Apuntes de lenguaje matemático

Texto e ilustraciones. Antoni Espinosa. 2013.

Retratos de personajes: Wikipedia

Introducción

Estos son unos apuntes personales de la asignatura «Lenguaje matematico, conjuntos y números» del grado de matemáticas de la UNED. La motivación de los mismos es que me ayuden a refrescarme en la aridez del estudio, de ahí los dibujitos, curiosidades y en ocasiones un tono ligeramente jocoso. También, ya que hago el esfuerzo, pienso en un posible lector. El texto no ha sido revisado adecuadamente, son unos apuntes, un boceto.

Consejos antes de empezar

Si uno no tiene mucha experiencia previa en el estudio de las matemáticas estas pueden representar un reto, puesto que su asimilación va más allá de la memorización de información y la comprensión de los conceptos. Buscando en foros he encontrado algunos consejos que me han parecido útiles para el estudio de las Matemáticas. A partir de estos he confeccionado un pequeño guión que creo que puede ser de utilidad.

Cómo estudiar matemáticas

- Leer el tema e intentar resolver los ejercicios con la teoría a mano.
- Estudiar los ejercicios resueltos (mejor si se han hecho).
- Fijarse en los métodos o teoremas utilizados.
- Comprender las demostraciones de los teoremas repitiéndolos como si fueran ejercicios.
- Puesto que los teoremas son como herramientas, conviene hacerse un esquema de los pasos, entendiéndolos de forma que se pudiera repetir. Si no se comprende un paso puede ser útil buscar en otros libros.
- Memorizar los teoremas, sus demostraciones razonadas y las definiciones.Los dibujos pueden ser útiles.
- Comprobar si podemos repetir las demostraciones, explicarlas o aplicar los teoremas en ejercicios.

Índice

1. Capítulo uno. Lógica matemática

"Logic is the begining of wisdom not the end"

Spock. Star Treck II (1982)

1.1. Lógica proposicional

Una **proposición simple** o atómica es la que describe una propiedad de un objeto a la que podemos dar sin ambiguedad un valor de cierto o falso. Son ejemplos de proposiciones simples: *la luna es un satélite, el cubo de tres es nueve.*

Una **proposición compuesta** o molecular es aquella que se obtiene a partir de otras simples. Son ejemplos de esta: *si llueve se mojan las calles.* Compuesta por las preposiciones simples, *llueve* y se *mojan las calles.*

Las proposiciones se expresan con letras minúsculas: p, q, r, etc.

1.2. Negación y conectores lógicos

1.2.1. Negación

Suele expresarse con los siguentes signos: $\neg p$,$-p$,$\bar{p}$,p'. El valor de la preposición negada es el contrario de la original. Hay que recordar que $\neg p \wedge q \neq \neg(p \wedge q)$, hay que vigilar donde se coloca la negación.

1.2.2. Disyunción

Se expresa con las formas: $p \vee q$, $p + q$, $p \cup q$. Es cierta cuando alguna de las dos proposiciones es cierta. No corresponde a nuestro "o" lingüístico[1].

p	q	$p \vee q$
0	0	0
0	1	1
1	0	1
1	1	1

Cuadro 1: Tabla de la verdad de la disyunción

Figura 1: Mueres si te falla el corazón o el cerebro

1.2.3. Disyunción excluyente

Se nota como $p \otimes q$. Resulta cierta cuando es cierta una de las dos preposiciones. Sería parecido a el "o" lingüístico, un ejemplo sería: Bebo agua o vino.

[1] Existe un chiste en el que en un departamento de matemáticas le preguntan a uno que pasa: -Oiga ¿este ascensor sube o baja?- y responde -Si-.

p	q	$p \otimes q$
0	0	0
0	1	1
1	0	1
1	1	0

Cuadro 2: Tabla de la verdad de la disyunción excluyente

1.2.4. Conjunción

Se expresa con las formas: $p \wedge q$, $p \times q$, $p \cap q$. Solo es cierta cuando todas las proposiciones son ciertas.

p	q	$p \wedge q$
0	0	0
0	1	0
1	0	0
1	1	1

Cuadro 3: Tabla de la verdad de la conjunción

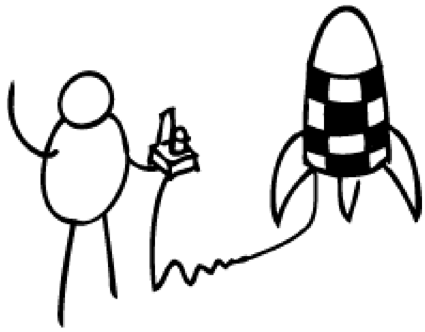


Figura 2: Para lanzar el cohete: quita el seguro y aprieta el botón

1.2.5. Condicional

El condicional, o la implicación, conecta dos proposiciones de forma que si p entonces q. Se expresa de esta forma: $p \rightarrow q$. Cabe señalar que, en general, la notación $\Rightarrow$se reserva para cuando el condicional es cierto. Por ejemplo; «si n es divisible por 2 entonces es impar» podría expresarse como $p \rightarrow q$ siendo falsa. Para la expresión: «si n es divisible por 2 entonces es par» utilizariamos $p \Rightarrow q$ (este sería también un ejemplo de bicondicional que veremos a continuación). El condicional solo es falso cuando en antecedente es cierto y el conseguente es falso, como puede verse en la tabla de la verdad.

p	q	$p \rightarrow q$
0	0	1
0	1	1
1	0	0
1	1	1

Cuadro 4: Tabla de la verdad del condicional

Figura 3: Si te disparan mueres
Pero que estes muerto no implica que te dispararan

Razon necesaria y razón suficiente En la expresión $p \to q$ tenemos que q es la razón necesaria y p la razón suficiente. fijándolos en la anterior figura, si q es «estar muerto» es el aspecto necesario para que la expresión sea cierta. Si se da p que sería «que te disparen» es razón suficiente para tan fatal desenlace. Así, tal como reza la tabla de la verdad, el único caso falso sería el de disparo y no defunción.

1.2.6. Bicondicional

Es el que expresamos como «sí y solo sí». En este caso hablaríamos de razón necesaria y suficiente, de hecho, notamos el bicondicional como una doble flecha: $p \longleftrightarrow q$[2]. Tal y como comentamos en el apartado del condicional, el símbolo $\Longleftrightarrow$se reserva para los casos ciertos. la doble implicación solo es cierta si las dos proposiciones tienen el mismo valor.

p	q	$p \longleftrightarrow q$
0	0	1
0	1	0
1	0	0
1	1	1

Cuadro 5: Tabla de la verdad del bicondicional

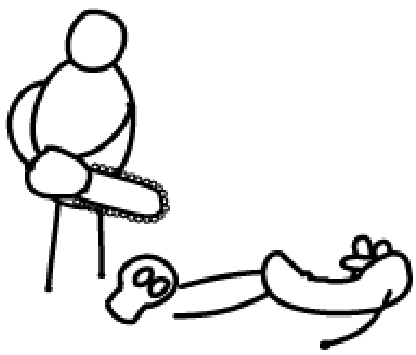


Figura 4: Un zombie muere si y solo si le cortas la cabeza

1.2.7. Miscelánea

Otras formas de condicional A partir del condicional $p \to q$ podemos expresar otros:

[2]También pueden encontrarse expresiones como «p sii q» que son equivalentes.

1. $q \to p$. Condicional recíproco
2. $\neg p \to \neg q$. Condicional contrario
3. $\neg q \to \neg p$. Condicional contrarecíproco

Conectores que actuan sobre una proposición Dada una proposición, podrémos contruir tantos conectores diferentes como no spermita la tabla de la verdad. En el caso de una proposición seran 2^2 en el caso de dos proposiciones 2^4. Y es interesante notar que los valores de la tabla corresponden a los números vinarios del 0 al 3 en el primer caso y del 0 al 15 en el segundo.

p	**q**	p0	p1	p2	p3	p4	p5	p6	p7	p8	p9	p10	p11	p12	p13	p14	p15
0	**0**	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
0	**1**	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
1	**0**	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
1	**1**	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1

Cuadro 6: Conectores posibles para dos proposiciones

Así, el conector p1 tiene el mismo valor que $p \wedge q$ y p14 podría corresponder a $\neg(p \wedge q)$.

Otros

Tautología. Es la proposición cuya tabla siempre tiene valor de verdad. Se denota como 1.

Contradicción. Es la proposición cuya tabla siempre tiene valor de falsedad. Se denota como 0.

1.3. Leyes lógicas

Doble negación $\neg\neg a \iff a$. La negación de una negación es una afirmación.

p	¬p	¬¬p
0	1	0
1	0	1

Cuadro 7: Tabla de la verdad de doble negación

Figura 5: Grouxo y la triple negación

«No puedo decir que no esté en desacuerdo con usted» (Groucho).

Si p = «Puedo decir que estoy en acuerdo con usted», entonces la primera expresión podía ser $\neg\neg\neg p \iff \neg p$. Así que, asumiendo que la frase no usa negaciones expletivas, parece que no ha convencido a Grouxo.

