 \end{array}\right\} \Rightarrow 3^{40} \equiv 1\,(100)$$

Por otra parte $\begin{matrix} 85 & 40 \\ 5 & 2 \end{matrix} \Rightarrow 85 = 40.2 + 5$

$3^{40} \equiv 1\,(100) \Rightarrow \left(3^{40}\right)^2 \equiv 1^2\,(100) \Rightarrow 3^{40.2} \equiv 1\,(100) \Rightarrow 3^{40.2}.3^5 \equiv 1.3^5\,(100) \Rightarrow$

$$\left.\begin{array}{l} \Rightarrow 3^{85} \equiv 3^5\,(100) \Rightarrow 3^{85} \equiv 243\,(100) \\ \text{como } 243 \equiv 43(100) \end{array}\right\} \Rightarrow 3^{85} \equiv 43\,(100)$$

Por lo tanto las últimas dos cifras de 3^{85} son 43.

▲ Inicio

FUNCIONES POLINÓMICAS

Recordemos:

1) Sean A y B dos conjuntos. Llamamos **relación** de A en B (anotamos $R : A \to B$) a un conjunto de pares ordenados de primera componente en A y segunda componente en B.

Mas sintéticamente:

$$R \text{ es una relación de A en B} \iff R \subseteq A \times B$$

2) Consideramos $R : A \to B$ si $(x,y) \in R$ decimos que **y** es **imagen** de **x**, y que **x** es **preimagen** de **y.**

3) Sea $R : A \to B$. Llamamos **dominio** de R (anot. D_R) al conjunto de los elementos de A que tienen al menos una imagen en B.

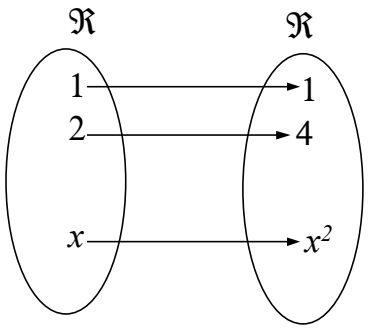
Llamamos **recorrido** de R (anot.R_R) al conjunto de los elementos de B que tienen al menos una preimagen en A.

Mas sintéticamente:

$$D_R = \{ x \in A / \exists y \in B ; (x, y) \in R \} \qquad R_R = \{ y \in B / \exists x \in A ; (x.y) \in R \}$$

4) Sea $F : A \to B$. Decimos que F es una **función** si y solo si todo elemento de A tiene una y solo una imagen en B.

Nota: Consideramos ahora $F = \{ (x, y) \in \Re \times \Re / y = x^2 \}$ Observemos que F es una función de $\Re \to \Re$; en donde abusando de la notación tenemos:



A F la anotaremos mas brevemente $F : \Re \to \Re \; ; \; F(x) = x^2$ Así con esta notación indicamos que la imagen de un *x* real cualquiera es x^2 .

Por ejemplo si anotamos F(2) hacemos referencia a la imagen de 2 según F y la calculamos $F(2) = 2^2 = 4$ simplemente sustituyendo *x* por 2 en $F(x) = x^2$.

Definición

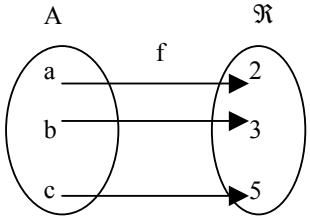
Consideramos: $f : A \to \Re$ y $g : B \to \Re$ siendo A y B dos conjuntos cualesquiera. Si $C = A \cap B \neq \varnothing$ definimos:

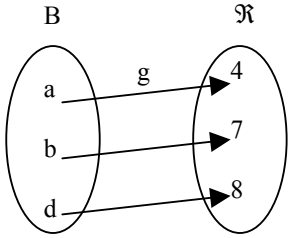
$$f + g : C \to \Re \; ; \; (f + g)(x) = f(x) + g(x)$$

$$f.g : C \to \Re \; ; \; (f.g)(x) = f(x).g(x)$$

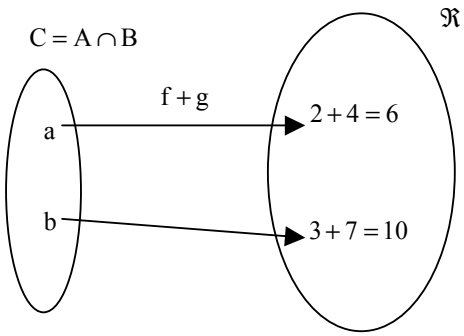
$$\frac{f}{g} : C' \to \Re \; ; \left(\frac{f}{g}\right)(x) = \frac{f(x)}{g(x)} \qquad \text{con } C' = \{ x \in C \,/\, g(x) \neq 0 \}$$

Así por ejemplo





Entonces



Ejercicios: 1) Hallar en este caso particular: $f.g$ y $\frac{f}{g}$

2) Si $h : \Re \to \Re \; ; \; h(x) = x^2$ y $t : \Re \to \Re \; ; \; t(x) = 2^x$ Determinar: $f + g$, $f.g$ y $\frac{f}{g}$

Nota: Si A es un conjunto no vacío anotaremos F_A al conjunto de todas las funciones de $A \to \Re$

Observaciones: Consideramos $f, g \in F_A$

1) $f = g \iff f(x) = g(x) \quad \forall x \in A$
2) La suma y el producto de funciones son operaciones en F_A

Teorema

$(F_A,+,\cdot)$ es un anillo conmutativo y con unidad.

Dem. $(F_A,+)$ grupo conmutativo

Asociativa $(f+g)+h=f+(g+h) \quad \forall f,g,h\in F_A$

$(f+g)+h=f+(g+h) \iff [(f+g)+h](x)=[f+(g+h)](x) \quad \forall x\in A$

$[(f+g)+h](x) = (f+g)(x)+h(x) = [f(x)+g(x)]+h(x) =_{(*)} f(x)+[g(x)+h(x)] = f(x)+(g+h)(x) =$

$= [f+(g+h)](x) \qquad \forall x\in A$

(*) Asociativa de la suma de reales.

Conmutativa $f+g=g+f \quad \forall f,g\in F_A$

$f+g=g+f \iff (f+g)(x)=(g+f)(x) \quad \forall x\in A$

$(f+g)(x) = f(x)+g(x) =_{(*)} g(x)+f(x) = (g+f)(x) \qquad \forall x\in A$ (*) Conmutativa de la suma de reales.

Neutro $\exists \theta\in F_A \ / \ f+\theta=f \quad \forall f\in F_A$

Definimos $\theta: A\to\Re \ ; \ \theta(x)=0 \quad \forall x\in A$ A la cual denominaremos **función nula**.

$(f+\theta)(x) = f(x)+\theta(x) = f(x)+0 = f(x) \quad \forall x\in A \Rightarrow f+\theta=f$ razonamiento válido $\forall f\in F_A$

Opuesto $\forall f\in F_A \ \exists -f\in F_A \ / \ f+(-f)=\theta$

Definimos $-f: A\to\Re \ ; \ (-f)(x)=-f(x) \quad \forall x\in A$

$(f+-(f))(x) = f(x)+(-f)(x) = f(x)-f(x) = 0 = \theta(x) \quad \forall x\in A \Rightarrow f+(-f)=\theta$

Asociativa de $(F_A,\cdot)$ $f.(g.h)=(f.g).h \quad \forall f.g,h\in F_A$ Demostración a cargo del lector.

Conmutativa de $(F_A,\cdot)$ $f.g=g.f \quad \forall f,g\in F_A$ " " " " "

Neutro de $(F_A,\cdot)$ $\exists \Gamma\in F_A \ / \ f.\Gamma=f \quad \forall f\in F_A$

Definimos $\Gamma: A\to\Re \ ; \ \Gamma(x)=1 \quad \forall x\in A$

$(f.\Gamma)(x)=f(x).\Gamma(x)=f(x).1=f(x) \quad \forall x\in A \Rightarrow f.\Gamma=f$ razonamiento válido $\forall f\in F_A$

Ejercicio: 1) ¿Es necesariamente cierto que si $f.g=\theta \Rightarrow f=\theta$ y / ó $g=\theta$?

2) ¿ $(F_A,+,\cdot)$ es un cuerpo?

3) ¿A que llamaría función polinómica? ¿Y grado de una función polinómica?

Definición

A las funciones de $\Re\to\Re$ cuya fórmula es $f: f(x)=k$ $(k\in\Re$ cte.) (Funciones constantes) o $f: f(x)=a_n x^n+a_{n-1}x^{n-1}+.....+a_1x+a_0$ con $n\in N^*$ y $a_n,a_{n-1},.....,a_1.a_0\in\Re$ las denominaremos **funciones polinómicas reales**.

Si $f: f(x)=a_n x^n+a_{n-1}x^{n-1}+.....+a_1x+a_0$ con $n\in N^*$ y $a_n\neq 0$ decimos que f tiene **grado n**. En caso que $f: f(x)=k$ $(k\in\Re \ ; \ k\neq 0)$ diremos que f tiene **grado 0**.

Con respecto a la función nula (que es una función polinómica) asumiremos que no tiene grado.

Nota: Al conjunto de todos las funciones polinómicas reales lo anotaremos $P_\Re$

Observaciones:

1) $P_{\Re} \subseteq F_{\Re}$

2) Consideramos: $f \in P_{\Re}\ f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots\ldots\ldots + a_1 x + a_0$ y $g \in P_{\Re}$ tal que $g(x) = b_n x^n + b_{n-1} x^{n-1} + \ldots\ldots\ldots + b_1 x + b_0$

$$\text{Si} \left\{ \begin{array}{l} a_n = b_n \\ a_{n-1} = b_{n-1} \\ \ldots\ldots\ldots\ldots\ldots \\ \ldots\ldots\ldots\ldots\ldots \\ a_1 = b_1 \\ a_0 = b_0 \end{array} \right\} \Rightarrow \quad f(x) = g(x) \quad \forall x \in \Re \quad \Rightarrow \quad f = g$$

3) La suma y el producto de funciones polinómicas es una función polinómica.

Si $f, g \in P_{\Re} \Rightarrow f + g \in P_{\Re}$ y además $gr(f+g) \leq \text{máx}\{gr(f), gr(g)\}$ ó $f + g = \theta$

Si $f, g \in P_{\Re} \Rightarrow f.g \in P_{\Re}$ y además $gr(f.g) = gr(f) + gr(g)$ ó $f.g = \theta$

4) $(P_{\Re}, +, \cdot)$ es un **anillo conmutativo y con unidad** (Le solicitamos al lector que fundamente tal afirmación).

DIVISIÓN ENTERA

Así como se define la división entera entre números naturales

$$\begin{array}{c|c} a & b \\ \hline r & q \end{array} \quad \Leftrightarrow \quad \left\{ \begin{array}{l} a = bq + r \\ r < b \end{array} \right.$$

intentaremos definir una división entera entre funciones polinómicas reales. Un proyecto "razonable" podría ser:

$$\begin{array}{c|c} f & g \\ \hline r & q \end{array} \quad \Leftrightarrow \quad \left\{ \begin{array}{l} f = g.q + r \\ gr(r) < gr(g) \ \text{ó} \ r = \theta \end{array} \right.$$

Antes de adoptarla como definición demostremos el siguiente:

Teorema

$$H) \left\{ \begin{array}{l} f, g \in P_{\Re} \\ g \neq \theta \end{array} \right. \qquad T) \quad \exists q, r \in P_{\Re} \text{ tal que}: \left\{ \begin{array}{l} i)\ f = gq + r \\ ii)\ gr(r) < gr(g) \quad \text{ó} \quad r = \theta \end{array} \right.$$

Dem.:

Consideramos $H = \{ f - gt \,;\, t \in P_{\Re} \}$ Analicemos dos casos:

Si $\theta \in H \Rightarrow \exists t_0 \in P_{\Re}\ ; f - g.t_0 = \theta \Rightarrow f = f.t_0 + \theta$

Por lo tanto en este caso $\exists q = t_0$ y $r = \theta$ que verifican la tesis.

Si $\theta \notin H \Rightarrow$ todos las funciones polinómicas de H tienen grado. Denominemos J al conjunto de los grados de los elementos de H.

$$\left. \begin{array}{l} J \subseteq N \\ J \neq \varnothing \ \text{(Basta tomar } t = \theta \Rightarrow f - g.\theta = f \in H \Rightarrow gr(f) \in J) \end{array} \right\} \Rightarrow_{\text{P.B.O}} \quad \exists j = \text{mín } J$$

Si $j = \text{mín } J \Rightarrow j \in J \Rightarrow \exists r \in H\ ; gr(r) = j \Rightarrow \exists q \in P_{\Re} / r = f - g.q \Rightarrow$

$\Rightarrow \quad f = g.q + r$ Faltaría demostrar que $gr(r) < gr(g)$

Llamamos n al grado de g. Probemos que $j < n$ por absurdo.
Suponemos entonces que $j \geq n$

Consideramos ahora $r_1 : r_1(x) = r(x) - \frac{c_j}{b_n} x^{j-n}.g(x)$ siendo c_j el coeficiente principal de r y b_n el de g. (termino que surge de proseguir el algoritmo de la división entera que conocemos)

Como $r = f - gq \quad \Rightarrow \quad r(x) = f(x) - g(x).q(x) \quad \forall x \in \Re$ sustituyendo en la definición de r_1 tenemos:

$$r_1(x) = f(x) - g(x).q(x) - \frac{c_j}{b_n} x^{j-n} g(x) = f(x) - g(x)\left[q(x) - \frac{c_j}{b_n} x^{j-n} \right] \quad \forall x \in \Re$$

$\Rightarrow \quad r_1 \in H \quad \Rightarrow \quad gr(r_1) \in J$

Pero por definición de $r_1 \quad gr(r_1) < j = \text{mín } J$ Lo cual es contradictorio.

Definición

Consideramos $f, g \in P_{\Re}$; $g \neq \theta$ Entendemos por realizar la **división entera** de f entre g a encontrar $q, r \in P_{\Re}$ tal que: i) $f = g.q + r$

ii) $gr(r) < gr(g) \quad$ ó $\quad r = \theta$

Como sabemos q recibe el nombre de **cociente** y r el de **resto**. El teorema inmediato anterior nos asegura que dados dos funciones polinómicas cualesquiera f y g con $g \neq \theta$ existen el cociente y el resto de la división entera de f entre g . Posteriormente demostraremos que dicho cociente y resto son únicos. No lo hacemos en este momento por carecer aún de los elementos necesarios para realizarlo.

Si f dividido g da cociente q y resto r lo esquematizamos

f	g
r	q

Ejercicio: Realizar las siguientes divisiones:

1) $6x^4 + 13x^3 - 18x^2 - 17x + 20$ entre $3x^2 + 5x - 7$
2) $10x^3 + 21x^2 + 4x + 2$ entre $2x + 1$
3) $x^4 + 3x^3 + 2x^2 + 3x + 6$ entre $x^3 + 2x^2 - x + 5$

Definición

Consideramos: $f \in P_{\Re}$ y $\alpha \in \Re$ Decimos que α es **raíz** de f $\Leftrightarrow \quad f(\alpha) = 0$

Ejercicio:

1) Probar que 2 es raíz de $f : f(x) = x^3 - 5x^2 + 7x - 2$
2) Demostrar que todos los reales son raíces de la función nula (θ)
3) Probar:

f	g
r	q

α raíz de g $\quad \Rightarrow \quad f(\alpha) = r(\alpha)$

Observación: Hallar todas las raíces de una función polinómica f es resolver en $(\Re, +, \cdot, \leq)$ la ecuación f(x)=0

Ejercicio: Consideramos $f : f(x) = 2x^3 + 6x^2 - 5x + 3$ 1) Dividir f entre $g : g(x) = x - 2$ y entre $h : h(x) = x - 1$
2) ¿ Que particularidades observa sobre el cociente y el resto? 3) Calcular f(2) y f(1)
¿Qué observa?. 4) Elija otro polinomio f cualquiera y reitere las partes anteriores. ¿Las observaciones realizados serán una casualidad para estos casos particulares.?

División entre x-α

Un caso que nos interesa particularmente es la división entre una función polínomica del tipo $g : g(x) = x - \alpha$ ya que presenta características y aplicaciones singulares.

$$\begin{array}{c|c} f & g \\ \hline r & q \end{array} \quad \Rightarrow \quad \begin{cases} f = gq + r \\ gr(r) < gr(g) \quad \text{ó} \quad r = \theta \end{cases}$$

Si $g : g(x) = x - \alpha \quad \Rightarrow \quad gr(r) = 1 \quad \Rightarrow \quad gr(r) = 0$ ó $r = \theta \quad \Rightarrow$ r es una función constante, en otras palabras $r(x) = k \quad \forall x \in \Re \quad (k \in \Re \text{ fijo}) \qquad$ Además si $gr(f) = n \quad \Rightarrow \quad gr(q) = n - 1$

Por otra parte si $f = g.q + r \quad \Rightarrow \quad f(x) = g(x).q(x) + r(x) \quad \forall x \in \Re \quad \Rightarrow \quad f(x) = (x - \alpha).q(x) + k \quad \forall x \in \Re$

$\Rightarrow \quad f(\alpha) = \underbrace{(\alpha - \alpha)}_{0}.q(\alpha) + k \quad \Rightarrow \quad f(\alpha) = k$

Proposición que podemos enunciar: " el resto de dividir f entre $x - \alpha$ es $f(\alpha)$" conocida como **ley del resto**.

Ejercicio: Demostrar: α es raíz de f $\Leftrightarrow$ f es divisible entre $g : g(x) = x - \alpha$ (Teorema de **Descartes**)

Esquema de Ruffini

Por todo lo dicho sería conveniente disponer de un procedimiento más eficiente para realizar la división entre $x - \alpha$ que el algoritmo de la división utilizado en ejercicios anteriores

Realizar la división entera de $f : f(x) = a_n x^n + a_{n-1} x^{n-1} + ... + a_1 x + a_0$ entre g:g(x)= $x - \alpha$ es determinar el cociente q y el resto r que cumplan con la definición.

