Ingeniería Matemática
FACULTAD DE CIENCIAS
FÍSICAS Y MATEMÁTICAS
UNIVERSIDAD DE CHILE
Oficina de Publicaciones

INTRODUCCIÓN AL ÁLGEBRA

Tutorías y Guías del Curso

Semestre Otoño 2021

(versión pandemia Covid19)

Índice general

Prefacio

La primera versión de este apunte fue elaborada el 2005 por Iván Rapaport y David Gómez.

Durante la segunda mitad de 2016 el apunte fue revisado, generándose esta segunda versión. Las modificaciones fueron realizadas por Marcos Kiwi, Martín Matamala y Leonardo Sánchez. Iván Rapaport participó en calidad de editor y Marcos Kiwi coordinó el proceso. Sebastián Pérez ayudó en la composición tipográfica y Natacha Astromujoff brindó apoyo administrativo.

Un insumo fundamental y punto de partida para la actualización del apunte fue un listado de sugerencias confeccionado durante la primera mitad de 2016 y en el cual colaboraron Pablo Dartnell, Marcos Kiwi, Martín Matamala, Daniel Quiroz, Iván Rapaport, Leonardo Sánchez, Maya Stein y José A. Soto.

La versión revisada del apunte fue utilizada a partir del 2017 en los cursos de Introducción al Álgebra (MA1101). Esto ha permitido detectar errores y omisiones que han sido corregidas por Marcos Kiwi (2018) y Martín Matamala (2019) basándose en las valiosas observaciones y sugerencias de Benjamín Alvial, Paulina Bernales, Nicolás Calbucura, Pablo Dartnell, Sebastián Donoso, Alexis Fuentes, Matías Godoy, Javiera Hernández, Daniel Lobos, Arturo Merino, Francisca Ramírez, Iván Rapaport, Juan Pedro Ross, Claudia San Martín, José A. Soto, Maya Stein y Mauricio Valderrama.

Producto de la pandemia de COVID19, la Facultad de Ciencias Físicas y Matemáticas de la Universidad de Chile optó por reducir en 1 semana la duración usual del semestre Otoño 2021. Por ello, los contenidos del curso y este apunte fueron adaptados y re-organizados en 14 semanas (en contraste con las tradicionales 15 semanas).

Abril 2021. Santiago, Chile.

Material opcional

En este apunte se incluyen algunas demostraciones y comentarios de caracter complementario. Estas partes aparecen enmarcadas en un recuadro de fondo gris. Su lectura para el alumno así como su discusión por parte del profesor son de caracter opcional.

Fe de erratas

Se mantendrá una página Web con una lista de errata a la cual se podrá acceder a través de la siguiente página: `http://docencia.dim.uchile.cl/ma1101/`

Se agradece notificar cualquier error que sea detectado para removerlo. Sugerencias y comentarios también son bienvenidos. Favor enviarlos a: `apuntealg@dim.uchile.cl`

SEMANA 01:

Lógica

Ingeniería Matemática
FACULTAD DE CIENCIAS
FÍSICAS Y MATEMÁTICAS
UNIVERSIDAD DE CHILE

1.1 Introducción

La lógica le proporciona a las matemáticas un lenguaje claro y un método preciso para demostrar nuevas afirmaciones a partir de otras ya establecidas o dadas (a estas últimas se les denomina axiomas). Por ejemplo, las definiciones, nociones primarias de geometría clásica y los axiomas de Euclides, junto con las reglas de deducción lógica, son los que dan lugar a los teoremas (afirmaciones correctas) de la geometría euclidiana.

Un ejemplo de noción primaria es la de punto. Un ejemplo de axioma es el que dice que por un punto ubicado fuera de una recta L pasa una y sólo una recta paralela a L. Un ejemplo de teorema es: *La suma de los ángulos interiores de cualquier triángulo es* $180°$.

Sin la lógica los axiomas serían un montón de verdades aceptadas, pero no tendrían consecuencias. La lógica, sin embargo, les da sentido y permite deducir nuevas verdades (teoremas) que antes no conocíamos.

Al ser la lógica la que estipula las reglas de deducción válidas, no es de extrañar que comencemos este apunte con su estudio. El punto de partida en ella son las nociones primarias tales como proposición, valor de verdad y las formas de operar con verdades preestablecidas a través de conectivos lógicos.

1.2 Proposiciones y valor de verdad

Definición 1.1 (Proposición lógica) *Una proposición es una afirmación que siempre toma uno de los valores de verdad posibles: verdadero (V) o falso (F).*

Ejemplo:

- V y F son proposiciones con valores de verdad verdadero y falso, respectivamente.
- En el contexto de la aritmética, $2+1=5$ y $1 \geq 0$ corresponden efectivamente a proposiciones. Más aún, sus valores de verdad son F y V, respectivamente.
- También son proposiciones: "Estoy estudiando ingeniería" y "Está lloviendo en Castro".

- Si E es un conjunto, la frase "e es un elemento de E" (o "e pertenece a E", que dice exactamente lo mismo) es una proposición, usualmente, denotada $e \in E$. La proposición es verdadera si el elemento e, realmente, está en el conjunto E, y es falsa en caso contrario.
- No es una proposición: "Siéntate".

$\diamondsuit$

Típicamente, notaremos a las proposiciones con letras minúsculas: p, q, r, etc., y en ocasiones las distinguiremos con sub-índices como $p_1, p_2, ..., p_n, ...$

1.3 Conectivos lógicos

Los conectivos lógicos permiten crear nuevas proposiciones a partir de otras ya conocidas. El valor de verdad de la nueva proposición dependerá de los valores de verdad de sus componentes. Esta dependencia se explicita a través de una tabla, llamada **tabla de verdad**.

Definición 1.2 (Negación) *La proposición $\overline{p}$ (a menudo también denotada $\neg p$ o $\sim p$) se lee "no p" y es aquella cuyo valor de verdad es siempre distinto al de p.*

Esto se explicita a través de la siguiente tabla de verdad.

p	$\overline{p}$
V	F
F	V

Ejemplo:

- La negación de "mi papá ya cumplió 55 años" es "mi papá aún no cumple 55 años".
- La negación de "e pertenece a E" es "e no pertenece a E" y se denota $e \notin E$.

$\diamondsuit$

Por actuar sobre una sola proposición, decimos que la negación es un conectivo lógico unario. El resto de los conectivos lógicos que definiremos actúan sobre dos proposiciones, por lo que nos referimos a ellos como conectivos lógicos binarios.

Definición 1.3 (O lógico o disyunción) *La proposición $p \vee q$, que se lee "p o q", es verdadera cuando al menos una de las proposiciones p o q es verdadera.*

En otras palabras, tal como se aprecia en la siguiente tabla de verdad, si se afirma que se tiene $p \vee q$ lo que se está diciendo es que p y q no son ambas falsas.

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

Ejemplo: La proposición "mañana lloverá o mañana no lloverá" es verdadera. ♢

Definición 1.4 (Y lógico o conjunción) *La proposición $p \wedge q$ se lee "p y q". Tal como se aprecia en la siguiente tabla de verdad, si se afirma que se tiene $p \wedge q$, lo que se está diciendo es que ambas proposiciones son verdaderas.*

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

Definición 1.5 (Implicancia) *La proposición $p \Rightarrow q$ se lee "p implica q" o "si p, entonces q".*

*Es falsa sólo cuando p es verdadera y q es falsa. A p se le llama la **hipótesis** y a q la **conclusión** de la proposición $p \Rightarrow q$.*

p	q	$p \Rightarrow q$
V	V	V
V	F	F
F	V	V
F	F	V

Ejemplo: La proposición "si el señor K está en Valdivia[1], entonces el señor K está en Chile" es verdadera. En efecto, según la definición de implicacia, la única opción para que la proposición sea falsa es que la hipótesis, "el señor K está en Valdivia", sea verdadera, y que la conclusión, " el señor K está en Chile", sea falsa. Como no puede ocurrir que alguien esté en Valdivia y no esté en Chile, la opción antes descrita nunca ocurre. ♢

Es importante insistir en que la implicancia $p \Rightarrow q$ puede ser verdadera en tres situaciones: cuando p y q son verdaderas, cuando p y q son falsas y, cuando p es falsa y q es verdadera. El siguiente es un ejemplo de la tercera posibilidad.

Ejemplo: Sea p la proposición "$1 = 2$", la que es evidentemente falsa en el contexto de la aritmética. Multiplicando ambos lados de la igualdad por 0 concluimos que $0 = 0 \cdot 1 = 0 \cdot 2 = 0$. Luego, si q es la proposición "$0 = 0$", sigue que, a partir de algo falso como p, es válida la deducción de algo verdadero como q. Es decir, es verdadero que $p \Rightarrow q$. ♢

Definición 1.6 (Equivalencia) *La proposición $p \iff q$ se lee "p es equivalente con q" (o "p si y sólo si q").*

Es verdadera cuando p y q tienen el mismo valor de verdad y falsa cuando estos valores difieren.

p	q	$p \iff q$
V	V	V
V	F	F
F	V	F
F	F	V

[1] Capital de la Región de los Ríos, Chile

Ejemplo: Por ejemplo "el paralelogramo dibujado en la pared tiene todos sus ángulos iguales" es equivalente con la proposición "las diagonales del paralelogramo dibujado en la pared miden lo mismo". O bien ambas son verdaderas o bien ambas son falsas. ♢

Dado un conjunto de proposiciones podemos formar otras más complejas combinándolas, recursivamente, mediante conectivos lógicos. Específicamente, si ϕ y φ son proposiciones, entonces también lo son $\overline{(\phi)}$ y $(\phi) \star (\varphi)$ donde $\star$ es cualquier conectivo lógico binario (por ejemplo, $\vee$, $\wedge$, $\Rightarrow$, ...).

Ejemplo: $((p \Rightarrow q) \vee s) \iff \overline{(p \wedge s)}$ es una proposición. ♢

Para evitar expresiones demasiado complicadas usaremos convenciones que nos permitirán dar por sobreentendidos, y por lo tanto eliminar, algunos paréntesis. Lo haremos de manera similar al caso de las operaciones aritméticas + y $\times$, donde estamos acostumbrados a omitir los paréntesis de una expresión como $2 + (3 \times 5)$, pero sabemos que no podemos omitirlos de $(2 + 3) \times 5$. Esto último porque la convención es que $\times$ se realiza primero, es decir, tiene "mayor precedencia" que +. Para los conectivos lógicos, adoptamos el siguiente orden de precedencia:

$$\begin{array}{rc} \text{Mayor:} & \neg \\ \text{Intermedio:} & \vee, \wedge, \\ \text{Menor:} & \Rightarrow, \iff . \end{array}$$

Si $\star$ y $\circ$ son dos conectivos lógicos y $\star$ tiene mayor precedencia que $\circ$, entonces podemos omitir, sin temor a generar ambigüedad, los paréntesis de la expresión $(p \star q) \circ r$. Dicho de otra forma, la expresión $p \star q \circ r$ se entenderá que denota $(p \star q) \circ r$ dado que $\star$ tiene mayor precedencia que $\circ$. Por la misma razón, no se pueden omitir los paréntesis de la expresión $p \star (q \circ r)$.

Ejemplo:

- $((p \Rightarrow q) \vee s) \iff \overline{(p \wedge s)}$ se puede escribir como $(p \Rightarrow q) \vee s \iff \overline{p \wedge s}$.
- $[(\overline{p} \Rightarrow q) \wedge (q \Rightarrow r)] \Rightarrow (p \Rightarrow r)$ se puede escribir como $(\overline{p} \Rightarrow q) \wedge (q \Rightarrow r) \Rightarrow (p \Rightarrow r)$.

♢

De ahora en adelante, normalmente, omitiremos los paréntesis superfluos.

1.4 Tautologías

Definición 1.7 (Tautología) *Una tautología es una proposición que, sin importar el valor de verdad de las proposiciones que la constituyen, es siempre verdadera.*

Ejemplo: Las siguientes proposiciones son tautologías:

- $p \vee \overline{p}$.
- $p \Rightarrow p \vee q$.

- $(p \iff q) \iff (q \iff p)$.

$\diamondsuit$

Un argumento que permite saber que una proposición es una tautología se llama una **demostración** de ésta. Las demostraciones serán presentadas en el siguiente formato:

Dem. $\leftarrow$ indicando el inicio del argumento

indicando el fin del argumento $\rightarrow$ $\square$

Las tablas de verdad que usamos en la definición de los conectivos lógicos permiten, de una forma sencilla, aunque tediosa y poco informativa, verificar que una proposición es una tautología. Estas son tablas cuyas primeras n columnas están asociadas a las n proposiciones que aparecen en la proposición. En estas columnas aparecen todos las posibles combinaciones de valores de verdad de las n proposiciones. Luego, la tabla de verdad tendrá 2^n filas. Las siguientes columnas de la tabla corresponden a cada uno de los conectivos lógicos que aparecen en la proposición. Para cada una de estas columnas, en cada fila, se anota el valor de verdad de la proposición que resulta del uso del conectivo cuando se da la combinación de valores de verdad a los que corresponde la fila de la tabla. El orden en que aparecen estas columnas es tal que permite su cálculo en base a las columnas previamente llenadas. La última columna corresponde a la proposición que se quiere determinar si es tautología, y se calcula igual que las recién descritas. Si ocurre que todas las filas de esta columna tienen el valor verdadero, entonces la proposición será una tautología.

Ejemplo: Demostraremos, desarrollando una tabla de verdad, que la primera proposición del ejemplo anterior es tautología.

p	$\overline{p}$	$p \vee \overline{p}$
V	F	V
F	V	V

$\diamondsuit$

Todas las tautologías son equivalentes entre sí y se pueden reemplazar por la proposición V. Por ejemplo $p \vee \overline{p} \iff V$. Esto es similar a lo que hacemos cuando reemplazamos el término $(x - x)$ por 0.

Definición 1.8 (Contradicción) *Así como existen las tautologías existen las contradicciones. Son proposiciones siempre falsas.*

Las contradicciones son todas equivalentes a la proposición F. Por ejemplo, $p \wedge \overline{p}$.

Claramente, una proposición p es una contradicción si y sólo si $\overline{p}$ es una tautología.

Vamos a listar una serie de tautologías de la forma $A \iff B$. El uso que se les dará es el siguiente. Cada vez que en una cierta proposición aparezca la expresión A, puede reemplazarse por B. Y viceversa. El lector debe dar, como ejercicio, una demostración de la condición de tautología de algunas de ellas usando tablas de verdad.

Proposición 1.9 (Tautologías básicas) *Las siguientes son tautologías:*

- *Dominancia:* $p \vee V \iff V, \quad p \wedge F \iff F.$
- *Identidad:* $p \wedge V \iff p, \quad p \vee F \iff p.$
- *Idempotencia:* $p \wedge p \iff p, \quad p \vee p \iff p.$
- *Doble negación:* $\neg(\neg p) \iff p$ *(recuerde que* $\neg p$ *es lo mismo que* $\overline{p}$*).*
- *Tercio excluso:* $p \vee \overline{p} \iff V.$
- *Consistencia:* $p \wedge \overline{p} \iff F.$
- *Absorción:* $p \vee (p \wedge q) \iff p, \quad p \wedge (p \vee q) \iff p.$
- *Relajación:* $p \wedge q \Rightarrow p, \quad p \Rightarrow p \vee q.$
- *Caracterización de la implicancia:* $(p \Rightarrow q) \iff \overline{p} \vee q.$

Proposición 1.10 (Álgebra Booleana) *Las siguientes son tautologías:*

- *Leyes de De Morgan:* $\overline{p \wedge q} \iff \overline{p} \vee \overline{q}, \quad \overline{p \vee q} \iff \overline{p} \wedge \overline{q}.$
- *Conmutatividad.*
  - *del* $\vee$*:* $p \vee q \iff q \vee p.$
  - *del* $\wedge$*:* $p \wedge q \iff q \wedge p.$
- *Asociatividad.*
  - *del* $\vee$*:* $p \vee (q \vee r) \iff (p \vee q) \vee r.$
  - *del* $\wedge$*:* $p \wedge (q \wedge r) \iff (p \wedge q) \wedge r.$
- *Distributividad.*
  - *del* $\wedge$ *con respecto al* $\vee$*:*

    $$p \wedge (q \vee r) \iff (p \wedge q) \vee (p \wedge r), \qquad (q \vee r) \wedge p \iff (q \wedge p) \vee (r \wedge p).$$

  - *del* $\vee$ *con respecto al* $\wedge$*:*

    $$p \vee (q \wedge r) \iff (p \vee q) \wedge (p \vee r), \qquad (q \wedge r) \vee p \iff (q \vee p) \wedge (r \vee p).$$

- *Transitividad.*
  - *del* $\Rightarrow$*:*

    $$(p \Rightarrow q) \wedge (q \Rightarrow r) \Rightarrow (p \Rightarrow r)$$

  - *de la* $\iff$ *:*

    $$(p \iff q) \wedge (q \iff r) \Rightarrow (p \iff r)$$

La asociatividad del $\wedge$ y del $\vee$ nos permite omitir algunos paréntesis. Al igual que la asociatividad del $+$ nos permite omitir algunos paréntesis de la expresión $(1+(2+(3+4)))$ y simplemente escribir $1+2+3+4$, podemos también omitir los paréntesis de $(p \wedge (q \wedge (r \wedge s)))$ y escribir $p \wedge q \wedge r \wedge s$.

Proposición 1.11 *Las siguientes afirmaciones son tautologías:*

*(*I*)* *Equivalencia dividida:* $(p \iff q) \iff (p \Rightarrow q) \wedge (q \Rightarrow p).$

*(*II*)* *Demostración por casos:*

$$(p' \vee p'' \implies q) \iff (p' \implies q) \wedge (p'' \implies q).$$

Verificación exploratoria y simbólica

Al verificar que cierta proposición es tautología evitaremos usar tablas de verdad y sólo nos permitiremos usar (como conocidas) las tautologías que aparecen en las secciones anteriores. Esto lo haremos de alguna de las dos formas que se ilustran a continuación.

Ejemplo (de demostración exploratoria): Demostremos exploratoriamente, que la siguiente proposición es tautología:

$$(p \Rightarrow \overline{q}) \wedge (r \Rightarrow q) \Rightarrow (p \Rightarrow \overline{r}).$$

Vamos a **asumir** que tanto $p \Rightarrow \overline{q}$ como $r \Rightarrow q$ son verdaderas. Es decir, nos ocupamos sólo del caso en que la hipótesis es verdadera (el otro caso es trivial, puesto que por definición de la implicancia ésta es verdadera cuando la hipótesis es falsa).

Lo que debemos hacer es concluir que $p \Rightarrow \overline{r}$ es verdadera.

- **Caso 1 (p es falsa):** Este caso es fácil, pues de la definición de implicancia se tiene inmediatamente que $F \Rightarrow \overline{r}$ es verdadera.
- **Caso 2 (p es verdadera):** Como asumimos que $p \Rightarrow \overline{q}$ es verdadera, se tiene que q es falsa. Como $r \Rightarrow q$ se asume verdadera y como q es falsa, r tiene que ser falsa. Por lo tanto, como r es falsa, se tiene que $p \Rightarrow \overline{r}$ es verdadera.