1. Leyes de simplificación

   a) $p \vee p \iff p$

   b) $p \wedge p \iff p$

c) $p \to p \Longleftrightarrow p$
d) $p \longleftrightarrow p \Longleftrightarrow p$

2. Ley del tercio exclusivo

a) $p \vee \neg p \Longleftrightarrow 1$

3. Ley de la contradicción

a) $p \wedge \neg p \Longleftrightarrow 0$

4. Leyes de identidad (equivalencias)

a) $p \vee 0 \Longleftrightarrow p$, $p \vee 1 \Longleftrightarrow 1$
b) $p \wedge 1 \Longleftrightarrow p$, $p \wedge 0 \Longleftrightarrow 0$
c) $1 \to p \Longleftrightarrow p$

5. Leyes conmutativas

a) $p \vee q \Longleftrightarrow q \vee p$
b) $p \wedge q \Longleftrightarrow q \wedge p$
c) $p \longleftrightarrow q \Longleftrightarrow q \longleftrightarrow p$

6. Leyes de Morgan

a) $\neg(p \vee q) \Longleftrightarrow \neg p \wedge \neg q$
    1) La negación de una disyunción es la conjunción de negaciones.
b) $\neg(p \wedge q) \Longleftrightarrow \neg p \vee \neg q$
    1) La negación de una conjunción es la disyunción de negaciones.

Figura 6: Augustus De Morgan (1806 - 1871)
Aparte del padre de las anteriores leyes, también fue el primer presidente de la Sociedad Matematica de Londres y tutor de Ada Lovelace; la primera programadora de la historia.

1. Leyes del condicional

a) $p \to q \Longleftrightarrow \neg p \vee q$
b) $p \to q \Longleftrightarrow \neg(p \wedge \neg q)$
c) $p \to q \Longleftrightarrow p \longleftrightarrow (p \wedge q)$
d) $p \to q \Longleftrightarrow q \longleftrightarrow (p \vee q)$

2. Ley bicondicional

a) $p \longleftrightarrow q \Longleftrightarrow (p \to q) \wedge (q \to p)$

3. Ley de reducción al absurdo

   a) $\neg p \to (q \wedge \neg q) \Longleftrightarrow p$

4. Leyes de transposición

   a) $p \to q \Longleftrightarrow \neg q \to \neg p$
   b) $p \longleftrightarrow q \Longleftrightarrow \neg pp \vee 0 \Longleftrightarrow p, \longleftrightarrow \neg q$

5. Leyes asociativas

   a) $(p \vee q) \vee r \Longleftrightarrow p \vee (q \vee r)$
   b) $(p \wedge q) \wedge r \Longleftrightarrow p \wedge (q \wedge r)$
   c) $(p \longleftrightarrow q) \longleftrightarrow r \Longleftrightarrow p \longleftrightarrow (q \longleftrightarrow r)$

6. Leyes distributivas

   a) $p \vee (q \wedge r) \Longleftrightarrow (p \vee q) \wedge (p \vee r)$
   b) $p \wedge (q \vee r) \Longleftrightarrow (p \wedge q) \vee (p \wedge r)$
   c) $p \to (q \vee r) \Longleftrightarrow (p \to q) \vee (p \to r)$
   d) $p \to (q \wedge r) \Longleftrightarrow (p \to q) \wedge (p \to r)$

7. Leyes de simplificación del condicional

   a) $p \wedge q \Rightarrow p$
   b) $p \Rightarrow p \vee q$

8. Leyes de inferencia

   a) $\neg p \wedge (p \vee q) \Rightarrow q$
   b) $p \wedge (\neg p \vee \neg q) \Rightarrow \neg q$

9. Ley modus ponendo ponens[3]

   a) $(p \to q) \wedge p \Rightarrow q$

10. Ley modus tollendo tollens[4]

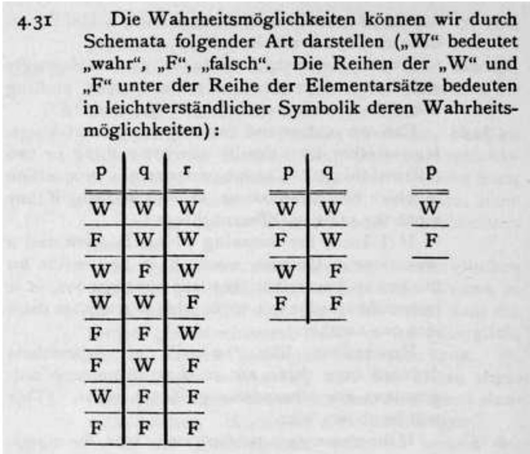
    a) $(p \to q) \wedge \neg q \Rightarrow \neg p$

1.4. Validación de proposiciones

1.4.1. Construcción de la tabla de la verdad

Es una tabla que indica el valor de verdad de las combinaciones de las proposiciones de una proposición compuesta. Aunque ya hay antecedentes en el S.XIX, la foma actual de debe a Wittgenstein, que la introdujo en su *Tractatus Logico-Philosophicus*[5].

[3] modo que afirmando afirma
[4] modo que negando niega
[5] http://es.wikipedia.org/wiki/Tabla_de_verdad



4.31 Die Wahrheitsmöglichkeiten können wir durch Schemata folgender Art darstellen („W" bedeutet „wahr", „F", „falsch". Die Reihen der „W" und „F" unter der Reihe der Elementarsätze bedeuten in leichtverständlicher Symbolik deren Wahrheitsmöglichkeiten):

p	q	r
W	W	W
F	W	W
W	F	W
W	W	F
F	F	W
F	W	F
W	F	F
F	F	F

p	q
W	W
F	W
W	F
F	F

p
W
F

Figura 7: Proposición 4.31 del Tractatus Logico-Philosophicus (1922)

Las posibilidades de verdad pueden ser representadas por esquemas de la siguiente clase («V» significa «verdadero», «F» significa «falso». La serie de «V» y de «F» bajo la serie de las proposiciones elementales significan, en un simbolismo fácilmente inteligible, sus posibilidades de verdad):

1.4.2. Refutación

Se aplica la reducción al absurdo. Se supone la proposición falsa y se busca una contradicción.
—Añadir ejercicio/ejemplo—–

1.4.3. Forma clausulada

Se trata en descomponer la proposición en una conjunción de proposiciones disjuntas. Solo se permiten proposiciones simples o sus negativos, por lo que no siempre es posible construirla. Ejemplo:

$$p \longleftrightarrow q \iff (p \to q) \land (q \to p) \text{ Ley del bicondicional}$$

$$\iff (\neg p \lor q) \land (\neg q \lor p) \text{ Por la ley del condicional}$$

De ese modo obtenemos la forma clausulada, donde todas las clausulas han de ser ciertas, puesto que estan asociada con conjunciones, cosa que facilita la validación de la proposición original.

Pasos recomendados para obtener la forma clausulada Aplicando las leyes adecuadas:

1. Reducir los bicondicionales.
2. Reducir los condicionales.
3. Utilizar Morgan para eliminar las negaciones sobre conjunciones o disjunciones.
4. Reordenar por medio de las propiedades distributivas, asociativas y conmutativas.

1.5. Lógica proposicional y conjuntos

Al referirse la lógica de predicados a objetos concretos, en ella no podemos utilizar expresiones como: «Los números naturales son pares o impares». En cambio, la lógica proposicional sí es capaz de referirse a propiedades de colecciones de objetos. De hecho también sería importante hablar aquí de conjuntos pero, presuponiendo unos conocimientos mínimos de teoría de conjuntos, preferimos dejarlo para otro apartado.

Predicados. La sentencia «En número natural elegido es par» se puede representar como P_x donde P es la propiedad «ser par» y $_x$ es la variable muda del número concreto que se elija. Así, P_3 es falsa y P_{24} es cierta. En este caso el predicado actua sobre $\mathbb{N}$ (conjunto de números naturales), a este conjunto se le conoce como **universo del predicado**. Podemos contruir expresiones como: $\neg P_x$, $P_x \wedge Q_x$, $P_x \rightarrow Q_x$,... Estos predicados permitirían definir subconjuntos de su universo, por ejemplo:

$$P = \text{Ser mayor que } 100$$

$$Q = \text{Ser par}$$

$$C = \{x \in \mathbb{N} | 1 \leq x < 110\}$$

$$P_x \wedge Q_x = \{102, 104, 106, 106, 108\} \text{ , nótese que } 110 \notin C.$$

1.6. Cuantificadores

1.6.1. Cuantificador universal

Cuando para todo x se cumple o se satisface P, podemos escribir: $(\forall_x \in C)P_x$. Si no hay confusión sobre el conjunto en que opera el predicado, podemos simplicarlo como: $\forall_x P_x$. El símbolo $\forall$ que leemos «para todo» es una generalización de la cojunción $(x_1 \wedge x_2 \wedge ... \wedge x_n)$.

1.6.2. Cuantificador existencial

En esta situación, si existe algun elemento del universo del predicado que cumple la condición de P, escribiremos: $(\exists_x \in C)P_x$. El símbolo $\exists$lo leemos «existe algun» y puede considerarse una generalización de la disjunción $(x_1 \vee x_2 \vee ... \vee x_n)$. Cuando ese elemento que existe es único se utiliza la expresión $\exists!$. Por ejemplo: $\exists! x \in \mathbb{N} | 100 < x < 102$, que vendría decir: «solo existe un número natural entre 100 y 102».

