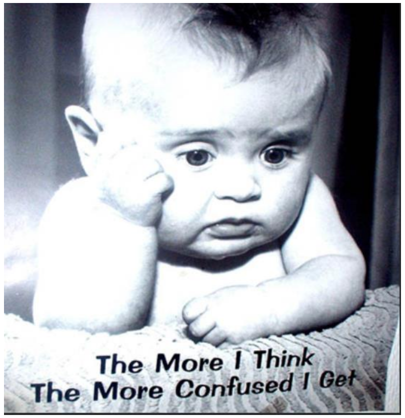


Introducción a las matemáticas

Madrid, 01/09/2020

Introducción: Las matemáticas antes y después de Galois

31 de mayo de 1832

No existía el concepto de algebra abstracta como hoy en día, era difícil tratar

Encajan las piezas del puzle, se axiomatiza desde entonces los conjuntos, operaciones y sus propiedades

Grupos, Anillos, Cuerpos, espacios vectoriales, álgebras, …
Se intenta aplicar a todos los conjuntos y no conjuntos matemáticos

ÍNDICE

¿Qué es un conjunto?

Todas las matemáticas se basan en conjuntos. Conjuntos de números, de polinomios, de funciones, de figuras geométricas, …

Pero, ¿qué es un conjunto?

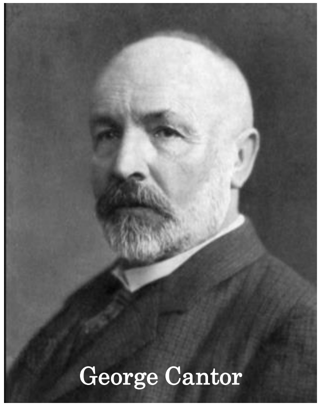
Un guardia pregunta a cada visitante de una isla: ¿Para qué viene usted aquí?

Si el viajero contesta la verdad, todo va bien y no hacen nada. Pero si contesta con una mentira es ahorcado allí mismo.

Un día, un visitante contestó: ¡He venido aquí para ser ahorcado!

Los guardias se quedaron perplejos. Si no ahorcasen al sujeto, éste habría mentido, y por ello debería ser ahorcado. Pero si lo ahorcasen, habría dicho la verdad, y no debería ser ajusticiado.

El Quijote, Miguel de Cervantes

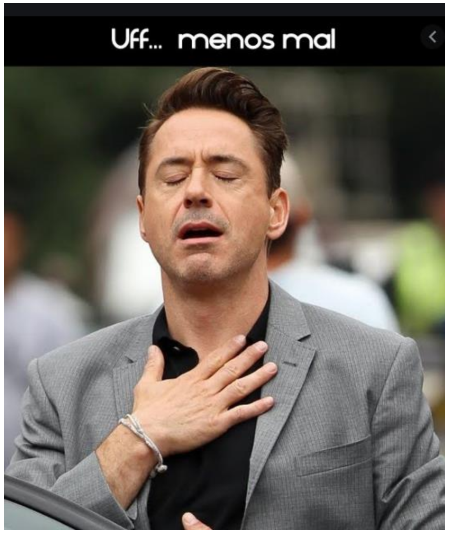


Creador de la teoría de conjuntos

¿Este visitante a que conjunto pertenece, al de los ahorcados o al de los no ahorcados?

¿Qué es un conjunto?