$\diamondsuit$

La aplicación iterada de la transitividad del $\Rightarrow$ o de la $\iff$ permite extender su uso a tres o más términos. En efecto, la proposición

$$(p \iff q) \wedge (q \iff r) \wedge (r \iff t) \Rightarrow (p \iff t)$$

es una tautología.

Al igual que en el ejemplo anterior, esto puede mostrarse mediante una demostración exploratoria. En este caso, suponiendo que $p \iff t$ es falsa y demostrando que la proposición $(p \iff q) \wedge (q \iff r) \wedge (r \iff t)$ es falsa. Para esto último bastará con ver que alguna de las proposiciones $(p \iff q)$, $(q \iff r)$ o $(r \iff t)$ es falsa.

Partamos suponiendo que p es verdadera y que t es falsa. Si q es falsa entonces $p \iff q$ es falsa y se obtiene la conclusión. Así, podemos continuar suponiendo que q es verdadera. Si r es falsa, entonces, $q \iff r$ es falsa y se termina. En otro caso, r es verdadera lo que nos dice que $r \iff t$ es falsa. Realice como ejercicio un análisis similar para el caso donde p es falsa y t es verdadera.

Para facilitar la lectura, proposiciones como

$$(p \iff q) \wedge (q \iff r) \qquad \text{y} \qquad (p \implies q) \wedge (q \implies r)$$

suelen escribirse verticalmente como se muestra a continuación (ver su uso en el ejemplo de demostración simbólica).

$$\begin{array}{lll} p & \iff & q \\ & \iff & r \end{array} \qquad \text{y} \qquad \begin{array}{lll} p & \implies & q \\ & \implies & r \end{array}$$

También se suele usar esta escritura cuando se combinan los conectivos $\iff$ y $\implies$. Por ejemplo, la proposición

$$[(p \iff q) \wedge (q \implies r) \wedge (r \iff s) \wedge (s \implies t)] \implies (p \implies t)$$

se muestra continuación escrita de manera vertical (ver como ejercicio que esta proposición es una tautología).

$$\begin{aligned} p &\iff q \\ &\implies r \\ &\iff s \\ &\implies t. \end{aligned}$$

Ejemplo (de demostración simbólica):

Probemos que la siguiente proposición es una tautología:

$$(p \iff q) \iff (\overline{p} \wedge \overline{q}) \vee (p \wedge q).$$

En efecto:

$$\begin{aligned} (p \iff q) &\iff (p \Rightarrow q) \wedge (q \Rightarrow p) && \text{(por Equivalencia dividida)} \\ &\iff (\overline{p} \vee q) \wedge (\overline{q} \vee p) && \text{(por Caracterización de la implicancia)} \\ &\iff [(\overline{p} \vee q) \wedge \overline{q}] \vee [(\overline{p} \vee q) \wedge p] && \text{(por Distributividad del } \wedge \text{ c/r al } \vee) \\ &\iff [(\overline{p} \wedge \overline{q}) \vee (q \wedge \overline{q})] \vee [(\overline{p} \wedge p) \vee (q \wedge p)] \\ & && \text{(por Distributividad del } \wedge \text{ c/r al } \vee) \\ &\iff [(\overline{p} \wedge \overline{q}) \vee F] \vee [F \vee (q \wedge p)] && \text{(por Consistencia)} \\ &\iff (\overline{p} \wedge \overline{q}) \vee (p \wedge q). && \text{(por Identidad)} \end{aligned}$$

Usando la transitividad de $\iff$ se concluye que $(p \iff q) \iff (\overline{p} \wedge \overline{q}) \vee (p \wedge q)$. $\diamondsuit$

Nota: Las constantes reiteraciones de "p es verdadera" o "A es una tautología" pronto se tornan molestas. En lo que sigue, se ocupan expresiones alternativas tales como "se tiene p", "entonces p", "se cumple p", "se deriva p", "p es cierta", etc.

1.5 Técnicas de demostración.

Las tautologías que se listan en la Proposición 1.11 y en el siguiente resultado son de gran utilidad para demostrar proposiciones pues cada una da lugar a una técnica de demostración. Como ejercicio el lector debe probarlas, ya sea de manera simbólica o exploratoria.

Proposición 1.12 *Las siguientes proposiciones son tautologías:*

*(1) Regla de separación (**Modus Ponens**):* $p \wedge (p \Rightarrow q) \Rightarrow q$.

(II) *Contrarrecíproca:* $(p \Rightarrow q) \iff (\overline{q} \Rightarrow \overline{p})$.

(III) *Contradicción o Reducción al absurdo:* $[(p \Rightarrow q) \iff V] \iff [p \wedge \overline{q} \Rightarrow F]$.

La tautología de la parte (III) de la proposición anterior nos dice que si queremos demostrar $p \Rightarrow q$, basta demostrar $p \wedge \overline{q} \Rightarrow F$. Otras formas alternativas son las siguientes.

Corolario 1.13 (Variantes de Contradicción) *Se tienen las siguientes proposiciones:*

- $(p \Rightarrow q) \iff (p \wedge \overline{q} \Rightarrow F)$.
- $(q \iff V) \iff (\overline{q} \Rightarrow F)$.

Dem. Ambas tautología vienen de la Proposición 1.12 parte (III). La primera notando que

$$(p \Rightarrow q) \iff [(p \Rightarrow q) \iff V].$$

La segunda, cambiando p por V y observando que $(V \Rightarrow q) \iff q$ y que $V \wedge \overline{q} \iff \overline{q}$. □

A continuación ilustramos cómo una de las tautologías de la Proposición 1.12 y otra del Corolario 1.13 dan lugar, cada una, a una importante estrategia de demostración. En las secciones siguientes haremos algo similar para las tautologías restantes.

Ejemplo (de demostración por Contrarrecíproca): Sabemos de la enseñanza preuniversitaria que a es un número racional, si $a = m/n$ con m y n enteros, $n \neq 0$. Probemos que:

$$3a \text{ no es racional} \implies a \text{ no es racional.}$$

La técnica de demostración por contrarrecíproca nos dice que es equivalente probar que

$$a \text{ es racional} \implies 3a \text{ es racional.}$$

Comprobemos lo último. Supongamos que a es racional. Luego, $a = m/n$ con m y n enteros, $n \neq 0$. Sigue que $3a = 3m/n$, o sea $3a = m'/n$ con $m' = 3m$ entero y $n \neq 0$ entero, por lo que concluimos que $3a$ es racional.

Nota: Es ilustrativo que el lector intente dar una demostración "directa". Es decir, suponga que $3a$ no es racional, y pruebe que a no es es racional. No es evidente cómo hacer dicha demostración. ♢

Ejemplo (de demostración por Contradicción): Probemos que $\sqrt{2}$ no es racional.

Recordemos de la enseñanza preuniversitaria que un número entero n es un factor de otro número entero m si existe un tercer entero k que cumple $nk = m$. También se dice que n es un divisor de m. Cuando 2 es un factor de m decimos que m es par y si no lo es, que m es impar. Con esto, se verifica que si un entero m es tal que m^2 es par, entonces m es par.

La técnica de demostración por contradicción (versión del Corolario 1.13) nos dice que para ver que $\sqrt{2}$ no es racional, basta suponer que $\sqrt{2}$ es racional y deducir algo falso.

Partamos suponiendo que $\sqrt{2} = m/n$ para m y n enteros positivos.

Por una parte, como podemos cancelar cualquier factor común que tengan m y n, podemos suponer que alguno de ellos no es par.

Por otra parte, elevando al cuadrado la identidad $\sqrt{2} = m/n$ y despejando, sigue que $m^2 = 2n^2$. Luego, m^2 es par y se tiene que m es par. O sea, $m = 2k$ para algún entero k. Reemplazando en la identidad $m^2 = 2n^2$ y despejando, obtenemos que $n^2 = 2k^2$, por lo que n^2 es par y, argumentando como antes, concluimos que n es par.

Pero esto no puede ser, puesto que entonces n y m son pares y habíamos dicho que alguno de ellos no lo era. Hemos deducido algo claramente falso, como queríamos (decimos que llegamos a una contradicción). $\diamondsuit$

Guía Básica

Determinar la veracidad de las siguientes afirmaciones:

1. 25-11 no corresponde a una proposición lógica.
2. "¿Podrás venir mañana?" es una proposición lógica.
3. $x - 11$ corresponde a una proposición lógica, si se reemplaza x por un número.
4. $25 - 11 \leq 0$ corresponde a una proposición lógica.
5. El valor de verdad de la proposición $\overline{p}$ es siempre distinto al de p.
6. Existen proposiciones lógicas p tales que $\overline{p}$ tiene el mismo valor de verdad que el de p.
7. Si p es falsa, entonces la proposición $p \vee q$ es siempre falsa.
8. La proposición $p \vee q$ es verdadera cuando p y q no son ambas falsas.
9. La proposición $p \vee q$ es verdadera cuando al menos una de las proposiciones p ó q es verdadera.
10. La proposición $p \wedge q$ es falsa sólo si p y q son falsas.
11. Existe una proposición lógica p tal que $p \wedge q$ es siempre verdadera, sin importar el valor de verdad de q.
12. Basta que p sea falsa, para que la proposición $p \wedge q$ sea siempre falsa.
13. Una proposición compuesta es tautología, si, sin importar el valor de verdad de las proposiciones que la constituyen, es verdadera.
14. Dada una proposición compuesta p, si existe una asignación de valores de verdad para las proposiciones que la constituyen que la haga verdadera, entonces p es una tautología.
15. Una tautología cualquiera q, es siempre equivalente a la proposición $p \implies p$.
16. El valor de verdad de la proposición $p \vee \overline{p}$ es siempre el mismo, sin importar el valor de verdad de p.
17. Existe un valor de verdad para p, tal que la proposición $p \vee \overline{p}$ es falsa.
18. El valor de verdad de la proposición $(p \wedge \bar{q}) \vee (p \implies q)$ puede ser falso.
19. La negación de la proposición $p \vee \bar{q}$ es $\overline{p} \vee q$.
20. La negación de la proposición $p \vee \bar{q}$ es $\overline{p} \wedge q$.
21. La negación de la proposición $p \vee q$ es $\overline{p} \vee \bar{q}$.
22. La proposición $(p \vee q) \vee r$ es equivalente a la proposición $(p \vee r) \vee (q \vee r)$.
23. La proposición $(p \vee q) \vee r$ siempre tiene el mismo valor de verdad que la proposición $(r \vee q) \vee p$.
24. La proposición $(p \vee q) \vee r$ siempre tiene el mismo valor de verdad que la proposición $(p \vee r) \wedge (q \vee r)$.
25. La proposición $(p \wedge q) \vee p$ es verdadera sólo cuando q es verdadera.
26. La proposición $(p \wedge q) \vee p$ es verdadera si p es verdadera.

27. Si la proposición $(p \wedge q) \vee p$ es falsa, necesariamente q es falsa.
28. La proposición $p \implies F$ es siempre falsa.
29. La proposición $p \implies \overline{p}$ es siempre falsa.
30. La proposición $p \implies q$ es siempre verdadera si el valor de verdad de p es falso.
31. Si la proposición $p \implies q$ es verdadera y p también lo es, necesariamente q es verdadera.
32. Si la proposición $p \implies (q \implies r)$ es verdadera y p también lo es, necesariamente r es verdadera.
33. Si la proposición $(p \implies q) \implies r$ es falsa y p es verdadera, necesariamente q es verdadera.
34. La proposición $p \iff V$ tiene siempre el mismo valor de verdad que p.
35. La proposición $p \iff F$ es equivalente a la proposición $\overline{p} \vee F$.
36. La proposición $(p \iff q) \implies (p \implies q)$ es una tautología.
37. Si la proposición $(r \implies p) \wedge (p \implies q)$ es verdadera, la proposición $r \implies q$ también lo es.
38. La proposición $(\bar{q} \implies \overline{p}) \wedge (q \implies r) \implies (\bar{r} \implies \overline{p})$ es una tautología.
39. La proposición $\overline{(p \implies q)} \iff (\overline{p} \implies \bar{q})$ es una tautología.
40. La negación de la proposición $p \implies q$ es $(p \wedge \bar{q})$.
41. La negación de la proposición $p \implies \bar{q}$ es $\overline{p} \implies q$.

Guía de Ejercicios

1. Demuestre usando tablas de verdad que las siguientes proposiciones, enunciadas en el texto del apunte, son tautologías:

   a) $p \vee \overline{p} \iff V$.
   b) $\overline{(p \implies q)} \iff \overline{p} \vee q$.
   c) $\overline{(p \vee q)} \iff \overline{p} \wedge \overline{q}$.
   d) $(q \vee r) \wedge p \iff (q \wedge p) \vee (r \wedge p)$.

2. Escriba las siguientes proposiciones lógicas, de manera equivalente, sólo usando los conectivos lógicos de implicancia ($\implies$) y negación ($\neg$):

   a) $p \vee q$.
   b) $p \wedge (q \vee \overline{r})$.
   c) $\overline{((p \wedge q) \implies r)} \iff \overline{r} \wedge q$.
   d) $\overline{(\overline{p} \wedge q)} \wedge \overline{(p \vee \overline{r})}$.

3. Se define el conectivo lógico $p|q \iff \overline{p} \vee \overline{q}$. Escriba usando sólo el conectivo $|$, proposiciones equivalentes a las siguientes:

a) $\overline{p}$.
b) $p \vee q$.
c) $p \wedge q$.
d) $p \implies q$.

4. Sean p, q, r proposiciones lógicas. Demostrar usando tablas de verdad que las siguientes proposiciones son tautologías:

a) $p \implies p \vee q$.
b) $(p \iff q) \iff (p \wedge q) \vee (\overline{p} \wedge \overline{q})$.
c) $(p \iff q) \wedge (q \iff r) \implies (p \iff r)$.
d) $\overline{(p \iff q)} \iff (\overline{p} \iff q)$.
e) $(p \wedge \overline{q} \implies \overline{p}) \implies (p \implies q)$.

5. Sean p, q, r proposiciones lógicas. Demostrar **sin** usar tablas de verdad que las siguientes proposiciones son tautologías:

a) $(p \implies \overline{q}) \wedge (\overline{r} \vee q) \wedge r \implies \overline{p}$.
b) $p \wedge (p \implies q) \implies q$.
c) $[(p \wedge \overline{q}) \implies \overline{p}] \implies (p \implies q)$.
d) $(p \wedge q \implies r) \iff (p \wedge \overline{r} \implies \overline{q})$.
e) $p \wedge q \iff (p \vee q) \wedge (p \iff q)$.

6. En cada caso, con la información entregada, determine el valor de verdad de la proposición r:

a) $r \implies q$ es falsa.
b) $q \implies \overline{r}$ es falsa.
c) $p \implies q \vee \overline{r}$ es falsa.
d) $\overline{r} \iff q$ es verdadera y $p \wedge q \implies s$ es falsa
e) $(r \implies p) \implies p \wedge \overline{q}$ es verdadera y q es verdadera.

Guía de Problemas

1. Sean p, q, r proposiciones. Probar sin usar tablas de verdad que la proposición presentada en cada item es una tautología. Trate de aprovechar la forma que tiene cada proposición, usualmente el hecho de que sea una implicancia.

a) (20 min.) $(p \vee q \iff p \wedge r) \implies (q \implies p) \wedge (p \implies r)$.
b) (20 min.) $(p \implies \overline{q}) \wedge (r \implies q) \implies (p \implies \overline{r})$.
c) (20 min.) $(p \implies q) \implies [\overline{(q \wedge r)} \implies \overline{(p \wedge r)}]$.
d) (20 min.) $(p \implies \overline{q}) \wedge (\overline{r} \vee q) \wedge r \implies \overline{p}$.

2. En esta parte, dada una hipótesis (una proposición que se sabe es verdadera), deberá estudiar el valor de verdad de otra proposición.

a) (20 min.) Sean p, q, r proposiciones. Averiguar si la equivalencia $p \vee (q \wedge r) \iff (p \vee r) \wedge q$ puede ser verdadera sin que lo sea la implicancia $p \implies q$.

b) (25 min.) Determine el valor de verdad de las proposiciones p, q, r y s si se sabe que la siguiente proposición es verdadera.

$$[s \implies r \vee \overline{r}] \implies \overline{(p \implies q)} \wedge s \wedge \overline{r}.$$

c) (25 min.) Sean p, q, r, s proposiciones que satisfacen que la siguiente proposición es verdadera:

(q es verdadera) $\wedge$ [$p \wedge q$ no es equivalente con ($r \iff s$)].

Demuestre que el valor de verdad de la proposición:

$$(p \wedge r) \vee (q \implies s) \implies p \vee (r \wedge s)$$

es verdadero para todas las combinaciones de valores veritativos que cumplen la hipótesis.

3. Para p, q y r proposiciones, determine cuáles de las siguientes proposiciones son tautologías, contradicciones o ni una ni la otra.

a) $[(p \iff q) \iff r] \iff [p \iff (q \iff r)]$.
b) $[(p \Rightarrow q) \Rightarrow r] \iff [p \Rightarrow (q \Rightarrow r)]$.
c) $(p \iff q) \wedge r \iff (p \wedge r \iff q \wedge r)$.
d) $(p \wedge q \iff r) \iff (p \iff r) \wedge (q \iff r)$.

4. Demuestre que si el producto de dos números es $1/3$, entonces ambos son racionales o ninguno lo es. ¿Qué estrategías de demostración son útiles?

5. Demuestre que si $\sqrt{3} = m/n$ con m y n enteros, entonces m y n son múltiplos de 3. Use esto para demostrar que $\sqrt{3}$ no es racional mediante un argumento por contradicción. Trate de repertir el argumento para $\sqrt{4}$ y explique por qué no es válido.

6. Sean p, q, r, s y t proposiciones. Sabiendo que las proposiciones en el lado izquierdo son tautologías determine cuáles de las tres proposiciones del lado derecho lo son.

a)
$$\begin{array}{rcl} p & \iff & q \\ & \iff & r \\ & \Rightarrow & s \\ & \iff & t \end{array}$$

1) $(p \Rightarrow r) \wedge (r \Rightarrow q) \wedge (q \Rightarrow s) \wedge (t \Rightarrow r)$
2) $(q \Rightarrow r) \wedge (r \Rightarrow s) \wedge (t \Rightarrow s) \wedge (q \Rightarrow p)$
3) $(p \Rightarrow s) \wedge (r \Rightarrow t) \wedge (q \Rightarrow p) \wedge (t \Rightarrow s)$

b)
$$\begin{array}{rcl} p & \iff & q \\ & \Rightarrow & t \\ & \Rightarrow & s \\ & \Rightarrow & q \end{array}$$

1) $(p \Rightarrow s) \wedge (t \Rightarrow s) \wedge (p \Rightarrow t) \wedge (t \iff q)$
2) $(q \Rightarrow t) \wedge (p \iff s) \wedge (t \Rightarrow p) \wedge (q \Rightarrow p)$
3) $(p \iff s) \wedge (s \Rightarrow t) \wedge (t \Rightarrow q) \wedge (t \Rightarrow p)$

1.6 Cuantificadores

La Lógica Proposicional, vista la semana anterior, no nos permite hacer ciertas deducciones que a todas luces quisiéramos (y necesitamos) poder hacer, como por ejemplo:

Toda persona que nace va a morir.
Yo nací.