Por lo dicho anteriormente; si gr(f) = n

$\Rightarrow \quad gr(q) = n - 1 \quad \Rightarrow \quad q(x) = b_n x^{n-1} + b_{n-2} x^{n-2} + ... + b_1 x + b_0 \quad \forall x \in \Re$ y además

$r = \theta$ ó $gr(r) = 0 \quad \Rightarrow \quad r(x) = k \quad (k \in K) \quad \forall x \in \Re$

$$\begin{array}{c|c} f & g \\ \hline r & q \end{array} \quad \Leftrightarrow \quad f = g.q + r \quad \Leftrightarrow \quad f(x) = g(x).q(x) + r(x) \quad \forall x \in \Re \quad \Leftrightarrow$$

$$\Leftrightarrow \quad a_n x^n + a_{n-1} x^{n-1} + ... + a_1 x + a_0 = (x - \alpha).(b_{n-1} x^{n-1} + b_{n-2} x^{n-2} + ... + b_1 x + b_0) + k \quad \forall x \in \Re \quad \Leftrightarrow$$

$$\Leftrightarrow a_n x^n + a_{n-1} x^{n-1} + ... + a_1 x + a_0 = b_{n-1} x^n + b_{n-2} x^{n-1} + ... + b_1 x^2 + b_0 x - \alpha.b_{n-1} x^{n-1} - \alpha.b_{n-2} x^{n-2} .... - \alpha.b_1 x - \alpha.b_0 + k$$

$$\Leftrightarrow \quad a_n x^n + a_{n-1} x^{n-1} + ... + a_1 x + a_0 = b_{n-1} x^{n-1} + (b_{n-2} - \alpha.b_{n-1}).x + ... + (b_0 - \alpha.b_1). + k - \alpha.b_0 \quad \forall x \in \Re$$

Es inmediato que si se cumple: $\begin{cases} b_{n-1} = a_n \\ b_{n-2} - \alpha.b_{n-1} = a_{n-1} \quad \Rightarrow \quad b_{n-2} = a_{n-1} + \alpha.b_{n-1} \\ ..... \\ b_0 - \alpha.b_1 = a_1 \quad \Rightarrow \quad b_0 = a_1 + \alpha.b_1 \\ k - \alpha.b_0 = a_0 \quad \Rightarrow \quad k = a_0 + \alpha.b_0 \end{cases}$ se verifica la igualdad anterior para cualquier real

Resultados que suelen presentarse mediante el siguiente diagrama:

	a_n	a_{n-1}	.....	a_1	a_0
α		$\alpha.b_{n-1}$	.....	$\alpha.b_1$	$\alpha.b_0$
	$\underbrace{a_n}_{b_{n-1}}$	$\underbrace{a_{n-1} + \alpha.b_{n-1}}_{b_{n-2}}$	.....	$\underbrace{a_1 + \alpha.b_1}_{b_0}$	$\underbrace{a_0 + \alpha.b_0}_{k}$

Ejercicio Utilizando el esquema de Ruffini realizar las siguientes divisiones:

1) $f : f(x) = 2x^4 + x^2 - 5x + 3$ entre $g : g(x) = x - 2$

2) f entre $g : g(x) = x + 1$

3) $h : h(x) = x^3 + x + 2$ entre $g : g(x) = x - 1$ y entre $t : t(x) = x + 2$

3) f entre $g : g(x) = 2x - 1$

4) Deducir un procedimiento que nos permita utilizando el diagrama de Ruffini realizar la división de un polinomio P entre $g : g(x) = a\,x + b$ Utilizando sus deducciones realizar las siguientes divisiones.

i) $f : f(x) = 4x^3 + 6x^2 + 10$ entre $g : g(x) = 2x - 1$

ii) $f : f(x) = 9x^3 - x + 4$ entre $g : g(x) = 3x - 2$

Ejercicio: 1) Hallar todas las raíces reales de $f : f(x) = x^3 + 3x^2 - 4x - 12$ sabiendo que admite raíz 2

2) " " " " " " $f : f(x) = x^3 + 2x^2 - x - 2$ " " " " -1

3) " " " " " " $f : f(x) = 4x^4 + 4x^3 - 25x^2 - x + 6$ sabiendo que tiene raíces 2 y –3

4) " " " " " " $F : f(x) = x^4 - x^3 + 11x^2 + 9x + 18$ " " " " 3 y –3

EJERCICIOS **REPARTIDO Nº 12**

I) Sea $P : P(x) = x^3 + 3x^2 + ax - 3$. Hallar $a \in \Re$ para que P dividido entre x-1 da resto 3

II) Consideramos $P : P(x) = 2x^3 + ax - 7$ Determinar $a \in \Re$ sabiendo que $P(2) = 17$

III) Siendo $: P(x) = 2x^3 + ax^2 + bx - 6$. Hallar a y b reales sabiendo que P admite raíz –2 y $P(-1) = 4$

IV) Sea $P : P(x) = 3x^3 - 2x^2 - 37x - 12$. Calcular todas las raíces de P sabiendo que una de ellas es –3

V) Dado $P : P(x) = 4x^4 + 5x^3 - 15x^2 - 20x - 4$ Hallar todas sus raíces sabiendo que dos de ellas son 2 y $-\frac{1}{4}$.

VI) Un polinomio dividido entre x-1 y x-2 da resto 6 y 18 respectivamente. Hallar el resto de dividir dicho polinomio entre $(x-1)(x-2)$.

VII) Sea $P : P(x) = 2x^4 + ax^3 - 4x^2 - 1$. Determinar $a \in \Re$ para que $P(-3) = 44$

VIII) Consideramos $P : P(x) = x^3 - 2x^2 + ax - 18$. Hallar $a \in \Re$ y las raíces de P sabiendo que una de ellas es 2.

IX) Dado $P : P(x) = x^4 + x^3 - 15x^2 + ax + b$. Determinar a ,b reales y las raíces de P sabiendo que dos de ellas son 2 y -3.

X) Un polinomio P dividido entre x-2 da resto 5, dividido entre x-4 da resto 7, y dividido entre x-5 da resto 8. Hallar el resto de dividir P entre $(x-2)(x-4)(x-5)$.
Si además se sabe que P es de tercer grado y que $P(0) = -77$; hallar P.

Nota: Consideramos $f \in P_{\Re}; f(x) = a_n x^n + a_{n-1} x^{n-1} + ...+ a_1 x + a_0$ una función polinómica de grado n.

1) Si α $(\alpha \in \Re)$ es raíz de f $\Rightarrow_{\text{T de Descartes}}$ f es divisible entre $g: g(x) = x - \alpha \Rightarrow \exists q \in P_{\Re} / f = g.q$
$\Rightarrow f(x) = g(x).q(x) = (x-\alpha)q(x) \quad \forall x \in \Re$
Además sabemos que $gr(q) = n-1$ y $q(x) = a_n x^{n-1} + ...$

En resumen:

$f \in P_{\Re}; f(x) = a_n x^n + a_{n-1} x^{n-1} + ...+ a_1 x + a_0$ una función polinómica de grado n
Si α $(\alpha \in \Re)$ es raíz de f $\Rightarrow \exists q \in P_{\Re}; gr(q) = n-1$ y $q(x) = a_n x^{n-1} + ...$ tal que $f(x) = (x-\alpha)q(x) \quad \forall x \in \Re$

2) Consideramos ahora dos raíces distintas de f $\alpha, \beta \in \Re \quad \alpha \neq \beta$

Si α $(\alpha \in \Re)$ es raíz de f $\Rightarrow \exists q \in P_{\Re}; gr(q) = n-1$ y $q(x) = a_n x^{n-1} + ...$ tal que
$f(x) = (x-\alpha)q(x) \quad \forall x \in \Re \Rightarrow f(\beta) = (\beta-\alpha)q(\beta)$ Como β es raíz de f $\Rightarrow f(\beta) = 0 \Rightarrow$
$\Rightarrow \underbrace{(\beta-\alpha)}_{\neq 0} q\beta) = 0 \Rightarrow q(\beta) = 0 \Rightarrow \beta$ es raíz de q $\Rightarrow$
$\Rightarrow \exists q' \in P_{\Re}; gr(q') = n-2$ y $q'(x) = a_n x^{n-2} + ...$ tal que $q(x) = (x-\beta).q'(x) \quad \forall x \in \Re$
Como $f(x) = (x-\alpha).q(x) \quad \forall x \in \Re$ sustituyendo nos queda $f(x) = (x-\alpha).(x-\beta).q'(x) \quad \forall x \in \Re$

En resumen:

$f \in P_{\Re}; f(x) = a_n x^n + a_{n-1} x^{n-1} + ...+ a_1 x + a_0$ una función polinómica de grado n
Si α y β $(\alpha \neq \beta)$ son raíces de f $\Rightarrow \exists q' \in P_{\Re}; gr(q') = n-2$ y $q'(x) = a_n x^{n-2} + ...$ tal que
$f(x) = (x-\alpha).(x-\beta).q'(x) \quad \forall x \in \Re$

Probar que:

$f \in P_{\Re}; f(x) = a_n x^n + a_{n-1} x^{n-1} + ...+ a_1 x + a_0$ una función polinómica de grado n
Si α, β, γ son raíces de f distintas dos a dos $\Rightarrow \exists q \in P_{\Re}; gr(q) = n-3$ y $q(x) = a_n x^{n-3} + ...$
tal que $f(x) = (x-\alpha).(x-\beta).(x-\gamma).q(x) \quad \forall x \in \Re$

Parece entonces razonable enunciar el siguiente teorema:

Teotema 1 de descomposición factorial

H) $\begin{cases} f \in P_{\Re} \; ; f(x) = a_n x^n + a_{n-1} x^{n-1} + ... + a_1 x + a_0 \quad gr(f) = n \\ \alpha_1, \alpha_2, ..., \alpha_p \quad p \text{ raíces diferentes dos a dos de } f \quad p \le n \end{cases}$

T) $\begin{cases} \exists q \in P_{\Re} \; ; f(x) = (x-\alpha_1).(x-\alpha_2).....(x-\alpha_p).q(x) \quad \forall x \in \Re \\ \text{con } gr(q) = n-p \quad \text{y coeficiente principar } a_n \end{cases}$

Dem:

Intentaremos una demostración por inducción completa sobre p. (la cantidad de raíces).

1º paso p=1 Proposición demostrada en la nota inmediata anterior

2º paso H) La proposición se verifica para p=h

T) La proposición se cumple para p=h+1

En otras palabras suponiendo que el teorema es cierto para h raíces debemos demostrar que lo es para h+1 raíces Debemos probar entonces:

$\begin{cases} f \in P_{\Re} \; ; f(x) = a_n x^n + a_{n-1} x^{n-1} + ... + a_1 x + a_0 \quad gr(f) = n \\ \alpha_1, \alpha_2, ..., \alpha_h, \alpha_{h+1} \quad h+1 \text{ raíces diferentes dos a dos de } f \quad h+1 \le n \end{cases} \Rightarrow$

$\Rightarrow \begin{cases} \exists q \in P_{\Re} \; ; f(x) = (x-\alpha_1).(x-\alpha_2).....(x-\alpha_h)(x-\alpha_{h+1}).q(x) \quad \forall x \in \Re \\ \text{con } gr(q) = n-(h+1) \quad \text{y coeficiente principar } a_n \end{cases}$

Como $\alpha_1, \alpha_2, ..., \alpha_h, \alpha_{h+1}$ son raíces distintas dos a dos de f $\Rightarrow$ $\alpha_1, \alpha_2, ..., \alpha_h$ son raíces distintas dos a dos de f. Además si $h+1 \le n \Rightarrow h \le n$ Estamos pues en condiciones de aplicar la hipótesis inductiva.

$\Rightarrow \exists q' \in P_{\Re} \; / \; f(x) = (x-\alpha_1).(x-\alpha_2).....(x-\alpha_h).q'(x)$ (*) $\forall x \in \Re$ con $gr(q') = n-h$ y coeficiente principal a_n.

Teniendo en cuenta que α_{h+1} es raíz de f $\Rightarrow$ $f(\alpha_{h+1}) = 0 \Rightarrow$

$\Rightarrow f(\alpha_{h+1}) = \underbrace{(\alpha_{h+1} - \alpha_1)}_{\neq 0}.\underbrace{(\alpha_{h+1} - \alpha_2)}_{\neq 0}.....\underbrace{(\alpha_{h+1} - \alpha_h)}_{0}.q'(\alpha_{h+1}) = 0 \Rightarrow q'(\alpha_{h+1}) = 0 \Rightarrow$

$\Rightarrow \alpha_{h+1}$ es raíz de q' Aplicando ahora el teorema para p=1 sobre q' tenemos que:

$\exists q \in P_{\Re} \; ; q'(x) = (x-\alpha_{h+1}).q(x) \quad \forall x \in \Re$ con $gr(q) = (n-h)-1 = n-(h+1)$ y coeficiente principal a_n

Sustituyendo en (*) nos queda:

$f(x) = (x-\alpha_1).(x-\alpha_2).....(x-\alpha_h).(x-\alpha_{h+1}).q(x) \quad \forall x \in \Re$

con $gr(q) = (n-h)-1 = n-(h+1)$ y coeficiente principal a_n l-q.q.d.

Un caso que nos interesa particularmente es para p=n (la cantidad de raíces coincide con el grado de la función polinómica)

Teorema 2 de descomposición factorial

H) $\begin{cases} f \in P_{\Re} \ ; f(x) = a_n x^n + a_{n-1} x^{n-1} + ...+ a_1 x + a_0 \quad gr(f) = n \\ \alpha_1, \alpha_2, ..., \alpha_n \quad \text{n raíces diferentes dos a dos de f} \end{cases}$

T) $f(x) = a_n (x-\alpha_1).(x-\alpha_2).....(x-\alpha_n) \qquad \forall x \in \Re$

Teorema

"Un polinomio de grado n no acepta mas de n raíces distintas"

Dem:

Por absurdo. Suponemos que $f \in P_{\Re} \ ; f(x) = a_n x^n + a_{n-1} x^{n-1} + ...+ a_1 x + a_0 \quad gr(f) = n$ acepta raíces $\alpha_1, \alpha_2, ..., \alpha_n, \alpha_{n+1}$ distintas dos a dos .

Como $\alpha_1, \alpha_2, ..., \alpha_n$ son raíces distintas dos a dos de f $\Rightarrow_{\text{T.2 de D.F.}}$

$\Rightarrow \quad f(x) = a_n (x-\alpha_1).(x-\alpha_2).....(x-\alpha_n) \quad \forall x \in \Re \quad \Rightarrow \quad f(\alpha_{n+1}) = a_n (\alpha_{n+1}-\alpha_1).(\alpha_{n+1}-\alpha_2).....(\alpha_{n+1}-\alpha_n)$

Además α_{n+1} es raíz de f $\Rightarrow \quad a_n \underbrace{(\alpha_{n+1}-\alpha_1)}_{\neq 0}.\underbrace{(\alpha_{n+1}-\alpha_2)}_{\neq 0}.....\underbrace{(\alpha_{n+1}-\alpha_n)}_{\neq 0} = 0 \quad \Rightarrow \quad a_n = 0$

Lo cual es contradictorio pues $gr(f) = n$

Teorema

Consideramos: $f \in P_{\Re} \ ; f(x) = a_n x^n + a_{n-1} x^{n-1} + ...+ a_1 x + a_0$

Si $\exists \ \alpha_1, \alpha_2, ..., \alpha_n, \alpha_{n+1} \in \Re$ raíces distintas dos a dos de f $\Rightarrow$ $\begin{cases} a_n = 0 \\ a_{n-1} = 0 \\ ..... \\ ..... \\ a_1 = 0 \\ a_0 = 0 \end{cases}$

Dem:

Si $a_i \neq 0$ para algún i entre 0 y n $\Rightarrow \quad \exists gr(f)$ y además $gr(f) \leq n$ Tendríamos entonces una función polinómica de grado menor o igual que n con n+1 raíces lo cual contradice el teorema inmediato anterior.

Teorema de identidad de polinomios

Consideramos: $f \in P_{\Re} : f(x) = a_n x^n + a_{n-1} x^{n-1} + ...+ a_1 x + a_0 \quad gr(f) = n$

$g \in P_{\Re} \ ; f(x) = b_m x^m + b_{m-1} x^{m-1} + ...+ b_1 x + b_0 \quad gr(g) = m$

$$f = g \quad \Leftrightarrow \quad n = m \quad y \quad \begin{cases} a_n = b_n \\ a_{n-1} = b_{n-1} \\ ..... \\ ..... \\ a_1 = b_1 \\ a_0 = b_0 \end{cases}$$

Dem: ($\Rightarrow$) Por absurdo Consideramos $h = f - g$

Si $n \neq m$ ó $a_i \neq b_i$ para algún i de 1 a n $\Rightarrow \quad \exists gr(h) = k$ Consideramos ahora $\alpha_1, \alpha_2, ..., \alpha_k, \alpha_{k+1}$ k+1 reales distintos dos a dos.

Como $h = f - g \Rightarrow h(x) = f(x) - g(x) \quad \forall x \in \Re \Rightarrow$ $\begin{cases} h(\alpha_1) = f(\alpha_1) - g(\alpha_1) = 0 \\ h(\alpha_2) = f(\alpha_2) - g(\alpha_2) = 0 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ h(\alpha_k) = f(\alpha_k) - g(\alpha_k) = 0 \\ h(\alpha_{k+1}) = f(\alpha_{k+1}) - g(\alpha_{k+1}) = 0 \end{cases} \Rightarrow$

$\Rightarrow \alpha_1, \alpha_2, \ldots\ldots, \alpha_k, \alpha_{k+1}$ son k+1 raíces distintas dos a dos de h . Pero $gr(h) = k$ lo cual es contradictorio

---

EJERCICIOS **REPARTIDO Nº 13**

I) Hallar a, b, c $\in \Re$ sabiendo que : $(x^2 + ax + 1)(x + b) = x^3 + cx^2 + 3x + 1 \quad \forall x \in \Re$

II) Determinar una función polinómica de coeficientes reales y tercer grado sabiendo que:
$P(x+1) = 3x^3 + 11x^2 + 12x + 8$

III) Sea $Q : Q(x) = cx^2 + dx + 2$ Hallar *c* y *d* reales sabiendo que: $Q(x-1) - Q(x+1) = 6 - 4x$

IV) Determinar una función polinómica P de coeficientes reales sabiendo que: $P(2x) - P(x+1) = 6x^2 - x - P(0) + 2$

V) Sea $P : P(x) = x^3 + 5x^2 + ax + b$ Hallar *a* y *b* reales sabiendo que *P* dividido entre $x^2 + 2x$ da igual cociente que Resto.