Relación entre cuantificadores. Es falso que para todo x se cumpla el predicado si existe algun x para el que el predicado no se cumple. En esquema:

$$\neg(\forall_x P_x) \iff \exists_x(\neg P_x)$$

Igualmente, es falso que se cumpla el predicado para algun x si el predicado no se cumple para ninguno. El esquema sería:

$$\neg(\exists_x P_x) \iff \forall_x(\neg P_x)$$

2. Capítulo 2. Conjuntos

«Me imagino un conjunto como un abismo»

"A set is a Many that allows itself to be thought of as a One"

Georg Cantor (1845-1918)

2.1. Conjuntos

Los definimos por extensión ($\{1,2,3,4,\}$) o por comprensión ($\{x \in \mathbb{N} | 0 < x < 5\}$). Hay que distinguir el elemento $a$del conjunto unitario $\{a\}$. Un elemento no puede ser conjunto y elemento a la vez. Se considera que $a \in a$ es falsa.

$$A = B \iff (A \subset B) \wedge (B \subset A)$$

Se suelen representar con diagramas de Venn. Complementario de un conjunto; $\bar{A} = \{x \in U | x \notin A\}$. En las partes de un conjunto siempre tenemos que $\emptyset \in P(A)$ y $A \in P(A)$.

2.2. Operaciones con conjuntos

2.2.1. Unión

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

Propiedades:

1. $A \subset A \cup B$ y $B \subset A \cup B$
2. Conmutativa; $A \cup B = B \cup A$
3. Asociativa; $A \cup (B \cup C) = (A \cup B) \cup C$
4. $A \cup \emptyset = A$
5. $A \cup A = A$

2.2.2. Intersección

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

Propiedades:

1. $A \cap B \subset A$ y $A \cap B \subset B$. Véase que es diferente que en el mismo punto de la unión.
2. Conmutativa; $A \cap B = B \cap A$
3. Asociativa; $A \cap (B \cap C) = (A \cap B) \cap C$
4. $A \cap \emptyset = A$
5. $A \cap A = A$

Por cierto, la unión y la intersección son respectivamente distributivas:

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

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

2.3. Familia de conjutos

También puede encontrarse en la literatura como conjuntos indizados

2.4. Diferencia de conjuntos

$$A \setminus B = \{x | (x \in A) \wedge (x \notin B)\}$$

Se verifica que:

1. $A \setminus B = A \setminus (A \cap B)$
2. Si $A, B \subset U$ entonces $U \setminus B = \bar{B}$ y $A \setminus B = A \cap \bar{B}$

2.5. Diferencia simétrica de conjuntos

$$A \triangle B = (A \cup B \setminus A \cap B)$$

$$A \triangle B = (A \setminus B \cup B \setminus A)$$

2.6. Leyes lógicas

Son las leyes ya vistas en el resumen sobre lógica matemática.

1. Interpolación
2. Asociativa, conmutativa y distributiva
3. Coplementario
4. Identidad
5. Morgan

2.7. Producto de dos conjuntos

Producto cartesiano del dos conjuntos. $A \times B = \{(x, y) \mid (x \in A) \wedge (y \in B)\}$. Así, si $A = B$ tenemos que $A^2 = A \times A$. El producto no es comnutativo, véase que por ejemlo en el plano $(2, 4) \neq (4, 2)$.

2.7.1. Propiedades

1. Si $A' \subset A$ y $B' \subset B$ entonces $A' \times B' \subset A \times B$.
2. Distributiva: $(A \cup B) \times C = (A \times C) \cup (B \times C)$ y $A \times (B \cup C) = (A \times B) \cup (A \times B)$. Ídem para la conjunción.
3. $A \times B = \emptyset \Leftrightarrow A = \emptyset \vee B = \emptyset$

Destacamos que el producto cartesiano de tres conjuntos lo llamamos terna y cuando tenemos n conjuntos, hablamos de n-uplas ordenadas.

2.8. Relaciones entre conjuntos. Lógica relacional

Para expresiones del tipo «el número elegido es menor que el que he pensado» se utiliza o que llamamos relación lógica o predicado simple de dos argumentos. En ella se utilizarian símbolos como M_{xy} donde M es la propiedad «ser menor» e y representa al número a elegir de un conjunto A y x al número pensado de un conjunto B. Nótese que xy es un elemento genérico del conjunto $A \times B$.

La lógica relacional es similar a la de predicados. Las proposiciones se refieren a relaciones sobre el producto cartesiano de dos conjuntos. Por ejemplo: para la relación R_{xy} siendo $R \subset A \times B$ podemos expresar: $(\forall x \in A)(\forall y \in B)R_{xy}$ o $(\exists x \in A)(\forall y \in B)R_{xy}$. Esto permite atribuir sin ambiguedad el valor de verdadero o falso a cada posible miembro de R. Si no existe posibilidad de confusión, se omite la indicación de la pertenecia a los conjuntos. Hay que fijarse en la posición de los cuantificadores ya que:

- $(\forall x \in \mathbb{R})(\exists n \in \mathbb{N})n > x$, significa «para cualquier número x hay número n mayor», siendo un predicado cierto.
- $(\exists n \in \mathbb{N})(\forall x \in \mathbb{R})n > x$, significa «existe un número n que és mayor que cualquier número x». que es un predicado falso.

2.8.1. Grafo de una relación lógica

Una relación R_{xy}sobre el producto cartesiano $A \times B$. Podemos expresar $R = \{(x,y) \in A \times B | R_{xy}$es verdader$\}$. R sería el grafo de esa relación lógica.

Dados A y B si $R \subset A \times B$, tenemos que R es una relación entre A y B. R también se llama correspondencia entre A y B y se emplea la notación $R : A \to B$. También, si $(x,y) \in R \subset A \times B$ decimos que $x \in A$ e $y \in B$ y escribimos xRy.

2.8.2. Expresiones de otros conceptos

- Relación inversa: $R^{-1}\{(y,x) \in B \times A | (x,y) \subset A \times B\}$
- Conjunto imagen: $R(A) = \{y \in B | \exists x \in A, xRy\}$
- Conjunto original: $R^{-1}(B) = \{x \in A | \exists y \in B, xRy\}$
- Composición de relaciones: Dada $R \subset A \times B$ y $S \subset B \times C$, $S \circ R = \{(x,z) \in A \times C | \exists y \in B | (x,y) \in R \wedge (y,z) \in S\}$.

3. Capítulo 3. Relaciones y aplicaciones

«Es el estudio riguroso de mundos hipotéticos. Es la ciencia de lo que

podría haber sido o podría ser, así como de lo que es».

Murray Gell-Mann (1929)

"[La matematiko] estas la rigora studi de hipotezaj mondoj, ĝi estas la

scienco de kio povus esti estita aŭ de kio povus esti kaj de kiel kio estas".

Traducción al esperanto

3.1. Propiedades básicas de una relación

Una relación R definida en U, de forma que $R \subset U \times U$ puede tener las siguentes propiedades:

1. Propiedad reflexiva: La relación es reflexiva sii $\{(x, x) | x \in U\} \subset R$ es decir $\forall x \in U$ se verifica que xRx.
2. Propiedad simétrica: La relación es simétrica sii $R^{-1} \subset R$ (es decir que la relación inversa también pertenece a $U \times U$). En otra expresión; $\forall x, y \in U$ tenemos que si xRy entonces yRx.
3. Propiedad antisimétrica: Podemos expresar que $\forall x, y \in U$, si xRy e yRx entonces $x = y$.
4. Propiedad transitiva: Es el caso que $R \circ R \subset U$, es decir $\forall x, y, z \in U$ verificamos que si xRy y yR

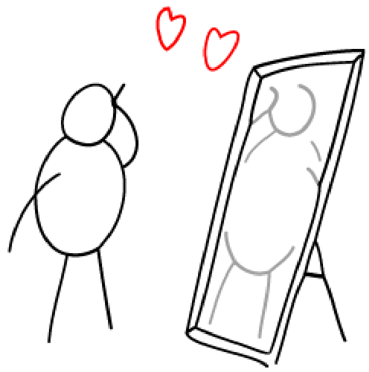


Figura 8: El amor narcisita es reflexivo

3.2. Relaciones de equivalencia

Permiten obtener clasificaciones de los elementos de un conjunto. Estas clasificaciones se obtienen por las **clases de equivalencia** que conducen al concepto de **conjunto cociente**. Una relación de equivalencia ha de tener las siguientes propiedades: reflexiva, simétrica y transitiva.

3.2.1. Clase de equivalencia

La definimos. Teniendo una relación Ren un conjunto U, la clase de equivalencia del elemento xRU al conjunto imagen de x se denota xR o $[x]$ y podemos notarlo así: $[x] = \{y \in U | xRy\}$. Cuanquier $y \in [x]$ se llama representante de la clase $[x]$.

3.2.2. Conjunto cociente

Podemos definirlo diciendo que dada la relación R y el conjunto , el conjunto cociente es el conjunto de todas las clases de equivalencia que genera R en U. Y lo denotamos U/R.

Podemos imaginarnos, como ejemplo, las doce horas del reloj como un conjunto cociente de la sclases de equivalencia de las horas.