Para resolver este entuerto, en el siglo XIX, Zermelo fijo los axiomas que determinan que una serie de elementos para formar un conjunto



- Axioma de elección (ó Lema de Zorn): Para una familia de conjuntos siempre podemos elegir un elemento de cada conjunto.
- Axioma de las partes: Para todo conjunto A, existe el conjunto de parte… refiere a todos los conjuntos que podemos … tos de A
- Axioma … todos A y B conjuntos, existe el conjunto … A ó $x \in B\}$.
- Axioma … Dos conjuntos son iguales si tienen los mism…

- Axioma d… Existe un conjunto sin elementos
- Axioma d… conjuntos X e Y, existe el conjunto de dos elementos $A = \{X, Y\}$
- Axioma d… un conjunto infinito.
- Axioma de especificación: Si $\varphi(v)$ es una fórmula de lenguaje de primer orden, $\forall\ X\ conjunto, \exists\ Y\ conjunto\ tales\ que\ sus\ elementos\ son\ los\ de\ X\ que\ cumplen\ Y$
- Axioma de regularidad: $\forall\ X\ conjunto, \exists\ Y\ tal\ que\ X \cap Y = \emptyset$
- Axioma de reemplazo: Si A es un conjunto y f una función en A, entonces f(A) es un conjunto llamado imagen de A.

www.vimat.info

¿Qué es un conjunto?

A finales del siglo XIX y después de las paradojas antes vistas, aparecieron dos corrientes:

CORRIENTE ACEPTADA MAYORITARIAMENTE

Intuicionismo

- No creían en el infinito
- Difícil admitir los números reales
- Muchos problemas difíciles de explicar

Formalismo

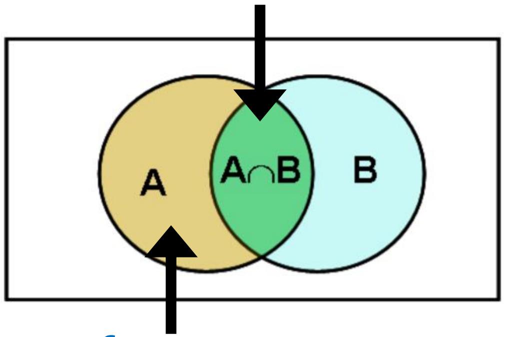
- Creían en el infinito
- Admitían que toda teoría matemática debe asentarse en axiomas, incluso la aritmética
- Toda afirmación debe ser demostrada a partir de los axiomas. Incluso $2+2=4$

- Cuestionó todo lo que proponía Hilbert puesto que no estaba seguro de que todo se pudiese demostrar en base a axiomas.
- Estudio la consistencia de los sistemas de axiomas
- Llego a la conclusión de que no todo es demostrable

Operaciones con conjuntos

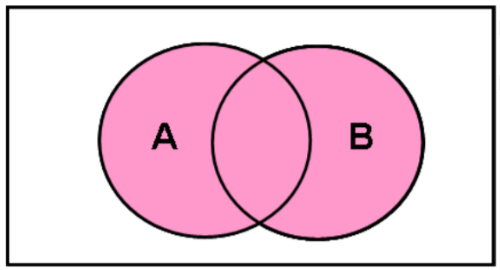
Una vez ya tenemos definidos los conjuntos ya podemos operar con ellos

Intersección $A \cap B$

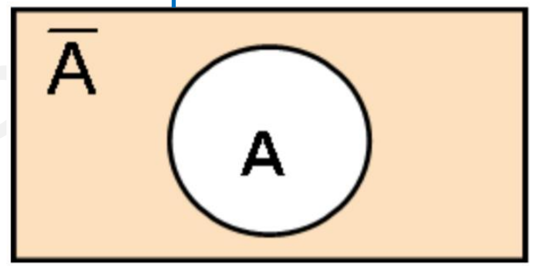


Diferencia $A - B$

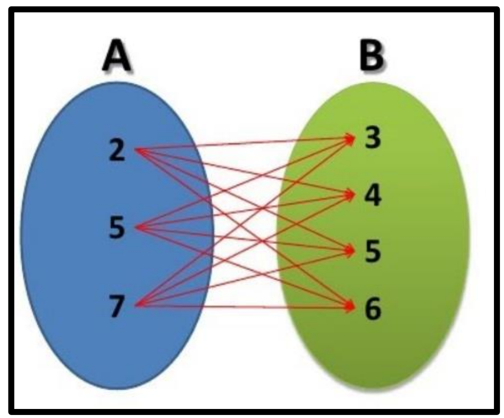
Unión



Complementario



Producto cartesiano:
$AxB = \{(a, b) : a \in A \ y \ b \in B\}$



Relación

<u>Definición</u>: Una **relación R** sobre un conjunto A es un subconjunto del producto cartesiano AxA .