Yo moriré.

Por otro lado, la Lógica Proposicional nos permite deducir que: si $p_1 \wedge p_2 \wedge \ldots \wedge p_n$ es una proposición verdadera e i un entero dado, $1 \leq i \leq n$, entonces debe ocurrir que p_i es verdadera. La conclusión es válida dado que la siguiente proposición es una tautología:

$$p_1 \wedge p_2 \wedge \cdots \wedge p_n \implies p_i. \tag{1}$$

Sin embargo, no tenemos el lenguaje matemático para escribir una expresión que nos permita afirmar que todas las proposiciones p_i son verdaderas, cualquiera sea el entero positivo i que cumpla $1 \leq i \leq n$. Tampoco podemos expresar que si tenemos una infinidad de proposiciones verdaderas, digamos $p_1, p_2, \ldots, p_n, \ldots$, e i es un entero positivo fijo, entonces p_i es verdadera. La Lógica de Primer Orden es una extensión de la Lógica Proposicional que valida este tipo de deducciones. Pero, más importante aún, describe cómo hacerlas correctamente. El primer concepto clave de este nuevo tipo de lógica es el siguiente:

Definición 1.14 (Función proposicional o predicado) *Una función proposicional $P(x, y, z, ...)$ es una expresión que depende de cero o más variables $x, y, z, \ldots$ que al ser reemplazadas por elementos de un conjunto de referencia E hacen que P se transforme en una proposición. Es decir, que sea verdadera o falsa.*

Siempre se asume que el conjunto de referencia E contiene al menos un elemento.

Las funciones proposicionales suelen denotarse por letras mayúsculas como $P, Q, R, S, \ldots$

Ejemplo:

- Si p es una proposición lógica, entonces p es un predicado constante, es decir, no depende de ninguna variable, cualquiera sea el conjunto de referencia.

- $P(x)$: "x es futbolista" es un predicado sobre el conjunto de referencia de personas.[2] Notar que $P($`Christiane Endler`$)$ es verdadera y que $P($`Nicolás Massu`$)$ es falsa.
- $Q(x) : x - 5 \leq 0$, es un predicado sobre el conjunto de números enteros. En particular, $Q(2)$ es verdadera, pero $Q(6)$ es falsa.
- $P(a, b, c) : 2a + b \geq c$ es un predicado sobre el conjunto de números reales. En particular, $P(1, 0, 0)$ es verdadera y $P(-\frac{1}{2}, 1, 1)$ es falsa.

$\diamondsuit$

Usaremos $P(x, y, z, ...)$ de dos formas distintas:

- Para referirnos al predicado mismo y mostrar que $x, y, z, \ldots$ son las variables que reemplazamos por elementos del conjunto de referencia.
- Para referirnos, cuando $x, y, z, ...$ son reemplazadas por elementos del conjunto de referencia, a la proposición que se obtiene de haber hecho el reemplazo en el predicado.

Mediante el uso de los conectivos lógicos podemos construir nuevos predicados a partir de otros. Si P y Q son predicados con conjunto de referencia E, entonces $\overline{P}$, $P \wedge Q$, $P \vee Q$, $P \Rightarrow Q$ y $P \iff Q$ son predicados con conjunto de referencia E.

La expresividad de la Lógica de Primer Orden viene dada por la posibilidad de "cuantificar universalmente", es decir, de poder hablar de **todos** los elementos de un conjunto, independiente de cuántos elementos tenga el conjunto. Para ello, se introduce el cuantificador universal. Este se representa con el símbolo $\forall$, que juega un rol similar al $\wedge$ en (1). Si $P(x)$ es un predicado en una única variable x con conjunto de referencia E y, recordando que la proposición "e es un elemento de E" la denotamos $e \in E$, entonces se tiene:

Definición 1.15 (Cuantificador universal) *La expresión $(\forall x \in E, P(x))$, que se lee "para todo equis en E, pe de equis", es una proposición verdadera si al reemplazar x por cualquier elemento en E se verifica que $P(x)$ es verdadera.*

En palabras, lo que la definición anterior nos dice es que $(\forall x \in E, P(x))$ corresponde a la proposición "$P(e)$ es verdadera siempre que e pertenece a E".

Ejemplo: La afirmación $(\forall x \in E, P(x) \vee \overline{P(x)})$ es verdadera, porque por Tercio excluso, $P(x) \vee \overline{P(x)} \iff V$, para cada elemento x de E. Luego, por definición de cuantificador universal, se tiene $(\forall x \in E, P(x) \vee \overline{P(x)})$. $\diamondsuit$

En general, una definición establece una equivalencia que aceptamos como verdadera. Por Equivalencia dividida (Proposición 1.11 parte (I)) sabemos que una equivalencia corresponde a una doble implicancia. A veces, como cuando se trabaja con cuantificadores, al utilizar una definición resulta más claro señalar cual de las dos implicancias involucradas se está utilizando. Para facilitar lo anterior, a continuación le asignamos un nombre a cada una de las dos implicancias implícitas en la Definición 1.15:

[2] Usamos la expresión $X : Y$ para nombrar X al objeto Y.

- Instanciación universal: Si $e \in E$ es un elemento arbitrario,[3] entonces se cumple que:

$$\big(\forall x \in E, P(x)\big) \Rightarrow P(e).$$

- Generalización universal: Si se cumple $P(e)$, para $e \in E$ arbitrario, entonces $(\forall x \in E, P(x))$ es verdadera.

Más que determinar el valor de verdad de expresiones como $(\forall x \in E, P(x))$, lo que usualmente haremos es derivar nuevas expresiones, potencialmente también cuantificadas, que son equivalentes o implicadas a partir de otras expresiones cuantificadas.

Ejemplo: Considerando nuevamente el ejemplo del comienzo de esta sección, o sea $P(x)$: "Si la persona x nace, entonces x morirá" y tomando como E el conjunto de todas las personas (nacidas o por nacer), por Instanciación universal, si es verdadero $(\forall x \in E, P(x))$, entonces aceptamos como válida la conclusión "si yo nací, entonces yo moriré". La hipótesis de esta última proposición, "yo nací", es verdadera por lo que la conclusión, "yo moriré" también lo es. ♢

Observar que si $P(x)$ tiene conjunto de referencia $E = \{e_1, \ldots, e_n\}$, y si $p_i : P(e_i)$, entonces

$$(\forall x \in E, P(x)) \iff p_1 \wedge p_2 \wedge \ldots \wedge p_n.$$

Luego, para tal conjunto E, Instanciación universal corresponde exactamente a la tautología (1).

Definición 1.16 (Contraejemplo) *Un elemento $e \in E$ tal que $P(e)$ es falsa se denomina contraejemplo de $(\forall x \in E, P(x))$.*

Ejemplo: Considerando otra vez el predicado $P(x)$: "x es futbolista" y el conjunto de referencia E de todas las personas, se tiene que `Nicolás Massu` es un contraejemplo a $(\forall x \in E, P(x))$. ♢

Notar además que si $P(x)$ es un predicado en una única variable x, entonces $(\forall x \in E, P(x))$ es una proposición. Pero, en el caso de funciones proposicionales en más de una variable, al cuantificarlas obtenemos otro predicado, por ejemplo, al cuantificar $Q(y, z)$ obtenemos $(\forall y \in E, Q(y, z))$ que es un predicado en la variable z. Si volvemos a cuantificar, obtenemos $(\forall z \in E, (\forall y \in E, Q(y, z))$ que por convención se escribe omitiendo paréntesis, simplemente, como $(\forall z \in E, \forall y \in E, Q(y, z))$.

A continuación veremos un ejemplo de proposición construida usando el cuantificador universal y cómo se prueba su veracidad. Aprovecharemos de ilustrar la técnica de demostración Equivalencia dividida, mencionada en la sección anterior. La técnica se basa en la tautología de la parte (i) de la Proposición 1.11. Es decir, en:

$$(r \iff s) \iff (r \Rightarrow s) \wedge (s \Rightarrow r).$$

[3] Por arbitrario entendemos que, aparte de pertenecer al conjunto de referencia E, no hay ninguna premisa establecida sobre e.

Esta nos permite dividir la demostración en dos partes, ya que en lugar de verificar que $r \iff s$, basta comprobar que se tienen $(r \Rightarrow s) \wedge (s \Rightarrow r)$. Esto, a su vez, lo hacemos verificando por separado que $r \Rightarrow s$ y que $s \Rightarrow r$.

Ejemplo: Verifiquemos que se tiene:

$$(\forall x \in E, P(x) \wedge Q(x)) \iff (\forall x \in E, P(x)) \wedge (\forall x \in E, Q(x)).$$

Sea r dada por $r : (\forall x \in E, P(x) \wedge Q(x))$.

Partamos mostrando que $r \Rightarrow (\forall x \in E, P(x)) \wedge (\forall x \in E, Q(x)))$. Ya sabemos que podemos suponer que r es verdadera y bajo este supuesto probar que $(\forall x \in E, P(x)) \wedge (\forall x \in E, Q(x))$ lo es. Por definición de $\wedge$ basta con demostrar que cada una de las proposiciones es verdadera.

En el razonamiento que sigue se aplican tautologias conocidas de la forma $A \Rightarrow B$, para A una proposición verdadera, lo que permite concluir que la proposición B también lo es.

Como r es verdadera también son verdaderas las siguientes proposiciones.

Paso	Proposición	Justificación/Tautología
(1)	$P(e) \wedge Q(e)$, con $e \in E$ arbitrario.	por Instanciación universal.
(2)	$P(e)$, con $e \in E$ arbitrario.	por Relajación.
(3)	$(\forall x \in E, P(x))$	por Generalización universal.
(4)	$Q(e)$, con $e \in E$ arbitrario.	por Relajación.
(5)	$(\forall x \in E, Q(x))$	por Generalización universal.

Nota: En realidad, es muy raro (y poco "amigable con el lector") presentar las derivaciones en forma de tabla. Lo usual es hacerlo en palabras, en el entendido que pueden reemplazarse por derivaciones con tablas si uno quisiera. Por ejemplo, lo natural es que la derivación anterior se presente así:

> Por hipótesis, asumimos que se tiene $(\forall x \in E, P(x) \wedge Q(x))$. Luego, para $e \in E$ arbitrario, se cumple $P(e) \wedge Q(e)$. Es decir, se tienen tanto $P(e)$ como $Q(e)$. Sigue que $(\forall x \in E, P(x))$ y $(\forall x \in E, Q(x))$ son verdaderas. Por definición de $\wedge$ obtenemos la conclusión deseada. Por lo tanto $(\forall x \in E, P(x)) \wedge (\forall x \in E, Q(x))$.

Notar que ni siquiera se explicitan las reglas de inferencia que involucran cuantificadores. Adoptaremos esta convención en el resto del curso, salvo por esta sección, donde seguiremos presentando las demostraciones tanto en tabla como en la forma recién ilustrada.

Veamos ahora que $(\forall x \in E, P(x)) \wedge (\forall x \in E, Q(x)) \Rightarrow r$. Como antes podemos suponer que $(\forall x \in E, P(x))$ y $(\forall x \in E, Q(x))$ son verdaderas. De donde se sigue que las siguientes proposiciones también son verdaderas.

Paso	Afirmación	Justificación/Tautología
(1)	$P(e)$, con $e \in E$ arbitrario	por Instanciación universal.
(2)	$Q(e)$, con $e \in E$ arbitrario	por Instanciación universal.
(3)	$P(e) \wedge Q(e)$, con $e \in E$ arbitrario	definición de $\wedge$
(4)	$(\forall x \in E, P(x) \wedge Q(x))$	por Generalización universal.

La forma usual de presentar esta demostración sería:

> Sea e arbitrario. Como por hipótesis, se cumple que $(\forall x \in E, P(x))$, se tiene $P(e)$. Análogamente, se tiene $Q(e)$. Por definición de $\wedge$, se tiene que $P(e) \wedge Q(e)$. Como $e \in E$ es arbitrario, se concluye que $(\forall x \in E, P(x) \wedge Q(x))$.

$\diamondsuit$

A menudo, se requiere decir que la proposición $(\forall x \in E, P(x))$ es falsa o, lo que es equivalente, que la negación de $(\forall x \in E, P(x))$ es verdadera. Para ello, se define un nuevo cuantificador como sigue:

Definición 1.17 (Cuantificador existencial) *La expresión $(\exists x \in E, P(x))$, que se lee "existe un equis en E tal que pe de equis", es una proposición que es verdadera si y sólo si $(\forall x \in E, \neg P(x))$ es falsa. Formalmente*

$$(\exists x \in E, P(x)) \iff \neg(\forall x \in E, \neg P(x)).$$

En palabras, lo que la definición anterior nos dice es que $(\exists x \in E, P(x))$ corresponde a la proposición "$P(e)$ es verdadera para algún e particular perteneciente a E".

Notar que si $P(x)$ es un predicado sobre $E = \{e_1, \ldots, e_n\}$, y si denotamos por p_i la proposición $P(e_i)$, entonces

$$(\exists x \in E, P(x)) \iff p_1 \vee p_2 \vee \ldots \vee p_n.$$

Al igual que para el caso de la definición del cuantificador universal, distinguimos con distintos nombre las dos implicancias implícitas en la definición del cuantificador existencial:

- Instanciación (o eliminación) existencial: Si se tiene que $(\exists x \in E, P(x))$, entonces para un elemento $e \in E$ particular se tiene que $P(e)$ es verdadera.
- Generalización existencial: Si se cumple $P(e)$ para un elemento $e \in E$ particular, entonces $(\exists x \in E, P(x))$ es verdadera.

Ejemplo: Probemos que $(\exists x \in E, P(x) \wedge Q(x)) \Rightarrow (\exists x \in E, P(x)) \wedge (\exists x \in E, Q(x))$.

Asumimos que $(\exists x \in E, P(x) \wedge Q(x))$ es verdadero. Entonces las siguientes proposiciones también lo son.

Paso	Proposición	Justificación/Tautología
(1)	$P(e) \wedge Q(e)$, para un $e \in E$ particular	por Eliminación existencial.
(2)	$P(e)$, para un $e \in E$ particular	por Relajación.
(3)	$(\exists x \in E, P(x))$	por Generalización existencial.
(4)	$Q(e)$, para un $e \in E$ particular	por Relajación.
(5)	$(\exists x \in E, Q(x))$	por Generalización existencial.
(6)	$(\exists x \in E, P(x)) \wedge (\exists x \in E, Q(x))$	por definición de $\wedge$.

Como ya lo dijimos, la forma de presentar la tabla sería más bien: Por hipótesis, tenemos que $(\exists x \in E, P(x) \wedge Q(x))$. Luego, se tiene $P(e)$ y $Q(e)$ para algún $e \in E$. En particular, se cumplen $(\exists x \in E, P(x))$ y $(\exists x \in E, Q(x))$. Por lo tanto, se debe tener que $(\exists x \in E, P(x)) \wedge (\exists x \in E, Q(x))$, como se quería demostrar. $\diamondsuit$

Proposición 1.18 (Negación de cuantificadores) *Se tiene que,*

(I) Negación del cuantificador existencial: $\neg(\exists x \in E, P(x)) \iff (\forall x \in E, \neg P(x))$,

(II) Negación del cuantificador universal: $\neg(\forall x \in E, P(x)) \iff (\exists x \in E, \neg P(x))$.

Hay un cuantificador más que se utiliza con frecuencia:

Definición 1.19 (Existencia y unicidad) *La expresión* $(\exists! x \in E, P(x))$*, que se lee "existe un único equis en* E *tal que pe de equis", es una proposición que es verdadera si y sólo si existe un* $e \in E$ *tal que* $P(e)$ *es verdadera y para todo* $x, x' \in E$*: si* $P(x)$ *y* $P(x')$ *son verdaderas, entonces* $x = x'$*. Formalmente,*

$$(\exists! x \in E, P(x)) \iff \underbrace{(\exists x \in E, P(x))}_{\text{existencia}} \wedge \underbrace{(\forall x \in E, \forall x' \in E, P(x) \wedge P(x') \Rightarrow x = x')}_{\text{unicidad}}.$$

En palabras, la definición anterior dice que $(\exists! x \in E, P(x))$ corresponde a la proposición "para un e perteneciente a E se tiene que $P(e)$ es verdadera y, no hay dos elementos e y e' distintos, ambos pertenecientes a E, tales que $P(e)$ y $P(e')$ sean ambas verdaderas".

Ejemplo:

- La expresión, $(\exists! n \in \mathbb{Z}, \forall m \in \mathbb{Z}, nm = 0)$ representa la afirmación "existe un único número entero que al multiplicarlo por cualquier otro entero da 0". Dicho elemento es el 0 y, efectivamente, la referida expresión es una proposición verdadera.
- Nuevamente, considerando nuestro predicado $P(x)$: "x es futbolista" y el conjunto de referencia E de todas las personas. ¿Cuál será el valor de verdad de $(\exists! x \in E, P(x))$?

  Podemos notar que tanto $x =$ `Christiane Endler` y $x' =$ `Matías Fernández` hacen que $P(x)$ sea verdadera. Es decir, si bien existe un x que hace a $P(x)$ verdadera, **no** es único. Así, $(\exists! x \in E, P(x))$ es falsa.

$\diamondsuit$

Concluimos nuestra discusión de lógica matemática listando varias tautologías que involucran cuantificadores. Haremos uso frecuente de éstas (sin mencionarlas) en las secciones siguientes.

Proposición 1.20 *Para* $P(x)$ *y* $Q(x)$ *predicados se cumple lo siguiente.*

1. *Modus Ponens Universal:* $P(e) \wedge (\forall x \in E, P(x) \Rightarrow Q(x)) \implies Q(e)$.
2. $(\forall x \in E, P(x)) \wedge (\forall x \in E, P(x) \Rightarrow Q(x)) \implies (\forall x \in E, Q(x))$.

Proposición 1.21 *Sean $P(x)$ y $Q(x)$ predicados con conjunto de referencia E. Las siguientes proposiciones se cumplen:*

(I) Distributividad del $\forall$ con respecto a $\wedge$:

$$(\forall x \in E, P(x) \wedge Q(x)) \iff (\forall x \in E, P(x)) \wedge (\forall x \in E, Q(x)).$$

(II) Distributividad del $\exists$ con respecto a $\vee$:

$$(\exists x \in E, P(x) \vee Q(x)) \iff (\exists x \in E, P(x)) \vee (\exists x \in E, Q(x)).$$

(III) $(\forall x \in E, P(x)) \vee (\forall x \in E, Q(x)) \implies (\forall x \in E, P(x) \vee Q(x))$.