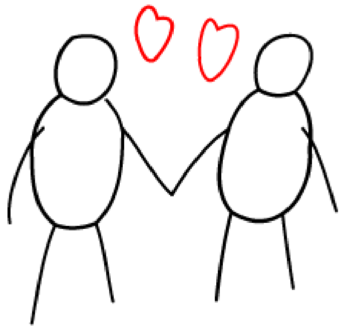


Figura 9: El amor romántico es simétrico

Al haber mencionado las horas, recordamos qeu dos números a y b son concruentes modulo p si tiene el mismo resto entero al dividirlos entre p o $a - b$ es múltiplo de p. (repasar)

3.2.3. Partición de un conjunto

La partición de un conjunto U es una familia Pd e subconjuntos de U disjunto dos a dos cuya unión es el conjunto U. En fórmulas: $\forall A, B \in P$, se satisface que $A \cap B = \emptyset$ y $\bigcup_{A \in P} A = U$.

Toda relación de equivalencia genera un apartición y toda partición genera una ralción de equivalencia.

3.3. Relaciones de orden

Una relación de orden tiene las propiedades reflexiva, antisimétrica y transitiva.

Un **conjunto ordenado** es aquel sobre el qeu se ha definido una relación de orden, solemos expresarlo como $(U, \preceq)$. Decimos que una relación es de **orden total** si $R^{-1} \cup R = U \times U$ es decir: $\forall x, y \in U$ tenemos que xRy o yRx. De lo contrario hablamos de un **orden parcial**.

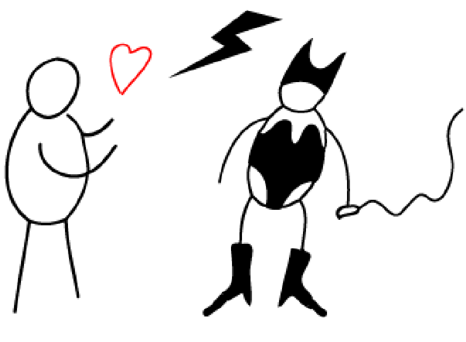


Figura 10: Una relación sadomasoquisa es antisimétrica

3.3.1. Intervalos en un conjunto ordenado

Dado un conjunto ordenado $(U, \preceq)$ de forma que $a, b \in U$ y $a \preceq b$.

- Intervalo abierto: $(a, b) = \{x \in U | a \prec x \prec b\}$
- Intervalo cerrado: $[a, b] = \{x \in U | a \preceq x \preceq b\}$

- Intervalo semiabierto: $[a, b)$ o $(a, b]$
- Intervalo incial (el final es similar) abierto: $(\leftarrow, a) = \{x \in U | x \prec a\}$
- Intervalo incial cerrado: $(\leftarrow, a] = \{x \in U | x \preceq a\}$

3.3.2. Más definiciones

Orden lexicográfico.

$$(a, b) \leq_L (c, d) \iff (a < c) \vee ((a = c) \wedge (b \leq d))$$

Orden producto.

$$(a, b) \leq_P (c, d) \iff (a \leq c) \wedge (b \leq d)$$

Figura 11: Las amistades de bar son transitivas

Dado un conjunto $(U, \preceq)$ y un subconjunto $A \subset U$, definiremos algunas cosillas.

Cota superior de A. Cualquier elemento $y \in U$ tal que $\forall x \in A, x \preceq y$.

Conjunto acotado superiormente. Si existe cota superior. Entendemos como conjunto acotado aquel qeu lo está superior e inferiormente.

Máximo. $M \in A | \forall x \in A, x \preceq M$ (el mínimo es equivalente pero a la inversa), se denota como $Max(A)$. Es único puesto que si $x \preceq M$ y $x \preceq M'$ tendremos que $M \preceq M'$ y $M' \preceq M$ que por la propiedad antisimétrica nos dice que $M = M'$.

Supremo. Es la menor de las cotas inferiores. $s \in U | s \preceq y$ siendo y una cota superior de A, (Ínfimo es equivalente).

Maximal. En A no existe elemento posterior a m. Si $m \preceq x$ y $x \in A$, entonces $m = x$. Hay que señalar que si el orden es total, el máximo y el maximal coinciden.

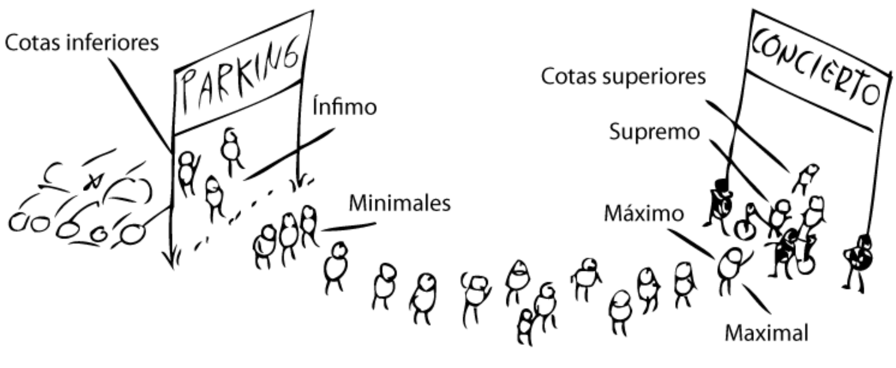


Figura 12: Posiciones relativas en la cola ordenada de un concierto

Propiedad del buen orden. En un conjunto ordenado, si cualquier subconjunto posee mínimo.

Propiedad de supremo. Un conjunto ordenado la satisface sii cualquier subconjunto de él no vacio y acotado superiormente posee supremo. Esta propiedad es característica de $\mathbb{R}$.

3.4. Aplicaciones

3.4.1. Aplicaciones entre conjuntos

Existe una aplicación entre conjuntos si dados los conjuntos A y B, si a cada elemento de A le corresponde un único elemento de B. La aplicación F es $F \subset A \times B$ tal que $\forall x \in A$ el conjunto $F(x)$ es un conjunto unitario. En general una aplicación inversa, no es un aplicación.

3.4.2. Definiciones

Aplicación canonica. Sii la imagen de cada elemento de A es el mismo elemento de B (un elemento en particular).

Proyección canónica. Aplica a cada elemento de A su clase de equivalencia en el conjunto cociente:

$$p : A \to A/\varepsilon$$

$$x \mapsto p(x) = [x]$$

Podemos ejemplificarlo para las horas del reloj (módulo 12): $p(13) = 1$, $p(26) = p(14) = 2$.

Aplicación identidad. La imagen de cada elemento de A es el propio elemento. Se suele representar con la notación 1_Ao Id_A.

$$Id_A : A \to A$$

$$x \mapsto Id_A(x) = x$$

Dominio de una función. Como nos dice Wikipedia: El dominio de definición de una función f:X→Y se define como el conjunto X de todos los elementos x para los cuales la función f asocia algún y perteneciente al conjunto Y de llegada, llamado codominio.

Podemos definir restricciones o extensiones de una función segun el subconjunto del del dominio utilizado. Por ejemplo:

$$y : \mathbb{N} \to \mathbb{Z}$$

$$x \mapsto y(x) = 2x$$

Con y podríamos obtener los pares positivos, al ser el dominio los números naturales y el condominio o el conjunto imagen, los números enteros. Sin embargo:

$$h : \mathbb{Z} \to \mathbb{Z}$$

$$x \mapsto h(x) = 2x$$

La función h nos da todos los números pares enteros, tanto positivos como negativos puesto que tanto el dominio como el condominio pertenece al conjunto de los números enteros.

Composición de funciones. Si tenemos las funciones $f : A \to B$ y $g : B \to C$ denotaremos la composición de las dos como $g \circ f$ (se escribe al revés) de forma que $\forall x \in A, (g \circ g)(x) = g(f(x))$. La composición de funciones no es en general conmutativa.

Función característica de un conjunto. Dado $A \subset U$, llamamos función característica de A y la denotamos como χ_A a la función que indica si un elemento pertenece o no al conjunto:

$$\chi_A : U \to \mathbb{R}$$

$$\chi_A(x) = \begin{cases} 1 & x \in A \\ 0 & x \notin A \end{cases}$$

Aplicación sobreyectiva. Siendo $f \in A \times B$ siendo $Im(f) = B$. Todo elemento de B está relacionado con algún elemento de A siendo f una función. Un ejemplo es la función $f : \mathbb{R} \to \mathbb{R}$, $x \mapsto f(x) = x^3 - x$. Por ejemplo, vemos que tres elementos de A tienen un mismo elemento de B: $f(-1) = 0, f(0) = 0, f(1) = 0$ al tiempo que todos los elementos de B tienen una contraimagen $f^{-1}(0) = \{-1, 0, 1\}$, lo noto así, pero no sería una función. Podemos ver la gráfica del ejemplo.

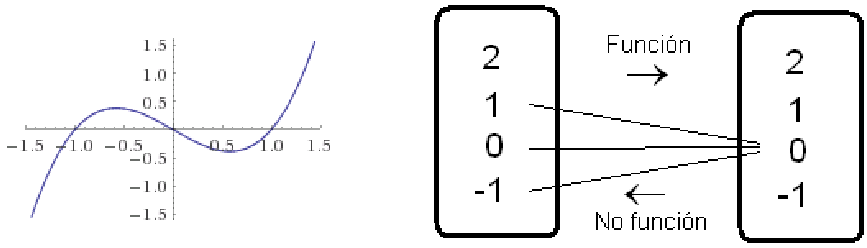


Figura 13: Función sobreyectiva

Aplicación inyectiva. No hay dos elementos del conjunto inicial que tengan la misma imagen. Tenemos que $f \in F(A, B)$. $\forall x, x' \in A$, si $f(x) = f(x') : x = x'$ y equivalentemente, si $x \neq x' : f(x) \neq f(x')$. Un ejemplo de función inyectiva es $y = 2^x$.