Relaciones entre coeficientes y raíces

Consideramos $f \in P_{\Re}$; $f(x) = a_3x^3 + a_2x^2 + a_1x + a_0$ una función polinómica real de 3º grado con raíces α, β y γ distintas dos a dos.
Pretendemos averiguar si existe una vinculación entre las raíces de f α, β, γ y sus coeficientes a_3, a_2, a_1, a_0

Si α, β y γ son raíces distintas dos a dos de f $\Rightarrow_{\text{T. de D.F.2}} \quad f(x) = a_3(x-\alpha).(x-\beta).(x-\gamma) \quad \forall x \in \Re \Rightarrow$

$\Rightarrow \quad f(x) = a_3(x^2 - \alpha.x - \beta.x + \alpha.\beta).(x-\gamma) = a_3\left[x^3 - \alpha.x^2 - \beta.x^2 + \alpha.\beta.x - \gamma.x^2 + \alpha.\gamma.x + \beta.\gamma.x - \alpha.\beta.\gamma\right] \quad \forall x \in \Re \Rightarrow$

$\Rightarrow \quad f(x) = a_3x^3 - a_3(\alpha+\beta+\gamma).x^2 + a_3(\alpha.\beta + \alpha.\gamma + \beta.\gamma) - a_3.\alpha.\beta.\gamma \quad \forall x \in \Re$
Como $f(x) = a_3x^3 + a_2x^2 + a_1x + a_0 \quad \forall x \in \Re$ $\Big\} \Rightarrow_{\text{T. de Identidad de Polinomios}}$

$\Rightarrow$ $\begin{cases} a_3 = a_3 \\ -a_3.(\alpha+\beta+\gamma) = a_2 \Rightarrow \alpha+\beta+\gamma = -\dfrac{a_2}{a_3} \\ a_3(\alpha.\beta + \alpha.\gamma + \beta.\gamma) = a_1 \Rightarrow \alpha.\beta + \alpha.\gamma + \beta.\gamma = \dfrac{a_1}{a_3} \\ -a_3.\alpha.\beta.\gamma = a_0 \Rightarrow \alpha.\beta.\gamma = -\dfrac{a_0}{a_3} \end{cases}$

En resumen si $f \in P_{\Re}$; $f(x) = a_3x^3 + a_2x^2 + a_1x + a_0$ es una función polinómica real de 3º grado con raíces α, β y γ distintas dos a dos se cumple que:

$$\alpha + \beta + \gamma = -\frac{a_2}{a_3}$$
$$\alpha.\beta + \alpha.\gamma + \beta.\gamma = \frac{a_1}{a_3}$$
$$\alpha.\beta.\gamma = -\frac{a_0}{a_3}$$

Análogamente se demuestra que si $f \in P_{\Re}$; $f(x) = a_2x^2 + a_1x + a_0$ es una función polinómica real de 2ºgrado con raíces α y β distintas estas cumplen:

$$\alpha + \beta = -\frac{a_1}{a_2}$$
$$\alpha.\beta = \frac{a_0}{a_2}$$

Y también si $f \in P_{\Re}$; $f(x) = a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$ es una función polinómica real de 4º grado con raíces α, β, γ y δ distintas dos a dos se verifica:

$$\alpha + \beta + \gamma + \delta = -\frac{a_3}{a_4}$$
$$\alpha.\beta + \alpha.\gamma + \alpha.\delta + \beta.\gamma + \beta.\delta + \gamma.\delta = \frac{a_2}{a_4}$$
$$\alpha.\beta.\gamma + \alpha.\beta.\delta + \alpha.\gamma.\delta + \beta.\gamma.\delta = -\frac{a_1}{a_4}$$
$$\alpha.\beta.\gamma.\delta = \frac{a_0}{a_4}$$

EJERCICIOS **REPARTIDO 14**

I) Sea $P: P(x) = x^3 - 6x^2 + 11x - 6$ con raíces $\alpha, \beta \; y \; \gamma$ que cumplen: $\alpha = \beta + \gamma$. Hallar α, β, γ y la descomposición factorial de *P*.

II) Consideramos $P: P(x) = 2x^3 + ax^2 - 2x - 4$. Hallar *a* y las raíces de *P* sabiendo que el producto de dos de ellas es –1.

III) Con $P: P(x) = 2x^3 - 7x^2 + ax + 10$ de raíces α, β y γ. Determinar *a* , las raíces de *P* y su descomposición factorial; sabiendo que: $2\alpha + 2\beta + \gamma = 9$.

IV) Sea $P: P(x) = x^3 + 2x^2 + x + c$. Hallar *c* y las raíces de *P* α, β y γ sabiendo que cumplen: $\alpha^2 + \beta^2 = \gamma^2$.

V) Consideramos $P: P(x) = 2x^3 + ax^2 - 2bx - b$. Hallar a y b para que $\frac{1}{\alpha\beta} + \frac{1}{\alpha\gamma} + \frac{1}{\beta\gamma} = -\frac{1}{3}$ y $P(0) + P(1) = -33$ siendo α, β y γ las raíces de *P*.

VI) Sea $P: P(x) = x^3 - 11x^2 + 36x - 36$ con raíces α, β y γ que cumplen: $\alpha\beta = \gamma$.
Hallar las raíces y la descomposición factorial de *P*.

VII) Con $P: P(x) = x^3 + ax^2 + bx + ab$; $P(0) \neq 0$ de raíces α, β y γ.

i) Hallar *a* para que: $\alpha^2\beta\gamma + \alpha\beta^2\gamma + \alpha\beta\gamma^2 = -2P(0)$

ii) Determinar *b* sabiendo que *P* dividido entre $x^2 - 5x + 5$ da igual cociente que resto.

iii) Resolver en $(\Re, +, \cdot, \leq)$ $P(x) = 0$ y escribir la descomposición factorial de *P*.

VIII) Consideramos $P: P(x) = x^3 + a^2 - 4x + b$ de raíces α, β y γ.

i) Determinar $\beta > 0$ para que: $\frac{\alpha}{\beta} + \frac{\alpha}{\gamma} + \frac{\beta}{\gamma} = -1$

ii) Hallar a<0 y b para que $x^4 - 5x^2 + 4$ sea divisible entre *P*.

Nota

Cabe destacar que las fórmulas anteriores también son válidas cuando alguna o todas las raíces son iguales. Así también como el teorema de descomposición factorial. No lo demostraremos en este caso; pues dicha demostración involucra elementos de divisibilidad en polinomios, cuyo tratamiento, en nuestra opinión excede los objetivos del curso.

También es posible deducir fórmulas de relaciones entre coeficientes y raíces para funciones polinómicas de grado mayor que cuatro; pero rara vez dichas fórmulas son usadas.

Ejercicio:

Consideramos: $f \in P_{\Re}$; $f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots\ldots\ldots + a_1 x + a_0$ Probar:

1) 0 es raíz de f $\Leftrightarrow$ $a_0 = 0$

2) 1 es raíz de f $\Leftrightarrow$ $a_n + a_{n-1} + \ldots\ldots\ldots + a_1 + a_0 = 0$

3) i) Si $n = \overset{\bullet}{2}$ -1 es raíz de f $\Leftrightarrow$ $a_n + a_{n-2} + \ldots\ldots\ldots + a_2 + a_0 = a_{n-1} + a_{n-3} + \ldots\ldots\ldots + a_1$

ii) Si $n \neq \overset{\bullet}{2}$ -1 es raíz de f $\Leftrightarrow$ $a_{n-1} + a_{n-3} + \ldots\ldots\ldots + a_2 + a_0 = a_n + a_{n-1} + \ldots\ldots + a_1$

Ejercicio:

Hallar la descomposición factorial de:

1) $f: f(x) = 2x^3 + 5x^2 + 2x$

2) $g: g(x) = 4x^3 - 4x^2 - x + 1$

3) $h: h(x) = 2x^3 + 2x^2 + 3x + 3$

4) $t: t(x) = x^4 + 5x^3 + 5x^2 - 5x - 6$

5) $w: w(x) = x^5 + 2x^3 - 3x$

Nota También es posible demostrar:

$$\left.\begin{array}{l} f \in P_{\Re} \; ; f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots\ldots\ldots + a_1 x + a_0 \\ \qquad a_n, a_{n-1}, \ldots\ldots\ldots, a_1, a_0 \in Z \\ \alpha = \dfrac{p}{q} \in Q \;\text{ raíz de f;}\quad \text{con p y q enteros primos entre si} \end{array}\right\} \Rightarrow \begin{cases} p / a_0 & (\text{p divide a } a_0) \\ q / a_n & (\text{q divide a } a_n) \end{cases}$$

Proposición conocida como teorema de la raíz racional. No haremos la demostración; ya que la misma involucra conceptos de divisibilidad que no tratamos anteriormente. Pero si lo utilizaremos.

Ejercicio: Resolver en $(\Re,+,\cdot,\leq)$: i) $3x^3 + 2x^2 - 6x - 4 = 0$ ii) $6x^4 - x^3 - 26x^2 + 4x + 8 = 0$

iii) $6x^4 - x^3 + 5x^2 - x - 1 = 0$

Teorema

$f, g \in P_{\Re}$ $\quad f \neq \theta$ y $g \neq \theta \;\Rightarrow\; f.g \neq \theta$

Dem:

$f \neq \theta \;\Rightarrow\; \exists\, gr\, f = n \;\Rightarrow$ f acepta a lo sumo n raíces distintas

$g \neq \theta \;\Rightarrow\; \exists gr\, g = m \;\Rightarrow$ g acepta a lo sumo m raíces distintas

Consideramos $\alpha \in \Re$ que no sea raíz de f ni de g.

$\Rightarrow\; f(\alpha) \neq 0$ y $g(\alpha) \neq 0 \;\Rightarrow\; (f.g)(\alpha) = f(\alpha).g(\alpha) \neq 0 \;\Rightarrow\; f.g \neq \theta$

Corolario

$$f, g \in P_{\Re} \qquad f.g = \theta \;\Rightarrow\; \begin{cases} f = \theta \\ \text{ó} \\ g = \theta \end{cases}$$

Dem: Es el contrarecíproco del teorema inmediato anterior.

Nota:

¿ Si f y g no son funciones polinómicas la proposición anterior es necesariamente cierta?

Sugerencia Analizar $f: \begin{cases} f(x) = 0 & \text{si } x \in Q \\ f(x) = 1 & \text{si } x \in \Re - Q \end{cases}$ y $g: \begin{cases} g(x) = 1 & \text{si } x \in Q \\ g(x) = 0 & \text{si } x \in \Re - Q \end{cases}$

Ahora sí estamos en condiciones de probar la unicidad del cociente y el resto de la división entera

Teorema

$$\begin{array}{c|c} f & g \\ \hline r & q \end{array} \quad \text{y} \quad \begin{array}{c|c} f & g \\ \hline r' & q'' \end{array} \quad \Rightarrow \quad q = q' \quad \text{y} \quad r = r'$$

Dem

$$\begin{array}{c|c} f & g \\ \hline r & q \end{array} \Rightarrow \begin{cases} f = g.q + r \\ r = \theta \quad \text{ó} \quad gr\, r < gr\, g \end{cases} \qquad \begin{array}{c|c} f & g \\ \hline r' & q' \end{array} \Rightarrow \begin{cases} f = g.q' + r' \\ r' = \theta \quad \text{ó} \quad gr\, r' < gr\, g \end{cases}$$

Por lo tanto $g.q + r = g.q' + r' \;\Rightarrow\; g.(q - q') = r' - r$

Ahora si $q \neq q' \;\Rightarrow\; q - q' \neq \theta \;\Rightarrow\; \exists\, gr\,(q - q')$ como además $g \neq \theta$ $(q - q').g \neq \theta$ y

$gr\, g.(q - q') = gr\,(g) + gr\,(q - q') \geq gr\,(g)$ Como $g.(q - q') = r' - r \neq \theta \;\Rightarrow\; gr\, g.(q - q') = gr\,(r' - r)$

$\Rightarrow\; gr\,(r' - r) \geq gr\,(g)$ Pero $gr\,(r' - r) \leq \text{máx}\{gr\,(r), gr\,(r')\} < gr\,(g)$ lo que es contradictorio $\Rightarrow$

$\Rightarrow\; q = q' \;\Rightarrow\; r = r'$

EJERCICIOS **REPARTIDO Nº 15**

I) i) Probar: $\left.\begin{array}{l} A, B \text{ polinomios de coeficientes reales} \\ \lambda, \mu \in \Re \\ \alpha \quad \text{raiz comun a A y B} \end{array}\right\} \Rightarrow \left\{\begin{array}{l} 1)\ \alpha \text{ es raiz de } \lambda.A + \mu.B \\ 2)\ \text{Si } \begin{array}{cc} A & B \\ R & Q \end{array} \Rightarrow \alpha \text{ es raiz de R} \end{array}\right.$

ii) Sean: $A : A(x) = 2x^3 + x^2 - 18x - 9$, $B : B(x) = 4x^3 + 12x^2 - x - 3$ y $C : C(x) = 2x^4 - 2x^3 - 11x^2 - x - 6$
Hallar las raíces de A,B, C y su descomposición factorial sabiendo que A y B como también A y C admiten raíces comunes.

II) Consideramos: $P : P(x) = m^2x^4 + 2m^2x^3 - (m^2 + m + 1)x^2 - (2m^2 + m + 1)x + 2m + 2$
i) Hallar todas las raíces de P sabiendo que admite dos raíces independientes de m.
ii) Hallar el o los valores de m para los cuales P admite una raíz doble.

III) Dado $P : P(x) = 2x^3 + 3x^2 + (-2m^2 - 2m + 1)x - m^2 - m$
i) Investigar si P admite una raíz independiente de m . En caso afirmativo hallarla.
ii) Probar que P admite tres raíces reales $\forall m \in \Re$.
iii) Determinar $m \in \Re^+$ para que: $\frac{3}{\alpha} + \frac{3}{\beta} + \frac{3}{\gamma} = \frac{11}{\alpha\beta} + \frac{11}{\alpha\gamma} + \frac{11}{\beta\gamma}$

IV) Sea $P : P(x) = (6m^2 + 3m)x^4 + (15m^2 + 2m + 1)x^3 + (3m^2 - m)x^2 + (-6m^2 + 13m - 2)x + 4 - 2m$
i) Hallar α raíz independiente de m.
ii) Verificar que $\beta = \frac{-1}{3m}$ es raíz de $P \quad \forall m \in \Re^*$
iii) Si llamamos Q al cociente de dividir P entre $(x - \alpha)(3mx + 1)$.
a) ¿Para que valores de m , Q acepta dos raíces reales del mismo signo?
b) ¿Para que valores de m $Q(x) < 0 \quad \forall x \in \Re$?

V) Consideramos: $P : P(x) = (2m + 2)x^3 + (3m - 1)x^2 - 4mx + m$
i) Probar que P admite una raíz independiente de m ; hallarla.
ii) Hallar los valores de m para los cuales P admite tres raíces reales positivas.

EJERCICIOS **REPARTIDO Nº 16**

I) Sea $P : P(x) = -35x^2 + 45x^n + 4x^{3n+1} - ax^{4n-1} - 14 + a$
i) Probar que P es divisible entre *x*-1.
ii) Determinar *n* y *a* sabiendo que el cociente de dividir *P* entre *x*-2 es de tercer grado y el resto vale –35
iii) Resolver en $(\Re, +, \cdot, \leq) \quad P(x) = 0$

II) Consideramos: $P: P(x) = \left(x^2 + \frac{1}{2}x - \frac{1}{2}\right)^h + \left(x^2 - \frac{1}{2}x - \frac{1}{2}\right)^h - 1$

i) Demostrar que P es divisible entre $x^2 - 1 \quad \forall h \in N$

ii) Sea $Q: Q(x) = m\,P(x) + 3x\,(x^2 - 1)$

a) Calcular h para que Q sea de cuarto grado y escribir la descomposición factorial de P para ese valor de *h*.
b) Para dicho valor de h determinar los valores de *m* para los cuales Q tiene cuatro raíces reales.
c) Determinar todos los valores de m para los cuales Q tiene una raíz doble.

III) Sea $P: P(x) = x^3 + px + q$

i) Probar que si *P* es divisible entre $x^2 + mx - 1$ entonces $P(m) = 0$

ii) En el caso anterior calcular *p,q* y *m* si además $p^2 + q^2 + m^2 = 33$ y $m \in \Re^-$.

IV) i) Hallar *a,b* y *c* para que $P: P(x) = (x+1)^{2n} + ax^{2n} + bx + c$ sea divisible entre $2x^3 + 3x^2 + x$

ii) Para a,b y c hallados calcular: $\dfrac{(x+1)^6 + ax^6 + bx + c}{2x^3 + 3x^2 + x}$.

V) i) Probar que: $\sum_{i=0}^{n} [P(i+1) - P(i)] = P(n+1) - P(0) \qquad \forall n \in N$ siendo *P* un polinomio cualquiera.

ii) Determinar un polinomio P de tercer grado sabiendo que:

$$\sum_{i=2}^{n} [P(i+1) - P(i)] = n^3 + 6n^2 + 8n + 5P(0) \quad \forall n \in N$$

VI) Sea *A* un polinomio de tercer grado y *B* otro polinomio no nulo tal que:

A	B
C	C

i) Probar: α raíz de C $\Rightarrow$ α raíz de A

ii) ¿Es posible que B sea de primer grado? Deducir y justificar el grado de B.

iii) Determinar B sabiendo que su coeficiente principal es 1 B(0)=1 y todas sus raíces son iguales y negativas.

iv) Determinar A sabiendo que su coeficiente principal es 2 y que $C(\frac{1}{2}) = 0$.

VII) Sean P y Q dos polinomios no nulos de los cuales se sabe que

P	Q
-1	Q

i) Probar: α raiz de P $\Leftrightarrow$ $\begin{cases} Q(\alpha) = 1 \\ \text{y / o} \\ Q(\alpha) = -1 \end{cases}$

ii) Determinar Q de coeficiente principal positivo sabiendo que $P: P(x) = x^4 + 2x^3 - x^2 - 2x$

iii) Resolver en $(\Re, +, \cdot, \leq)$ $P(x) = 0$ y escribir la descomposición factorial de *P*.

VIII) Sea $P: P(x) = x^3 + ax^2 + bx + ab$

i) Probar que $x+a$ divide a P.

ii) Probar que si $b>0$ P acepta solamente una raíz real.

iii) Hallar a y b no nulos sabiendo que: $\alpha^2\beta\gamma + \alpha\beta^2\gamma + \alpha\beta\gamma^2 = 2P(0)$ y que

$\frac{b}{\alpha} + \frac{b}{\beta} + \frac{b}{\gamma} = 2$ siendo α, β y γ las raíces de P.

iv) Resolver en $(\Re, +, \cdot, \leq)$: $2^{P(x)} < \frac{2^x}{4}$

IX) i) Sea $P: P(x) = x^3 + ax^2 - 12x + 36$ Determinar a y las raíces de P α, β, γ sabiendo que

$\frac{1}{\alpha} + \frac{1}{\beta} = \frac{1}{\gamma}$

ii) Si $\begin{array}{c|c} \text{A} & \text{B} \\ \hline \text{C} & \text{C} \end{array}$ **a)** Probar que si $B(\delta) = -1 \Rightarrow \delta$ es raíz de A

b) Probar: ε raíz de A y $B(\varepsilon) \neq -1 \Rightarrow \varepsilon$ es raíz de C.

iii) Determinar un polinomio Q sabiendo que P dividido Q da igual cociente que resto y $Q(\gamma) \neq -1$ siendo γ el valor hallado en i).

iv) Resolver en $(\Re, +, \cdot, \leq)$: $\frac{P(x)}{Q(x)+1} \geq 1$

X) i) Determinar un polinomio Q de segundo grado sabiendo que $Q(1) = 1$ $Q(0) = 0$ y $Q(-1) = 3$

ii) Sea $P: P(x) = Q(x)x^n + [Q(x) - 1]x^{n-1} + fx + g$

Hallar f y g sabiendo que P es divisible entre $x^2 - x$.

iii) a) Probar que si n es impar entonces P es divisible entre $x^3 - x$

b) Para n par hallar el resto de dividir P entre $x + 1$

iv) Determinar P sabiendo que P dividido ente $x^3 - x$ da cociente $Q(-x) + 1$

v) Para P hallado resolver en $(\Re, +, \cdot, \leq)$ $\frac{P(x)}{x^3 - x} \leq 7$

XI) Sea $P(x) = \left[(x-1)^{2h} + x^h\right]\left[(x-1)^{2h} - x^h\right] + ax + b$

i) Hallar a y b sabiendo que P es divisible entre $x^2 - x$

ii) Determinar P y su descomposición factorial sabiendo que el cociente de la división indicada anteriormente es de segundo grado.