(IV) $(\exists x \in E, P(x) \wedge Q(x)) \implies (\exists x \in E, P(x)) \wedge (\exists x \in E, Q(x))$.

Las partes (I) y (IV) ya fueron establecidas en ejemplos previos. La demostración de las demás propiedades queda como ejercicio propuesto.

Observación: Notar que las afirmaciones de la proposición anterior son válidas para predicados P y Q cualesquiera. No ocurre lo mismo con el recíproco de la penúltima implicancia. Es decir, hay predicados P y Q que no necesariamente cumplen que

$$(\forall x \in E, P(x) \vee Q(x)) \implies (\forall x \in E, P(x)) \vee (\forall x \in E, Q(x)).$$

Para justificar este hecho necesitamos mostrar predicados donde la afirmación no se cumpla. Abusando del lenguaje, diremos que estos predicados son un contraejemplo de la afirmación. Es claro que los siguientes predicados son un contraejemplo: $P(x)$: "x es par", $Q(x)$: "x es impar", y $E = \mathbb{N}$. Como ejercicio, dé un contraejemplo del recíproco de la última implicancia. □

Proposición 1.22 *Sea p una proposición, es decir, un predicado constante, y sea $Q(x)$ predicado con conjunto de referencia E. Se tienen las siguientes equivalencias.*

(I) $(\forall x \in E, p) \iff p$.

(II) $(\exists x \in E, p) \iff p$.

(III) $p \vee (\forall x \in E, Q(x)) \iff (\forall x \in E, p \vee Q(x))$.

(IV) $p \wedge (\exists x \in E, Q(x)) \iff (\exists x \in E, p \wedge Q(x))$.

Proposición 1.23 (Reglas de intercambio de cuantificadores) *Sea $P(x, y)$ predicado con conjunto de referencia E. Se cumplen las siguientes tautologías.*

(I) $(\forall x \in E, \forall y \in E, P(x, y)) \iff (\forall y \in E, \forall x \in E, P(x, y))$.

(II) $(\exists x \in E, \exists y \in E, P(x, y)) \iff (\exists y \in E, \exists x \in E, P(x, y))$.

(III) $(\exists x \in E, \forall y \in E, P(x, y)) \implies (\forall y \in E, \exists x \in E, P(x, y))$.

Observación: Notar que las afirmaciones de la Proposición 1.23 son válidas para cualquiera predicado P. No ocurre lo mismo con el recíproco de la última implicancia. Veamos que $E = \mathbb{N}$ y $P(x, y)$: "$x > y$" es un contraejemplo de esta afirmación.

Para $y \in \mathbb{N}$ arbitrario, $x = y + 1$ es tal que $x > y$. Luego, se cumple que $(\forall y \in \mathbb{N}, \exists x \in \mathbb{N}, x > y)$. No obstante, no es cierto que $(\exists x \in \mathbb{N}, \forall y \in \mathbb{N}, x > y)$ porque ningún entero es mayor que todos los números naturales.

Intentaremos explicar informalmente porqué, en general, no se cumple el recíproco. Supongamos que hacemos una tabla cuyas filas y columnas están indexadas por elementos de E, denotados por e y f respectivamente. Supongamos que colocamos en la fila e y columna f una X si $P(e, f)$ es verdadera y nada en caso contrario. Consideremos dos situaciones como las ilustradas por las siguientes tablas:

	$\longleftarrow f \in E \longrightarrow$						
			X	X		X	
		X		X			
$\uparrow$	X	X	X	X	X	X	$\cdots$
$e \in E$	X						
$\downarrow$		X		X		X	
	X		X			X	
			$\vdots$				$\ddots$

	$\longleftarrow f \in E \longrightarrow$						
	X						
		X					
$\uparrow$			X				$\cdots$
$e \in E$				X			
$\downarrow$					X		
						X	
			$\vdots$				$\ddots$

Consideremos además, las siguientes afirmaciones:

- Afirmación 1: Hay una fila en que en todas las columnas aparece una X.
- Afirmación 2: En toda columna hay una fila en que aparece una X.

Observar que si la Afirmación 1 es cierta, entonces la Afirmación 2 debe también ser verdadera. Pero no así el recíproco. La tabla de la izquierda más arriba es un ejemplo para el cual la Afirmación 1 es cierta (y por lo tanto también la Afirmación 2 es cierta). La tabla de la derecha es un ejemplo para el cual la Afirmación 2 es cierta pero que no satisface la Afirmación 1. □

Para concluir, a continuación enumeramos algunas prácticas que se adoptan al trabajar con cuantificadores y que facilitan su uso:

Convención (sobre el uso de cuantificadores):

- Se suele omitir el paréntesis de más afuera de $(\forall x \in E, P(x))$ y escribir $\forall x \in E, P(x)$.
- Al usar un mismo cuantificador para varias variables distintas tomando valores en un mismo conjunto de referencia, no es necesario repetir el cuantificador. Por ejemplo, $\forall x \in A, \forall y \in A, P(x, y)$ se escribe $\forall x, y \in A, P(x, y)$ (análogamente si reemplazamos $\forall$ por $\exists$).

SEMANA 02:

Principio de inducción

Ingeniería Matemática
FACULTAD DE CIENCIAS
FÍSICAS Y MATEMÁTICAS
UNIVERSIDAD DE CHILE

2.1 Introducción

Dados dos números enteros n y m, otra forma para decir que n es un factor de m es decir que n divide a m o que m es divisible por n. Además, un número que sólo es divisible por 1 y por sí mismo se llama número primo. En otro caso se llama número compuesto. Es decir, para $n \geq 2$:

$$n \text{ es compuesto } \iff (\exists d \in \{2, \ldots, n-1\}, d \text{ divide a } n).$$

Dos números que no tienen divisores comunes se llaman primos relativos o coprimos.

Una categoría importante de proposiciones y teoremas involucra propiedades de los números naturales, es decir, de $\mathbb{N} = \{0, 1, 2, ...\}$. Notar que, a diferencia de lo que habitualmente se usa en la enseñanza preuniversitaria, la proposición $0 \in \mathbb{N}$ es verdadera. Si retiramos 0 de $\mathbb{N}$ obtenemos el conjunto de los enteros positivos $\mathbb{N}^* = \{1, 2, 3, ...\}$. Ejemplos de proposiciones acerca de números naturales son:

- $\forall n \in \mathbb{N},\ n < 2^n$.
- $\forall n \in \mathbb{N}, n$ es primo y $n \neq 2 \Rightarrow n$ es impar.
- $\forall n \in \mathbb{N},\ 3^{2n+1} + 2^{n+2}$ es divisible por 7.

En general, si $n_0 \in \mathbb{N}$ y $P(n)$ es una función proposicional con conjunto de referencia los $n \in \mathbb{N}$ tales que $n \geq n_0$, el **Principio de inducción** nos proporciona una proposición equivalente a aquella que afirma que para cada $n \geq n_0$ la proposición $P(n)$ es verdadera. Esta proposición se escribirá

$$\forall n \in \mathbb{N}, n \geq n_0 \implies P(n),$$

adoptando la convención que un predicado evaluado fuera de su conjunto de referencia da como resultado la proposición F.

(Para no recargar la notación, la proposición anterior suele denotarse $\forall n \geq n_0, P(n)$). Formalmente, asumimos como correcta la siguiente regla de inferencia:

Axioma 2.1 (Principio de inducción) *Si $n_0 \in \mathbb{N}$ y $P(n)$ es un predicado en el conjunto de referencia de los $n \in \mathbb{N}$ tales que $n \geq n_0$, entonces*

$$\big[\underbrace{P(n_0)}_{\text{caso base}} \wedge \big(\forall n \geq n_0{+}1, \underbrace{P(n_0) \wedge P(n_0{+}1) \wedge \ldots \wedge P(n{-}1)}_{\text{Hipótesis Inductiva (H.I.)}} \Rightarrow P(n)\big)\big] \iff (\forall n \geq n_0, P(n)).$$

Ejemplo: Usemos el Principio de inducción para demostrar que

$$\forall n \geq 1, \underbrace{1 + 2 + \ldots + n = \frac{1}{2} n(n+1)}_{P(n)}.$$

El caso base $P(n_0)$ a demostrar en esta ocasión es con $n_0 = 1$. Aquí, tenemos que demostrar que $1 = \frac{1}{2}(1+1)$, lo que es trivialmente cierto.

Sea $n \geq 2$. Supongamos ahora que la propiedad vale para $1, 2, ..., n-1$, es decir, que se cumplen $P(1)$, $P(2)$, ..., $P(n-1)$ (H.I.). Debemos demostrar que la propiedad también es cierta para n. Es decir, que

$$1 + 2 + \ldots + (n-1) + n = \frac{1}{2} n(n+1).$$

En efecto ([4])

$$\begin{aligned} 1 + 2 + \ldots + (n-1) + n &= (1 + 2 + \ldots + (n-1)) + n \\ &= \frac{1}{2}(n-1)n + n \qquad \text{(Porque se tiene } P(n-1) \text{ por H.I.)} \\ &= \frac{1}{2}\big((n-1)n + 2n\big) \\ &= \frac{1}{2} n(n+1). \end{aligned}$$

Usando que $=$ es transitiva concluimos que se tiene $P(n)$. Gracias al Principio de inducción, concluimos que $(\forall n \geq 1, P(n))$. $\diamondsuit$

Ejemplo: Nuevamente usemos inducción, ahora para probar la siguiente propiedad:

$$\forall n \geq 1, \underbrace{1 \cdot (1) + 2 \cdot (1 \cdot 2) + 3 \cdot (1 \cdot 2 \cdot 3) + ... + n \cdot (1 \cdot 2 \cdot ... \cdot n) = 1 \cdot 2 \cdot ... \cdot (n+1) - 1.}_{P(n)}$$

Primero observamos que el caso base $P(n_0) = P(1)$ se cumple porque $1 \cdot 1 = 1 = 1 \cdot 2 - 1$. Para $n \geq 2$, asumimos entonces que se cumplen $P(1)$, $P(2)$, ..., $P(n-1)$ (H.I.). Luego,

$$\begin{aligned} &1 \cdot (1) + 2 \cdot (1 \cdot 2) + 3 \cdot (1 \cdot 2 \cdot 3) + ... + n \cdot (1 \cdot 2 \cdot ... \cdot n) \\ &\quad = 1 \cdot 2 \cdot ... \cdot n - 1 + n \cdot (1 \cdot 2 \cdot ... \cdot n) \qquad \text{(Porque por H.I. se cumple } P(n-1)) \\ &\quad = 1 \cdot 2 \cdot ... \cdot n \cdot (n+1) - 1, \end{aligned}$$

[4] Al igual que lo hecho con $\Rightarrow$ y $\iff$, podemos escribir proposiciones como $(a = b) \wedge (b = c) \wedge (c = d)$ o $(a = b) \wedge (b \leq c) \wedge (c = d)$ en forma vertical.

y se concluye la veracidad de la propiedad gracias a la transitividad de $=$ y al principio de inducción. $\diamondsuit$

Ejemplo: También es posible probar por inducción que se cumplen desigualdades. Esto lo ilustraremos probando que si $x > -1$, entonces

$$\forall n \in \mathbb{N}, \underbrace{1 + nx \leq (1+x)^n}.$$

Claramente se cumple el caso base $P(n_0) = P(0)$. Para $n \geq 1$, asumimos que se cumplen $P(0)$, ..., $P(n-1)$ (H.I.). Luego,

$$\begin{aligned}(1+x)^n &= (1+x)^{n-1}(1+x) \\ &\geq (1+(n-1)x)(1+x) \qquad \text{(Porque } 1+x>0 \text{ y por H.I. se cumple } P(n-1)\text{)} \\ &= 1 + nx + (n-1)x^2 \\ &\geq 1 + nx. \qquad \text{(Porque } x^2 \geq 0 \text{ y } n \geq 1\text{)}\end{aligned}$$

Luego, por la transitividad de $\geq$ y el Principio de inducción concluimos que la desigualdad planteada se cumple para todo $n \in \mathbb{N}$. $\diamondsuit$

A menudo cuando se hace una demostración de tipo inductiva, para completar la inducción se requiere establecer la validez de una afirmación (distinta a la hipótesis) y que a su vez puede ser demostrada por inducción. Este tipo de argumento se conoce como inducción anidada que ilustramos a continuación.

Ejemplo: Verifiquemos usando inducción que

$$\forall n \geq 1, \underbrace{2 \cdot 34^n - 3 \cdot 23^n + 1 \text{ es divisible por } 726}_{P(n)}.$$

El caso base es con $n_0 = 1$ y se tiene porque $2 \cdot 34 - 3 \cdot 23 + 1 = 0$ es divisible por 726. Para $n \geq 2$, asumimos que se cumplen $P(1), ..., P(n-1)$ (H.I.). Veamos que se tiene $P(n)$. En efecto,

$$\begin{aligned}2 \cdot 34^n - 3 \cdot 23^n + 1 &= 34 \cdot 2 \cdot 34^{n-1} - 23 \cdot 3 \cdot 23^{n-1} + 1 \\ &= 23 \cdot (2 \cdot 34^{n-1} - 3 \cdot 23^{n-1} + 1) + 22 \cdot (34^{n-1} - 1) \\ &= 23 \cdot 726 \cdot k + 22 \cdot (34^{n-1} - 1). \\ &\qquad \text{(Por H.I. } \underbrace{\exists k \in \mathbb{Z}, 2 \cdot 34^{n-1} - 3 \cdot 23^n + 1 = 726 \cdot k}_{P(n-1)}.\text{)}\end{aligned}$$

Para concluir la inducción, necesitamos establecer que $22 \cdot (34^{n-1} - 1)$ es divisible por 726 si $n \geq 2$. ¿Cómo lo demostramos? ¡por inducción! En efecto, consideremos el predicado $Q(n) =$"$22 \cdot (34^{n-1} - 1)$ es divisible por 726". Demostremos por inducción que $\forall n \geq 2, Q(n)$. Ahora el caso base es con $n_0 = 2$, el cual se cumple porque $22 \cdot (34 - 1) = 726$ que es obviamente divisible por 726. Asumimos que se tienen $Q(1), ..., Q(n-1)$ (nueva H.I.). Luego, si $n \geq 3$,

$$\begin{aligned}22 \cdot (34^{n-1} - 1) &= 22 \cdot 34 \cdot (34^{n-2} - 1) + 726 \\ &= 34 \cdot 726 \cdot k' + 726. \qquad \text{(Por H.I. } \underbrace{\exists k' \in \mathbb{Z}, 22 \cdot (34^{n-2} - 1) = 726 \cdot k'}_{Q(n-1)}.\text{)}\end{aligned}$$

Sigue entonces que $22 \cdot (34^{n-1} - 1)$ es divisible por 726 lo que concluye la demostración inductiva de la afirmación $\forall n \geq 2, Q(n)$, que a su vez permite establecer que $2 \cdot 34^n - 3 \cdot 23^n + 1$ es divisible por 726 y por lo tanto que $\forall n \geq 1, P(n)$ como se deseaba probar.

La razón por la que es válido hacer la segunda inducción "anidada dentro de la primera" es porque podríamos haber probado (por inducción), pero antes de partir la primera inducción, que $\forall n \geq 2, Q(n)$, y luego haber usado que esta afirmación es cierta para probar $\forall n \geq 1, P(n)$. Se prefiere el argumento de inducción anidada porque partir probando $\forall n \geq 2, Q(n)$ es artificial en el sentido que no se entendería bien la necesidad de comenzar la demostración de esa forma. $\diamondsuit$

Ejemplo: Una de las razones de la importancia del Principio de inducción está dada por su amplio espectro de aplicabilidad, el que no está limitado a establecer identidades o desigualdades entre expresiones aritméticas. Para ilustrar el punto probaremos que,

$$\forall n \geq 1, \underbrace{(p_1 \vee p_2 \vee \cdots \vee p_n \Rightarrow q) \iff (p_1 \Rightarrow q) \wedge (p_2 \Rightarrow q) \wedge \cdots \wedge (p_n \Rightarrow q)}_{P(n)}.$$

El caso base con $n_0 = 1$ es directo del hecho que $(r \iff r)$ es una tautología cualquiera sea la proposición r. Para $n \geq 2$, asumimos que se cumplen $P(1), ..., P(n-1)$ (H.I.). Luego,

$$\begin{aligned}(p_1 \vee p_2 \vee \cdots \vee p_n \Rightarrow q) &\iff \big(p_1 \vee p_2 \vee \cdots \vee p_{n-1} \Rightarrow q\big) \wedge (p_n \Rightarrow q) \\ &\qquad \text{(por Proposición 1.11 Parte (II))} \\ &\iff (p_1 \Rightarrow q) \wedge (p_2 \Rightarrow q) \wedge \cdots \wedge (p_n \Rightarrow q) \\ &\qquad \text{(H.I. y asociatividad de } \wedge)\end{aligned}$$

La transitividad de $\iff$ nos dice que $P(n)$ es cierta. Por el Principio de inducción se concluye que la afirmación planteada se cumple para todo $n \geq 1$. $\diamondsuit$

El lector habrá notado que en los ejemplos anteriores para establecer que $P(n)$ es verdadera, no se usó que $P(n_0)$, $P(n_0 + 1)$, ... , $P(n-1)$ eran todas verdaderas, sino algo más débil que se deriva de la hipótesis inductiva; a saber, que $P(n-1)$ es verdadera. En ciertas situaciones (como en el ejemplo que sigue) es crucial que, por hipótesis inductiva, se tenga que $P(n_0), P(n_0+1), \ldots, P(n-1)$ sean todas verdaderas. Para resaltar este tipo de situaciones a veces uno se refiere a ellas por "inducción fuerte".

Ejemplo (de inducción fuerte):

Probaremos el siguiente resultado por inducción: *Todo $n \in \mathbb{N}$, $n \geq 2$, posee al menos un divisor que es un número primo. Es decir, $\forall n \geq 2$, $\exists p \in \mathbb{N}$ primo tal que p divide a n.*

El caso base es con $n_0 = 2$, para el cual observamos que $p = 2$ es primo y divide a 2.