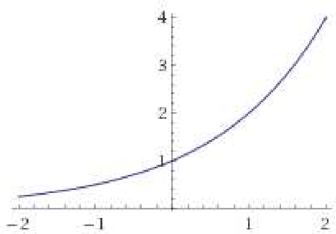


Figura 14: Función inyectiva

Dado $f \circ F(A, B), g \in F(B, C)$ y $g \circ f \in F(A, C)$, tenemos que si f y g son sobreyectivas $g \circ f$ también lo es. Lo demostramos así: como $f(A) = B$ puesto que f es sobreyectiva, también tenemos que $g(B) = C$, por lo tanto $g(f(A)) = g(B) = C$.

Si f y g son inyectivas, $g \circ f$ es inyectiva. Vemos que dados x y x' de forma que $g \circ f(x) = g \circ f(x')$, al ser g inyectiva, tenemos que $f(x) = f(x')$y como f es también inyectiva: $x = x'$, cumpliéndose la propiedad característica de la inyección. Sea $f \in F(A, B)$.

1. f es sobreyectiva sii $\exists h \in F(B, A) | f \circ h = I_B$.

2. f es inyectiva sii $\exists g \in F(B, A) | g \circ f = I_A$.

Aplicación biyectiva. Es una aplicación que es inyectiva y sobreyectiva al mismo tiempo. Todos los elementos del conjunto final estan asociados a un único elemento del conjunto incicial. En signos: $\forall y \in B \exists! x \in A | f(x) = y$. Un ejemplo de función es $y = x^3$, puede verse la gráfica a continuación.

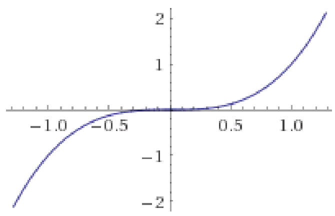


Figura 15: Función biyectiva

Una aplicación $f \in F(A, B)$ es biyectiva sii existe $g \in (B, A) | f \circ g = I_B$ y $g \circ f = I_A$.

3.5. Factorización canónica de una aplicación

Una función f se descompone en:

1. p: proyección canónica
2. b: proyección canónica
3. i: inyección canónica

Vamos a mostrarlo ejemplificadamente, tomando la siguente función:

$$f : \mathbb{R} \to \mathbb{R}$$

$$x \mapsto f(x) = x^2$$

La función no es inyectiva puesto que no se da que si $f(x) = f(x')$ entonces $x = x'$ pues $f(1) = f(-1)$. Tampoco es sobreyectiva pues $\nexists x \in (-\infty, 0)$ que le corresponda ningun elemento en el conjunto original.

Proyección canónica.

$$p : \mathbb{R} \to \mathbb{R}/\varepsilon$$

$$x \mapsto p(x) = \{x, -x\}$$

Tenemos que ε es la siguente relación $x \varepsilon x' \iff f(x) = f(x')$. La función p relaciona a cada elemento con su clase de equivalencia, en esta caso los elmentos del conjunto original se relacionana con elementos binomiales de la siguente manera: $p(2) = [2] = \{2, -1\}$, $p(\sqrt{2}) = [\sqrt{2}] = \{\sqrt{2}, -\sqrt{2}\}$. La función es suprayectiva ya que para cualquier elemento del conjunto cociente, existe algun elemento qu le corresponde en el conjunto original (que será de mayor tamaño).

Biyección canónica.

$$b : \mathbb{R}/\varepsilon \to f(\mathbb{R})$$

$$[x] = \{x, -x\} \mapsto b([x]) = x^2 = f(x)$$

La función b relaciona cada elemento del conjunto cociente $\mathbb{R}/\varepsilon$ (que se escribe así puesto que es el resultado de que en $\mathbb{R}$ la relación ε haga de las suyas), lo relaciona con algun elemento del conjunto de imagens por f. Puesto que $f(\mathbb{R}) = [0, \infty)$ existe una biyección entre los elementos del conjunto $\mathbb{R}/\varepsilon$ y $f(\mathbb{R})$ ya que existe una correspondencia unívoca entre cada elemento $\{x, -x\}$ y cada elemento x^2.

Inyección canónica.

$$i : f(\mathbb{R}) \to \mathbb{R}$$

$$x \mapsto i(x) = x$$

También llamada aplicación inclusión y reperesentada con el símbolo $\hookrightarrow$que asociaa a cada enlemto $x \in f(\mathbb{R}) \subseteq \mathbb{R}$ consigo mismo en $\mathbb{R}$. La función determina un subconjunto, de ahí lo de inclusión.

De esa forma conseguimos el esquema famoso de la descomposición de una función.

$$\begin{array}{ccc} \mathbb{R} & \xrightarrow{f} & \mathbb{R} \\ {\scriptstyle p}\downarrow & & \uparrow{\scriptstyle i} \\ \mathbb{R}/\varepsilon & \xrightarrow{b} & f(\mathbb{R}) \end{array} \qquad \begin{array}{ccc} x \in (-\infty, \infty) & \to & x \in [0, \infty) \\ \downarrow & & \uparrow \\ \{-x, x\} & \to & x^2 \end{array}$$

Y vemos que $(i \circ b \circ p)(x) = (i \circ b) \circ p(x) = i \circ b([x]) = i(f(x)) = f(x)$.

3.6. Equipotencia de conjuntos

Cardinal de 0. Todos los conjuntos equipotentes con $\emptyset$, se representa con 0.

Carinal n. El conjunto equipotente con $\{1, ..., n\} \in \mathbb{N}^*$

Cardinal de $\mathbb{N}$ o de $\aleph_0$. El conjunto equipotente con los numeros naturales. El signo hebreo se llama «álef sub cero».

Cardinal de $\mathbb{R}$. El conjunto equipotente con los números reales, también se designa como una c gótica minúscula.

El conjunto A es finito si $\exists n \in \mathbb{N} | Card(A) = n$. El conjuto A es infinito si no es finito. El conjunto A es numerable si existe una biyección con los números naturales, se denota $Card(A) = \aleph_0$.

4. Capítulo 4. Estructuras algebraicas

«Las matemáticas son un modo de caracterizar o expresar estructura».

Chaitin, Gregory. Meta Maths. (2005).

4.1. Conceptos

Operacion interna. Tambien llamada ley de composición interna, es una aplicación $E \times E$ en E, de forma que cada par de elementos (a, b) se relaciona con un únoco lemento de E al que denotamos $a \star b$, siendo $\star$ el símbolo para el operador (aunque podría utilizarse cualquiera, por ejemplo a♫b). Ejemplos: las operaciones $\cdot, +, -$ son operaciones internas en $\mathbb{Z}$ o $\mathbb{R}$, sin embargo $-$no lo es en $\mathbb{N}$ puesto que $1 - 2 = -1 \notin \mathbb{N}$.

Propiedades de las operaciones internas.

- Asociativa. $(a \star b) \star c = a \star (b \star c)$. Esta propiedad permite que prescindamos de paréntesis.
- Conmutativa. $a \star b = b \star a$. El orden es indiferente.

Cuando las operaciones son asociativas y conmutativas, podemos utilizar las siguentes espresiones:

- $\sum_{i=1}^{n} a_i$ que es igual a $a_1 + a_2 + ... + a_n$.
- $\prod_{i=1}^{n} a_i$equivalente a $a_1 \cdot a_2 \cdot ... \cdot a_n$.
- $\bigcap_{i=1}^{n} A_i$que sería la intersección de los conjuntos $A_1, A_2, ..., A_n$.
- $\bigcup_{i=1}^{n} A_i$el mismo caso para la unión.

Elemento neutro. Para la operación interna $\star$ en E, $\exists e \in E | \forall a \in E$ tenemos que $a \star e = e \star a = a$.

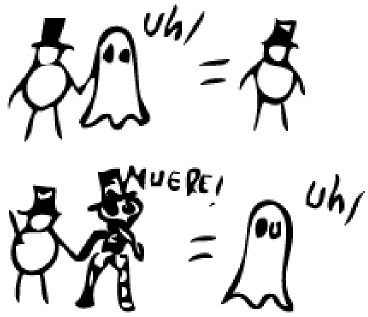


Figura 16: Representación del elemento neutro y del simétrico

Este elemento es único. Supongamos que e y e' son elementos neutros de E. Tendríamos que $e \star e' = e$ y que $e \star e' = e'$ por lo que $e = e'$.

Elemento simétrico. Sería $a \star a' = a' \star a = e$. En un conjunto con elemento neutro, si existe simétrio este és único para cada elemento. Demostración. Digamos que a' y a'' son dos elementos simétricos de a. Entonces:

$$a' \star (a \star a'') = a' \star e = a'$$

$$(a' \star a) \star a'' = e \star a'' = a''. \text{ Por lo tanto } a' = a''$$

4.2. Grupos

Siendo $G \neq \emptyset$, $(G, \star)$ es un grupo sí:

- $\star$ es asociativa
- $\exists e$ de $\star$ en G
- Si $\forall a \in G$, $\exists$ simétrico de a respecto a $\star$.
- El grupo es abeliano si $\star$ es conmutativa.