XII) i) Determinar un polinomio de tercer grado y coeficientes reales sabiendo que: * Tiene coeficiente principal 6

** La suma de sus raíces vale $-1/6$ *** Dividido x - 2 da resto 45 **** P(1)=4.

ii) Escribir la descomposición factorial de P y resolver en $(\Re, +, \cdot, \leq)$ $\log_{x+1}^{P(x)} \leq 2$

XIII) Completar el siguiente esquema de Ruffini.

				1	2
		-8		10	
	4	11			

XIV) Determinar dos polinomios P y Q sabiendo que: $P(x)+Q(x)=6x^3-x^2+5x-3$

$P(x)-Q(x)=2x^4+7x^2-3x+1$

XV) Hallar un polinomio P de tercer grado y otro Q de segundo grado sabiendo que al dividir P entre Q el cociente es $5x+1$ y el resto es $10x+2$. Además $P(x)-x\,Q(x)=4x^3+x^2-10x-3$

XVI) Hallar un polinomio *A* de tercer grado divisible entre x^2-2 y $x+1$ Además A dividido entre *x* da resto 20.

XVII) Sean P y Q dos polinomios tales que Q es de cuarto grado, P y Q admiten raíces comunes 2,3 y 7; P dividido Q da cociente C y resto R.

i) Hallar R sabiendo además que su coeficiente principal es –2

ii) Determinar Q si además se sabe que: Q(1)=0 y Q(0)=42

iii) Hallar P si C:C(x)=2x-1

iv) Hallar las raíces de $H: H(x)=P(x)-Q(x)$

XVIII) Hallar un polinomio P de cuarto grado, coeficiente principal –2 que cumple:

* $P(x)=Q(x).(-2x)+R(x)$ con R de primer grado. ** P y Q tienen una raíz común

*** $P(-1)=0$ **** $Q(-1)=-6$ ***** $P(0)=10$ ****** La suma de las otras dos raíces de Q vale –1.

TRIGONOMETRÍA

Algunas consideraciones previas

Ya que no es la primera vez que nos enfrentamos al tema, sabemos que en su tratamiento se involucran además de los números reales entes geométricos (puntos, rectas, circunferencias, ángulos) lo cual nos lleva necesariamente a manejar proposiciones desarrolladas en otra asignatura; de las cuales resaltamos:

1) Si llamamos Ω al conjunto de puntos del plano; existe una función $d : \Omega \times \Omega \to \Re$ a la que llamamos función **distancia** que cumple:

i) $d(X, Y) \geq 0 \quad \forall X, Y \in \Omega$

ii) $d(X, Y) = d(Y, X) \quad \forall X, Y \in \Omega$

iii) Si $Z \in \overline{XY} \Rightarrow d(X, Y) = d(X, Z) + d(Z, Y)$

iv) Si $Z \notin \overline{XY} \Rightarrow d(X, Y) < d(X, Z) + d(Z, Y)$

v) Para cada recta orientada $\vec{r}$, para cada punto $X \in \vec{r}$ y para cada real $t; t \geq 0$ existe un único punto $Y \in \vec{r}$ tal que $X \prec Y$ y $d(X,Y) = t$.

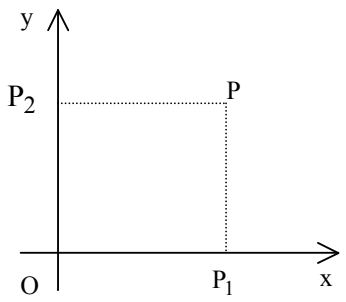
2) Para cada recta orientada $\vec{r}$ y para cada punto $O \in \vec{r}$ existe una única función biyectiva $f : \vec{r} \to \Re$ creciente que cumple:

i) f(O)=0

ii) $d(X,Y) = \left| f(X) - f(Y) \right| \quad \forall X, Y \in \vec{r}$

Si $P \in \vec{r}$, $x \in \Re$ y $f(P) = x$ decimos que x es la **abscisa** de P y también que P es el **afijo** de x.

3)



Consideramos $\vec{x}$ e $\vec{y}$ dos rectas orientadas que se cortan. en O

A cada punto $P \in \Omega$ le hacemos corresponder (P_1, P_2) un par de puntos, proyecciones de P sobre cada uno de los ejes según la dirección del otro.

Ahora $P_1 \in \vec{x}$ y por lo tanto tiene una abscisa x_0 análogamente como P_2 también pertenece a un eje orientado le podemos asignar una y solo una abscisa y_0. Por lo tanto al par de puntos (P_1, P_2) le corresponde el par de reales (x_0, y_0)

En resumen

$$P \quad \to \quad (P_1, P_2) \quad \to \quad (x_0, y_0)$$

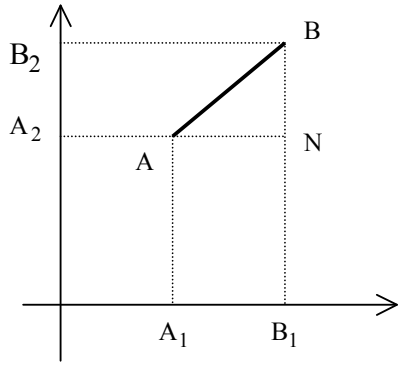
Componiendo ambas relaciones le asignamos a cada punto del plano un par ordenado de números reales. Estableciendo de esta forma una correspondencia entre Ω y $\Re \times \Re$.

Justifique el lector que tal correspondencia es una función biyectiva.

Si mediante la biyección recién descrita (x_0, y_0) son las imágenes del punto P decimos que x_0 es la **abscisa** de P e y_0 su **ordenada**. También decimos que el par (x_0, y_0) son las **coordenadas** del punto P o que P es el **afijo** de (x_0, y_0) Si (x_0, y_0) son las coordenadas del punto P, anotamos: $P(x_0, y_0)$.

Es innecesario mencionar que las rectas orientadas x e y (llamadas ejes cartesianos) no tienen por qué ser perpendiculares. Si lo son (que es lo mas habitual) decimos que estamos frente a un sistema de coordenadas cartesiano ortogonal

4)



Consideramos dos puntos del plano $A(x_0, y_0)$ y $B(x_1, y_1)$ en un sistema de coordenadas cartesiano ortogonal.
Si la recta AB no es paralela a ninguno de los ejes de cartesianos se forma un triángulo rectángulo ANB.
Aplicando Pitágoras a dicho triángulo tenemos:

$$d^2(A,B) = d^2(A,N) + d^2(N,B) = d^2(A_1,B_1) + d^2(A_2,B_2) \Rightarrow$$

$$d^2(A,B) = |x_1 - x_0|^2 + |y_1 - y_0|^2 = (x_1 - x_0)^2 + (y_1 - y_0)^2$$

Entonces

$$\boxed{d(A,B) = \sqrt{(x_1 - x_0)^2 + (y_1 - y_0)^2}}$$

Justifique el lector que la fórmula obtenida es válida independientemente de la posición particular que ocupen los puntos A y B con respecto a los ejes.

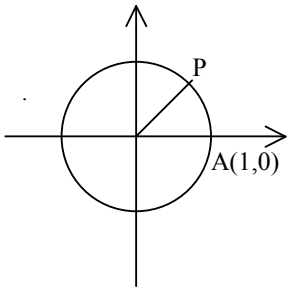
5) Asumimos que la longitud de una circunferencia de radio r es $2\pi r$; por lo tanto si denominamos C_0 a la circunferencia de centro O(0,0) y radio 1 esta tiene longitud 2π.

6) También aceptamos que los arcos de circunferencia son medibles.

En particular:

i) $\forall \beta \in [0,2\pi)$ existe y es único $P \in C_0$ tal que $\overleftarrow{AP} = \beta$

ii) $\forall P \in C_0$ existe y es único $\beta \in [0,2\pi)$ tal que $\overleftarrow{AP} = \beta$



Anotamos $\overleftarrow{AP}$ a la medida del arco de C_0 que nos lleva de A a P en sentido antihorario.

En otras palabras asumimos que existe una biyección entre C_0 y $[0,2\pi)$

7) También existe una biyección entre los ángulos al centro y los puntos de una circunferencia.

En particular si denominamos γ al ángulo AOP ; al ángulo γ le corresponde un y solo un punto $P \in C_0$ y como vimos recién a P le corresponde un y solo un número $\beta \in [0,2\pi)$. Componiendo ambas funciones al ángulo γ le corresponde el real β . Como ambas funciones son biyectivas la compuesta también lo es, por lo tanto queda así establecida una biyección entre los ángulos al centro de C_0 y $[0,2\pi)$
Decimos que el real β . es la medida en radianes del ángulo γ. Obsérvese que C_0 tiene radio 1 y en consecuencia estamos utilizando el radio como unidad para medir el arco $\overleftarrow{AP}$

Nota

Somos conscientes que la justificación de las proposiciones 5) 6) y 7) encierran tales dificultades que exceden los objetivos de Geometría I y por lo tanto el lector deberá esperar cursos posteriores para ver tales justificaciones.

Teorema

$\forall \alpha \in \Re$ existen y son únicos $\beta \in [0,2\pi)$ y $k \in Z$; $\alpha = \beta + 2k\pi$

Dem Existencia $\alpha = \beta + 2k\pi \iff \beta = \alpha - 2k\pi$

Ahora $\beta \in [0,2\pi) \iff 0 \le \beta < 2\pi \iff 0 \le \alpha - 2k\pi < 2\pi \iff 2k\pi \le \alpha < 2\pi(k+1) \iff k \le \frac{\alpha}{2\pi} < k+1$

Entonces llamando $k = \left[\frac{\alpha}{2\pi}\right]$ (parte entera de $\frac{\alpha}{2\pi}$) tenemos que: $k \le \frac{\alpha}{2\pi} < k+1$ volviendo atrás en el razonamiento anterior llegamos a que: $0 \le \alpha - 2k\pi < 2\pi$

En resumen: $\forall \alpha \in \Re \quad \exists k = \left[\frac{\alpha}{2\pi}\right] \in Z$ y $\exists \beta = \alpha - 2k\pi \in [0,2\pi)$ tal que $\alpha = \beta + 2k\pi$

Unicidad Suponemos: $\left.\begin{array}{l} \alpha = \beta + 2k\pi \,;\ \beta \in [0,2\pi) \text{ y } k \in Z \\ \alpha = \beta' + 2k'\pi \,;\ \beta' \in [0,2\pi) \text{ y } k' \in Z \end{array}\right\} \Rightarrow \beta + 2k\pi = \beta' + 2k'\pi \Rightarrow (k-k')2\pi = \beta' - \beta$

$$\left.\begin{array}{l} \text{Ahora } 0 \le \beta' < 2\pi \\ 0 \le \beta < 2\pi \Rightarrow -2\pi < -\beta \le 0 \end{array}\right\} \Rightarrow -2\pi < \beta' - \beta < 2\pi \Rightarrow -2\pi < (k-k')2\pi < 2\pi \Rightarrow$$

$$\Rightarrow -1 < k - k' < 1 \quad \text{como } k - k' \in Z \Rightarrow k - k' = 0 \Rightarrow k = k' \Rightarrow \beta = \beta'$$

Nota

Utilizando el teorema anterior podemos definir la función $\varphi : \Re \to [0,2\pi)$; $\varphi(\alpha) = \beta$ Por lo dicho anteriormente también existe una función $f : [0,2\pi) \to C_0$; $f(\beta) = P$ con $P \in C_0$ tal que $\overleftarrow{AP} = \beta$

Componiendo φ y f tenemos una función mediante la cual a cada número real α le corresponde un punto P de C_0

$$\alpha \xrightarrow{\varphi} \beta \xrightarrow{f} P$$

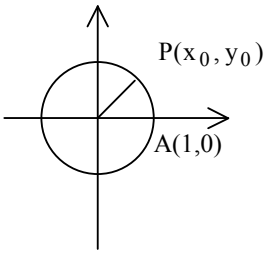
Si $f \circ \varphi(\alpha) = P$ (la imagen según la mencionada función compuesta del real α es el punto P) diremos que P es el **asociado** de α.

Observemos que φ y $f \circ \varphi$ no son inyectivas ; es mas: $\varphi(\alpha + 2h\pi) = \varphi(\alpha) \quad \forall h \in Z \quad \forall \alpha \in \Re \Rightarrow$
$\Rightarrow f \circ \varphi(\alpha + 2h\pi) = f \circ \varphi(\alpha) \quad \forall h \in Z \quad \forall \alpha \in \Re$.
Así $\alpha, \alpha + 2\pi, \alpha + 4\pi, \alpha - 2\pi, \ldots\ldots\ldots\ldots, \alpha - 1034\pi, \ldots\ldots\ldots\ldots$ tienen el mismo punto asociado.

Le sugerimos al lector que haga una interpretación geométrica de estos hechos.

Definición

Consideramos $\alpha \in \Re$ y $P(x_0, y_0) \in C_0$ su asociado. Llamamos **coseno** de α (anotamos $\cos\alpha$) a la abscisa del punto P; en otras palabras: $\cos\alpha = x_0$. Y denominamos **seno** de α (anot. $\operatorname{sen}\alpha$) a la ordenada de P; o sea: $\operatorname{sen}\alpha = y_0$.



$\alpha \xrightarrow{\varphi} \beta \xrightarrow{f} P(x_0, y_0)$ Definimos $\cos\alpha = x_0$ y $\operatorname{sen}\alpha = y_0$.

Recordemos que $\alpha = \beta + 2k\pi$ con $\beta \in [0,2\pi)$, $k \in Z$ y $P \in C_0$; $\overset{\frown}{AP} = \beta$

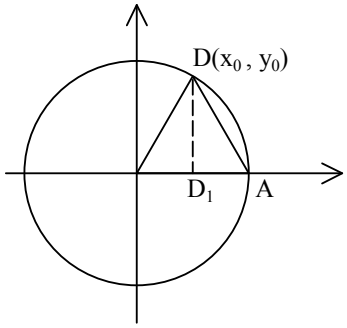
Ejemplos

El asociado de 0 es A(1,0) $\Rightarrow$ $\cos 0 = 1$ y $\operatorname{sen} 0 = 0$

El asociado de $\frac{\pi}{2}$ es B(0,1) $\Rightarrow$ $\cos\frac{\pi}{2} = 0$ y $\operatorname{sen}\frac{\pi}{2} = 1$

Como $431\pi = \pi + 2.(215)\pi$ $\Rightarrow$ el asociado de 431π es C(−1,0) $\Rightarrow$ $\cos(431\pi) = -1$ y $\operatorname{sen}(431\pi) = 0$

Busquemos ahora el seno y el coseno de $\frac{\pi}{3}$



Si $D(x_0, y_0)$ es el asociado a $\frac{\pi}{3}$ consideraciones geométricas elementales nos llevan a que el triángulo OAD es equilátero $\Rightarrow$

$\Rightarrow$ D_1 es el punto medio de OA $\Rightarrow$ $D_1\left(\frac{1}{2},0\right) \Rightarrow x_0 = \frac{1}{2} \Rightarrow \cos\frac{\pi}{3} = \frac{1}{2}$

Ahora $d(O,D) = \sqrt{(x_0-0)^2 + (y_0-0)^2} = 1$ $\Rightarrow$ $x_0^2 + y_0^2 = 1$ $\Rightarrow$

$\Rightarrow$ $\frac{1}{4} + y_0^2 = 1$ $\Rightarrow$ $y_0^2 = \frac{3}{4}$ $\Rightarrow$ $y_0 = \pm\frac{\sqrt{3}}{2}$ en este caso $y_0 > 0$

$\Rightarrow$ $\operatorname{sen}\frac{\pi}{3} = \frac{\sqrt{3}}{2}$

Ejercicios Calcular seno y coseno de $\frac{\pi}{6}$ y $\frac{\pi}{4}$

Observaciones Como el asociado de α y $\alpha + 2k\pi$ es el mismo $\forall\alpha \in \Re$ $\forall k \in Z$ entonces

$\cos(\alpha + 2k\pi) = \cos\alpha$	$\forall\alpha \in \Re$ $\forall k \in Z$
$\operatorname{sen}(\alpha + 2k\pi) = \operatorname{sen}\alpha$	$\forall\alpha \in \Re$ $\forall k \in Z$

Ejercicios Calcular $\cos\left(\frac{573}{4}\pi\right)$ y $\operatorname{sen}\left(-\frac{241}{3}\pi\right)$

Ejercicios Resolver en $(\Re,+,\cdot,\leq)$: i) $\cos x = 0$ ii) $\operatorname{sen} x = 0$

Observaciones

$-1 \leq \cos\alpha \leq 1$	$\forall\alpha \in \Re$
$-1 \leq \operatorname{sen}\alpha \leq 1$	$\forall\alpha \in \Re$

Cabe resaltar que hemos definido **seno y coseno de un número real**; no de un ángulo.

Si consideramos las funciones $f: \Re \to \Re$; $f(x) = \operatorname{sen} x$ y $g: \Re \to \Re$; $g(x) = \cos x$ las últimas dos observaciones realizadas nos permiten afirmar que f y g son funciones periódicas (de periodo 2π) y acotadas (entre –1 y 1).

Definición

Consideramos $\alpha \in \Re$

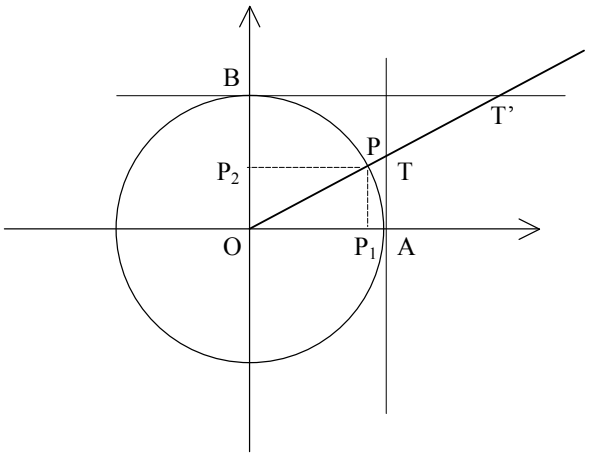
1) Si $\alpha \neq \frac{\pi}{2} + 2k\pi \quad (k \in Z)$ definimos **tangente** de α (anotamos $\operatorname{tg}\alpha$) $\quad \operatorname{tg}\alpha = \dfrac{\operatorname{sen}\alpha}{\cos\alpha}$

2) Si $\alpha \neq \frac{\pi}{2} + 2k\pi \quad (k \in Z)$ definimos **secante** de α (anotamos $\sec\alpha$) $\quad \sec\alpha = \dfrac{1}{\cos\alpha}$

3) Si $\alpha \neq k\pi \quad (k \in Z)$ definimos **cosecante** de α (anotamos $\operatorname{cos\,ec}\alpha$) $\quad \operatorname{cos\,ec}\alpha = \dfrac{1}{\operatorname{sen}\alpha}$

4) Si $\alpha \neq k\pi \quad (k \in Z)$ definimos **cotangente** de α (anotamos $\operatorname{cot g}\alpha$) $\quad \operatorname{cot g}\alpha = \dfrac{\cos\alpha}{\operatorname{sen}\alpha}$

Nota Consideramos $\alpha \in \Re\,;\, 0 < \alpha < \frac{\pi}{2}$ y P su asociado.