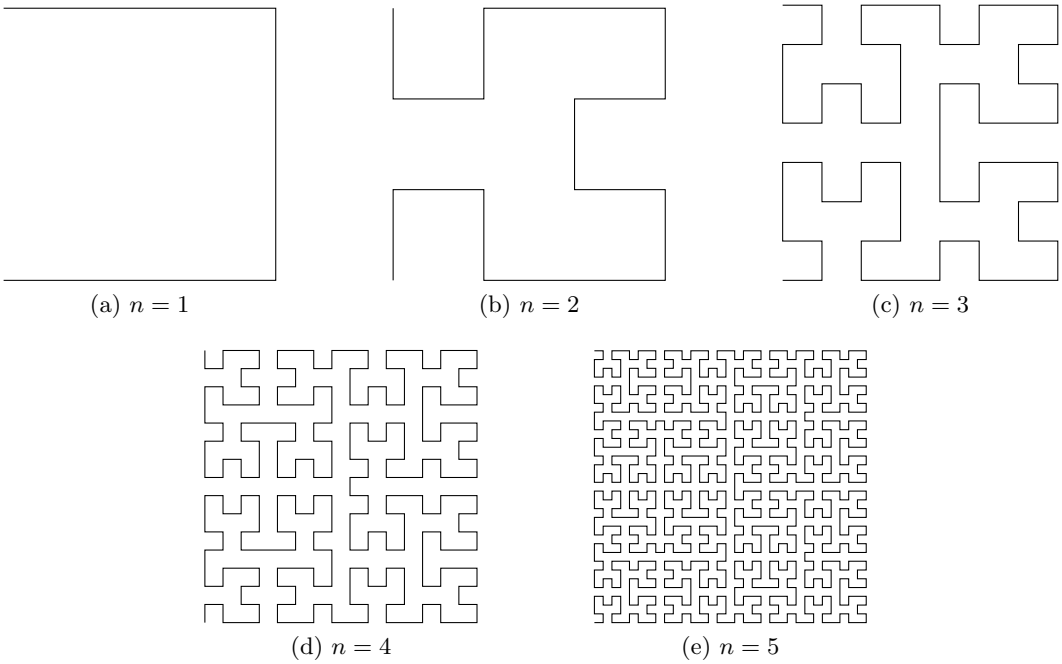
Sea $n \geq 3$, y supongamos ahora que para todo valor $k = 2, 3, \ldots, n-1$ se tiene que k posee un divisor que es primo (H.I.). Separamos por casos:

- Caso n es primo: Entonces $p = n$ es un número primo tal que p divide a n.
- Caso n no es primo: Entonces existe $d \in \{2, \ldots, n-1\}$ tal que d divide a n. Por hipótesis inductiva y notando que $d \leq n - 1$, debe existir un número primo p que divide a d. Tenemos entonces que p divide a d y d divide a n. Sigue que p divide a n.

$\diamondsuit$

2.2 Recurrencias

En matemáticas, una recurrencia es una ecuación o procedimiento que define una secuencia de términos (u objetos matemáticos), cada uno definido como función de términos anteriores. A menudo las recurrencias permiten describir objetos de una manera muy elegante y concisa. Por ejemplo, en la Figura 1 se muestran curvas de Hilbert de orden n, denotada H_n, para $n = 1, 2, ..., 5$. Cada H_n se representa en un cuadrado cuyo lado asumimos es 1. La curva H_n se obtiene haciendo 4 copias a escala de H_{n-1}. La primera (respectivamente, cuarta) copia de H_{n-1} se gira en 90° (respectivamente, 270°) en el sentido horario y se coloca en la parte superior (respectivamente, inferior) izquierda de un nuevo cuadrado de lado de largo 1. La segunda y tercera copia de H_{n-1} se colocan (sin girar) en las partes superior e inferior derecha del nuevo cuadrado. Posteriormente, se une con trazos rectos los extremos de cada copia con la que le sigue. La curva de Hilbert es muy interesante. Es un ejemplo de una curva continua que "en el límite llena el espacio". Informalmente, esto quiere decir que podemos acercarnos tanto como queramos a cualquier punto del cuadrado de lado 1 tomando un n suficientemente grande y dibujando la curva de Hilbert de orden n. El objeto que se obtiene en "el límite" cuando n tiende a infinito, ¡llena el cuadrado! Más aún, la curva cambia de dirección (gira en 90°) ¡en cada punto! ¡Todas estas propiedades en un objeto descrito por una simple recurrencia!



(a) $n = 1$ (b) $n = 2$ (c) $n = 3$

(d) $n = 4$ (e) $n = 5$

Figura 1: Curva de Hilbert de orden 1, 2, 3, 4, y 5.

A continuación nos enfocamos en el estudio de un cierto tipo de recurrencias.

Definición 2.2 (Fórmulas de recurrencia) *Las **fórmulas de recurrencia** son reglas del tipo:*

$$x_n = \begin{cases} a, & \text{si } n = 0, \\ f(n, x_0, \ldots, x_{n-1}), & \text{si } n \in \mathbb{N}^*, \end{cases}$$

*donde a es la llamada **base de la recurrencia** y f está dada por alguna expresión aritmética o procedimiento.*

Observación: A menudo es más conveniente (aunque no agrega generalidad) expresar una fórmula de recurrencia partiendo de un caso base $n = m \in \mathbb{N}$. Es decir, escribirla de la siguiente forma:

$$x_n = \begin{cases} a, & \text{si } n = m, \\ f(n, x_m, \ldots, x_{n-1}), & \text{si } n \in \mathbb{N},\ n > m. \end{cases}$$

□

En ocasiones es más simple indicar los primeros términos de una recurrencia explícitamente. Así, en lugar de dar una expresión $f(1, a)$ para x_1 y $f(2, a, x_1)$ para x_2, podemos dar su valor, por ejemplo, $x_1 = 1$ y $x_2 = 1$ (ver más abajo Números de Fibonacci).

Las fórmulas de recurrencia nos permiten definir secuencias de números. Por ejemplo, la secuencia $2, 4, 6, 8, 10, \ldots$ de números pares positivos se define así:

$$x_n = \begin{cases} 2, & \text{si } n = 0, \\ 2 + x_{n-1}, & \text{si } n > 0. \end{cases}$$

Otros ejemplos de definiciones por fórmulas de recurrencia son:

- **Progresión aritmética:** Sea $a \in \mathbb{R}$ y $d \in \mathbb{R}$, se dice que $a_0, a_1, a_2, ...$ es una progresión aritmética de paso d si $a_0 = a$ y $a_n = a_{n-1} + d$ para todo $n \in \mathbb{N}^*$.
- **Progresión geométrica:** Sea $a \in \mathbb{R}$ y $r \in \mathbb{R}$, se dice que $a_0, a_1, a_2, ...$ es una progresión geométrica de razón r si $a_0 = a$ y $a_n = r \cdot a_{n-1}$ para todo $n \in \mathbb{N}^*$.
- **Factorial:** Sea $n \in \mathbb{N}$. Se define $n!$ (se lee "n factorial") por $0! = 1$ y $n! = (n-1)! \cdot n$ para todo $n \in \mathbb{N}^*$ (por ejemplo, $1! = 1$, $2! = 1! \cdot 2 = 2$, $3! = 3 \cdot 2! = 6$, $4! = 4 \cdot 3! = 24$).
- **Números de Fibonacci:** Sea $n \in \mathbb{N}$. Se define el n-ésimo número de Fibonacci f_n por $f_0 = 0$, $f_1 = 1$ y $f_n = f_{n-1} + f_{n-2}$ para todo $n \in \mathbb{N}$, $n \geq 2$ (por ejemplo, $f_2 = 0 + 1 = 1$, $f_3 = 1 + 1 = 2$, $f_4 = 1 + 2 = 3$, $f_5 = 2 + 3 = 5$).

  Los números de Fibonacci están relacionados con muchos otros temas (para más detalles ver `http://es.wikipedia.org/wiki/Sucesión_de_Fibonacci`).

A menudo el estudio de las fórmulas de recurrencia da lugar a conjeturas que se demuestran utilizando el principio de inducción, como se ilustra a continuación.

Ejemplo: Consideremos la fórmula de recurrencia

$$x_n = \begin{cases} 1, & \text{si } n = 0, \\ 1 + \left(\frac{x_{n-1}}{2}\right)^2, & \text{si } n \in \mathbb{N}^*. \end{cases}$$

Reemplazando por $n = 0, 1, 2, ...$ vemos que $x_0 = 1$, $x_1 = \frac{5}{4} = 1,25$, $x_2 = \frac{57}{32} = 1,78125$, $x_3 = 1,79321...$, $x_4 = 1,80390....$ Conjeturamos que $(\forall n \in \mathbb{N}, x_n \leq 2)$. Demostraremos la conjetura utilizando el principio de inducción. El caso base resulta ser cierto pues corresponde a demostrar que $x_0 \leq 2$ (recordemos que $x_0 = 1$).

Sea $n \in \mathbb{N}$ tal que $x_n \leq 2$. Luego, por hipótesis inductiva,

$$x_n = 1 + \left(\frac{x_{n-1}}{2}\right)^2 = 1 + \frac{x_{n-1}^2}{4} \leq 1 + \frac{2^2}{4} = 2,$$

con lo que $x_n \leq 2$, y se concluye la demostración. ♢

Como en el ejemplo anterior, se puede establecer lo siguiente. La demostración se propone como ejercicio.

Proposición 2.3 (Término general de progresiones aritméticas y geométricas)

(I) *Sean $a, d \in \mathbb{R}$ tales que $a_0 = a \in \mathbb{R}$ y $a_n = a_{n-1} + d$ para todo $n \in \mathbb{N}^*$. Entonces, $a_n = a + n \cdot d$.*

(II) *Sean $a, r \in \mathbb{R}$ tales que $a_0 = a \in \mathbb{R}$ y $a_n = r \cdot a_{n-1}$ para todo $n \in \mathbb{N}^*$. Entonces, $a_n = r^n \cdot a$.*

Ejemplo (Números de Fibonacci): Entre muchas propiedades que cumplen los números de Fibonacci, demostraremos por inducción que, $\forall n \in \mathbb{N}$, f_{4n} es divisible por 3.

Caso base: Tenemos que probar que f_0 es divisible por 3. Esto es directo, pues como ya vimos, $f_0 = 0$.

Paso inductivo: Sea $n \geq 1$ y supongamos que $f_{4(n-1)}$ es divisible por 3. Existe, entonces, un $k \in \mathbb{N}$ tal que $f_{4(n-1)} = 3k$. Debemos demostrar que f_{4n} es divisible por 3. Como $n \geq 1$ se cumple que $4n \geq 4$ por lo que podemos utilizar la fórmula de recurrencia que cumplen los números de Fibonacci:

$$\begin{aligned}
f_{4n} &= f_{4(n-1)+3} + f_{4(n-1)+2} && \text{(definición de } f_m\text{)} \\
&= (f_{4(n-1)+2} + f_{4(n-1)+1}) + (f_{4(n-1)+1} + f_{4(n-1)}) && \text{(definición de } f_m\text{)} \\
&= f_{4(n-1)+2} + 2f_{4(n-1)+1} + f_{4(n-1)} \\
&= (f_{4(n-1)+1} + f_{4(n-1)}) + 2f_{4(n-1)+1} + f_{4(n-1)} && \text{(definición de } f_m\text{)} \\
&= 3f_{4(n-1)+1} + 2f_{4(n-1)} \\
&= 3f_{4(n-1)+1} + 2 \cdot 3k && \text{(hipótesis inductiva)} \\
&= 3(f_{4(n-1)+1} + 2k)
\end{aligned}$$

con lo que f_{4n} también es divisible por 3, que era lo que deseábamos establecer. ♢

Notar que en la demostración anterior el valor de f_1 es irrelevante. Esto quiere decir que $\forall n \in \mathbb{N}, g_{4n}$ es divisible por 3, para cualquier secuencia g_n tal que $g_0 = 0$ (o cualquier múltiplo de 3), g_1 arbitrario y $g_n = g_{n-1} + g_{n-2}$, para $n \geq 2$.

Guía Básica

Determinar la veracidad de las siguientes afirmaciones:

1. La negación de la proposición lógica $\forall x \in E, P(x)$ es $\exists x \in E, \overline{P(x)}$.
2. La negación de la proposición lógica $\forall x \in E, P(x)$ es $\exists x \notin E, \overline{P(x)}$.
3. La negación de la proposición lógica $\exists x \in E, P(x)$ es $\forall x \notin E, \overline{P(x)}$.
4. La proposición cuantificada $\forall x \in E, P(x)$ es verdadera si $P(x)$ es verdadera para cualquier elemento de E.
5. Si la proposición $\forall x \in E, P(x)$ es verdadera, entonces la proposición $\exists x \in E, P(x)$ es también verdadera.
6. Si $Q(x)$ es una función proposicional y $x_0 \in E$ es tal que $Q(x_0)$ es verdadera, entonces la proposición cuantificada $\exists x \in E, Q(x)$ es verdadera.
7. Es siempre cierto que si la proposición $\exists x \in E, P(x)$ es verdadera, entonces la proposición $\exists! x \in E, P(x)$ es verdadera.
8. Si $P(x)$ es una función proposicional y $x_0 \in E$ es tal que $P(x_0)$ es falsa, entonces la proposición cuantificada $\forall x \in E, P(x)$ es falsa.
9. Si las proposiciones $\forall x \in E, P(x)$ y $\forall x \in E, Q(x)$ son verdaderas, entonces la proposición $\forall x \in E, P(x) \wedge Q(x)$ es verdadera.
10. Si la proposición $\forall x \in E, P(x) \vee Q(x)$ es verdadera, entonces la proposición $(\forall x \in E, P(x)) \vee (\forall x \in E, Q(x))$ es verdadera.
11. Si la proposición $(\forall x \in E, P(x)) \vee (\forall x \in E, Q(x))$ es verdadera, entonces la proposición $\forall x \in E, P(x) \vee Q(x)$ es verdadera.
12. La negación de la proposición $\exists! \in E, P(x)$ es $(\forall x \in E, \overline{P(x)}) \vee (\exists x, y \in E, x \neq y \Rightarrow \overline{P(x)} \vee \overline{P(y)})$.
13. La proposición $\forall n \in \mathbb{N}, P(n)$ es verdadera si y sólo si $P(0)$ y $\forall n \in \mathbb{N}, P(n) \Rightarrow P(n+1)$ son verdaderas.
14. La proposición $\forall n \in \mathbb{N}, P(n)$ es verdadera si y sólo si $P(0) \wedge \forall n \in \mathbb{N}, P(n) \Rightarrow P(n+1)$ es verdadera.
15. La proposición $\forall n \in \mathbb{N}, P(n)$ es verdadera si y sólo si $P(0) \vee \forall n \in \mathbb{N}, P(n) \Rightarrow P(n+1)$ es verdadera.
16. La proposición $\forall n \in \mathbb{N}, P(n)$ es verdadera si y sólo si $P(0)$ y $\forall n \in \mathbb{N}, P(n+1) \Rightarrow P(n)$ son verdaderas.
17. La proposición $\forall n \in \mathbb{N}, P(n)$ es verdadera si y sólo si $P(0)$ y $\forall n \in \mathbb{N}, P(n) \Rightarrow P(2n)$ son verdaderas.
18. La proposición $\forall n \in \mathbb{N}, P(n)$ es verdadera si y sólo si $P(0)$ y $\forall n \in \mathbb{N}, P(2n) \Rightarrow P(2n+1)$ son verdaderas.
19. La proposición $\forall n \in \mathbb{N}, P(n)$ es verdadera si y sólo si $P(0), \forall n \in \mathbb{N}, P(2n) \Rightarrow P(2n+1)$ y $\forall n \geq 1, P(2n-1) \Rightarrow P(2n)$ son verdaderas.

20. La proposición $\forall n \in \mathbb{N}, P(n)$ es verdadera si y sólo si $P(0)$ y $\forall n \in \mathbb{N}, P(2n) \Rightarrow P(2n+1) \vee (\forall n \geq 1, P(2n-1) \Rightarrow P(2n))$ son verdaderas.
21. La proposición $\forall n \in \mathbb{N}, P(n)$ es verdadera si y sólo si $P(0)$ y $\forall n \geq 1, P(n-1) \Rightarrow P(n)$ son verdaderas.
22. La proposición $\forall n \in \mathbb{N}, P(n)$ es verdadera si y sólo si $P(0)$ y $\forall n \geq 1, P(n-1) \Rightarrow P(n+1)$ son verdaderas.
23. La proposición $\forall n \in \mathbb{N}, P(n)$ es verdadera si y sólo si $P(0)$ y $P(1) \wedge ... \wedge P(n)$ son verdaderas para algún $n \in \mathbb{N}$.
24. La proposición $\forall n \in \mathbb{N}, P(n)$ es verdadera si y sólo si $P(0)$ y $\forall n \geq 1, P(0) \wedge ... \wedge P(n-1) \wedge P(n) \Rightarrow P(n+1)$ son verdaderas.
25. La proposición $\forall n \in \mathbb{N}, P(n)$ es verdadera si y sólo si $P(0)$ y $\forall n \geq 1, P(0) \wedge ... \wedge P(n-1) \Rightarrow P(n+1)$ son verdaderas.
26. La proposición $\forall n \in \mathbb{N}, P(n)$ es verdadera si y sólo si $P(0)$ y $\forall n \geq 1, P(0) \wedge ... \wedge P(n-1) \Rightarrow P(n)$ son verdaderas.
27. La proposición $\forall n \in \mathbb{N}, P(n)$ es verdadera si y sólo si $P(0)$ y $\forall n > k, P(k) \wedge ... \wedge P(n-1) \Rightarrow P(n)$ son verdaderas para algún $k \in \mathbb{N}$.
28. La proposición $\forall n \in \mathbb{N}, P(n)$ es verdadera si y sólo si $\forall n > k, P(k) \wedge ... \wedge P(n-1) \Rightarrow P(n)$ es verdadera para algún $k \in \mathbb{N}$.
29. La proposición $\forall n \in \mathbb{N}, P(n)$ es verdadera si y sólo si $P(k) \wedge ... \wedge P(n)$ es verdadera para algunos $k, n \in \mathbb{N}$.
30. La proposición $\forall n \in \mathbb{N}, P(n)$ es verdadera si y sólo si $P(0)$ y $\forall n \in \mathbb{N}, P(n) \iff P(n+1)$ son verdaderas.

Guía de Ejercicios

1. Sean $P(x), Q(x)$ funciones proposicionales. Determinar la negación de las siguientes proposiciones cuantificadas:

   a) $\exists x \in E, \forall y \in E,\ P(x) \wedge Q(y)$.
   b) $\forall x \in E, \forall y \in E,\ P(x) \implies \overline{Q(y)}$.
   c) $\exists! x \in E,\ P(x)$.
   d) $\forall x \in E,\ Q(x) \implies (\exists y \in E, P(y))$.
   e) $\exists x \in E, \exists y \in E, P(x) \iff Q(y)$.
   f) $\exists x \in \mathbb{R},\ \forall y \in \mathbb{R},\ x < y$.
   g) $\forall x \in \mathbb{R},\ \forall y \in \mathbb{R},\ x \geq y$.
   h) $\exists x \in \mathbb{R},\ \forall y \in \mathbb{R}, x > 1 \wedge y \leq 1$.