Tipos de relaciones:

<u>Relaciones Reflexivas</u>.- Cuando un elemento está relacio-nado consigo mismo . Si $\forall a \in A,\ (a, a) \in R,$

<u>Relaciones Simétricas</u>.- Una relación es simétrica si $\forall(a,b) \in R$ *se cumple que el par ordenado* $(b, a) \in R$

<u>Relaciones transitivas</u>.- Una relación es transitiva si $\forall(a,b)$ *y* $(b,c) \in R$*, se cumple que el par ordenado* $(a,c) \in R$

<u>Relaciones antisimétricas</u>.- Una relación es antisimétrica cuando si $\forall(a;b)$ *y* $(b;a) \in R$*, se cumple que* $a = b$

Relación de orden

<u>Definición</u>: Una **relación es de orden** si cumple las propiedades reflexiva, antisimétrica y transitiva.

<u>Ejemplos</u>:

- "Una caja más grande que otra"
- "Una caja más grande o igual que otra"
- "Una caja con mayor volumen que otra"
- "Una caja con mayor o igual volumen que otra"
- "Una caja sin tapa con mayor o igual área de la base que otra"

Relación de orden

Definición: Una **relación es de orden** si cumple las propiedades reflexiva, antisimétrica y transitiva.

Ejemplos:

- "Una caja más grande que otra"
- "Una caja más grande o igual que otra"
- "Una caja con mayor volumen que otra"
- "Una caja con mayor o igual volumen que otra"
- "Una caja sin tapa con mayor o igual área de la base que otra"

Relación de equivalencia

<u>Definición</u>: Una **relación es de equivalencia si cumple** las propiedades reflexiva, simétrica y transitiva.