El triángulo OP_1P es semejante al OAT entonces

$\dfrac{d(P_1,P)}{d(O,P_1)} = \dfrac{d(A,T)}{d(O,A)}$ como d(O,A)=1 $\quad d(P_1,P) = d(O,P_2) = \operatorname{sen}\alpha$

y $d(O,P_1) = \cos\alpha \;\Rightarrow\; \dfrac{\operatorname{sen}\alpha}{\cos\alpha} = d(A,T) \;\Rightarrow\; \operatorname{tg}\alpha = d(A,T)$

Probar que:

$\sec\alpha = d(O,T) \quad \operatorname{cos\,ec}\alpha = d(O,T') \quad$ y $\quad \operatorname{cot g}\alpha = d(B,T')$

Le sugerimos al lector hacer las correspondientes interpretaciones geométricas cuando
$\frac{\pi}{2} < \alpha < \pi \quad$ ó $\quad \pi < \alpha < \frac{3\pi}{2} \quad$ ó $\quad \frac{3\pi}{2} < \alpha < 2\pi$

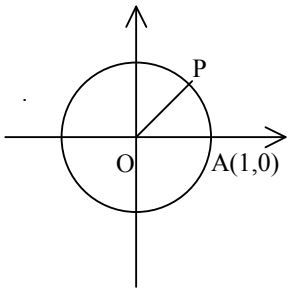
Nota

También le recomendamos revisar la bibliografía referida al tema utilizada en secundaria; sobre todo si no maneja el tema con profundidad.
La pretensión de este trabajo es definir (de forma clásica) las funciones trigonométricas, estudiar sus propiedades algebraicas y resolver algunas ecuaciones e inecuaciones que las involucran. No trabajaremos sobre resolución de triángulos y los múltiples problemas que ello nos permite encarar (calcular la distancia a un punto inaccesible, la altura de una montaña, etc.) Tampoco estudiaremos a las funciones trigonométricas bajo el punto de vista del análisis (continuidad, derivabilidad, desarrollo en serie de potencias, etc.)

Algunas fórmulas

Formulas fundamentales

1) $\boxed{\cos^2\alpha + \operatorname{sen}^2\alpha = 1 \qquad \forall \alpha \in \Re}$



Consideramos $\alpha \in \Re$ y P su asociado $\Rightarrow$ $P(\cos\alpha, \operatorname{sen}\alpha)$

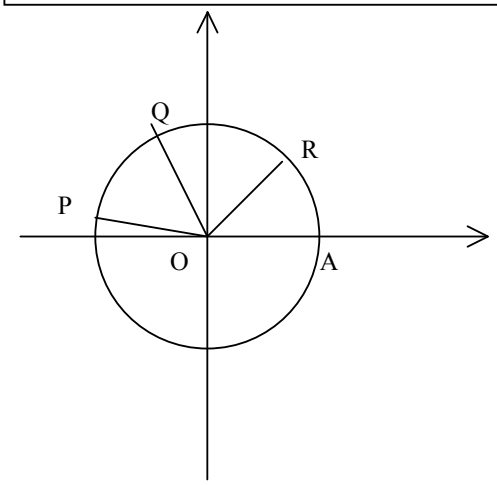
Ahora $d(O,P) = 1 \Rightarrow \sqrt{(\cos\alpha - 0)^2 + (\operatorname{sen}\alpha - 0)^2} = 1 \Rightarrow$

$$\Rightarrow \sqrt{\cos^2\alpha + \operatorname{sen}^2\alpha} = 1 \Rightarrow \cos^2\alpha + \operatorname{sen}^2\alpha = 1$$

Ejercicio Probar: i) $1 + \operatorname{tg}^2\alpha = \dfrac{1}{\cos^2\alpha} = \sec^2\alpha \qquad \forall \alpha \in \Re\,;\, \alpha \neq \frac{\pi}{2} + k\pi \quad (k \in Z)$

ii) $1 + \operatorname{cot g}^2\alpha = \dfrac{1}{\operatorname{sen}^2\alpha} = \operatorname{cos ec}^2\alpha \qquad \forall \alpha \in \Re\,;\, \alpha \neq k\pi \quad (k \in Z)$

2) $\boxed{\cos(\alpha - \beta) = \cos\alpha\cos\beta + \operatorname{sen}\alpha\operatorname{sen}\beta \qquad \forall \alpha, \beta \in \Re}$



Consideramos $\alpha, \beta \in \Re$

Denominamos: P,Q y R a los asociados de α, β y $\alpha - \beta$ respectivamente.

Entonces $P(\cos\alpha, \operatorname{sen}\alpha)$ $Q(\cos\beta, \operatorname{sen}\beta)$ y $R(\cos(\alpha - \beta), \operatorname{sen}(\alpha - \beta))$

Además si $\alpha = \alpha' + 2k\pi$; $\alpha' \in [0, 2\pi)$ y $k \in Z \Rightarrow \overleftarrow{AP} = \alpha'$

$\beta = \beta' + 2h\pi$; $\beta' \in [0, 2\pi)$ y $h \in Z \Rightarrow \overleftarrow{AQ} = \beta'$

Supongamos que $\alpha' > \beta' \Rightarrow \overleftarrow{QP} = \overleftarrow{AP} - \overleftarrow{AQ} = \alpha' - \beta'$ Además $\alpha' - \beta' \in [0, 2\pi)$

Como $\alpha - \beta = \alpha' - \beta' + 2(k - h)\pi$ con $\alpha' - \beta' \in [0, 2\pi)$ y $k - h \in Z \Rightarrow \overleftarrow{AR} = \alpha' - \beta'$

Por lo tanto

$$\overleftarrow{QP} = \overleftarrow{AR} \Rightarrow d(Q,P) = d(A,R) \Rightarrow \sqrt{(\cos\alpha - \cos\beta)^2 + (\operatorname{sen}\alpha - \operatorname{sen}\beta)^2} = \sqrt{(\cos(\alpha - \beta) - 1)^2 + (\operatorname{sen}(\alpha - \beta) - 0)^2}$$

$$\Rightarrow (\cos\alpha - \cos\beta)^2 + (\operatorname{sen}\alpha - \operatorname{sen}\beta)^2 = (\cos(\alpha - \beta) - 1)^2 + \operatorname{sen}^2(\alpha - \beta) \Rightarrow$$

$$\Rightarrow \underbrace{\cos^2\alpha + \operatorname{sen}^2\alpha}_{1} + \underbrace{\cos^2\beta + \operatorname{sen}^2\beta}_{1} - 2\cos\alpha\cos\beta - 2\operatorname{sen}\alpha\operatorname{sen}\beta = \underbrace{\cos^2(\alpha - \beta) + \operatorname{sen}^2(\alpha - \beta)}_{1} + 1 - 2\cos(\alpha - \beta)$$

Entonces $2-2\cos\alpha\cos\beta-2\operatorname{sen}\alpha\operatorname{sen}\beta=2-2\cos(\alpha-\beta) \Rightarrow \cos(\alpha-\beta)=\cos\alpha\cos\beta+\operatorname{sen}\alpha\operatorname{sen}\beta$

Ejercicio Probar que $\forall\alpha\in\Re$ se cumple:

i) $\cos\left(\frac{\pi}{2}-\alpha\right)=\operatorname{sen}\alpha$
ii) $\cos(\pi-\alpha)=-\cos\alpha$
iii) $\operatorname{sen}(\pi-\alpha)=\operatorname{sen}\alpha$
iv) $\cos(-\alpha)=\cos\alpha$
v) $\operatorname{sen}(-\alpha)=-\operatorname{sen}\alpha$
vi) $\cos(\pi+\alpha)-\cos\alpha$
vii) $\operatorname{sen}(\pi+\alpha)=-\operatorname{sen}\alpha$

Demostremos iii) como ejemplo.

$$\operatorname{sen}(\pi-\alpha) =_{i)} \cos\left(\tfrac{\pi}{2}-(\pi-\alpha)\right) = \cos\left(\alpha-\tfrac{\pi}{2}\right) = \cos\alpha\underbrace{\cos\tfrac{\pi}{2}}_{0}+\operatorname{sen}\alpha\underbrace{\operatorname{sen}\tfrac{\pi}{2}}_{1} = \operatorname{sen}\alpha$$

Ejercicio Probar que $\forall\alpha,\beta\in\Re$ se cumple:

$$\cos(\alpha+\beta) = \cos\alpha\cos\beta-\operatorname{sen}\alpha\operatorname{sen}\beta$$
$$\operatorname{sen}(\alpha-\beta) = \operatorname{sen}\alpha\cos\beta-\cos\alpha\operatorname{sen}\beta$$
$$\operatorname{sen}(\alpha+\beta) = \operatorname{sen}\alpha\cos\beta+\cos\alpha\operatorname{sen}\beta$$

Demostremos la primera de ellas a manera de ejemplo

$$\cos(\alpha+\beta)=\cos(\alpha-(-\beta))=\cos\alpha\underbrace{\cos(-\beta)}_{\cos\beta}+\operatorname{sen}\alpha\underbrace{\operatorname{sen}(-\beta)}_{-\operatorname{sen}\beta}=\cos\alpha\cos\beta-\operatorname{sen}\alpha\operatorname{sen}\beta$$

Ejercicio Probar que en condiciones de existencia se cumple:

i) $\operatorname{tg}(\alpha+\beta) = \dfrac{\operatorname{tg}\alpha+\operatorname{tg}\beta}{1-\operatorname{tg}\alpha\operatorname{tg}\beta}$ **ii)** $\operatorname{tg}(\alpha-\beta) = \dfrac{\operatorname{tg}\alpha-\operatorname{tg}\beta}{1+\operatorname{tg}\alpha\operatorname{tg}\beta}$

iii) $\operatorname{tg}\left(\alpha+\tfrac{\pi}{2}\right) = \dfrac{-1}{\operatorname{tg}\alpha} = -\operatorname{cot g}\alpha$ **iv)** $\operatorname{tg}\left(\alpha-\tfrac{\pi}{2}\right) = \dfrac{-1}{\operatorname{tg}\alpha} = -\operatorname{cot g}\alpha$

Nota

Aplicando i) tenemos que $\operatorname{tg}(\alpha+\pi)=\dfrac{\operatorname{tg}\alpha+\overbrace{\operatorname{tg}\pi}^{0}}{1-\operatorname{tg}\alpha\underbrace{\operatorname{tg}\pi}_{0}} = \operatorname{tg}\alpha$ lo cual nos hace sospechar que

$\operatorname{tg}(\alpha+k\pi)=\operatorname{tg}\alpha \quad \forall k\in Z \ \forall\alpha\in\Re$ en condiciones de existencia. Probémoslo.

$\underline{\text{Si } k=\overset{\bullet}{2}} \Rightarrow k=2h \ ; \ h\in Z \Rightarrow \operatorname{tg}(\alpha+k\pi)=\operatorname{tg}(\alpha+2h\pi)=\dfrac{\operatorname{sen}(\alpha+2h\pi)}{\cos(\alpha+2h\pi)}=\dfrac{\operatorname{sen}\alpha}{\cos\alpha}=\operatorname{tg}\alpha$

$\underline{\text{Si } k\neq\overset{\bullet}{2}} \Rightarrow k=2h+1 \ ; h\in Z \Rightarrow \operatorname{tg}(\alpha+k\pi)=\operatorname{tg}(\alpha+(2h+1)\pi)=\operatorname{tg}(\alpha+2h\pi+\pi)=\operatorname{tg}(\alpha+2h\pi)=\operatorname{tg}\alpha$

Por lo tanto: $\operatorname{tg}(\alpha+k\pi) = \operatorname{tg}\alpha \quad \forall k\in Z$ y $\forall\alpha\in\Re$ en condiciones de existencia

En otras palabras hemos probado que la función tangente es periódica de periodo π.

Ejercicios Probar que $\forall \alpha \in \Re$ en condiciones de existencia se cumple:

$$\boxed{\begin{aligned} \operatorname{sen} 2\alpha &= 2\operatorname{sen}\alpha\cos\alpha \\ \cos 2\alpha &= \cos^2\alpha - \operatorname{sen}^2\alpha \\ \operatorname{tg} 2\alpha &= \frac{2\operatorname{tg}\alpha}{1-\operatorname{tg}^2\alpha} \end{aligned}}$$

Por ejemplo: $\cos 2\alpha = \cos(\alpha+\alpha) = \cos\alpha\cos\alpha - \operatorname{sen}\alpha\operatorname{sen}\alpha = \cos^2\alpha - \operatorname{sen}^2\alpha$

Fórmulas de factoreo

Consideramos las igualdades ya demostradas

$$\operatorname{sen}(\alpha+\beta) = \operatorname{sen}\alpha\cos\beta + \cos\alpha\operatorname{sen}\beta$$
$$\operatorname{sen}(\alpha-\beta) = \operatorname{sen}\alpha\cos\beta - \cos\alpha\operatorname{sen}\beta$$

Sumando miembro a miembro tenemos

$$\operatorname{sen}(\alpha+\beta) + \operatorname{sen}(\alpha-\beta) = 2\operatorname{sen}\alpha\cos\beta$$

Y restando nos queda: $\operatorname{sen}(\alpha+\beta) - \operatorname{sen}(\alpha-\beta) = 2\cos\alpha\operatorname{sen}\beta$

Si ahora llamamos $a = \alpha+\beta$ y $b = \alpha-\beta \Leftrightarrow \alpha = \frac{a+b}{2}$ y $\beta = \frac{a-b}{2}$ sustituyendo en las igualdades anteriores llegamos a:

$$\boxed{\begin{aligned} \operatorname{sen} a + \operatorname{sen} b &= 2\operatorname{sen}\tfrac{a+b}{2}\cos\tfrac{a-b}{2} \\ \operatorname{sen} a - \operatorname{sen} b &= 2\cos\tfrac{a+b}{2}\operatorname{sen}\tfrac{a-b}{2} \end{aligned}}$$

Análogamente se demuestra:

$$\boxed{\begin{aligned} \cos a + \cos b &= 2\cos\tfrac{a+b}{2}\cos\tfrac{a-b}{2} \\ \cos a - \cos b &= -2\operatorname{sen}\tfrac{a+b}{2}\operatorname{sen}\tfrac{a-b}{2} \end{aligned}}$$

Seno, coseno y tangente de x en función de tg x/2

Vimos anteriormente que $\cos 2\alpha = \cos^2\alpha - \operatorname{sen}^2\alpha$ Si cambiamos 2α por x ($2\alpha = x \Leftrightarrow \alpha = \frac{x}{2}$) tenemos:

$$\cos x = \cos^2\tfrac{x}{2} - \operatorname{sen}^2\tfrac{x}{2} = \cos^2\tfrac{x}{2}\left[1 - \frac{\operatorname{sen}^2\frac{x}{2}}{\cos^2\frac{x}{2}}\right] = \cos^2\tfrac{x}{2}\left[1 - \operatorname{tg}^2\tfrac{x}{2}\right] \qquad (*)$$

También vimos que: $1+\operatorname{tg}^2\alpha = \frac{1}{\cos^2\alpha} \Rightarrow \cos^2\alpha = \frac{1}{1+\operatorname{tg}^2\alpha} \Rightarrow \cos^2\frac{x}{2} = \frac{1}{1+\operatorname{tg}^2\frac{x}{2}}$ Sustituyendo en (*) nos queda:

$$\boxed{\cos x = \frac{1-\operatorname{tg}^2\frac{x}{2}}{1+\operatorname{tg}^2\frac{x}{2}}} \qquad \forall x \in \Re \text{ ; x en condiciones de existencia}$$

Demostrar: $\forall x \in \Re$; x en condiciones de existencia

$$\boxed{\operatorname{sen} x = \frac{2\operatorname{tg}\frac{x}{2}}{1+\operatorname{tg}^2\frac{x}{2}}} \qquad \boxed{\operatorname{tg} x = \frac{2\operatorname{tg}\frac{x}{2}}{1-\operatorname{tg}^2\frac{x}{2}}}$$

Nota

Ya vimos que las funciones trigonométricas son periódicas y en consecuencia no son inyectivas; por lo tanto la proposición $\operatorname{sen}\alpha = \operatorname{sen}\beta \Leftrightarrow \alpha = \beta$ es falsa. Busquemos una condición necesaria y suficiente que si sea cierta.

$$\operatorname{sen}\alpha = \operatorname{sen}\beta \Leftrightarrow \operatorname{sen}\alpha - \operatorname{sen}\beta = 0 \Leftrightarrow 2\cos\frac{\alpha+\beta}{2}\operatorname{sen}\frac{\alpha-\beta}{2} = 0 \Leftrightarrow \begin{cases} \cos\frac{\alpha+\beta}{2} = 0 \\ \vee \\ \operatorname{sen}\frac{\alpha-\beta}{2} = = \end{cases} \Leftrightarrow$$

$$\Leftrightarrow \begin{cases} \frac{\alpha+\beta}{2} = \frac{\pi}{2} + k\pi \quad (k \in Z) \Leftrightarrow \alpha = \pi - \beta + 2k\pi \\ \vee \\ \frac{\alpha-\beta}{2} = k\pi \quad (k \in Z) \Leftrightarrow \alpha = \beta + 2k\pi \end{cases}$$

En resumen:

$$\boxed{\operatorname{sen}\alpha = \operatorname{sen}\beta \Leftrightarrow \begin{cases} \alpha = \beta + 2k\pi \quad (k \in Z) \\ \vee \\ \alpha = \pi - \beta + 2k\pi \quad (k \in Z) \end{cases}}$$

Análogamente se demuestra:

$$\boxed{\cos\alpha = \cos\beta \Leftrightarrow \begin{cases} \alpha = \beta + 2k\pi \quad (k \in Z) \\ \vee \\ \alpha = -\beta + 2k\pi \quad (k \in Z) \end{cases}}$$

$$\boxed{\operatorname{tg}\alpha = \operatorname{tg}\beta \Leftrightarrow \alpha = \beta + k\pi \quad (k \in Z)}$$

Algunos ejercicios resueltos:

Ejemplo 1 Resolver en $(\Re,+,\cdot,\leq)$: $\operatorname{sen}(2x+\pi) = \frac{\sqrt{3}}{2}$

$$\operatorname{sen}(2x+\pi) = \frac{\sqrt{3}}{2} \Leftrightarrow_{(*)} \begin{cases} 2x+\pi = \frac{\pi}{3} + 2k\pi \Leftrightarrow x = -\frac{\pi}{3} + k\pi \quad (k \in Z) \\ 2x+\pi = \frac{2\pi}{3} + 2k\pi \Leftrightarrow x = -\frac{\pi}{6} + k\pi \end{cases}$$

(*) Tengamos en cuenta que la función seno es una función periódica de periodo 2π. Por lo tanto una posible estrategia consiste en hallar las preimágenes de $\frac{\sqrt{3}}{2}$ en el intervalo $[0,2\pi)$ lo cual hacemos en este caso mediante la tabla de arcos notables, que se adjunta al final de estas notas, y luego cada uno de esas soluciones $\left(\frac{\pi}{3}\right.$ y $\left.\frac{2\pi}{3}\right)$ genera una familia de raíces que difieren entre sí en $2k\pi \quad (k \in Z)$. En el último paso simplemente "despejamos" x.