2. Demuestre las siguientes afirmaciones, usando inducción. Indique claramente sobre qué variable la está usando y cuál es la hipótesis inductiva.

   a) $\forall n \in \mathbb{N}$, la suma de los primeros n naturales es divisible por n o por $n+1$.

b) $\forall n \in \mathbb{N},\ n^3 + 5n$ es divisible por 6.
c) $\forall n \in \mathbb{N},\ 5^{2n+1} + 7^{2n+1}$ es divisible por 6.
d) $\forall n \in \mathbb{N},\ (x - y)$ divide a $x^n - y^n$.
e) $\forall n \in \mathbb{N}, n \geq 1,\ 1 + \frac{1}{4} + \frac{1}{9} + ... + \frac{1}{n^2} \leq 2 - \frac{1}{n}$.
f) $\forall n \in \mathbb{N},\ -1 \cdot 3 + 2 \cdot 5 - 3 \cdot 7 + \cdots + 2n(4n + 1) = \alpha n$, y determine el valor de la constante α.
g) $\forall n \in \mathbb{N}$, demuestre que el producto de n números naturales mayores estrictos que uno y no necesariamente consecutivos es mayor estricto que n.
h) $\forall n \in \mathbb{N}$, demuestre que si tiene n rectas en el plano, de modo tal que no existen rectas paralelas y además ningún punto del plano está en más de dos rectas, entonces el total de regiones formadas es $(1 + \cdots + n) + 1$.
i) $\forall n \in \mathbb{N}$, demuestre que n puntos sobre una recta generan $n + 1$ segmentos.

Guía de Problemas

1. Determine si $(\forall x \in E, P(x) \iff Q(x)) \Rightarrow ((\forall x \in E, P(x)) \iff (\forall x \in E, Q(x)))$.
2. Determine si $((\forall x \in E, P(x)) \iff (\forall x \in E, Q(x))) \Rightarrow (\forall x \in E, P(x) \iff Q(x))$.
3. Determine si $(\forall x \in E, \neg(\exists y \in E, P(x, y))) \iff \forall x, y \in E, \neg P(x, y)$.
4. (20 min.) Probar por inducción que para todo $n \geq 1$, $2 \cdot 7^n + 3 \cdot 5^n - 5$ es divisible por 24.
5. (20 min.) Demuestre que $(\forall n \in \mathbb{N}, n \geq 10, n^3 < 2^n)$.
6. Consideremos la siguiente sucesión $\{a(n)\}_{n \geq 1}$ definida por recurrencia.

$$a(n) = \begin{cases} 1, & \text{si } n = 1 \text{ o } n = 2, \\ 3[a(n-1) + a(n-2)] + 1, & \text{si } n > 2. \end{cases}$$

Queremos probar que para todo $n \in \mathbb{N}^*$, $a(3n) + a(3n + 1)$ es divisible por 32.

a) (20 min.) Pruebe usando inducción que para todo $n \in \mathbb{N}$, $a(3n+2)-1$ es divisible por 2.
b) (20 min.) Pruebe usando inducción que para todo $n \in \mathbb{N}$, $3a(3n + 1) + 5$ es divisible por 8.
c) (20 min.) Pruebe usando inducción que para todo $n \in \mathbb{N}^*$, $a(3n) + a(3n + 1)$ es divisible por 32.

7. (20 min.) Demuestre usando inducción que para todo $n \in \mathbb{N}, n \geq 1$ y para todo $x \in \mathbb{R}, x \neq 1$ se tiene que:

$$(1 + x)(1 + x^2)(1 + x^{2^2})(1 + x^{2^3})...(1 + x^{2^{n-1}}) = \frac{x^{2^n} - 1}{x - 1}.$$

8. Busque una recurrencia para el largo de la curva de Hilbert de orden n.

SEMANA 03:

Conjuntos

Ingeniería Matemática
FACULTAD DE CIENCIAS
FÍSICAS Y MATEMÁTICAS
UNIVERSIDAD DE CHILE

3.1 Introducción

En la Lógica Proposicional aceptamos que $x \in E$ es una proposición que es verdadera cuando x es un elemento del conjunto E y falsa cuando no lo es. En la Lógica de Primer Orden se vió la noción de predicado como una expresión que depende de variables que al ser reemplazadas por elementos de un conjunto de referencia lo transforman en una proposición.

En ambos casos, el uso que le dimos a las palabras conjunto y elemento fue el de la noción intuitiva que tenemos de ellos: un conjunto es una colección de cosas, sus elementos.

Sorprendentemente, no es fácil definir de manera rigurosa la noción de conjunto. De hecho, la importancia de tener una noción formal fue aceptada recién a fines de los 1800's, cuando nace la teoría axiomática de conjuntos. Aquí no veremos esta teoría y seguiremos usando la noción intuitiva. Lo que sí se verá en detalle es cómo obtener nuevos conjuntos a partir de otros dados o conocidos (como los reales $\mathbb{R}$, los naturales $\mathbb{N}$, los enteros $\mathbb{Z}$, etc.).

Partamos discutiendo la definición de un conjunto en términos de un predicado. Dado un predicado $P(x)$ sobre un conjunto de referencia E, podemos construir un nuevo conjunto A indicando que sus elementos son aquellos $e \in E$ para los cuales se tiene $P(e)$. Es decir,

$$\forall x \in E,\ x \in A \iff P(x),$$

lo que a menudo también denotamos $A = \{x \in E \mid P(x)\}$, donde hemos usado la convención que consiste en denotar la función proposicional "x pertenece a A" por "$x \in A$" (y cuya negación, el lector recordará, denotamos "$x \notin A$").

Otra forma de escribir un conjunto es listar sus elementos (cuando esto es posible). Por ejemplo, $A = \{a\}$, $B = \{a, b\}$.

Ejemplo:

- El intervalo cerrado $[a, b] = \{x \in \mathbb{R} \mid a \leq x \leq b\}$ y el intervalo abierto $(a, b) = \{x \in \mathbb{R} \mid a < x < b\}$, donde $a, b \in \mathbb{R}$, $a < b$.[5]
- El conjunto de múltiplos de 7 es el conjunto $\{x \in \mathbb{N} \mid \frac{1}{7}x \in \mathbb{N}\}$.
- Los racionales $\mathbb{Q} = \{x \in \mathbb{R} \mid \exists p, q \in \mathbb{Z}, q \neq 0 \wedge x = \frac{p}{q}\}$ y los irracionales $\{x \in \mathbb{R} \mid x \notin \mathbb{Q}\}$.

[5] $a \leq x \leq b \iff a \leq x \wedge x \leq b$ y $a < x < b \iff a < x \wedge x < b$

- Los enteros positivos $\mathbb{N}^* = \{1, 2, 3, 4, \ldots\}$.

$\diamondsuit$

Los conjuntos suelen denotarse con letras mayúsculas, como $A, B, C, \ldots, X, Y, Z$. En lo que sigue, a menos que se diga lo contrario, estas letras mayúsculas denotan conjuntos arbitrarios, cuyos elementos suponemos que siempre están en el conjunto de referencia E.

Diagramas de Venn

Un **Diagrama de Venn** es una ilustración que muestra la relación matemática o lógica entre conjuntos y/o entre conjuntos y sus elementos (ver Figura 2). Cumplen el rol de ayudarnos a desarrollar una **intuición** frente al concepto de conjunto y a las relaciones entre estos. Sin embargo, **no** podemos usarlos para demostrar propiedades, ni para sacar conclusiones generales (que se apliquen a todo conjunto).

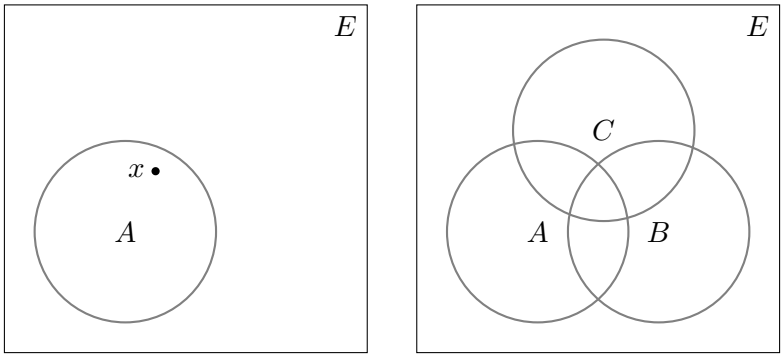


Figura 2: Diagramas de Venn. El de la izquierda representa al conjunto A y la relación de pertenencia $x \in A$. El de la derecha, representa a los conjuntos A, B, y C.

3.2 Preliminares

Hay ciertos conjuntos particulares a los que les daremos un tratamiento específico. A algunos inclusive les daremos un nombre y los denotaremos con un símbolo especial.

Conjunto de referencia

Como ya adelantamos, asumiremos la existencia de un conjunto de referencia que usualmente denotaremos E y al que pertenecen todos los elementos con los que se va a trabajar. Formalmente, E es tal que la función proposicional $e \in E$ es siempre verdadera o dicho de otra forma la proposición $\forall x \in E, x \in E$, es verdadera. En ocasiones, el conjunto de referencia será uno conocido, como $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{R}$, etc.

Siempre asumiremos que un conjunto de referencia contiene al menos un elemento.

Conjunto vacío

Definición 3.1 (Conjunto vacío) *El conjunto vacío, denotado $\emptyset$, es un conjunto que no tiene elementos, es decir, cumple que cualquiera que sea el conjunto de referencia E*

$$\forall x \in E, x \in \emptyset \iff F.$$

3.3 Relaciones entre conjuntos

Primero, especificamos cuándo consideramos que dos conjuntos son iguales.

Definición 3.2 (Igualdad) *Se dice que los conjuntos A y B son iguales, denotado $A = B$, si A y B tienen los mismos elementos. Es decir,*

$$A = B \iff (\forall x \in E,\ x \in A \iff x \in B).$$

Notar que de la definición sigue que $\{a, a\} = \{a\}$. En particular, si $A = \{a, b\}$ se tiene que $a = b$ si y sólo si $\{a, b\} = \{a\}$.

Definición 3.3 (Inclusión) *Se dice que A es subconjunto de B (o que A está contenido en B, o que A esta incluido en B), denotado $A \subseteq B$, si todos los elementos de A están también en B. Es decir,*

$$A \subseteq B \iff (\forall x \in E, x \in A \Rightarrow x \in B).$$

La Figura 3 muestra una representación en términos de Diagrama de Venn de la relación de inclusión entre A y B.

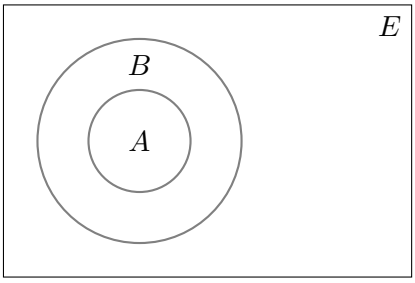


Figura 3: Diagrama de Venn representando $A \subseteq B$.

A continuación enunciaremos las principales propiedades que involucran a la igualdad e inclusión de conjuntos. Sus demostraciones consisten en reducirlas a proposiciones cuya validez se establece a través de la lógica.

Proposición 3.4 *Para $A, B, C \subseteq E$ se cumplen las siguientes propiedades:*

(I).- Reflexividad de la $\subseteq$: $A \subseteq A$.
(II).- Antisimetría de la $\subseteq$: $A = B \iff A \subseteq B \wedge B \subseteq A$.
(III).- Transitividad de la $\subseteq$: $A \subseteq B \wedge B \subseteq C \implies A \subseteq C$.

Dem. Sólo probaremos la segunda propiedad. En efecto,

$$\begin{aligned} A = B &\iff (\forall x \in E, x \in A \iff x \in B) && \text{(def. de igualdad de conjuntos)} \\ &\iff (\forall x \in E, (x \in A \Rightarrow x \in B) \wedge (x \in B \Rightarrow x \in A)) && \text{(Equivalencia dividida)} \\ &\iff (\forall x \in E, x \in A \Rightarrow x \in B) \wedge (\forall x \in E, x \in B \Rightarrow x \in A) \\ & && \text{(Distributividad de } \forall \text{ c/r a } \wedge) \\ &\iff A \subseteq B \wedge B \subseteq A. && \text{(def. de la } \subseteq) \end{aligned}$$

La transitividad de la equivalencia nos dice que $A = B \iff A \subseteq B \wedge B \subseteq A$. □

Aprovechando la transitividad de $\subseteq$ escribiremos $A \subseteq B \subseteq C$ en lugar de $A \subseteq B \wedge B \subseteq C$. En este sentido, la siguiente propiedad dice que $\emptyset \subseteq A \wedge A \subseteq E$.

Proposición 3.5 $\emptyset \subseteq A \subseteq E$.

Dem. Sea x arbitrario. Notar que

$$\begin{aligned} x \in \emptyset &\implies x \in A && \text{(porque } x \in \emptyset \iff F \text{ y definición de } \Rightarrow) \\ &\implies x \in E. && \text{(porque } x \in E \iff V \text{ y definición de } \Rightarrow) \end{aligned}$$

La transitividad de $\Rightarrow$ nos dice que $x \in \emptyset \Rightarrow x \in E$. Como x es arbitrario, por definición de $\subseteq$, se concluye el resultado enunciado. □

Otras propiedades importantes que se establecen de manera similar a las dos recién vistas, y que quedan propuestas como ejercicios, son:

Proposición 3.6 *Para $A, B, C \subseteq E$ se cumplen las siguientes propiedades:*

- *Reflexividad del $=$:* $A = A$.
- *Simetría del $=$:* $A = B \iff B = A$.
- *Transitividad del $=$:* $A = B \wedge B = C \implies A = C$.

Al igual que en el caso de $\subseteq$, la transitividad de $=$ motiva escribir $A = B = C$ en lugar de $A = B \wedge B = C$.

3.4 Álgebra de conjuntos.

A partir de conjuntos conocidos se pueden definir nuevos conjuntos. A continuación ilustraremos varias formas de hacerlo. Nuevamente, A, B, C denotan subconjuntos de E.

Unión e intersección de conjuntos

Definición 3.7 (Unión) *La unión de A y B, denotada $A \cup B$, es el conjunto que reúne a los elementos que están en al menos uno de los dos conjuntos A o B. Formalmente,*

$$\forall x \in E, x \in A \cup B \iff x \in A \vee x \in B.$$

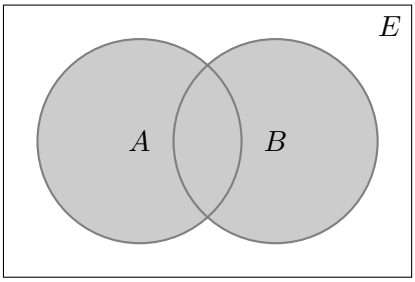


Figura 4: Diagrama de Venn representando la unión de A y B (área sombreada).

Definición 3.8 (Intersección) *La intersección de A y B, denotada $A \cap B$, es el conjunto de los elementos que están tanto en A como en B. Formalmente,*

$$\forall x \in E, x \in A \cap B \iff x \in A \wedge x \in B.$$

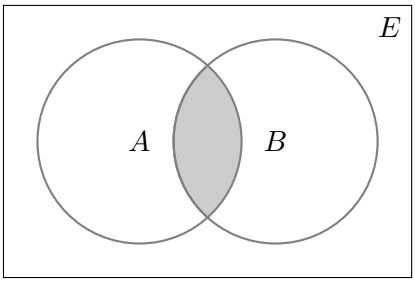


Figura 5: Diagrama de Venn de la intersección entre A y B (área sombreada).

A continuación, veremos propiedades que involucran a la unión e intersección de conjuntos.

Proposición 3.9 $X \subseteq Y \ \wedge \ W \subseteq Z \implies X \cap W \subseteq Y \cap Z \ \wedge \ X \cup W \subseteq Y \cup Z.$

Dem. Por hipótesis, suponemos que $X \subseteq Y$ y $W \subseteq Z$. Sea x arbitrario. Notar que

$$\begin{aligned} x \in X \cap W &\iff x \in X \wedge x \in W && \text{(definición de } \cap) \\ &\implies x \in Y \wedge x \in Z && \text{(porque por hipótesis } X \subseteq Y \text{ y } W \subseteq Z) \\ &\implies x \in Y \cap Z. && \text{(definición de } \cap) \end{aligned}$$

Por transitividad se obtiene que $x \in X \cap W \Rightarrow x \in Y \cap Z$. Como x es arbitrario, por definición de inclusión, se concluye que $X \cap W \subseteq Y \cap Z$. De manera similar se prueba que, bajo las mismas hipótesis $X \cup W \subseteq Y \cup Z$. □

Proposición 3.10 *Se tienen las siguientes igualdades de conjuntos:*

- *Idempotencia:* $A \cap A = A, \quad A \cup A = A.$
- *Vacío es neutro para* $\cup$*:* $A \cup \emptyset = A.$
- *Vacío es absorbente para* $\cap$*:* $A \cap \emptyset = \emptyset,$
- *El conjunto de referencia es neutro para* $\cap$*:* $A \cap E = A.$
- *El conjunto de referencia es absorbente para* $\cup$*:* $A \cup E = E.$
- *Conmutatividad:*
  - *de la* $\cup$*:* $A \cup B = B \cup A.$
  - *de la* $\cap$*:* $A \cap B = B \cap A.$
- *Asociatividad:*
  - *de la* $\cup$*:* $A \cup (B \cup C) = (A \cup B) \cup C.$
  - *de la* $\cap$*:* $A \cap (B \cap C) = (A \cap B) \cap C.$
- *Distributividad:*
  - *de la* $\cup$ *c/r a* $\cap$*:* $A \cup (B \cap C) = (A \cup B) \cap (A \cup C).$
  - *de la* $\cap$ *c/r a* $\cup$*:* $A \cap (B \cup C) = (A \cap B) \cup (A \cap C).$

Dem. Todas las propiedades son consecuencia directa de las definiciones de unión e intersección de conjuntos y las propiedades análogas para $\wedge$ y $\vee$. Queda como ejercicio realizar dichas demostraciones. □

Corolario 3.11

(I) $A \cap B \subseteq A \subseteq A \cup B$ *(análogamente,* $A \cap B \subseteq B \subseteq A \cup B$*).*

(II) $A \subseteq B \ \wedge \ A \subseteq C \implies A \subseteq B \cap C.$

(III) $A \subseteq B \ \wedge \ C \subseteq B \implies A \cup C \subseteq B.$

Dem. Las tres propiedades son casos particulares de la Proposición 3.9. La parte (I) se obtiene reemplazando, en la proposición mencionada, X e Y por A, W por B, y Z por E, para obtener que $A \cap B \subseteq A$. Si por otro lado se reemplaza X e Y por A, W por $\emptyset$, y Z por B, se concluye que $A \subseteq A \cup B$. (Intercambiando el rol de A y B se obtiene el resultado análogo para B.) La parte (II), se obtiene reemplazando X y W por A, Y por B, y Z por C. La parte (III), se obtiene reemplazando X por A, W por C, e Y y Z por B. □

Hasta ahora hemos reducido todas las demostraciones de afirmaciones que involucran conjuntos a verificar que ciertas proposiciones lógicas son verdaderas. La demostración del siguiente resultado es particularmente novedosa, puesto que usa las propiedades ya establecida para demostrar nuevas propiedades. Esta nueva forma de argumentar es más directa y elegante; la preferiremos por sobre los referidos argumentos que hasta ahora hemos realizado.

Proposición 3.12 $A \subseteq B \implies A \cup B = B \ \wedge \ A \cap B = A$.