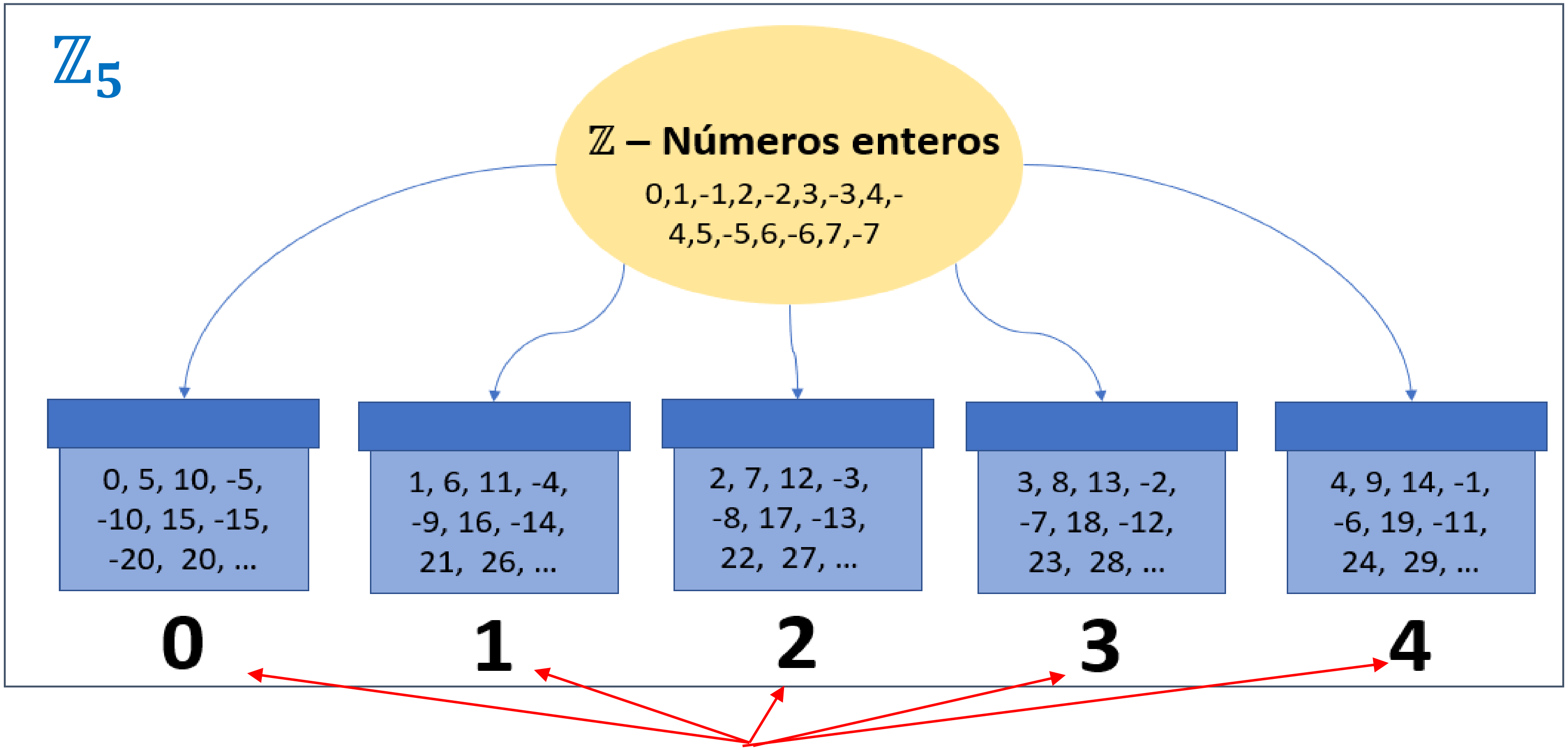
<u>Ejemplos</u>: En el conjunto de personas de la tierra:

- "El parentesco directo"
- "El partido al que votan"
- "Tener el mismo sexo"

Relación de equivalencia

<u>Definición</u>: Una **relación es de equivalencia si cumple** las propiedades reflexiva, simétrica y transitiva.

Números congruentes: $a \equiv b(mod n) \Leftrightarrow a - b \equiv 0(mod n)$ →*Relación de equivalencia*