Ejercicios: Resolver en $(\Re,+,\cdot,\leq)$: i) $\operatorname{tg} x = -1$ ii) $\sec(2x+\pi) = 2$

Respuestas: i) $x = \frac{7\pi}{4} + k\pi$ ii) $x = -\frac{\pi}{3} + k\pi \quad \vee \quad x = \frac{\pi}{3} + k\pi \qquad (k \in Z)$

Ejemplo 2 Resolver en $(\Re,+,\cdot,\leq)$: $\cos(2x) = \operatorname{sen}(x+\pi)$

Intentemos utilizar las condiciones necesarias y suficientes vistas en el punto anterior. Para ello Necesitamos tener una igualdad entre senos o entre cosenos; para ello usamos que:
$\operatorname{sen}\alpha = \cos\left(\frac{\pi}{2} - \alpha\right) \quad \forall \in \Re$

$$\cos 2x = \operatorname{sen}(x+\pi) \iff \cos 2x = \cos\left(\tfrac{\pi}{2} - (x+\pi)\right) \iff \cos 2x = \cos\left(-\tfrac{\pi}{2} - x\right) \iff$$

$$\iff \begin{cases} 2x = -\frac{\pi}{2} - x + 2k\pi \iff x = -\frac{\pi}{6} + 2k\frac{\pi}{3} \\ \quad \vee \qquad\qquad\qquad\qquad\qquad\qquad (k \in Z) \\ 2x = \frac{\pi}{2} + x + 2k\pi \iff x = \frac{\pi}{2} + 2k\pi \end{cases}$$

Ejercicio: Resolver en $(\Re,+,\cdot,\leq)$: $\operatorname{sen}(2x+\pi) = \operatorname{sen} 3x$ Respuesta: $x = \pi + 2k\pi \quad \vee \quad x = 2k\frac{\pi}{5}$

:**Ejemplo 3** Resolver en $(\Re,+,\cdot,\leq)$: $\operatorname{sen}^2 x - 5\operatorname{sen} x = \cos^2 x + 2$

$$\operatorname{sen}^2 x - 5\operatorname{sen} x = \cos^2 x + 2 \iff \operatorname{sen}^2 x - 5\operatorname{sen} x = 1 - \operatorname{sen}^2 x + 2 \iff 2\operatorname{sen}^2 x - 5\operatorname{sen} x - 3 = 0$$

Si denominamos $z = \operatorname{sen} x$ sustituyendo nos queda: $2z^2 - 5z - 3 = 0 \iff z = -\frac{1}{2} \quad \vee \quad z = 3$

$$\text{Como } \operatorname{sen} x = z \implies \begin{cases} \operatorname{sen} x = -\frac{1}{2} \iff \begin{cases} x = \frac{7\pi}{6} + 2k\pi \\ x = \frac{11\pi}{6} + 2k\pi \end{cases} \\ \operatorname{sen} x = 3 \quad \text{ec. con solución } \varnothing \text{ ya que } -1 \leq \operatorname{sen} x \leq 1 \ \ \forall x \in \Re \end{cases}$$

Ejercicio Resolver en $(\Re,+,\cdot,\leq)$: $2\cos^2 x - \cos x - 3 = 0$ Respuesta: $x = \pi + 2k\pi \quad (k \in Z)$

Ejemplo 4 $(\Re,+,\cdot,\leq)$: $\operatorname{sen} 2x + 4\cos^2 x = 3$

$\operatorname{sen} 2x + 4\cos^2 x = 3 \iff 2\operatorname{sen} x \cos x + 4\cos^2 x = 3$ Dividimos entre $\cos^2 x$ Observemos que $\forall x \in \Re$; $\cos x = 0$ x no es solución.

$$\frac{2\operatorname{sen} x \cos x}{\cos^2 x} + 4\frac{\cos^2 x}{\cos^2 x} = \frac{3}{\cos^2 x} \qquad \text{Como } \frac{1}{\cos^2 x} = 1 + \operatorname{tg}^2 x \implies \frac{3}{\cos^2 x} = 3 + 3\operatorname{tg}^2 x$$

Sustituyendo nos queda: $2\operatorname{tg} x + 4 = 3 + 3\operatorname{tg}^2 x \iff 3\operatorname{tg}^2 x - 2\operatorname{tg} x - 1 = 0$ si $\operatorname{tg} x = z$

$3z^2 - 2z - 1 = 0 \iff z = 1 \quad \vee \quad z = -\frac{1}{3}$

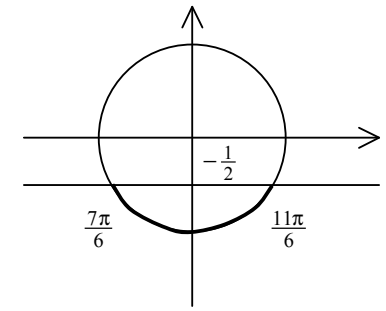
$$\text{Como tgx = z} \iff \begin{cases} \operatorname{tg} x = 1 \iff x = \frac{\pi}{4} + k\pi \\ \operatorname{tg} x = -\frac{1}{3} \iff x = \operatorname{Arc\,tg}\left(-\frac{1}{3}\right) + k\pi \end{cases}$$

Nota Denominamos $\text{Arc tg}\left(\frac{-1}{3}\right)$ al único real del intervalo $\left(-\frac{\pi}{2},\frac{\pi}{2}\right)$ cuya tangente vale $-\frac{1}{3}$

Ejercicio $(\Re,+,\cdot,\leq)$: $3\cos^2 x - \text{sen}^2 x - \text{sen}\, 2x = 0$ Respuesta: $x = \frac{\pi}{4} + k\pi \quad \vee \quad x = \text{Arc tg}\left(\frac{-3}{2}\right) + k\pi$

Ejemplo 5 Resolver en $[0,2\pi)$: $2\,\text{sen}\, x + 1 \leq 0$

$$2\,\text{sen}\, x + 1 \leq 0 \quad \Leftrightarrow \quad \text{sen}\, x \leq -\frac{1}{2} \quad \Leftrightarrow \quad \frac{7\pi}{6} \leq x \leq \frac{11\pi}{6}$$



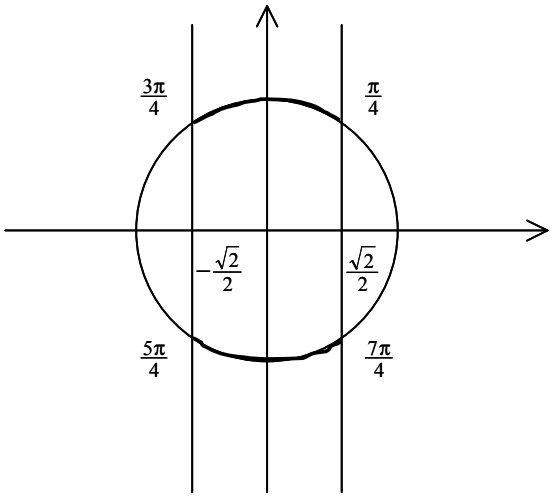
Ejercicio Resolver en $[0,2\pi)$: $2\cos x > \sqrt{3}$ Respuesta: $\left[0,\frac{\pi}{6}\right) \cup \left(\frac{11\pi}{6},0\right)$

Ejemplo 6 Resolver en $[0,2\pi)$: $2\cos^2 x - 1 \leq 0$

Si denominamos $z = \cos x$ sustituyendo nos queda: $2z^2 - 1 \leq 0$

$$2z^2 - 1 \leq 0 \quad \Leftrightarrow \quad -\frac{\sqrt{2}}{2} \leq z \leq \frac{\sqrt{2}}{2}$$

Entonces: $2\cos^2 x - 1 \leq 0 \quad \Leftrightarrow \quad -\frac{\sqrt{2}}{2} \leq \cos x \leq \frac{\sqrt{2}}{2} \quad \Leftrightarrow \quad \begin{cases} \frac{\pi}{4} \leq x \leq \frac{3\pi}{4} \\ \vee \\ \frac{5\pi}{4} \leq x \leq \frac{7\pi}{4} \end{cases}$



Ejercicio Resolver en $[0.2\pi)$: $\cos^2 x + 5\cos x + 3 > \text{sen}^2 x$ Respuesta: $\left(\frac{\pi}{3},\frac{5\pi}{3}\right)$

EJERCICIOS **REPARTIDO Nº 17**

I) Resolver en $(\Re,+,\cdot,\leq)$: **i)** $\cos x = -\frac{1}{2}$ **ii)** $tg(x-\frac{\pi}{2})=1$ **iii)** $\cos 3x = \cos(x+\frac{\pi}{4})$ **iv)** $tg(2x-\frac{\pi}{3}) = tg\,4x$

v) $\cos(2x+\frac{\pi}{6}) = \text{sen}\,4x$ **vi)** $\text{sen}\,3x + \cos 2x = 0$ **vii)** $2\cos^2 x - 3\cos x + 1 = 0$ **viii)** $2\,\text{sen}^2 x + 7\,\text{sen}\,x + 3 = 0$

ix) $4\cos^4 x + 5\,\text{sen}^2 x = 4$ **x)** $4\,\text{sen}^2(2x-\frac{\pi}{6}) - 8\cos(2x-\frac{\pi}{6}) = 4$ **xi)** $\text{sen}\,x - \cos x = \sqrt{3}$ **xii)** $\cos 2x - 2\,\text{sen}\,2x = 1$

xiii) $\cos(2x+\frac{\pi}{3}) + \cos(\frac{\pi}{3}-2x) = \frac{1}{2}$ **xiv)** $\log_{\text{sen}\,x}\cos^2 x = 2$ (resolver en $[0,\pi)$)

xv) $\log_{|\text{sen}\,x|}(\text{sen}^2 x - \cos^2 2x + 1) = 2$ **xvi)** $16^{\cos^2 x + 2sn^2 x} + 4^{2\cos^2 x} = 40$

II) Resolver en $[0,2\pi)$ las siguientes inecuaciones:

i) $2\,\text{sen}\,x - 1 > 0$ **ii)** $tg\,x > \sqrt{3}$ **iii)** $\left(\frac{1}{2}\right)^{4\cos x} \geq 4$

iv) $4\cos^2 x - 3 < 0$ **v)** $\text{sen}^2 x + 5\,\text{sen}\,x \geq \cos^2 x + 2$ **vi)** $\cos^2 x - 3\,\text{sen}^2 x \leq 0$ en $\left[0,\frac{\pi}{2}\right]$

vii) $2\,\text{sen}^2 x + (4-\sqrt{3})\,\text{sen}\,x - 2\sqrt{3} \geq 0$

III) Hallar la medida del lado del lado de un pentágono regular inscrito en una cfa. de 10cm. de radio.

NÚMERO COMPLEJO

Introducción

Recordemos que los números reales no cubren todas las necesidades algebraicas; así por ejemplo la ecuación $x^2+1=0$ tiene solución vacía en $(\Re,+,\cdot,\leq)$.

Ya en el siglo XVI se introdujo el símbolo $\sqrt{-1}$ como raíz de la ecuación anterior. Este símbolo mas tarde se sustituyó por i considerado como un número ficticio o "imaginario" que debía tratarse algebraicamente como un real, salvo que $i^2=-1$. Así la ecuación $x^2+1=0$ tiene raíces $\pm i$ y $x^2+1=(x-i)(x+i)$

Números del tipo $a+bi$ $(a,b\in\Re)$ fueron llamados números complejos y se utilizaban formalmente como si fuesen reales. Por ejemplo si $z=a+bi$ y $z'=a'+b'i$

$$z+z'=a+a'+(b+b')i$$

$$z.z'=(a+bi)(a'+b'i)=a.a'+ab'i+a'bi+bb'\overbrace{i^2}^{-1}=aa'-bb'+(a'b+ab')i$$

Este tratamiento carente de todo rigor duró casi trescientos años, hasta que a mediados del siglo XIX describieron a los números complejos que puede considerarse satisfactoria en la actualidad.

Observemos que si informalmente consideramos $a+bi$ como un número complejo, con $a,b\in\Re$ en definitiva lo estamos viendo como el par ordenado (a,b). y además los operamos:

$$(a,b)+(a',b')=(a+a',b+b')$$
$$(a,b).(a',b')=(aa'-bb',a'b+ab')$$

Lo cual da origen a la siguiente definición.

Definición

Si llamamos $C=\Re\times\Re$ y definimos:

1) $(a,b)=(a',b') \iff a=a' \wedge b=b'$

2) $\oplus: C\times C\to C;\ (a,a')\oplus(b+b')=(a+a',b+b')$

3) $\otimes: C\times C\to C;\ (a,b)\otimes(a',b')=(aa'-bb',ab'+a'b)$

A $(C,\oplus,\otimes)$ la denominamos **estructura de los números complejos**, o simplemente **números complejos**

Teorema

$(C,\oplus,\otimes)$ es un cuerpo conmutativo

Dem:

Es inmediato que $\oplus$ y $\otimes$ por como fueron definidas son operaciones en C. En consecuencia nos falta probar:

.

S_1) Asociativa $(a,b)\oplus[(a',b')\oplus(a'',b'')]=[(a,b)\oplus(a',b')]\oplus(a'',b'')$ $\forall(a,b),(a',b'),(a'',b'')\in C$

S_2) Conmutativa $(a,b)\oplus(a',b')=(a',b')\oplus(a,b)$ $\forall(a,b),(a',b')\in C$

S_3) Neutro $\exists(0,0)\in C;(a,b)\oplus(0,0)=(0,0)\oplus(a,b)=(a,b)$ $\forall(a,b)\in C$

S_4) Opuesto $\forall(a,b)\in C$ $\exists(-a,-b)\in C$; $(a,b)\oplus(-a,-b)=(-a,-b)\oplus(a,b)=(0,0)$

P_1) Asociativa $(a,b)\otimes[(a',b')\otimes(a'',b'')]=[(a,b)\otimes(a',b')]\otimes(a'',b'')$ $\forall(a,b),(a',b'),(a'',b'')\in C$

P_2) Conmutativa $(a,b)\otimes(a',b')=(a'.b')\otimes(a,b) \quad \forall(a,b),(a',b')\in C$

P_3) Neutro $\exists(1,0)\in C\,;\,(a,b)\otimes(1,0)=(1,0)\otimes(a,b)=(a,b) \quad \forall(a,b)\in C$

P_4) Inverso $\forall(a,b)\in C\,;\,(a,b)\neq(0,0) \;\; \exists \mathrm{inv}(a,b)\in C\,;\,(a,b)\otimes \mathrm{inv}(a,b)=\mathrm{inv}(a,b)\otimes(a,b)=(1,0)$

SP) Distributiva $(a,b)\otimes\left[(a',b')\oplus(a'',b'')\right]=\left[(a,b)\otimes(a',b')\right]\oplus\left[(a,b)\otimes(a'',b'')\right] \quad \forall(a,b),(a',b'),(a'',b'')\in C$

Demostremos alguna de ellas como ejemplo:

S_1) Asociativa

$$(a,b)\oplus\left[(a',b')\oplus(a'',b'')\right]=(a,b)\oplus(a'+a'',b'+b'')=(a+[a'+a''],b+[b'+b''])=_{\text{Asoc. en }(\Re,+)}$$
$$=([a+a']+a'',[b+b']+b'')=(a+a',b+b')\oplus(a'',b'')=\left[(a,b)\oplus(a',b')\right]\oplus(a'',b'')$$

P_4) Inverso A diferencia del opuesto aquí no es inmediato cual es el inverso de (a,b). Para hallarlo nos planteamos un par (x,y) incógnita que intentaremos hallar.

$$(a,b)\otimes(x,y)=(1,0) \quad\Leftrightarrow\quad (ax-by,ay+bx)=(1,0) \quad\Leftrightarrow\quad \begin{cases} ax-by=1 \\ ay+bx=0 \end{cases}$$

Si $a\neq 0$ como $ay+bx=0 \;\Rightarrow\; y=\dfrac{-bx}{a}$ sustituyendo en la primera igualdad nos queda: $ax-b.\left(\dfrac{-bx}{a}\right)=1$

$$\Rightarrow\; a^2x+b^2x=a \;\Rightarrow\; (a^2+b^2)x=a \;\Rightarrow\; x=\frac{a}{a^2+b^2} \quad \text{como } y=\frac{-bx}{a} \;\Rightarrow\; y=-\frac{b}{\cancel{a}}.\frac{\cancel{a}}{a^2+b^2}=\frac{-b}{a^2+b^2}$$

Por lo tanto si $a\neq 0$ encontramos el inverso de (a,b) que es $\left(\dfrac{a}{a^2+b^2},\dfrac{-b}{a^2+b^2}\right)$ Probemos que este resultado es válido también cuando $a=0$ (y $b\neq 0$)

$$(a,b)\otimes\left(\frac{a}{a^2+b^2},\frac{-b}{a^2+b^2}\right)=\left(a.\frac{a}{a^2+b^2}-b.\frac{-b}{a^2+b^2},a.\frac{-b}{a^2+b^2}+b.\frac{a}{a^2+b^2}\right)=\left(\frac{a^2+b^2}{a^2+b^2},0\right)=(1,0)$$

En consecuencia

$$\forall(a,b)\in C\,;\,(a,b)\neq(0,0) \;\; \exists\left(\frac{a}{a^2+b^2},\frac{-b}{a^2+b^2}\right)\in C \quad \text{tal que} \quad (a,b)\otimes\left(\frac{a}{a^2+b^2},\frac{-b}{a^2+b^2}\right)=(1,0)$$

Veamos : si $(a,b)\neq(0,0) \;\Rightarrow\; a\neq 0 \;\vee\; b\neq 0 \;\Rightarrow\; a^2+b^2\neq 0$

Observación

El teorema anterior muestra que $(C,\oplus,\otimes)$ satisface el axioma 1 visto en $(\Re,+,\cdot)$. Por consiguiente las propiedades deducidas exclusivamente del axioma 1 también son válidas para $(C,\oplus,\otimes)$; en particular la posibilidad de restar y dividir, las cancelativas de la suma y el producto, la propiedad de absorción y la ausencia de divisores de cero.