Dem. Veamos que $A \subseteq B \implies A \cup B = B$. En efecto,

$$\begin{aligned} A \subseteq B &\iff A \subseteq B \wedge B \subseteq B && \text{(def. de } \wedge \text{ y porque } B \subseteq B) \\ &\implies A \cup B \subseteq B && \text{(Corolario 3.11 parte (III))} \\ &\implies A \cup B = B. && \text{(Corolario 3.11 parte (I) y def. de } = \text{ de conjuntos)} \end{aligned}$$

Veamos ahora que $A \subseteq B \implies A \cap B = A$. En efecto,

$$\begin{aligned} A \subseteq B &\iff A \subseteq A \wedge A \subseteq B && \text{(def. de } \wedge \text{ y porque } A \subseteq A) \\ &\implies A \subseteq A \cap B && \text{(Corolario 3.11 parte (II))} \\ &\implies A = A \cap B. && \text{(Corolario 3.11 parte (I) y def. de } = \text{ de conjuntos)} \end{aligned}$$

□

Antes de concluir esta sección, discutiremos cómo realizar y operar con uniones e intersecciones de más de dos conjuntos. Específicamente, supongamos que tenemos conjuntos $A_1, A_2, \ldots, A_n$. Su unión la podemos expresar en término de sucesivas uniones de pares de conjuntos por:

$$((\ldots((A_1 \cup A_2) \cup A_3) \ldots \cup A_{n-1}) \cup A_n).$$

Dado que, tal como hemos visto, $\cup$ es asociativa, los paréntesis en la expresión anterior son irrelevantes y pueden ser omitidos, obteniéndose la siguiente expresión:

$$A_1 \cup A_2 \cup A_3 \cup \ldots \cup A_{n-1} \cup A_n,$$

que suele denotarse de las siguientes dos formas:

$$\bigcup_{i=1}^{n} A_i, \quad \text{o} \quad \bigcup_{i \in \{1,\ldots,n\}} A_i,$$

y que se leen "unión de $i = 1$ a n de los A_i" y "unión de los i en $\{1, \ldots, n\}$ de los A_i", respectivamente.

El lector puede probar (por inducción en n) que

$$x \in \bigcup_{i \in \{1,\ldots,n\}} A_i \iff (\exists i \in \{1, \ldots, n\}, x \in A_i). \tag{2}$$

Consideremos ahora que hay una cantidad infinita de conjuntos. Más precisamente, pensemos que tenemos un conjunto de índices Λ y para todo $\lambda \in \Lambda$ tenemos un conjunto A_λ. El caso considerado más arriba corresponde a $\Lambda = \{1, \ldots, n\}$. Pero si Λ es un conjunto de índices que tiene una infinidad de elementos, la forma (esencialmente recursiva) en que definimos la unión de la colección finita de conjuntos $A_1, \ldots, A_n$ falla puesto que nunca termina. No obstante, la expresión a la derecha de la equivalencia (2) es fácilmente extensible al caso infinito y da lugar a la siguiente definición de unión de los A_λ con $\lambda \in \Lambda$.

Definición 3.13 (Unión sobre conjuntos de índices) *Sea Λ conjunto de índices y, para todo $\lambda \in \Lambda$, sea $A_\lambda \subseteq E$ conjunto. Se define la unión de los A_λ con $\lambda \in \Lambda$, denotado $\bigcup_{\lambda\in\Lambda} A_\lambda$, como el conjunto de los x tal que $x \in A_\lambda$ para algún $\lambda \in \Lambda$. Formalmente,*

$$\forall x \in E, x \in \bigcup_{\lambda\in\Lambda} A_\lambda \iff (\exists \lambda \in \Lambda, x \in A_\lambda).$$

Un razonamiento análogo pero para el caso de la intersección nos lleva a la siguiente:

Definición 3.14 (Intersección sobre conjuntos de índices) *Sea Λ conjunto de índices y para todo $\lambda \in \Lambda$ sea $A_\lambda \subseteq E$ conjunto. Se define la intersección de los A_λ con $\lambda \in \Lambda$, denotado $\bigcap_{\lambda\in\Lambda} A_\lambda$, como el conjunto de los x tal que $x \in A_\lambda$ para todo $\lambda \in \Lambda$. Formalmente,*

$$\forall x \in E, x \in \bigcap_{\lambda\in\Lambda} A_\lambda \iff (\forall \lambda \in \Lambda, x \in A_\lambda).$$

Ejemplo:

- Sea el conjunto de índices $\mathbb{N}$ y para $i \in \mathbb{N}$, sea $A_i = \{-i, \ldots, -1, 0, 1, \ldots, i\}$. Notar que
$$\bigcup_{i\in\mathbb{N}} A_i = \mathbb{Z}, \quad \text{y} \quad \bigcap_{i\in\mathbb{N}} A_i = \{0\}.$$
- Si para $i \in \mathbb{Z}$ se define $B_i = \{i, i+1, \ldots, i+10\}$, entonces
$$\bigcup_{i\in\mathbb{Z}} B_i = \mathbb{Z}, \quad \text{y} \quad \bigcap_{i\in\mathbb{Z}} B_i = \emptyset.$$

♢

Convención: Cuando el conjunto de índices Λ es vacío, adoptamos como convención que:

$$\bigcup_{\lambda\in\Lambda} A_\lambda = \emptyset \quad \text{y} \quad \bigcap_{\lambda\in\Lambda} A_\lambda = E.$$

Observación: En las expresiones $\bigcup_{\lambda\in\Lambda} A_\lambda$ y $\bigcap_{\lambda\in\Lambda} A_\lambda$, el símbolo λ se llama **índice mudo**. Es decir, dicho λ puede ser reemplazado por otro símbolo (por ejemplo, $\alpha, \beta, \gamma, ...$ o $i, j, ...$) y la expresión que se obtiene denotará el mismo conjunto. Por ejemplo,

$$\bigcup_{\lambda\in\Lambda} A_\lambda = \bigcup_{\alpha\in\Lambda} A_\alpha = \bigcup_{\beta\in\Lambda} A_\beta = ... = \bigcup_{i\in\Lambda} A_i = ...$$

□

Diferencia y complemento

Definición 3.15 (Conjunto complemento) *El complemento de un conjunto A (con respecto a E), denotado A^c, es el conjunto de los elementos que están en E pero no están en A. Formalmente,*

$$\forall x \in E, x \in A^c \iff x \notin A.$$

El diagrama de Venn de A^c se muestra en la Figura 6

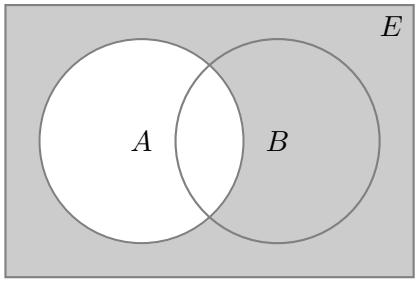


Figura 6: Diagrama de Venn representando el complemento de A (área sombreada).

Ejemplo: Si nuestro conjunto de referencia fuese $\mathbb{Z}$ y $A = \{m \in \mathbb{Z} \mid m \text{ es par}\}$, entonces $A^c = \{m \in \mathbb{Z} \mid m \text{ es impar}\}$. ♢

Algunas propiedades:

Proposición 3.16

- *Leyes de De Morgan:* $(A \cup B)^c = A^c \cap B^c$ *y* $(A \cap B)^c = A^c \cup B^c$.
- *Doble complementación:* $(A^c)^c = A$.
- $A \cap A^c = \emptyset$ *y* $A \cup A^c = E$.

Dem. Demostraremos sólo la primera Ley de De Morgan. Sea $x \in E$ arbitrario.

$$\begin{aligned}
x \in (A \cup B)^c &\iff \overline{x \in A \cup B} && \text{(definición de conjunto complemento)} \\
&\iff \overline{x \in A \vee x \in B} && \text{(definición de } \cup\text{)} \\
&\iff \overline{x \in A} \wedge \overline{x \in B} && \text{(Leyes de De Morgan de la lógica proposicional)} \\
&\iff x \in A^c \wedge x \in B^c && \text{(definición de conjunto complemento)} \\
&\iff x \in A^c \cap B^c. && \text{(definición de } \cap\text{)}
\end{aligned}$$

Por transitividad de $\iff$ se obtiene que $x \in (A \cup B)^c \iff x \in A^c \cap B^c$. Como x es arbitrario, por definición de igualdad de conjuntos, se concluye que $(A \cup B)^c = A^c \cap B^c$. □

Proposición 3.17 *Las siguientes son todas equivalentes:*

(I) $A \subseteq B$.
(II) $B^c \subseteq A^c$.
(III) $A \cap B^c = \emptyset$.
(IV) $A^c \cup B = E$.

Definición 3.18 (Diferencia) *La diferencia de A con B, que notamos $A \setminus B$, es el conjunto formado por los elementos que están en A y que no están en B. Formalmente:*

$$A \setminus B = A \cap B^c.$$

El diagrama de Venn de $A \setminus B$ se muestra en la Figura 7

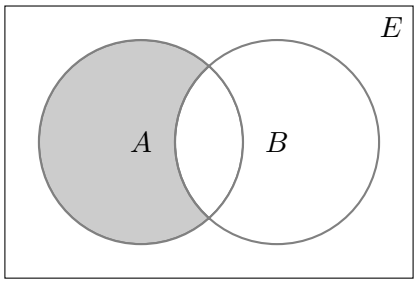


Figura 7: Diagrama de Venn representando la diferencia de A con B (área sombreada).

Observación: $A^c = E \setminus A$. □

Diferencia simétrica

Un elemento x se dice que pertenece a la **diferencia simétrica** entre A y B, que se denota $A\Delta B$, si y solamente si x está o bien en A o bien en B pero no en ambos (Ver diagrama de Venn en Figura 8).

Definición 3.19 (Diferencia simétrica) *La diferencia simétrica entre A y B, que denotamos $A\Delta B$, es el conjunto formado por los elementos que están en A pero no en B, o que están en B pero no en A. Formalmente:*

$$A\Delta B = (A \setminus B) \cup (B \setminus A).$$

A continuación, estableceremos algunas de las propiedades de la diferencia simétrica.

Proposición 3.20

- $A\Delta B = (A \cup B) \setminus (A \cap B)$.
- $A\Delta A = \emptyset$.

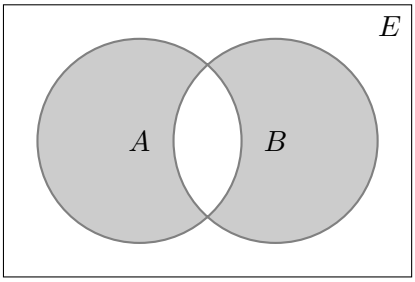


Figura 8: Diagrama de Venn representando la diferencia simétrica entre A y B (área sombreada).

- *Vacío es neutro para* Δ*:* $A\Delta\emptyset = A$.
- *Conmutatividad de* Δ*:* $A\Delta B = B\Delta A$.
- *Asociatividad de* Δ*:* $(A\Delta B)\Delta C = A\Delta(B\Delta C)$.
- *Distributividad de la* $\cap$ *c/r a* Δ*:* $A \cap (B\Delta C) = (A \cap B)\Delta(A \cap C)$.

Dem. Demostraremos sólo la primera.

$$\begin{aligned}
A\Delta B &= (A \setminus B) \cup (B \setminus A) && \text{(definición de } \Delta\text{)} \\
&= (A \cap B^c) \cup (B \cap A^c) && \text{(definición de } \setminus\text{)} \\
&= [(A \cap B^c) \cup B] \cap [(A \cap B^c) \cup A^c] && \text{(distrib. de } \cup \text{ c/r a } \cap\text{)} \\
&= [(A \cup B) \cap (B^c \cup B)] \cap [(A \cup A^c) \cap (B^c \cup A^c)] && \text{(distrib. de } \cup \text{ c/r a } \cap\text{)} \\
&= [(A \cup B) \cap E] \cap [E \cap (B^c \cup A^c)] && \text{(porque } A^c \cup A = B^c \cup B = E\text{)} \\
&= (A \cup B) \cap (B^c \cup A^c) && \text{(porque } X \cap E = E \cap X = X\text{)} \\
&= (A \cup B) \cap (B \cap A)^c && \text{(Leyes de De Morgan)} \\
&= (A \cup B) \setminus (A \cap B). && \text{(definición de } \setminus\text{)}
\end{aligned}$$

Por transitividad de $=$ se concluye que $A\Delta B = (A \cup B) \setminus (A \cap B)$ □

Cabe destacar que si bien $\cap$ distribuye con respecto a Δ, no es cierto que $\cup$ distribuya con respecto a Δ. En efecto, basta considerar el siguiente contraejemplo donde $A \neq \emptyset$:

$$A \cup (A\Delta A) = A \neq \emptyset = (A \cup A)\Delta(A \cup A).$$

Guía Básica

Determinar la veracidad de las siguientes afirmaciones:

1. Una definición formal del conjunto $A = \{1, 2, 3\}$ es
$$\forall x \in E, x \in A \iff x = 1 \vee x = 2 \vee x = 3.$$
2. Una definición formal del conjunto $A = \{1, 2, 3\}$ es
$$\forall x \in E, x \in A \iff x = 1 \wedge x = 2 \wedge x = 3.$$
3. Dado el conjunto $B = \{x \in A \mid P(x)\}$, la proposición $x \in B$ está definida por
$$\forall x \in E, x \in B \iff x \in A \vee P(x).$$
4. Dado el conjunto $B = \{x \in A \mid P(x)\}$, la proposición $x \in B$ está definida por
$$\forall x \in E, x \in B \iff x \in A \wedge P(x).$$
5. Dado el conjunto $B = \{x \in A \mid P(x)\}$, la proposición $x \in B$ está definida por
$$\forall x \in E, x \in B \iff (x \in A \implies P(x)).$$
6. Dado un conjunto $A \neq \mathbb{N}$, se tiene que $\emptyset = \{x \in \mathbb{N} \mid x \neq x\} \neq \{x \in A \mid x \neq x\}$.
7. Dado un conjunto A, es cierto que $\emptyset = \{x \in A \mid x \neq x\}$.
8. La siguiente proposición lógica es falsa: $\exists! x \in E, x \in \emptyset$.
9. La siguiente proposición lógica es verdadera: $\forall x \in E, x \notin \emptyset$.
10. La siguiente proposición lógica es falsa: $\exists x \in E, x \notin \emptyset$.
11. Dos conjuntos A y B son iguales si $\exists x \in E, x \in A \iff x \in B$.
12. Dos conjuntos A y B son iguales si $\forall x \in E, x \in A \iff x \in B$.
13. Dos conjuntos A y B son iguales si $\forall x \in E, x \in A \wedge x \in B$.
14. Un conjunto A está incluido en un conjunto B si $\forall x \in E, x \in B \implies x \in A$.
15. Un conjunto A está incluido en un conjunto B si $\forall x \in E, x \notin B \implies x \notin A$.
16. Un conjunto A está incluido en un conjunto B si $\forall x \in E, x \in A \implies x \in B$.
17. Dados A, B conjuntos, si $A \subseteq\subseteq A$, no necesariamente se tiene que $A = B$.
18. Dados A, B conjuntos se tiene que $A = B \iff A \subseteq B \subseteq A$.
19. Dados A, B conjuntos, se tiene que $A = B \iff A \subseteq B \vee B \subseteq A$.
20. Dados A, B, C conjuntos, si $A \subseteq B \subseteq C$, entonces $B = A$ ó $B = C$.
21. Dados A, B, C conjuntos, si $A \subseteq B \subseteq C$, entonces $B = A = C$.
22. Dados A, B, C conjuntos, si $A \subseteq B \subseteq C$, entonces $A \subseteq C$.

23. Para cualquier conjunto A, se tiene que $\emptyset \subseteq A$.
24. Dado un conjunto A, se tiene que $\{\emptyset\} \subseteq A$.
25. Dado $A \neq \emptyset$ conjunto, la proposición $\exists x \in E, x \in \emptyset \implies x \in A$ es verdadera.
26. La unión entre los conjuntos A y B, se define formalmente como:

$$\forall x \in E, x \in A \cup B \iff x \in A \wedge x \in B.$$

27. La unión entre los conjuntos A y B, se define formalmente como:

$$\forall x \in E, x \in A \cup B \iff x \in A \vee x \in B.$$

28. Dados A y B conjuntos, un elemento x que satisface $x \notin A \wedge x \in B$, pertenece a $A \cup B$.
29. Para que $A \cup B = A$, el conjunto B debe ser vacío.
30. La intersección entre los conjuntos A y B, se define formalmente como:

$$\forall x \in E, x \in A \cap B \iff x \in A \wedge x \in B.$$

31. La intersección entre los conjuntos A y B, se define formalmente como:

$$\forall x \in E, x \in A \cap B \iff x \in A \vee x \in B.$$

32. Sean A, B conjuntos. Como $A \cap B \subseteq A$, basta que un elemento x pertenezca a A, para que $x \in A \cap B$ sea verdadera.
33. El conjunto de referencia E se define de manera que la proposición $x \in E$ es siempre verdadera para los elementos de interés.
34. Dado un conjunto de referencia E y un conjunto $A \subseteq E$, luego $A^c = E \setminus A$.
35. Dados un conjunto de referencia E y un conjunto A, se tiene que $A \cap E = A$.
36. Dados un conjunto de referencia E y un conjunto A, se tiene que $A \cap A^c = E$.
37. Dado un conjunto de referencia E y cualquier par de conjuntos A y B, se tiene que $A^c \cup B^c = E$.
38. Si dos conjuntos A y B satisfacen que $A \subseteq B$, entonces $A^c \subseteq B^c$.
39. Existen conjuntos A y B para los cuales $A \subseteq B^c \wedge A^c \subseteq B$.
40. Si dos conjuntos A y B satisfacen que $A \subseteq B$, entonces $B^c \subseteq A^c$.
41. El complemento del conjunto $A \cup B^c$ es $A^c \cap B$.
42. El complemento del conjunto $A \cup B^c$ es $B^c \cap A^c$.
43. El complemento del conjunto $A \cap B^c$ es $B \cup A^c$.
44. Dados A, B conjuntos, se tiene que $A \Delta B = (A \cup B) \setminus (A \cap B)$.
45. Dados A, B conjuntos, se tiene que $A \Delta B \subseteq A$.
46. Dados A, B conjuntos, se tiene que $A \Delta B = (A \cup B) \setminus (A \cap B) = A^c \Delta B^c$.

Guía de Ejercicios

1. Sean $A, B, C \subseteq E$ conjuntos. Emplear los teoremas del álgebra de conjuntos para probar las siguientes propiedades:

   a) $(A \cap B)^c = A^c \cup B^c$.
   b) $A \subseteq B \iff B^c \subseteq A^c$.
   c) $(A^c)^c = A$.
   d) $(A \Delta B) \Delta C = A \Delta (B \Delta C)$.
   e) $A \Delta \emptyset = A$.
   f) $A \cap (B \Delta C) = (A \cap B) \Delta (A \cap C)$.
   g) $(A \setminus C) \cup (B \setminus C) = (A \cup B) \setminus C$.
   h) $(A \setminus B) \cap (A \setminus C) = A \setminus (B \cup C)$.
   i) $(A \setminus C) \setminus (B \setminus C) = (A \setminus B) \setminus C$.
   j) $[A \setminus (B \setminus A)] \cup [(B \setminus A) \setminus A] = A \cup B$.
   k) $(A \cap B) \setminus (A \cap C) = (A \cap B) \setminus (A^c \cup C)$.
   l) $A \subseteq B \subseteq C \implies C \setminus (B \setminus A) = A \cup (C \setminus B)$.
   m) $B = (A \cap B^c) \cup (A^c \cap B) \iff A = \emptyset$.