Clases de equivalencia: $[0]_5 = 0, [1]_5 = 1, \ldots$

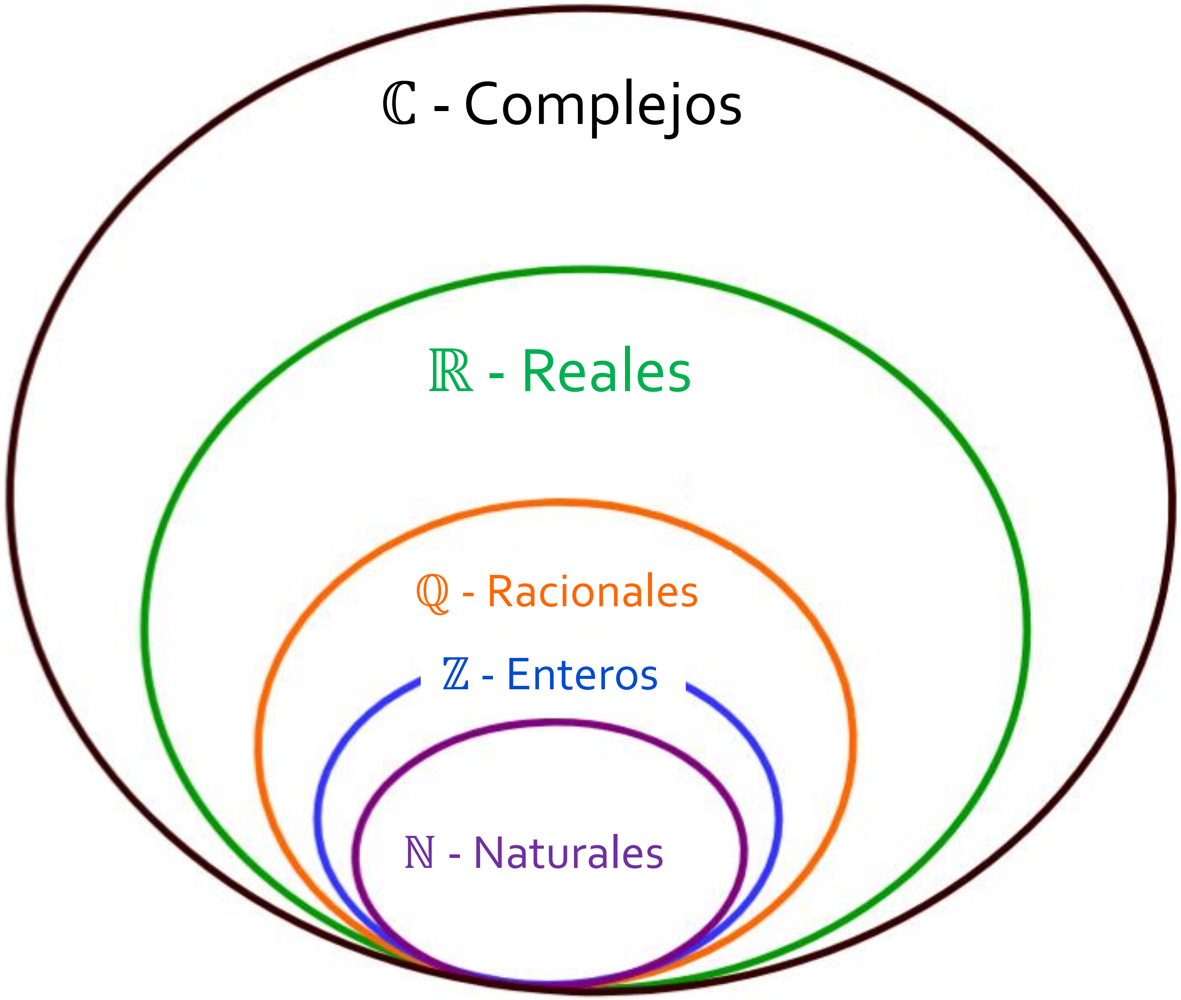
www.vimat.info

Estructuras algebraicas

A continuación mencionaremos las estructuras básicas más típicas

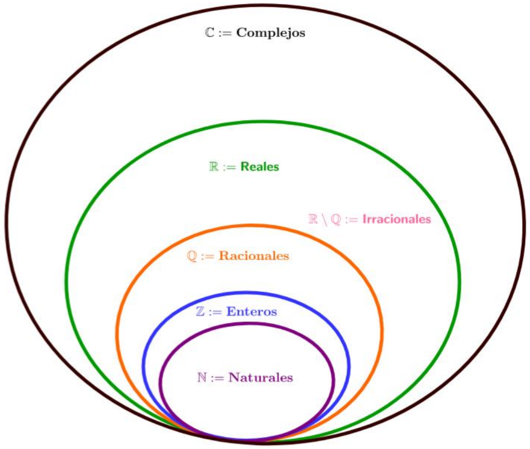
	Grupo (G)	Anillo (A)	Cuerpo (K)	Espacio Vectorial (V)
Número de leyes de composición	1 Interna (+)	2 Internas (+,·)	2 Internas (+,·)	1 interna (+) 1 externa ($*_k$)
Propiedades	**Operación (+)** Asociativa Elemento neutro Elemento simétrico	**Operación (+)** (A,+) grupo abeliano **Operación (·)** $(A^*,\cdot$ $)$ asociativa **Operaciones (+,·)** Distributiva	**Anillo** **+** **Inverso para (·)**	**Operación (+)** (V,+) grupo abeliano **Operaciones** $(+,\cdot_k)$ Distributiva re a la suma de vectores: • Distributiva respecto a la suma de escalares: • Asociativa respecto al producto de escalares y vectores: • Existe elemento neutro escalar:

Conjuntos numéricos



www.vimat.info

Conjuntos numéricos: Números naturales ℕ



Informalmente: Los números de contar
¿y con el 0?
Siempre hay un mínimo en cualquier conjunto.

Formalmente: Axiomas de Peano

i. El **0** está en el conjunto ℕ, (es decir, hay un número menor que todo el resto, para lo cual tiene que haber una relación de orden total que luego veremos)

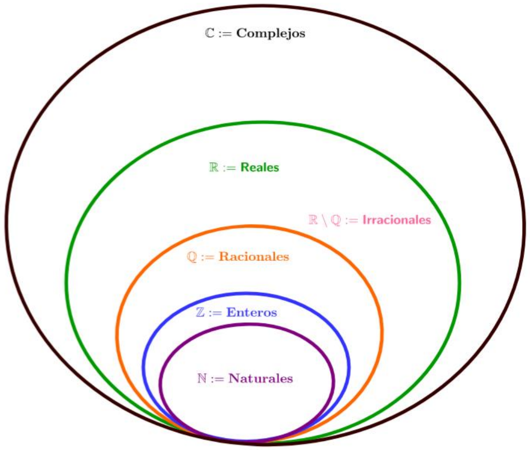
ii. Todo número natural $n \in \mathbb{N}$ tiene un **sucesor** o siguiente en el conjunto ℕ, al que denotaremos con $n^+, s(n)$ o $\sigma(n)$.

iii. El **0 no es sucesor** de ningún número natural

iv. Si hay dos números naturales n y m con el mismo sucesor, entonces n y m son el mismo número natural

v. Axioma de recurrencia (o inducción). Si el 0 pertenece a un subconjunto de números naturales S, y dado un elemento cualquiera $n \in S$, el sucesor también pertenece a dicho conjunto $s(n) \in S$ entonces $S = \mathbb{N}$.

Conjuntos numéricos: Números enteros $\mathbb{Z}$



Informalmente: Los números naturales y los negativos

Objetivo: Tener el opuesto dentro del conjunto, para que sean grupo (recordemos que matemáticamente restar se define como sumar el opuesto, y no al revés)

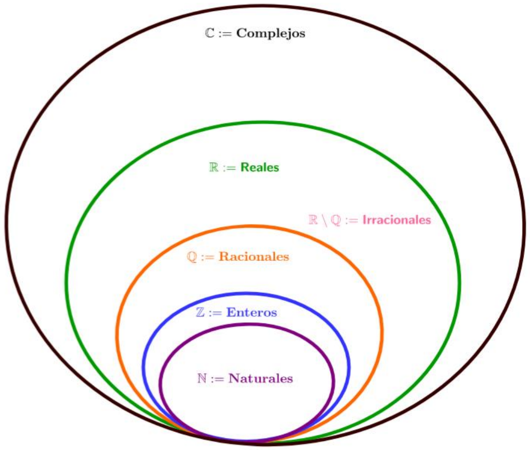
Formalmente: En $\mathbb{N}$x$\mathbb{N}$(producto cartesiano) se define la relación (de equivalencia)

$$(a, b) \sim (c, d) \Leftrightarrow a + d = b + c$$

Dicho de otra forma, los pares de números naturales que al restarlos resultan el mismo número natural.