Los números complejos como una extensión de los reales

Consideramos $C_0 = \{(x,0) \in C\}$. Observemos que:

1) $C_0 \subseteq C$
2) $(x,0) \oplus (y,0) = (x+y, 0+0) = (x+y,0)$
3) $(x,0) \otimes (y,0) = (xy - 0.0, x.0 - 0.y) = (xy,0)$

Por lo tanto $\oplus$ y $\otimes$ son operaciones en C_0. En consecuencia $(C_0, \oplus, \otimes)$ es una subestructura de $(C, \oplus, \otimes)$. Además tengamos en cuenta que sumamos y multiplicamos los complejos de C_0 sumando y multiplicando sus primeras componentes

Observemos también: que ambos neutros $(0,0)$ y $(1,0) \in C_0$, $-(x,0) = (-x,0)$, $\text{inv}(x,0) = \left(\frac{1}{x},0\right)$

En otras palabras $(C_0, \oplus, \otimes)$ y $(\Re, +, \cdot)$ se comportan del mismo modo. Por este motivo habitualmente no hacemos distinción entre el real x y el complejo (x,0); escribiendo " x=(x,0) ".

¿Qué justifica formalmente identificar un real a un par de reales? Afinemos esta idea.

Definición

Consideramos: $(A, *)$ y $(B, \circ)$ dos estructuras algebraicas

$f : A \to B$ una función

Decimos que f es un **homomorfismo** $\Leftrightarrow \quad f(a) \circ f(b) = f(a * b) \quad \forall a, b \in A$

Si además f es biyectiva la denominamos **isomorfismo**.

Dos estructuras algebraicas se dice que son homomorfas (isomorfas) si existe un homomorfismo (isomorfismo) entre ellas.

Observación:

Sean $(A, *)$ y $(B, \circ)$ dos estructuras algebraicas isomorfas. ¿Porqué esta denominación? Intentemos responder.

Denominamos f al isomorfismo

Si $(A, *)$ es conmutativa $\Rightarrow \quad a * b = b * a \quad \forall a, b \in \Re \quad \Rightarrow \quad f(a * b) = f(b * a) \quad \forall a, b \in A \quad \Rightarrow$

$\Rightarrow \quad f(a) \circ f(b) = f(b) \circ f(a) \quad \forall f(a), f(b) \in B$ Como f es biyectiva y por lo tanto sobreyectiva todo elemento de B es imagen de uno de A. Entonces $x \circ y = y \circ x \quad \forall x, y \in B \quad \Rightarrow \quad (B, \circ)$ es conmutativa

Si n es neutro de $(A, *) \quad \Rightarrow \quad a * n = n * a = a \quad \forall a \in A \quad \Rightarrow \quad f(a * n) = f(n * a) = f(a) \quad \forall a \in A$

$\Rightarrow \quad f(a) \circ f(n) = f(n) \circ f(a) = f(a) \quad \forall f(a) \in B \quad \Rightarrow \quad x \circ f(n) = f(n) \circ x \quad \forall x \in B \quad \Rightarrow \quad f(n)$ es neutro de $(B, \circ)$

Análogamente puede probarse que toda propiedad que cumpla $(A, *)$ se trasmite a $(B, \circ)$ por f. También es posible demostrar que f^{-1} es un isomorfismo con lo cual toda propiedad que cumpla $(B, \circ)$ se trasmite a $(A, *)$. En consecuencia $(A, *)$ y $(B, \circ)$ tienen exactamente las mismas propiedades. En otras palabras dos estructuras isomorfas son algebraicamente idénticas.

En la práctica da lo mismo operar con $a \in A$ según $*$ que con $f(a) \in B$ según $\circ$. Por ese motivo suele identificarse a con f(a) anotando $a = f(a)$ a pesar de no ser el mismo elemento; pero se comporta algebraicamente como si lo fuera. También ambas operaciones ($*$ y $\circ$) se anotan con el mismo símbolo. Idénticas consideraciones son válidas para estructuras algebraicas mas "complicadas" (con mas de una operación, con una relación de orden).

Ejercicio Consideramos: $a \in \Re$ y $f : \Re \to \Re^+$; $f(x) = a^x$ Probar que f es un isomorfismo entre $(\Re,+)$ y $(\Re^+,\cdot)$

Teorema

H) $f : \Re \to C_0$; $f(x) = (x,0)$ T) f es un isomorfismo entre $(\Re,+,\cdot)$ y $(C_0,\oplus,\otimes)$

Dem: Debemos probar: i) f es sobreyectiva
ii) f es inyectiva
iii) $f(a+b) = f(a) \oplus f(b) \quad \forall a, b \in \Re$
iv) $f(a.b) = f(a) \otimes f(b) \quad \forall a, b \in \Re$

i) $\forall (x,0) \in C_0 \quad \exists x \in \Re ; f(x) = (x,0)$

ii) Si $x \neq x' \quad \Rightarrow \quad (x,0) \neq (x',0) \quad \Rightarrow \quad f(x) \neq f(x')$

iii) $f(a+b) = (a+b,0) = (a,0) \oplus (b,0) = f(a) \oplus f(b) \quad \forall a, b \in \Re$
iv) $f(a.b) = (a.b,0) = (a,0) \otimes (b,0) = f(a) \otimes f(b) \quad \forall a, b \in \Re$

Una vez demostrado este teorema podemos considerar a $\Re$ como a C_0. Teniendo en cuenta que $C_0 \subseteq C$ podemos considerar a C como una extensión de $\Re$.
A partir de este momento no haremos distinción entre los símbolos de suma de reales y suma de complejos; de la misma forma procederemos respecto al producto.

Hasta ahora manejamos las similitudes entre la estructura de los reales y la de los complejos. Analicemos ahora las diferencias.

La unidad imaginaria

Observemos que: $(0,1).(0,1) = (0.0 - 1.1 , 0.1 + 1.0) = (-1,0)$ Gracias al isomorfismo visto en el punto anterior podemos anotar x en lugar de (x,0). Si denominamos i al complejo (0,1) tenemos que

$$\boxed{i^2 = .-1}$$

Tenemos pues que en $(C,+,\cdot)$ la ecuación $x^2 + 1 = 0$ no tiene solución vacía como en $(\Re,+,\cdot)$ Con los números complejos no solamente ganamos que la mencionada ecuación tenga solución no vacía. En 1799 Gauss demostró que todo polinomio de coeficientes reales o complejos de grado n $(n \geq 1)$ tiene al menos una raíz compleja. Proposición que se conoce como teorema fundamental del álgebra. El lector interesado puede encontrar la demostración en "Álgebra Moderna" de Birkhoff-MacLane. Tal demostración excede los objetivos de este curso.

Ahora estamos en condiciones de vincular la idea del número complejo como un par ordenado de reales con la notación utilizada por los antiguos matemáticos.

Observemos primero que $b.i = (b,0).(0,1) = (b.0 - 0.1 , 0.0 + b.1) = (0,b) \quad \forall b \in \Re$

$\forall z = (a,b) \in C \quad (a,b) = (a,0) + (0,b) = a + b.i$ A la expresión $a + b.i$ la denominamos **forma binómica** de z

Imposibilidad de ordenar a los números complejos

Al desarrollar la teoría de los números reales no solamente introdujimos en el la suma y el producto; también lo dotamos de una relación de orden compatible con las operaciones. Lo cual fue hecho a través del axioma de orden.

Veamos si es posible establecer una proposición análoga en $(C,+,\cdot)$

Suponemos entonces que $\exists C^+ \subseteq C$ que verifica:

1) $\forall x \in C$ se cumple una y solo una de las siguientes proposiciones
i) $x \in C^+$ ii) $x = 0$ iii) $-x \in C^+$

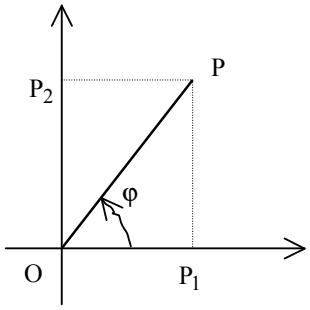
2) Si $x, y \in C^+ \Rightarrow \begin{cases} x+y \in C^+ \\ \wedge \\ x.y \in C^+ \end{cases}$

Como

$$i \neq 0 \begin{cases} i \in C^+ \Rightarrow_{2)} i^2 = i.i = -1 \in C^+ \Rightarrow_{2)} (-1).(-1) = 1 \in C^+ \text{ como } -1 \in C^+ \text{ tenemos una contradición} \\ \text{ó} \\ -i \in C^+ \Rightarrow (-i)^2 = i^2 = -1 \in C^+ \Rightarrow (-1).(-1) = 1 \in C^+ \text{ como } -1 \in C^+ \text{ tenemos una contradicción} \end{cases}$$

Esto prueba que es imposible ordenar a los complejos con las características que lo fueron los reales.

Representación gráfica



Como un complejo es en definitiva un par ordenado de reales, si en un plano establecemos un sistema de coordenadas cartesianas (en este caso ortogonales) a cada complejo z = (a,b) le podemos asociar un y solo un punto P del plano; justamente el de coordenadas (a,b), que denominamos **afijo** de z.
Establecemos de esta forma una biyección entre C y los puntos del plano

En consecuencia determinar el complejo z es equivalente a determinar el punto P. Y esto puede hacerse no solamente mediante las coordenadas cartesianas sino también dando la distancia de O a P y la medida del ángulo $\overleftarrow{OP_1OP}$

Si $d(O,P) = \rho$ y la medida de $\overleftarrow{OP_1OP} = \varphi$; el punto P y por lo tanto el complejo z está determinado por el par de reales ρ, φ. Anotamos $z = \rho \langle \varphi$ y decimos que es su **forma polar**. ρ se denomina **módulo** de z y φ su **argumento**

Puede demostrarse que si $z = (a,b)$ y $z = \rho\langle\varphi$ se cumple:

$$\begin{cases} a = \rho.\cos\varphi \\ b = \rho.\operatorname{sen}\varphi \end{cases}$$

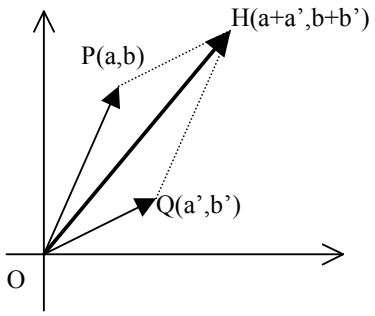
$$\rho = \sqrt{a^2 + b^2}$$
si $a \neq 0$ $\operatorname{tg}\varphi = \frac{b}{a}$
si $a = 0$ y $b > 0 \Rightarrow \varphi = \frac{\pi}{2}$
si $a = 0$ y $b < 0 \Rightarrow \varphi = \frac{3\pi}{2}$

También puede probarse:

$$\rho\langle\varphi = \rho'\langle\varphi' \Leftrightarrow \begin{cases} \rho = \rho' \\ \varphi = \varphi' + 2k\pi \quad (k \in Z) \end{cases}$$

Otra interpretación geométrica útil es asociar al complejo z = (a,b) el vector $\overrightarrow{OP}$ con P(a,b).

Consideraciones geométricas permiten afirmar que el vector asociado a la suma de dos complejos es la suma de los vectores asociados



Teorema

$$\rho\langle\varphi \,.\, \rho'\langle\varphi' \;=\; \rho.\rho'\langle\varphi+\varphi'$$

Dem:

$$\rho\langle\varphi \,.\, \rho'\langle\varphi' \;=\; (\rho\cos\varphi, \rho\,\text{sen}\,\varphi)\,.\,(\rho'\cos\varphi', \rho'\,\text{sen}\,\varphi') \;=\; (\rho.\rho'\cos\varphi\cos\varphi' - \rho.\rho'\,\text{sen}\,\varphi\,\text{sen}\,\varphi', \rho.\rho'\cos\varphi\,\text{sen}\,\varphi' + \rho.\rho'\,\text{sen}\,\varphi\cos\varphi') =$$

$$= \left(\rho.\rho'\left[\cos\varphi\cos\varphi' - \text{sen}\,\varphi\,\text{sen}\,\varphi'\right], \rho.\rho'\left[\cos\varphi\,\text{sen}\,\varphi' - \text{sen}\,\varphi\cos\varphi'\right]\right) \;=\; (\rho.\rho'\cos(\varphi+\varphi'), \rho.\rho'\,\text{sen}(\varphi+\varphi')) \;=\; \rho.\rho'\langle\varphi+\varphi'$$

Ejercicio Consideramos: $z = \rho\langle\varphi$, $w = 1\langle\frac{\pi}{4}$ y $t = 2\langle\frac{\pi}{4}$ Calcular: z.w , z.t y z.i Interpretar geométricamente

Generalice su observación.

Ejercicio Si $z = \rho\langle\varphi \quad (z \neq 0)$ probar que: $\frac{1}{z} \;=\; \frac{1}{\rho}\langle -\varphi$

Potencia de exponente entero

Definición

Consideramos: $\alpha \in C$ y $z \in Z$

Si $\alpha = 0$ y $z > 0$ definimos $\alpha^z = 0^z = 0$

Si $\alpha \neq 0$ y $z = 0$ definimos $\alpha^z = \alpha^0 = 1$

Si $\alpha \neq 0$ y $z > 0$ definimos $\alpha^z = \alpha.\alpha^{z-1}$

Si $\alpha \neq 0$ y $z < 0$ definimos $\alpha^z = \dfrac{1}{\alpha^{-z}}$

Observación: La definición hecha es idéntica a la realizada en los reales. Como además ya vimos que $(C,+,\cdot)$ y $(\Re,+,\cdot)$ son ambos cuerpos conmutativos; la potencia de base compleja y exponente entero cumple idénticas propiedades algebraicas que la potencia de base real y exponente entero. Es innecesario mencionar que carece de sentido cualquier planteo sobre la variación de la potencia recién definida.

Teorema

$$H)\begin{cases}\alpha \in C\,;\, \alpha = \rho\langle\varphi \\ m \in Z\end{cases} \qquad T)\;\; \alpha^m \;=\; \rho^m\langle m\varphi$$

Dem:

Si $m \geq 0 \Rightarrow m \in N$ Tiene sentido entonces intentar una demostración por I.C.

1º paso

$$\left.\begin{array}{l} \alpha^0 = 1 \\ \rho^0 \langle 0.\varphi = 1 \langle 0 = 1 \end{array}\right\} \Rightarrow \alpha^0 = \rho^0 \langle 0.\varphi$$

2º paso

H) $\alpha^h = \rho^h \langle h.\varphi$ T) $\alpha^{h+1} = \rho^{h+1} \langle (h+1).\varphi$

$$\alpha^{h+1} = \alpha.\alpha^h = \rho\langle\varphi \,.\, \rho^h \langle h.\varphi = \rho.\rho^h \langle \varphi + h\varphi = \rho^{h+1} \langle (h+1).\varphi$$

Si $m < 0 \Rightarrow m = -n \;;\; n \in N \Rightarrow \alpha^m = \alpha^{-n} = \dfrac{1}{\alpha^n} = \dfrac{1}{(\rho\langle\varphi)^n} = \dfrac{1}{\rho^n \langle n\varphi} = \rho^{-n}\langle -n.\varphi = \rho^m \langle m\varphi$

Nota:

Si $z = \rho \langle \varphi \Rightarrow z = (\rho\cos\varphi, \rho \operatorname{sen}\varphi) = \rho(\cos\varphi + i\operatorname{sen}\varphi)$

Por otra parte $z^n = \rho^n \langle n.\varphi = (\rho^n \cos n.\varphi, \rho^n \operatorname{sen} n.\varphi) = \rho^n(\cos n.\varphi + i \operatorname{sen} n.\varphi)$

Entonces:

$$\boxed{[\rho(\cos\varphi + i.\operatorname{sen}\varphi)]^n = \rho^n(\cos n.\varphi + i \operatorname{sen} n.\varphi)}$$

Para $\rho = 1$ la fórmula anterior nos queda:

$$\boxed{(\cos\varphi + i.\operatorname{sen}\varphi)^n = \cos n.\varphi + i.\operatorname{sen} n\varphi \qquad \forall n \in Z}$$

Conocida como fórmula de De-Moivre.

Si aplicamos esta fórmula para n = 2 tenemos:

$$(\cos\varphi + i.\operatorname{sen}\varphi)^2 = \cos 2\varphi + i.\operatorname{sen} 2\varphi \Rightarrow \cos^2\varphi + 2\cos\varphi.\operatorname{sen}\varphi.i + i^2 \operatorname{sen}^2\varphi = \cos 2\varphi + i.\operatorname{sen} 2\varphi \Rightarrow$$

$$\Rightarrow \cos^2\varphi - \operatorname{sen}^2\varphi + 2\cos\varphi.\operatorname{sen}\varphi.i = \cos 2\varphi + i \operatorname{sen} 2\varphi \Rightarrow \begin{cases} \cos 2\varphi = \cos^2\varphi - \operatorname{sen}^2\varphi \\ \operatorname{sen} 2\varphi = 2\cos\varphi.\operatorname{sen}\varphi \end{cases}$$

Fórmulas vistas oportunamente cuando tratamos trigonometría.

Ejercicio: Obtener fórmulas para $\cos 3\varphi$ y $\operatorname{sen} 3\varphi$ en función de $\cos\varphi$ y $\operatorname{sen}\varphi$

Radicación

Consideramos $z \in C$, $n \in N$; $n \geq 2$ Definir: $\sqrt[n]{z} = w \Leftrightarrow w^n = z$ resulta la opción mas previsible. Antes de adoptar tal definición debemos discutir acerca de su existencia.

Si $z = \rho\langle\varphi$ y $w = r\langle\delta$ $w^n = z \Leftrightarrow r^n\langle n\delta = \rho\langle\varphi \Leftrightarrow \begin{cases} r^n = \rho \\ n\delta = \varphi + 2k\pi \end{cases} \Leftrightarrow \begin{cases} r = \sqrt[n]{\rho} \\ \delta = \dfrac{\varphi + 2k\pi}{n} \end{cases}$

Por lo tanto:

$$\forall z = \rho\langle\varphi \in C \text{ y } \forall n \in N\,;\, n \geq 2 \quad \exists w = \sqrt[n]{\rho}\,\langle\, \frac{\varphi + 2k\pi}{n} \quad (k \in Z) \quad \text{tal que } w^n = z$$

Estamos ahora sí en condiciones de asumir como definición de raíz n-esima la planteada al comienzo. Y además obtuvimos un procedimiento para calcularla en forma polar.