El elemento neutro se llama nulo en la adición y unidad en la multiplicación. Respectivamente el simétrico suele llamarsele opuesto e inverso. Señalar que respecto al elemento inverso, la notación $\frac{1}{a}$ se reserva para números, en general se utiliza a^{-1}.

4.3. Propiedades de un grupo

- Propiedad cancelativa, $a, b, c \in G$, $a \star b = a \star c$, $b = c$. Demostración: $a \star b = a \star c; a^{-1} \star (a \star b) = a^{-1} \star (a \star c) \rightarrow e \star b = e \star c \rightarrow b = c$.
- $\forall a, b \in G$, $\exists! x \in G | a \star x = b$. Demostración; $a \star x = b; a^{-1} \star a \star x = a^{-1} \star b \Rightarrow x = a^{-1} \star b$.
- Si a^{-1} y b^{-1} son simétricos de a y b entonces, $(a \star b)^{-1} = a^{-1} \star b^{-1}$. Demostración, $(b^{-1} \star a^{-1}) \star (a \star b) = e = (a \star b) \star (b^{-1} \star a^{-1})$.

4.4. Subgrupos

Siendo $H \subset G$, hay que verificar:

- La operación es interna, si $a, b \in H$ entonces $a \star b \in H$.
- El elemento neutro de G, aparece en H.
- Los elementos de H también tienen allí su simétrico.

A la práctica hay que demostrar que teniendo $(G, \star)$ es un grupo y $H \subset G, H \neq \emptyset$, H es subgrupo de G si y solo si $\forall a, b \in H, a \star b^{-1} \in H$.

Congruencia modulo un subgrupo. Pendiente

4.5. Anillos

Tenemos un conjunto A con dos operaciones $+, \cdot$. Ha de satisfacer que:

- $(A, +)$sea grupo abeliano o conmutativo.
- La operación $\cdot$ sea asociativa.
- La operación $\cdot$ sea destributiva respecto a la operación $+$.
  - Anillo conmutativo si $\cdot$ lo es.
  - Anillo unitario si $\cdot$ tiene elemento neutro.

4.5.1. Propiedades del anillo

- $\forall a \in A; a0 = 0a = 0$. El 0 es absorvente para el producto.
- $\forall a, b \in A, (-a)b = a(-b) = -(ab)$ y $(-a)(-b) = ab$.
- Si A es conmutativo se satisface que $(a + b)^2 = a^2 + b^2 + ab$ y lo mismo para el Binomio de Newton (es decir, podemos generalizar). -recuperar la chuleta del blog-

Divisores de 0. Si tenemos $(A, +, \cdot), a \in A, a \neq 0$. Este a es un divisor de cero si $\exists b \in A$ de forma que $b \neq 0$ y $ab = 0$. Un **anillo integro** es el que no tiene divisores de 0.

4.5.2. Subanillos

Un subanillo H de un anillo A es el subconjunto de elementos que conservan las propiedades de anillo.

Caracterización. Tenemos que $(A, +, \cdot)$ es un anillo $A \neq \emptyset$ y $H \subset A$. Ha de cumplirse que $\forall a, b \in H$:

1. $a - b \in H$
2. $ab \in H$
3. Si el anillo original es unitario, entonces $1 \in H$.

4.5.3. Ideales

Siendo $(A, +, \cdot)$ un anillo conmutativo y $\emptyset \neq I \subset A$, entonces I es ideal si:

1. $a - b \in I, \forall a, b \in I$
2. $ac \in I \forall a \in I$ y $\forall c \in A$

4.6. Cuerpos

$(K, +, \cdot)$ es un cuerpo si satisface:

1. Es un anillo conmutativo unitario con elemento neutro para las dos operaciones.
2. Existe simetrico para las dos operaciones.

4.6.1. Subcuerpos

Caracterización:

1. $a - b \in H, \forall a, b \in H$
2. $ab^{-1} \in H, \forall a, b \in H^*$

Grupos ordenados. Sin comentarios

4.7. Homomorfismos

$f : G \to G', f(a + b) = f(a) + f(b), \forall a, b \in G.$

4.8. Apéndices

4.8.1. Esquema de estructuras algebraicas

4.8.2. Memotecnia para el Binomio de Newton

$$(a+b)^3$$
$$a^0 + a^1 + a^2 + a^3$$

$$b^3 + b^2 + b^1 + b^0$$

$$\binom{3}{0} + \binom{3}{1} + \binom{3}{2} + \binom{3}{3}$$

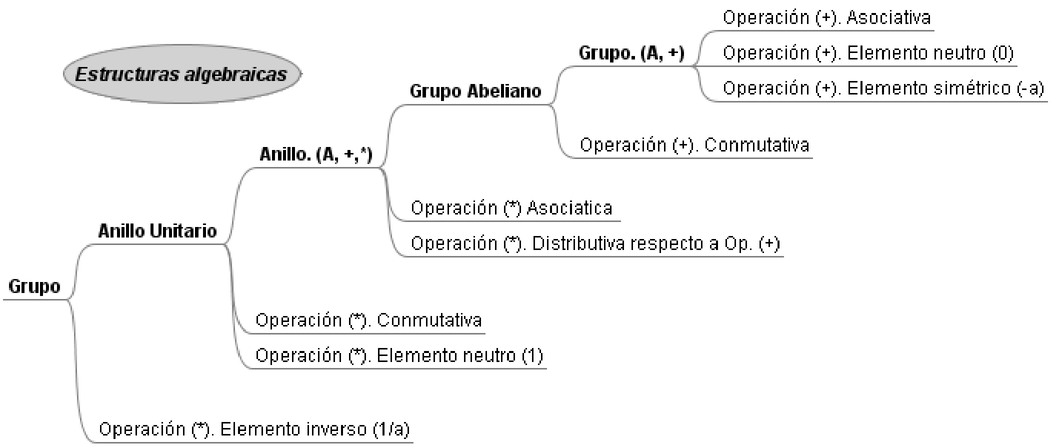


Figura 17: Esquema de estructuras algebraicas

Recordamos como se calcula un "número" combinatorio y factorial:

$$\binom{n}{x} = \frac{n!}{x!(n-x)!}$$

$$n! = 1 \cdot 2 \cdot 3 \cdot ... \cdot (n-1) \cdot n$$

$$3! = 1 \cdot 2 \cdot 3 = 6$$

Y si lo unimos todo tenemos:

$$(a+b)^3 = \binom{3}{0} a^0 b^3 + \binom{3}{1} a^1 b^2 + \binom{3}{2} a^2 b^1 + \binom{3}{3} a^3 b^0$$

$$(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$$

Cuando el binomio es negativo se alternan los signos - y + (-,+,-,+,...).Y efectivamente, $\binom{3}{1} = \binom{3}{2}$ y el primero $\binom{3}{0}$, lo suprimimos.

5. Capítulo 5. Números naturales y enteros

"Certains mystères échapperont toujours à l'esprit humain. Pour nous en convaincre, il suffit de jeter un œil aux tableaux des nombres premiers, et on verra qu'il n'y règne ni ordre, ni règles".

Évariste Galois (1811-1832)

«Algunos misterios siempre escaparán a la mente humana. Para convencernos de ello, sólo hay que echar un vistazo a las tablas de los números primos, y ver que no reina ni orden, ni reglas»

5.1. Numeros naturales, los Axiomas de Peano

1. 0 es un número natural.
2. $\forall n$ tiene un número sucesor que es número natural.
3. 0 no es sucesor de ningun número natural.
4. Dos números naturales cuyos sucesores son iguales, son iguales.
5. Si un conjunto tiene a 0 y a todos los sucesores contiene a todos los números naturales.

5.2. Suma en $\mathbb{N}$

Se define por recurrencia

1. $m + 0 = m, \forall m \in \mathbb{N}$
2. $\forall (a, b, n) \in \mathbb{N}^* \times \mathbb{N}^* \times \mathbb{N}$, $a^n b^n = (ab)^n$

5.3. Ordenación en $\mathbb{N}$

$m \leq n$ si existe $p \in \mathbb{N} | m + p = n$, $m < n \iff m + 1 \leq n$. La relación $\leq$ es de orden total en $\mathbb{N}$, siendo compatible con la suma y el producto. $m \leq n$ entonces $m + p \leq n + p$ y $mp \leq np$.

5.3.1. Propiedades

- El intervalo $(n, n+1)_{\mathbb{N}}$ es vacio.
- El conjunto $(\mathbb{N}, \leq)$ es bien ordenado, es decir, todo subconjunto no vacio tiene mínimo.
- En $\mathbb{N}$, todo subconjunto no vacio y acotado tiene máximo.