Clase de equivalencia $[(1,2)] = \{(1,2), (2,3), (3,4), \dots \dots\}$ *, lo denominaremos* 1
Clase de equivalencia $[(1,3)] = \{(1,3), (2,4), (-3,-1), \dots \dots\}$ *, lo denominaremos* 2
Clase de equivalencia $[(2,1)] = \{(-1,-2), (4,3), (6,5), \dots \dots\}$*, lo denominaremos* -1

Conjuntos numéricos: Números racionales



Informalmente: Las fracciones, es decir, la división de dos enteros o decimales exactos o periódicos

Objetivo: Tener el inverso dentro del conjunto, para que sean grupo (recordemos que matemáticamente dividir se define como multiplicar por el inverso, y no al revés)

Formalmente: En $\mathbb{Z}x\mathbb{Z}$ (producto cartesiano) se define la relación (de equivalencia)

$$(a, b) \sim (c, d) \Leftrightarrow a \cdot d = b \cdot c$$

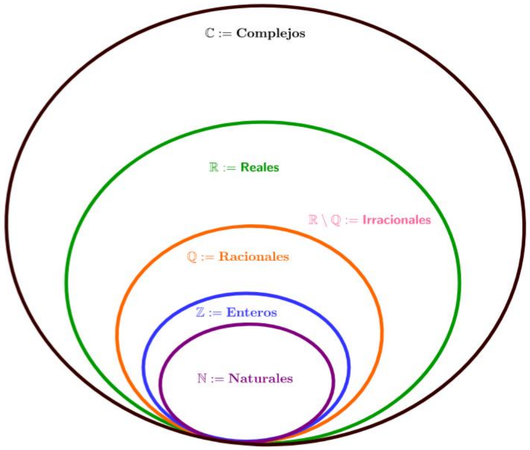
Dicho de otra forma, los pares de números enteros que forman una fracción equivalente a una dada.

Clase de equivalencia $[(1,2)] = \{(1,2), (2,4), (3,6), \dots \dots\}$ *, lo denominaremos* $\frac{1}{2}$

Clase de equivalencia $[(1,3)] = \{(1,3), (2,6), (-3,-9), \dots \dots\}$ *, lo denominaremos* $\frac{1}{3}$

Clase de equivalencia $[(-2,3)] = \{(-2,3), (4,-6), (4,3), \dots \dots\}$*, lo denominaremos* $-\frac{2}{3}$

Conjuntos numéricos: Números reales



Informalmente: Incluimos las raíces y los decimales no periódicos

Objetivo: Cada conjunto de números racionales debe tener un supremo en ese conjunto. (por simetría ínfimo). Estamos completando $\mathbb{Q}$.

$$A = \{x \in \mathbb{Q} : x^2 < 2\}$$

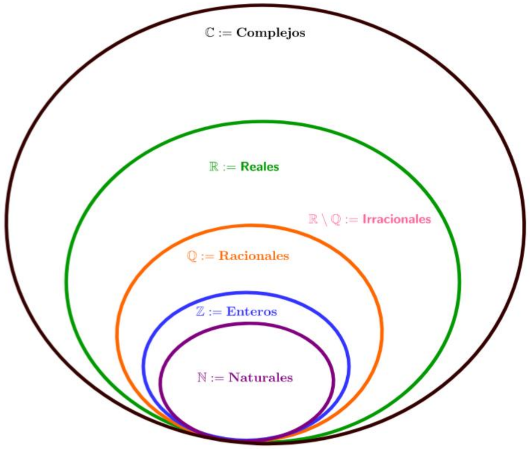
Formalmente: Sucesiones de Cauchy, Una sucesión $\{a_n\}$ tal que $a_n \in \mathbb{Q}$, es de Cauchy si $\forall \epsilon > 0 \; \exists \, n_0 \in \mathbb{N} \; tal \; que \; si \; n, m > n_0 \;\; \Rightarrow \; |a_n - a_m| < \epsilon$

Se definen también las suma y producto de sucesiones de Cauchy, a través de las que se comprueba que cumplen todas las propiedades de los axiomas mencionados.