Ejemplo: Calculemos $\sqrt[3]{i}$ Para ello tengamos en cuenta que $i = 1\langle\frac{\pi}{2}$

$$\sqrt[3]{i} = \sqrt[3]{1\langle\frac{\pi}{2}} = \sqrt[3]{1}\left\langle\frac{\frac{\pi}{2}+2k\pi}{3}\right. = 1\left\langle\frac{\pi}{6}+\frac{2k\pi}{3}\right. \qquad (k \in Z) \qquad \text{Si llamamos } w_k = 1\langle\frac{\pi}{6}+\frac{2k\pi}{3} \text{ tendríamos}$$

aparentemente tantas raíces cúbicas de i como enteros hay. Todas ellas con módulo 1 y argumento $\alpha_k = \frac{\pi}{6}+\frac{2k\pi}{3}$

Observemos que: $w_0 = 1\langle\frac{\pi}{6}$, $w_1 = 1\langle\frac{5\pi}{6}$, $w_2 = 1\langle\frac{3\pi}{2}$, $w_3 = 1\langle\frac{13\pi}{6} = 1\langle\frac{\pi}{6}+2\pi = w_0$

$w_4 = 1\langle\frac{17\pi}{6} = 1\langle\frac{5\pi}{6}+2\pi = w_1$, ...

Parece que solamente hay tres raíces cúbicas de i: w_0, w_1 y w_2 ya que aparentemente

$w_0 = w_3 = w_6 = ...$

$w_1 = w_4 = w_7 = ...$

$w_2 = w_5 = w_8 = ...$

Intentemos generalizar y justificar esta observación.

Consideramos $z = \rho\langle\varphi$, $n \in N$; $n \geq 2$ vimos que $w_k = \sqrt[n]{\rho}\left\langle\frac{\varphi+2k\pi}{n}\right.$ es una raíz n-esima de z $\forall k \in Z$

Todos los w_k tienen el mismo módulo $\left(\sqrt[n]{\rho}\right)$ y distinto argumento $\left(\alpha_k = \frac{\varphi+2k\pi}{n}\right)$.

Probemos que z admite n y solo n raíces n-esimas; a saber: $w_0, w_1, w_3, ..., w_{n-1}$ Para ello debemos probar:

1) $\forall w_h, w_j$ con $0 \leq h < n$, $0 \leq j < n$ si $h \neq j \Rightarrow w_h \neq w_j$

2) $\forall k \in Z \quad \exists r \in Z ; 0 \leq r < n$ tal que : $w_k = w_r$

1) $\alpha_h = \frac{\varphi+2h\pi}{n}$, $\alpha_j = \frac{\varphi+2j\pi}{n} \Rightarrow \alpha_h - \alpha_j = \frac{2(h-j)\pi}{n}$

$$\left.\begin{array}{l} 0 \leq h < n \\ 0 \leq j < n \Rightarrow -n < -j \leq 0 \end{array}\right\} \Rightarrow -n < h-j < n \Rightarrow -1 < \frac{h-j}{n} < 1 \qquad \text{como } h \neq j \qquad \frac{h-j}{n} \neq 0 \Rightarrow$$

$$\Rightarrow \frac{h-j}{n} \notin Z \Rightarrow \alpha_h - \alpha_j = \frac{2(h-j)\pi}{n} \neq \overset{\bullet}{2\pi} \Rightarrow w_h \neq w_j$$

2) $\forall k \in Z$ realizamos la división entera

k	n
r	q

Entonces: $\begin{cases} k = nq + r \\ 0 \le r < n \end{cases} \Rightarrow \alpha_k = \dfrac{\varphi + 2k\pi}{n} = \dfrac{\varphi + 2(nq+r)\pi}{n} = \dfrac{\varphi + 2r\pi}{n} + 2q\pi = \alpha_r + 2q\pi \Rightarrow$

$\Rightarrow \quad w_k = w_r \quad \text{con} \quad 0 \le r < n$

Observación

Como las n raíces n-esimas de $z = \rho\langle\varphi$ todos ellas tienen el mismo módulo; sus afijos pertenecen a una circunferencia de centro en el origen de coordenadas y radio $\sqrt[n]{\rho}$.

Además la diferencia entre dos argumentos consecutivos $\alpha_{j+1} - \alpha_j = \dfrac{\varphi + 2(j+1)\pi}{n} - \dfrac{\varphi + 2j\pi}{n} = \dfrac{2\pi}{n}$

Por lo tanto los afijos de las n raíces n-esimas de z son los vértices de un polígono regular de n lados inscrito en una circunferencia de centro en el origen y radio la raíz n-esima del módulo de z.

Ejercicio Hallar y representar gráficamente las cinco raíces quintas de 1.

Raíz cuadrada de un complejo en forma binómica

Consideramos $z = a + b.i$ Queremos hallar las dos raíces cuadradas de z sin pasar por la forma polar.

$w = x + y.i$ es raíz cuadrada de z $\Leftrightarrow \quad w^2 = z \quad \Leftrightarrow \quad (x + y.i)^2 = a + b.i \quad \Leftrightarrow \quad x^2 + 2xy.i + y^2 i^2 = a + bi \quad \Leftrightarrow$

$\Leftrightarrow \quad x^2 - y^2 + 2xy.i = a + b.i \quad \Leftrightarrow \quad \begin{cases} x^2 - y^2 = a \quad \Rightarrow \quad (x^2 - y^2)^2 = a^2 \quad \Rightarrow \quad x^4 - 2.x^2y^2 + y^4 = a^2 \\ 2xy = b \quad \Rightarrow \quad 4.x^2y^2 = b^2 \end{cases}$

Sumando tenemos: $\underbrace{x^4 + 2.x^2y^2 + y^4}_{(x^2+y^2)^2} = \underbrace{a^2 + b^2}_{\rho \text{ módulo de z}} \quad \Rightarrow \quad (x^2 + y^2)^2 = \rho^2 \quad \Rightarrow \quad x^2 + y^2 = \rho$

$\begin{cases} x^2 + y^2 = \rho \\ x^2 - y^2 = a \end{cases} \Rightarrow \begin{cases} 2x^2 = \rho + a \quad \Rightarrow \quad x = \pm\sqrt{\dfrac{\rho + a}{2}} \\ 2y^2 = \rho - a \quad \Rightarrow \quad y = \pm\sqrt{\dfrac{\rho - a}{2}} \end{cases}$

Por lo tanto:

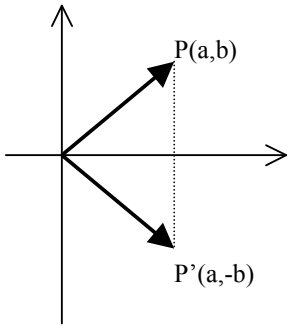
$$\boxed{\sqrt{a + bi} = \pm\sqrt{\frac{\rho + a}{2}} \pm \sqrt{\frac{\rho - a}{2}}\, i}$$

Observemos que haciendo todas las combinaciones de signo posibles tendríamos cuatro raíces cuadradas, lo cual es imposible. Ocurre que al elevar al cuadrado se introdujeron raíces. ¿Cómo averiguar cuales son las verdaderas? Recordemos que: 2xy = b Por lo tanto si b > 0 x e y tienen el mismo signo; en cambio si b < 0 x e y tienen distinto signo Ejercicio: Hallar i) $\sqrt{3 + 4i}$ ii) $\sqrt{5 - 12i}$

Conjugado de un complejo

Definición

Consideramos $z = (a, b) \in C$. Llamamos **conjugado** de z (anotamos $\bar{z}$) al complejo (a,–b)



Observaciones : 1) Si $z = a + b.i \quad \Rightarrow \quad \bar{z} = a - b.i$

2) $z + \bar{z} = 2a = 2\,\mathrm{Re}(z)$

3) $z.\bar{z} = (a + bi)(a - bi) = a^2 + b^2 = |z|^2$

4) El afijo de $\bar{z}$ es el simétrico con respecto a Ox del afijo de z.

Nota

Si $z=(a,b)$ decimos que a es su parte real (anotamos Re(z) = a) y b su parte imaginaria (anotamos Im(z) = b)
Al módulo de z lo escribimos $|z|$.

Teorema

1) Si $z=\rho\langle\varphi \Rightarrow \bar{z}=\rho\langle -\varphi$

2) $\overline{(\bar{z})}=z \qquad \forall z\in C$

3) $z=\bar{z} \Leftrightarrow z\in C_0$

4) $\overline{x+y}=\bar{x}+\bar{y} \qquad \forall x,y\in C$

5) $\overline{x.y}=\bar{x}.\bar{y} \qquad \forall x,y\in C$

6) $\overline{x^n}=(\bar{x})^n \qquad \forall x\in C \ \ \forall n\in N$ excluyendo $x=n=0$.

Dem 4)

Si $x=a+bi$ e $y=a'+b'i \Rightarrow x+y=a+a'+(b+b')i \Rightarrow \overline{x+y}=a+a'-(b+b').i$

$\left.\begin{array}{l}\bar{x}=a-bi\\ \bar{y}=a'-b'i\end{array}\right\} \Rightarrow \bar{x}+\bar{y}=a-bi+a'-b'i=a+a'-(b+b')i$ Entonces $\overline{x+y}=\bar{x}+\bar{y}$

Teorema

Consideramos : $f:C\to C\,;\, f(x)=a_n x^n+a_{n-1}x^{n-1}+.....+a_1x+a_0$ con $a_n,a_{n-1},.....,a_1,a_0\in C_0$
$\alpha\in C$

Si $f(\alpha)=0 \Rightarrow f(\bar{\alpha})=0$

Dem

$f(\alpha)=a_n\alpha^n+a_{n-1}\alpha^{n-1}+.....+a_1\alpha+a_0=0 \Rightarrow \overline{a_n\alpha^n+a_{n-1}\alpha^{n-1}+.....+a_1\alpha+a_0}=\bar{0} \Rightarrow$

$\overline{a_n\alpha^n}+\overline{a_{n-1}\alpha^{n-1}}+.....+\overline{a_1\alpha}+\overline{a_0}=0 \Rightarrow \underbrace{\overline{a_n}}_{a_n}.\overline{\alpha^n}+\underbrace{\overline{a_{n-1}}}_{a_{n-1}}\overline{\alpha^{n-1}}+.....+\underbrace{\overline{a_1}}_{a_1}.\bar{\alpha}+\underbrace{\overline{a_0}}_{a_0}=0 \Rightarrow$

$\Rightarrow a_n.(\bar{\alpha})^n+a_{n-1}.(\bar{\alpha})^{n-1}+.....+a_1.\bar{\alpha}+a_0=0 \Rightarrow f(\bar{\alpha})=0$

En un lenguaje menos cuidadoso; hemos demostrado que un polinomio de coeficientes reales si acepta una raíz compleja necesariamente acepta su conjugada. Lo que trae como consecuencia que los polinomios de coeficientes reales presentan sus raíces complejas de a pares. Así si una función polinómica P de coeficientes reales acepta raíz 2+3i necesariamente acepta también la raíz 2-3i.
Que las raíces complejas de los polinomios de coeficientes reales vengan de a dos implica entre otras cosas que los polinomios de coeficientes reales y grado impar aceptan al menos una raíz real.

Ejemplo 1 Hallar la parte real y la parte imaginaria de $z=\dfrac{5+3i}{1-2i}$

La idea consiste en multiplicar y dividir por el conjugado del denominador.

$z=\dfrac{5+3i}{1-2i}=\dfrac{(5+3i)(1+2i)}{(1-2i)(1+2i)}=\dfrac{5+3i+10i+6i^2}{1^2+2^2}=\dfrac{-1+13i}{5}=-\dfrac{1}{5}+\dfrac{13}{5}i \Rightarrow \text{Re}(z)=-\frac{1}{5} \ , \ \text{Im}(z)=\frac{13}{5}$

Ejercicio Hallar la parte real y la parte imaginaria de $w=\dfrac{1+i}{3+i}$

Ejemplo 2 Determinar una función polinómica de coeficientes reales del menor grado posible que admita como raíces $\alpha = 3$, $\beta = 1+i$ y tenga coeficiente principal 1.

Denominamos f a la función buscada. Como f es de coeficientes reales y $f(\beta) = 0 \Rightarrow f(\bar{\beta}) = 0$
Por lo tanto f admite al menos como raíces $\alpha = 3$, $\beta = 1+i \wedge \bar{\beta} = 1-i$ teniendo en cuenta además que el coeficiente principal es 1 tenemos:

$$f(x) = 1.(x-\alpha).(x-\beta).(x-\bar{\beta}) = (x-3).(x^2-(\beta+\bar{\beta})x+\beta.\bar{\beta}) = (x-3).(x^2-2\,Re(\beta)x+|\beta|^2) = (x-3)(x^2-2x+2)$$

Ejer Hallar una función polinómica de coeficientes reales y del menor grado posible que tenga raíces: 2 , 1+2i y 3+i

---

EJERCICIOS **REPARTIDO Nº 18**

I) Expresar en forma polar: $(-\sqrt{3},1)$, $(1,-1)$, $(1,\sqrt{3})$, $(-\sqrt{3},1)$

II) Dados: $z_1 = 4\langle\frac{\pi}{6}$ $z_2 = 2\langle\frac{5\pi}{4}$ $z_3 = 3\langle 0$ $z_4 = 2\langle\frac{\pi}{2}$ $z_5 = 4\langle\pi$ $z_6 = 6\langle\frac{3\pi}{2}$ $z_7 = 3\langle\frac{11\pi}{6}$ y $z_8 = 4\langle\frac{13\pi}{6}$

i) Representarlos gráficamente. **ii)** Expresarlos en forma binómica. **iii)** Calcular $z_1.z_2$, $(z_1)^5$, $\frac{z_5}{z_7}$, $\frac{z_4.z_6}{z_8}$

III) Hallar la parte real y la parte imaginaria de:

i) $2.(\sqrt{2}-3i).(\sqrt{2}+3i)-\frac{2-i}{4-6i}$ **ii)** $\frac{1}{1-i}+\frac{1}{2-i}+\frac{1}{1-2i}$ **iii)** $\left(-\sqrt{3}+\sqrt{3}.i\right)^6$ **iv)** $\frac{(1+i)^9}{(1-i)^7}$

IV) Consideramos $z = \frac{3-2mi}{4-3i}$ $(m \in \Re)$ Hallar m para que: **i)** $Re(z) = 0$ **ii)** $z \in C_0$

V) Hallar los complejos cuyo cuadrado sea igual a su conjugado.

VI) Sea $w = (1+i).m^2-(3+i).m+2-12i$ $(m \in \Re)$ Hallar los valores de m para los cuales:

i) Re(w) = 0. **ii)** El afijo de w pertenece al cuarto cuadrante. **iii)** $w \in C_0$ **iv)** $Arg(w) = \frac{\pi}{4}$

VII) Calcular: $\sqrt{2i}$, $\sqrt{-8i}$, $\sqrt{3-4i}$, $\sqrt{-8+6i}$, $\sqrt{-3-4i}$, $\sqrt{2-2\sqrt{3}.i}$, $\sqrt[4]{-1}$, $\sqrt[5]{1-i}$, $\sqrt[3]{-2+2i}$, $\sqrt[5]{\frac{-32}{i}}$ y $\sqrt[3]{\frac{1-i}{1+i}}$

VIII) Resolver en $(C,+,\cdot)$: **1)** $(x+1)^2 = -49$ **2)** $x^4+16=0$ **3)** $x^8-1=0$ **4)** $x^3-25=0$
5) $x^4-30x^2+289=0$ **6)** $x^2-(2+i)x+7i-1=0$ **7)** $x^2-(3-2i)x+5-5i=0$ **8)** $x^4-3x^2+4=0$

IX) 1) Hallar $z_1, z_2 \in C$; $z_1^3 = z_2^3 = -27$ $Re(z_1) \neq 0$ y $Re(z_2) \neq 0$

2) Determinar $m, a \in \Re$ para que la ecuación $x^2-2mx+4m+a=0$ acepte raíces $\alpha = z_1+z_2$ y $\beta = z_1 z_2$

X) Resolver en $(C,+,\cdot)$ **1)** $2x^3 - 19x^2 + 58x - 51 = 0$ sabiendo que admite raíz 4+i

2) $x^4 + 6x^3 + 33x^2 - 306x - 74 = 0$ sabiendo que admite raíz -5 - 7i

3) $x^3 - (3-i)x^2 + (7-2i)x - 5 - 5i = 0$ sabiendo que admite raíz i.

XI) 1) Hallar $p, q \in \Re$ de modo que la ecuación $x^4 + 2x^3 + 3x^2 + px + q = 0$ admita a 1+i como raíz.

2) Para los valores hallados resolver completamente la ecuación en $(C,+,\cdot)$.

3) Construir una función polinómica de cuarto grado y coeficiente principal 1 cuyas raíces sean los cuadrados de las raíces de la ecuación de la parte 1).

XII) Representar gráficamente el conjunto de los complejos z que cumplen:

1) $|z| = 2$ **2)** $\bar{z} = z^{-1}$ **3)** $z + \bar{z} = 1$ **4)** $z^2 \in C_0$ **5)** $|z| \leq 2$ **6)** $|z| < 2$

XIII) Siendo $z_1 = 5 + 6i$; hallar $z_2 \in C$ para que los afijos de 0 z_1 y z_2 sean los vértices de un triángulo Equilátero.

XIV) Hallar los complejos z_1, z_2 y z_3 cuyos afijos son vértices de un triángulo equilátero con centro en el origen sabiendo además que: $z_1.z_2.z_3 = 8i$ Representar el triángulo y calcular su perímetro.

XV) Con $z_1 = 2 + 5i$; hallar los complejos z_2 y z_3 para que los afijos de $0, z_1, z_2, z_3$ sean los vértices de un cuadrado.

XVI) 1) Consideramos el complejo $w = \sqrt{2}\langle\frac{\pi}{4}$ Para cada $z \in C$ denominamos $z_1 = w.z$, $z_2 = w.z_1$, $z_3 = w.z_2$

Estudiar la naturaleza del cuadrilátero de vértices los afijos de $0, z, z_1$ y z_2

2) Determinar los complejos z para los cuales el área del mencionado cuadrilátero vale 6.

XVII) Resolver en $(C,+,\cdot)$: $1 + x + x^2 + x^3 + x^4 + x^5 + x^6 = 0$

(Sugerencia: recordar que $a^n - b^n = (a-b).(a^{n-1} + a^{n-2}.b + ...+ b^{n-1})$)

XXI) 1) Hallar los complejos z tal que $z^3 \in C_0$ Representarlos gráficamente.

2) De los complejos de módulo constante ρ que verifican 1), determinar su módulo para que el área del polígono convexo formado por sus afijos valga $6.\sqrt{3}$.

3) Sea $P \in \Re[x]$, y coeficiente principal 1 del menor grado posible que acepta por raíces los complejos hallados en 2) parte real positiva. Resolver en $(\Re,+,\cdot,\leq)$: $\log_{x-2} P(x) \leq 3$

91