Conjuntos finitos. En el libro se explican fatal

Conjuntos infinitos. Ojo combinatoria

5.4. Los números enteros: caracterización del conjunto $\mathbb{Z}$

En el conjunto $\mathbb{N} \times \mathbb{N}$ se define una relación ε de equivalencia:
$(a, b)\varepsilon(a', b') \iff a + b' = a' + b$ así definimos $\mathbb{Z} = (\mathbb{N} \times \mathbb{N})/\varepsilon$ que son los elementos: $\{..., (0, 2), (0, 1), (0, 0), (1, 0), (2, 0), ...\}$

5.4.1. Operaciones en $\mathbb{Z}$

$\alpha = (a, b), \beta = (c, d)$ que pertenecen al grupo anterior, tenemos que: $\alpha + \beta = [(a + c, b + d)]$ y $\alpha\beta = [(ac + bd, bc + ad)]$. Por sus propiedades decimos que $(\mathbb{Z}, +, \cdot)$ es un anillo conmutativo unitario.

5.4.2. Orden en $\mathbb{Z}$

Propiedad aquimediana de $\mathbb{Z}$. $\forall \alpha \in \mathbb{Z} | \alpha > 0$ y $\forall \beta \in \mathbb{Z}, \exists n \in \mathbb{N} | n\alpha > \beta$

División entera o euclidea. $a, b \in \mathbb{Z} | b > 0, \exists! q, z | a = qb + r$ y $0 \leq r < b$

Mínimo comun núltiplo. $a, b \in \mathbb{N}^*, \exists! m \in \mathbb{N}^* | a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$

Máximo comun divisor. $a, b \in \mathbb{N}^*, \exists! d \in \mathbb{N}^* | a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$

Identidad de Bézout. $a, b \in \mathbb{N}^*$ y $d = mcd(a, b), \exists u, v \in \mathbb{Z}$ tales que $d = au + bv$. ademas d es el mínimo número natural expresable como $am + bn$ siendo m y n enteros.

5.4.3. Algoritmo de Eucides para mcd

Al dividir a entre b (números enteros), se obtiene un cociente q y un residuo r. Es posible demostrar que el máximo común divisor de a y b es el mismo que el de b y r (Sea c el máximo común divisor de a y b,.Como $a = bq + r$ y c divide a a y a b divide también a r.Si existiera otro número mayor que c que divide a b y a r, también dividiría a a , por lo que c no sería el mcd de a y b, lo que contradice la hipótesis). Éste es el fundamento principal del algoritmo. También es importante tener en cuenta que el máximo común divisor de cualquier número a y 0 es precisamente a (fuente Wikipedia).

Paso	Operación	Significado
1	2366 dividido entre 273 es 8 y sobran 182	mcd(2366,273)=mcd(273,182)
2	273 dividido entre 182 es 1 y sobran 91	mcd(273,182)=mcd(182,91)
3	182 dividido entre 91 es 2 y sobra 0	mcd(182,91)=mcd(91,0)

Dos enteros son primos entre sí, si $mcd(|a|, |b|) = 1$.

5.4.4. Teorema de Bézout

$a, b \in \mathbb{Z}^*$ a y b son primos entre sí si y solo sí $\exists u, v \in \mathbb{Z} | au + bv = 1$

5.4.5. Teorema de Gauss

Si a y b son primos entre sí y a divide bc entonces a divide a c.

Figura 18: Étienne Bézout (1730-1783)

6. Capítulo 6. Números racionales y reales

«Los números, como otros objetos matemáticos, son construcciones mentales cuyas raíces

se encuentran en la adaptación del cerebro humano a las regularidades del universo».

Dehaene, Stanislas. The Number Sense. (1999).

6.1. El conjunto de los racionales

Definimos en $\mathbb{Z} \times \mathbb{Z}^*$ una relación ε, de forma que $(a,b)\varepsilon(a',b') \Longleftrightarrow ab' = ba'$. De ese modo tenemos que $\mathbb{Q} = \mathbb{Z} \times \mathbb{Z}^*/\varepsilon$. Por ejemplo $\frac{2}{1} = \frac{4}{2}$ dado que $(2,1)\varepsilon(4,2)$.

Representante canónico. También fracción irreductible. Si $(a,b) \in \mathbb{Z} \times \mathbb{Z}^*$ y $d = mcd(|a|,|b|)$,entonces $a = da'$ y $b = db'$ siendo $1 = mcd(|a'|,|b'|)$. (a',b') es el representante canónico.

Operaciones en $\mathbb{Q}$. $\alpha = (a,b)$ y $\beta = (c,d)$ son dos números racionales:
$\alpha + \beta = [ad + bc, bd]$; es decir $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$
$\alpha\beta = [(ac, bd)]$;o lo que es lo mismo $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$

6.1.1. Orden en $\mathbb{Q}$

- Se puede dividir en conjunto en una parte positiva $a/b|b \neq 0$ y $ab \geq 0$ y otra negativa en que $b \neq 0$ y $ab \leq 0$
- Dados dos números racionales α y β, $\alpha \leq \beta \Longleftrightarrow \beta - \alpha \in \mathbb{Q}_+$
- $(\mathbb{Q}, +, \cdot, \leqslant)$ satisface las propiedades para ser un cuerpo ordenado. Podemos considerar a $\mathbb{Z}$ como un anillo ordenado de $\mathbb{Q}$, vemos que podemos especificar la aplicación inyectiva $f : \mathbb{Z} \to \mathbb{Q}$, $f(a) = [(a,1)]$, $f(a + a') = f(a) + f(a')$, $f(aa') = f(a)f(a')$ y si $a \leqslant a'$ entonces $f(a) \leqslant f(a')$.

6.1.2. Propiedad arquimediana de $\mathbb{Q}$

- Para todo $\alpha \in \mathbb{Q}|\alpha > 0$ y para todo $\beta \in \mathbb{Q}\exists n \in \mathbb{N}|n\alpha > \beta$

  Demostración: $\alpha = \frac{a}{b}, \beta = \frac{c}{d}$ y tenemos que $b,d > 0$. $n\alpha > \beta$ es cierto si $n\alpha - \beta > 0$ (propiedad para saber que número es mayor que otro). Explicitamos esa sustracción $n\frac{a}{b} - \frac{c}{d} = \frac{nad-bc}{bd} > 0$ puesto que los denominadores han de ser positivos (si β es negativo no hay nada que demostrar) nos quedamos con $nad - bc > 0$, como $\alpha > 0$ y $b > 0$ entonces $a > 0$ y siendo también positivo d existirá un n que cumpla $n(ad) > bc$.
- El orden en $\mathbb{Q}$ es divisible
- Para cualquier número racional $\alpha < \beta\exists\psi \in \mathbb{Q}|\alpha < \psi < \beta$. Vemos que $\psi = \frac{\alpha+\beta}{2}$ cumple el requisito.

6.1.3. Números decimales

Se trata de un número racional qeu tenga un representante cuyo denominador sea una potencia de 10. Por ejemplo: $3838'73 = 383873/10^2$ o $\frac{1}{5} = \frac{2}{10}$, otros números como $\frac{1}{3}$ o $\frac{3}{7}$ no son decimales. Más formalmente decimos que un racional es decimal si y solo sí, su fracción irreductible es de la forma $a/2^n5^p$siendo que $n,p \in \mathbb{N}$. Vemos que $\frac{a}{b} = \frac{x}{10^m}$; $a10^m = bx$ puesto que a y b son primos entre sí, en virtud de un teorema gaussiano de un tema anterior tenemos que b obligatoriamente ha de dividir a 10^m y por lo tanto $b = 2^n5^b$ siendo que $n,b \in \mathbb{N}$.

Aproximación decimal a un número racional. Pasando...

6.2. Números reales

6.2.1. Axioma del supremo

Todo subconjunto de $\mathbb{R}$ no vacío y acotado superiormente tiene supremo y si es acotado inferiormente tiene ínfimo.

$(\mathbb{R}, +, \cdot, \leqslant)$ es un cuerpo ordenado.

Decimal de un número real. Podemos expresar que $x \in \mathbb{R}, \exists z \in \mathbb{Z} | z \leqslant x < z + 1$, a z se le llama parte entera de x, se suele presentar como $e(x)$ o $[x]$.

6.2.2. Propiedad arquimediana de $\mathbb{R}$

$\forall x \in \mathbb{R} | x > 0, \forall y \in \mathbb{R}, \exists n \in \mathbb{N} | nx > y$. Vemos que si $y \leqslant 0$ podemos tomar $n = 1$. Si $y > 0$ podemos tomar $n = e(\frac{y}{x}) + 1$ siendo $nx > y$.

6.2.3. Intervalos en $\mathbb{R}$

Un conjunto $I \subset \mathbb{R}$ es un intervalo si y solo sí cualquier x, y de I tales que $x < y$ cumple que $[x, y] \subset I$.

Racionales y reales son conjuntos densos. Tenemos que para cualquier $a, b \in \mathbb{R}, a < b$: $(a, b) \cap \mathbb{Q} \neq \emptyset$ y que $(a, b) \cap \mathbb{R}/_{\mathbb{Q}} \neq \emptyset$. Es decir: entre dos racionales hay un irracional: si $x < y$ son racionales tenemos que $z = x + \frac{(y-x)\sqrt{2}}{2}$ es irracional y $x < z < y$. Y que entre dos irracionales hay un racional: Si $x < y$ son irracionales, $n = entero(\frac{1}{y-x} + 1)$ vemos que $n > \frac{1}{y-x}$, $1 < n(y - x)$. Por otro lado $m = entero(nx)$. Y así tenemos un número racional que cumple $x < \frac{m+1}{n} < y$.