Dos sucesiones de Cauchy $\{a_n\} \; y \; \{b\}$ se consideran **equivalentes** $(\sim)$ si $\lim_{n\to\infty}(a_n - b_n) = 0$.

Las clases de equivalencia $S \, / \sim$ donde
S: *"Conjunto de sucesiones de Cauchy de números racionales"*

Conjuntos numéricos: Números complejos



Informalmente: Los números $a + bi$, donde $a, b \in \mathbb{R}$ y

$$i = \sqrt{-1}$$

Objetivo: Cada polinomio con coeficientes reales tenga solución, y sea un número

Formalmente: En $\mathbb{R}x\mathbb{R}$ se definen las dos operaciones $(+\ y\ \cdot\ )$:

$$(a, b) + (c, d) = (a + c, b + d)$$

$$(a, b) \cdot (c, d) = (ab - cd, ad + bc)$$

Este conjunto será $\mathbb{C}$: $(\mathbb{R}x\mathbb{R}, +, \cdot)$ y será cuerpo, y algebraicamente cerrado

Nomenclatura matemática

- **Axioma**: afirmación que se da por demostrada y se toma como base para el desarrollo de teorías complejas.
- **Postulado**: afirmación que se da por demostrada pero no es tan evidente como el axioma
- **Conjetura**: Enunciado que se cree correcto y en muchas ocasiones se toma como base para futuras demostraciones pero que todavía no ha sido demostrado.
- **Proposición**: Enunciado demostrable que se usa como base para demostrar enunciados más complejos.
- **Lema**: Proposición demostrada que se usa como base para demostrar enunciados más complejos
- **Teorema**: Enunciado demostrable de dificultad elevada y para lo que se requiere de axiomas, postulados, proposiciones y lemas.
- **Corolario**: Conclusión que se obtiene de los anteriores y que tiene utilidad práctica.

¿Qué es demostrar?

- ¿Cuándo podemos decir que algo está demostrado?

  Hipótesis $\Rightarrow$ Tesis

  No tesis $\Rightarrow$ No hipótesis

- ¿Cualquier enunciado puede ser demostrado?. **NO**

  -Teorema de indecibilidad (David Hilbert)

  -Teoremas de incompletitud (Kurt Gödel)

Tipos de demostraciones

1. **Principio de inducción**: Es un método de probar proposiciones que dependen de un número n (que normalmente está dentro de un conjunto o subconjunto de los números naturales, pero que es posible que sean un número entero a partir de un número fijo).
   - Se demuestra para un valor dado, al que llamaremos $\boldsymbol{P_1}$
   - Suponemos que se cumple para P_n, a lo que llamaremos hipótesis de inducción, y utilizándolo debemos demostrar que se cumple para P_{n+1}

2. **Reducción al absurdo**: este método de demostración consiste en suponer una hipotética la veracidad o falsedad, y se llega a una contradicción lógica, un absurdo, con lo cual se concluye que la hipótesis de partida ha de ser falsa.

Tipos de demostraciones

3. **Por contraposición**: Esta regla se infiere una sentencia condicional a partir de su contraposición. En otras palabras, la conclusión «si A, entonces B» se extrae de la premisa simple «si no B, entonces no A.

4. **Doble implicación**: Para probar que dos condiciones P_1 *y* P_2 son equivalentes, se puede demostrar que $P_1 \Rightarrow P_2$ *y* $P_2 \Rightarrow P_1$, y con ello, estarán demostradas ambas.

5. **Conjunto contenido en otro**: Para demostrar que un conjunto A está contenido en otro B se procede a coger un elemento cualquiera de A y se procederá a ver que está contenido en B. Así, si un elemento cualquiera de A está en B, significa que todos lo están y será $A \subseteq B$.

6. **Conjuntos iguales**: Para probar que un conjunto está contenido en otro, se utiliza frecuentemente la doble inclusión, es decir, que el conjunto A está contenido en B y viceversa, así, serán iguales.