6.2.4. Intervalos encajados

La propiedad es: $[a_0, b_0] \subset [a_1, b_1] \subset ... \subset [a_n, b_n]$. Siendo $a_{n \leqslant} b_n$:

1. $\bigcap_{n \in \mathbb{N}} [a_n, b_n] \neq \emptyset$
2. Si la distancia $b_n - a_n$de $[a_n, b_n]$ tiende a cero cuando $n \to \infty$, entonces existe un único punto $\alpha \in \bigcap_{n \in \mathbb{N}} [a_n, b_n]$.

7. Capítulo 7. Los números complejos

«En matemáticas es inútil tratar de entender algo. Sólo hay que usarlo»

Johann von Neumann (1903-1957)

7.1. Algunas nociones para su manejo

Teniendo un número complejo de la forma $z = a + bi$:

- Suma: $z + z' = (a + a') + i(b + b')$
- Producto: $z \cdot z' = (a \cdot a' - b \cdot b') + i(a \cdot b' + a' \cdot b)$

Recordamos que $(\mathbb{C}, +, \cdot)$es un cuerpo, existiendo el opuesto y el inverso para cualquier $z \in \mathbb{C}$. El inverso es un número z tal que $z \cdot z^{-1} = (1, 0)$ siendo \((1,0)\) el elemento nulo del producto. z^{-1} es:

$$z^{-1} = (\frac{a}{a^2 + b^2}, \frac{-b}{a^2 + b^2})$$

7.2. Formas de un número complejo

7.2.1. Forma binómica

$$z = a + bi$$

Siendo a la parte real, expresada también como $\Re(z)$ o $Re(z)$. La parte imaginaria $b$se expresa como $\Im(z)$ o $Im(z)$.

7.2.2. Forma trigonométrica

$$z = r(cos\alpha + isen\alpha)$$

Vemos que $a = rcos\alpha$ y que $b = rsen\alpha$La forma trigonométrica facilita la multiplicación de números complejos, sin demostrarlo señalamos: $z \cdot z' = r \cdot r'((cos(\alpha + \alpha')) + i(sen(\alpha + \alpha')))$

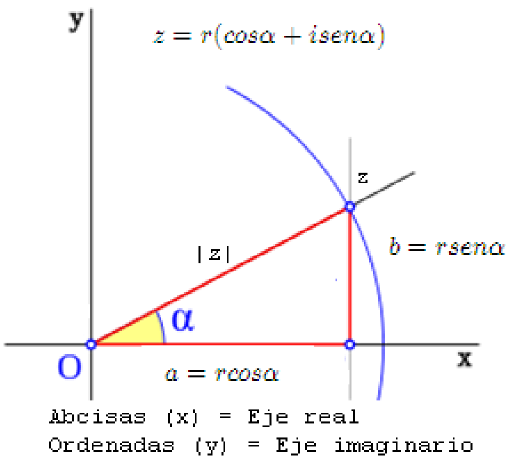


Figura 19: Representación geométrica de un número complejo

Fórmula de Moivre, cuando $|z| = 1$ (r=1):

$$z^n = (cos\alpha + i \cdot sen\alpha)^n = cos \cdot n \cdot \alpha + i \cdot sen \cdot n \cdot \alpha$$

7.2.3. Forma polar

$$z = r_\alpha$$

$r$sería el módulo y α el argumento de z (ángulo).

7.2.4. Forma exponencial

$$e^{i\alpha} = cos\alpha + i \cdot sen\alpha$$

Y vemos que aquí tenemos la famosa **Identidad de Euler**:

$$e^{i\pi} = cos\pi + i \cdot sen\pi = -1 = e^{i\pi} + 1 = 0$$

Que pone en relación a 5 de los más importantes números de las matemáticas (o abstracciones capaces aprehender la naturaleza si quieren ser más poéticos): π, $\sqrt{-1}$, e,0 y 1. Esta notación facilita los cálculos, por ejemplo con las siguientes reglas:

$$-(re^{i\alpha}) = re^{i(\alpha+\pi}$$

Se suma π al exponente porque se le da "media vuelta" al número.

$$(re^{i\alpha})(r'e^{i\alpha'}) = (rr')(e^{i(\alpha+\alpha'})$$

$$(re^{i\alpha})^n = r^n e^{in\alpha})$$

7.2.5. Cálculo de potencias de i

$i^1 = i$, $i^2 = -1$, $i^3 = -i$, $i^4 = 1$. Y ahora vemos que; $i^5 = i^4 \cdot i = i$ y se puede continuar; $i^6 = ...$. Ejemplo de cálculo de i^n: $i^{27} = i^{4 \cdot 6+3} = (i^4)^6 \cdot i^3 = 1^6 \cdot i^3 = 1 \cdot -i = -1$. O por ejemplo: $i^{2664} = i^{666 \cdot 4} = (i^4)^{666} = 1^{666} = 1$.

7.2.6. Conjugado de z

El conjugado de z es $z = a - ib$, siendo alguna de sus propiedades:

$$z + \bar{z} = 2\Re\{z\}$$

$$z - \bar{z} = 2i\Im\{z\}$$

$$z \cdot \bar{z} = a^2 + b^2$$

$$\bar{\bar{z}} = z$$

$$z \bar{+} z' = \bar{z} + \bar{z'}$$

7.2.7. Cuestiones geométricas

$Z_M$es el afijo del punto M en el plano cartesiano. Es decir, un punto del plano con un sistema de coordenadas ortogonal (ejes perpendiculares). Similarmente, z es también el afijo del vector $\overrightarrow{V_z}$ del plano. $|z| = r = \sqrt{a^2 + b^2}$ es el módulo de z, siendo la distáncia euclidiana del punto M al origen de las coordenadas (la hipotenusa). El argumento de z, que expresamos como $arg(z) = \alpha$ sería el ángulo que forma el módulo respecto al eje x (o real), por expresarlo de una forma intuitiva. De esta forma sabremos que z es real si $arg(z) = 0$ y z es un imaginario puro si $arg(z) = \frac{\pi}{2}[Mod2\pi]$.

Cálculo de la forma polar y trigonométrica de un número complejo. Para un número complejo tal como $z = a + ib$, en primer lugar se calcula el módulo de z.

$$[z] = \sqrt{a^2 + b^2}$$

Después se ha de obtener el argumento de z. Para eso obtenemos la tangente $tg\frac{Im}{Re}$ y obtenemos la que correspondiera al primer cuadrante. Será muy útil dibujar un plano cartesiano para representar el número. Hay que conocer la tabla de grados para seno, coseno y tangente, aquí chuleta memotécnica:

	0º	30º	45º	60º	90º
$Sen\ \alpha =$	$\sqrt{0}$	1	2	3	4
			2		
$Cos\ \alpha =$	$\sqrt{4}$	3	2	1	0
			2		
$Tg\ \alpha =$	$\sqrt{0}$	1	2	3	4
	$\sqrt{4}$	3	2	1	0

Se utiliza la tangente que corresponde al primer cuadrante, cambiando el signo. Después se resta el valor del ángulo del cuadrante que corresponda (o, 90, 180, 270, 360) y obtenemos el valor del mismo. Sabiendo las correspondencias de los grados y valores de π damos los valores en radianes. Conociendo el módulo y el argumento se pueden obtener las formas trigonométricas y la polar de un número complejo.

Determinación de las raíces enésimas de un número complejo. Se calcula la forma polar y se aplica la siguiente fórmula:

$$\sqrt[n]{z} = (\sqrt[n]{|z|})_{\frac{\alpha+2k\pi}{n}}$$

Donde$k = 0, 1, 2, ..., n-1$. Ejemplo: Calcular las raíces cúbicas de -1. Obtenemos el módulo de -1, que es igual a 1. Su argumento es π, véase que se el número estaría en el cuadrante 2. De ese modo la forma polar de -1+i0 sería \(1_{\pi}\). Ahora aplicamos la fórmula anterior, obteniendo:

$$k = 0; 1_{\frac{\pi}{3}}$$

$$k = 1; 1_{\pi}$$

$$k = 2; 1_{\frac{5\pi}{3}}$$

Si se desea podemos pasar a la notación binómica de la siguiente forma (a través de la trigonométrica de hecho).

$$1_{\frac{\pi}{3}} = 1(cos\frac{\pi}{3} + i \cdot sen\frac{\pi}{3}) = cos60^{\underline{o}} + i \cdot sen60^{\underline{o}} = \frac{1}{2} + i\frac{\sqrt{3}}{2}$$

Véase que$\frac{\pi}{3} = \frac{180^{\underline{o}}}{3} = 60^{\underline{o}}$

$$1_{\pi} = 1(cos\pi + i \cdot sen\pi) = cos0^{\underline{o}} + i \cdot sen0^{\underline{o}} = -1 + i \cdot 0$$

Se indica cos$0^{\underline{o}}$ porque se calculan los ángulos según el primer cuadrante, pero hay que mirar en que cuadrante estan realmente para utilizar el signo que corresponda.

$$1_{\frac{5\pi}{3}} = cos\frac{5 \cdot 180^{\underline{o}}}{3} + i \cdot sen300^{\underline{o}} = cos60 + i \cdot cos60 = \frac{1}{2} - i\frac{\sqrt{3}}{2}$$

Se ha procedido igual que antes, calculando la correspondencia del grado y el valor fraccionario del número.