2. Sea Λ un conjunto de índices tales que para todo $\lambda \in \Lambda$ tenemos conjuntos A_λ y B_λ. Pruebe que:

   (I).- $\left(\bigcup_{\lambda\in\Lambda} A_\lambda\right)^c = \bigcap_{\lambda\in\Lambda} A_\lambda^c$ y $\left(\bigcap_{\lambda\in\Lambda} A_\lambda\right)^c = \bigcup_{\lambda\in\Lambda} A_\lambda^c$.
   (II).- $(\forall \lambda \in \Lambda, A_\lambda \subseteq B_\lambda) \implies \bigcup_{\lambda\in\Lambda} A_\lambda \subseteq \bigcup_{\lambda\in\Lambda} B_\lambda \ \wedge \ \bigcap_{\lambda\in\Lambda} A_\lambda \subseteq \bigcap_{\lambda\in\Lambda} B_\lambda$.

Guía de Problemas

1. Sean A, B, C, D conjuntos. Emplear los teoremas del álgebra de conjuntos para probar que

   a) 1) (10 min.) $(B \setminus A) \subseteq C \iff C^c \subseteq (B^c \cup A)$.
      2) (30 min.) $(B \setminus A) \subseteq C \implies (D \setminus C) \subseteq (D \setminus B) \cup A$.
      Hint: Use lo anterior.
   b) (20 min.) $A \cup B = A \cap C \iff B \subseteq A \wedge A \subseteq C$.

2. (35 min.) Sean $A, B \subseteq E$ y $C = (A \cup B)^c$. Probar que

$$(A \Delta B) \Delta C = A \cup B \cup C \iff A \cap B = \emptyset.$$

3.5 Pares ordenados y producto cartesiano

Notemos que los conjuntos $\{a, b\}$ y $\{b, a\}$ son idénticos. Esto porque, ambos contienen los mismos elementos. Quisiéramos introducir un objeto que distinga el orden de los elementos.

La solución no es difícil y viene dada en la siguiente definición.

Definición 3.21 (Par ordenado) *Dados dos elementos a y b en conjuntos de referencia E y F, respectivamente, se define el par ordenado o 2-tupla de a y b como el conjunto $\{\{a\}, \{a, b\}\}$ que se anota (a, b).*

Los elementos a y b se llaman, respectivamente, la primera y la segunda coordenada del par ordenado.

La propiedad fundamental de los pares ordenados es la siguiente.

Proposición 3.22 *Para todo $a, a' \in E$ y $b, b' \in F$ se tiene:*

$$(a, b) = (a', b') \iff a = a' \wedge b = b'.$$

Dem. Haremos la demostración por equivalencia dividida.

$\Leftarrow$) Por hipótesis, $a = a'$ y $b = b'$. Luego, por definición de par ordenado,

$$(a, b) = \{\{a\}, \{a, b\}\} = \{\{a'\}, \{a', b'\}\} = (a', b').$$

$\Rightarrow$) Dividimos el análisis en dos casos:

- Caso $a = b$: En este caso, $(a, b) = \{\{a\}, \{a, b\}\} = \{\{a\}\}$. Por definición de par ordenado e hipótesis,
$$\{\{a'\}, \{a', b'\}\} = (a', b') = (a, b) = \{\{a\}\}.$$
Luego, por definición de igualdad de conjuntos, $\{a'\} = \{a', b'\} = \{a\}$. Sigue que $a = a' = b'$. Como $a = b$, se concluye que $a = a'$ y $b = b'$.

- Caso $a \neq b$: Por hipótesis y definición de par ordenado, $\{\{a\},\{a,b\}\} = \{\{a'\},\{a',b'\}\}$. En este caso, $\{a'\} \neq \{a,b\}$, porque a y b no pueden ser simultáneamente iguales a a'. Por lo tanto, se debe tener que $\{a'\} = \{a\}$ y $\{a',b'\} = \{a,b\}$. Por definición de igualdad de conjuntos, sigue que $a = a'$ y $b = b'$, como queríamos establecer.

□

La noción de 2-tupla se puede generalizar para poder especificar un orden entre los elementos de un conjunto de más de 2 elementos dando lugar a la noción de n-tupla en que $(a_1, a_2, ..., a_n)$ denota una colección ordenada de tamaño n de forma que el i-ésimo elemento, llamado i-ésima coordenada, es a_i. Hay varias formas de definir una n-tupla, pero no discutiremos ninguna de ellas, salvo para decir que de todas ellas se deduce la propiedad fundamental de una tupla, a saber que dos n-tuplas son iguales si y sólo si son iguales coordenada a coordenada. Formalmente,

$$(a_1, a_2, \ldots, a_n) = (a'_1, a'_2, \ldots, a'_n) \iff \forall i \in \{1, \ldots, n\}, a_i = a'_i.$$

Definición 3.23 (Producto cartesiano) *Se define el producto cartesiano de $A \subseteq E$ con $B \subseteq F$, denotado $A \times B$, como el conjunto de pares ordenados (a, b) tales que $a \in A$ y $b \in B$. Formalmente,*

$$\forall a \in E, \forall b \in F, (a, b) \in A \times B \iff a \in A \ \wedge \ b \in B.$$

En general, se define el producto cartesiano de los conjuntos $A_1, \ldots, A_n$, $A_i \subseteq E_i$ para todo $i \in \{1, \ldots, n\}$, denotado $A_1 \times \ldots \times A_n$, por

$$\forall a_1 \in E_1, \ldots, \forall a_n \in E_n, (a_1, \ldots, a_n) \in A_1 \times \ldots \times A_n \iff \forall i \in \{1, \ldots, n\}, a_i \in A_i.$$

Ejemplo: El plano cartesiano es, formalmente, el conjunto $\mathbb{R} \times \mathbb{R}$.

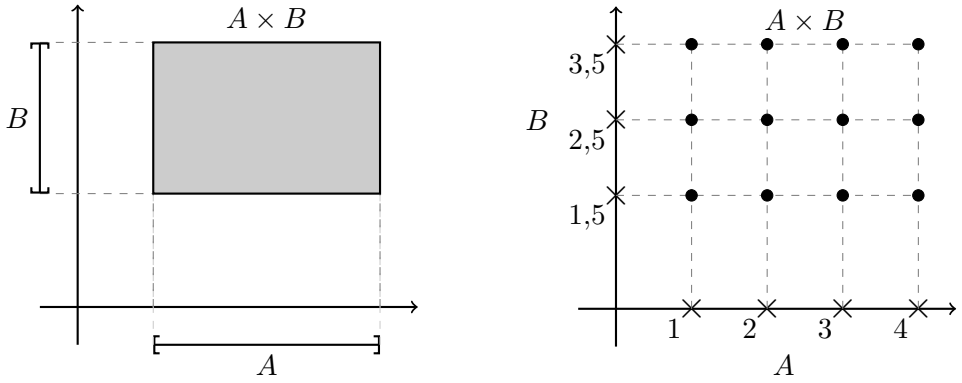
Si $A = \{1, 2, 3\}, B = \{a, b\}, E = \{1, 2, 3, 4\}$ y $F = \{a, b, c\}$ entonces

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

En particular, $A \times B \neq B \times A$. Es decir, $\times$ no conmuta. ♢

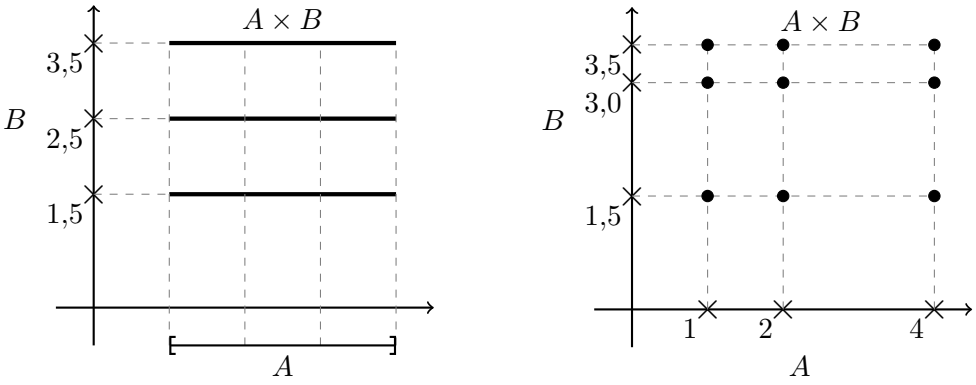
A menudo resulta conveniente representar/visualizar conceptos matemáticos pues esto ayuda a asimilarlos y manipularlos. En particular, hay una representación muy útil del producto cartesiano que está motivada por instancias en que A y B son subconjuntos de $\mathbb{R}$, y por lo tanto $A \times B$ corresponde a una región del plano cartesiano. En la Figura 9 se muestran dos ejemplos. Estos ejemplos motivan a pensar en el producto cartesiano $A \times B$ como un rectángulo de lados paralelos a los ejes cartesianos. Esto es una abstracción, pues es discutible que los ejemplos de la Figura 10 parezcan rectángulos. No obstante, en seguida tendremos la oportunidad de comprobar la utilidad de esta representación.

A continuación, establecemos algunas de las propiedades del producto cartesiano.



(a) $A = [1, 4]$ y $B = [\frac{3}{2}, \frac{7}{2}]$ (b) $A = \{1, 2, 3, 4\}$ y $B = \{\frac{3}{2}, \frac{5}{2}, \frac{7}{2}\}$

Figura 9: Representaciones de $A \times B$ para distintos $A, B \subseteq \mathbb{R}$. Los elementos de $A \times B$ se representan por áreas sombreadas (izquierda) o puntos (derecha).



(a) $A = [1, 4]$ y $B = \{\frac{3}{2}, \frac{5}{2}, \frac{7}{2}\}$ (b) $A = \{1, 2, 4\}$ y $B = \{\frac{3}{2}, 3, \frac{7}{2}\}$

Figura 10: Ejemplos adicionales de representaciones de $A \times B$. Los elementos de $A \times B$ se representan por segmentos de recta (izquierda) o puntos (derecha).

Proposición 3.24 *Si $A, A' \subseteq E$ y $B, B' \subseteq F$[6], entonces*

(I) $A \times \emptyset = \emptyset \times B = \emptyset$.
(II) $A \subseteq A' \ \wedge \ B \subseteq B' \implies A \times B \subseteq A' \times B'$.
(III) $(A \times B) \cap (A' \times B') = (A \cap A') \times (B \cap B')$.
(IV) $(A \times B) \cup (A' \times B') \subseteq (A \cup A') \times (B \cup B')$.

Antes de proceder con la demostración de la proposición, intentaremos visualizar las propiedades y desarrollar intuición de la razón por la que deben cumplirse. Para la parte (I) visualizamos $A \times \emptyset$ como un "rectángulo" tal que uno sus lados es A y el otro es $\emptyset$. Es decir, un "rectángulo" tal que uno de sus lados no contiene elementos. De aquí parece razonable pensar que el "rectángulo" $A \times \emptyset$ no debiese contener elementos. Para la parte (II) consideramos la Figura 11a que ilustra la situación. Dado que los lados de los "rectángulos" $A \times B$ y $A' \times B'$ están incluidos los primeros en los segundos, se percibe que el primer "rectángulo" debiese estar incluido en el segundo. Para la parte (III) consideremos la Figura 11b, donde resalta que la intersección de dos "rectángulos" de lados paralelos a los ejes es otro "rectángulo" de lados paralelos a los ejes cuyos lados son la intersección de los correspondientes lados de los "rectángulos". La Figura 11b también nos permite visualizar la propiedad de la parte (IV). Su interpretación queda propuesta como ejercicio.

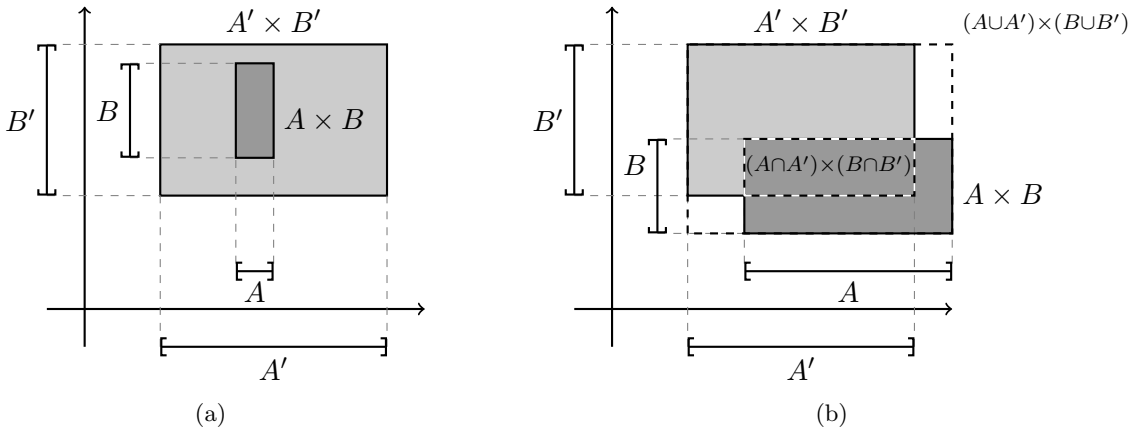


Figura 11

Dem. (de la Proposción 3.24): Demostraremos las partes (II) y (III).

Veamos que se cumple (II). Por hipótesis tenemos que $A \subseteq A'$ y $B \subseteq B'$. Debemos probar que $A \times B \subseteq A' \times B'$. Notar que si $a \in E$ y $b \in F$ son arbitrarios, entonces

$$\begin{aligned} (a,b) \in A \times B &\iff a \in A \wedge b \in B && \text{(definición de } \times) \\ &\implies a \in A' \wedge b \in B' && \text{(hipótesis y definición de } \subseteq) \\ &\iff (a,b) \in A' \times B'. && \text{(definición de } \times) \end{aligned}$$

[6]Aquí $X, X' \subseteq E$ es una manera resumida de decir $X \subseteq E \wedge X' \subseteq E$

Como a y b son arbitrarios, de la transitividad de $\Rightarrow$ y de la definición de $\times$ sigue que $A \times B \subseteq A' \times B'$.

Veamos que se cumple (III). Sea $(a, b) \in E \times F$ arbitrario. Notar que

$$\begin{aligned}
&(a,b) \in (A \times B) \cap (A' \times B') \\
&\quad \iff (a,b) \in (A \times B) \wedge (a,b) \in (A' \times B') && \text{(definición de } \cap) \\
&\quad \iff a \in A \wedge b \in B \wedge a \in A' \wedge b \in B' && \text{(definición de } \times \text{ y asociatividad del } \wedge) \\
&\quad \iff a \in A \cap A' \wedge b \in B \cap B' && \text{(conmutatividad de } \wedge \text{ y definición de } \cap) \\
&\quad \iff (a,b) \in (A \cap A') \times (B \cap B'). && \text{(definición de } \times)
\end{aligned}$$

Como (a, b) es arbitrario, de la transitividad de $\iff$ y de la definición de $\times$ sigue que se tiene la igualdad del enunciado. □

Queda como ejercicio probar las siguientes propiedades:

Proposición 3.25 *Sean $A, A' \subseteq E$ y $B, B' \subseteq F$.*

(I) $(A \cup A') \times B = (A \times B) \cup (A' \times B)$ *y* $A \times (B \cup B') = (A \times B) \cup (A \times B')$.

(II) $(A \cap A') \times B = (A \times B) \cap (A' \times B)$ *y* $A \times (B \cap B') = (A \times B) \cap (A \times B')$.

Concluimos esta sección adoptando un par de convenciones.

Notación:

- El conjunto $\underbrace{A \times A \times \ldots \times A}_{n \text{ veces}}$ se suele notar A^n.
- Por analogía con el caso de uniones e intersecciones sobre conjuntos de índices, el conjunto $A_1 \times A_2 \times \ldots \times A_n$ se notará también por $\times_{i=1}^{n} A_i$.

3.6 Conjunto potencia y partición de conjuntos

A continuación describiremos una importante forma de construir conjuntos a partir de conjuntos existentes. Como ya es costumbre, asumiremos que hay un conjunto de referencia E en el que nos encontramos trabajando.

Definición 3.26 (Conjunto potencia) *Llamamos conjunto potencia de A (o partes de A), denotado $\mathcal{P}(A)$, al conjunto de todos los subconjuntos de A. Entonces $\mathcal{P}(A)$ queda determinado por:*

$$C \in \mathcal{P}(A) \iff (\forall x \in E, x \in C \Rightarrow x \in A)$$

o equivalentemente,

$$C \in \mathcal{P}(A) \iff C \subseteq A.$$

Note que siempre $\emptyset \in \mathcal{P}(A)$ y $A \in \mathcal{P}(A)$. En particular, $\mathcal{P}(A)$ nunca es vacío.

Ejemplo:

- Si $A = \{1, 2, 3\}$, entonces $\mathcal{P}(A) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}\{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$.
- Suponga ahora que $A = \emptyset$. ¿Cuáles son los subconjuntos de $\emptyset$? Solamente el mismo $\emptyset$. Luego $\mathcal{P}(\emptyset) = \{\emptyset\}$. Note que $\emptyset \neq \{\emptyset\}$ pues el primer conjunto no tiene ningún elemento mientras que el segundo tiene un elemento. En efecto: $\emptyset \in \{\emptyset\}$.

  Calculemos ahora $\mathcal{P}(\mathcal{P}(\emptyset)) = \mathcal{P}(\{\emptyset\})$.

  Obviamente, un conjunto de un solo elemento tiene solamente como subconjuntos los triviales: al vacío y a él mismo. O sea $\mathcal{P}(\{\emptyset\}) = \{\emptyset, \{\emptyset\}\}$. El lector debe ser capaz ahora de calcular $\mathcal{P}(\mathcal{P}(\mathcal{P}(\emptyset)))$. Note que este proceso puede no detenerse nunca. ¡Y lo que estamos generando es una infinidad de conjuntos!

$\diamondsuit$

Proposición 3.27

(I) $\mathcal{P}(A) \cup \mathcal{P}(B) \subseteq \mathcal{P}(A \cup B)$.

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

Dem.

(I) Sea $X \subseteq E$ arbitrario. Notar que

$$\begin{aligned} X \in \mathcal{P}(A) \cup \mathcal{P}(B) &\iff X \in \mathcal{P}(A) \vee X \in \mathcal{P}(B) && \text{(definición de } \cup) \\ &\iff X \subseteq A \vee X \subseteq B && \text{(definición conjunto potencia)} \\ &\implies X \subseteq A \cup B && \text{(porque } A, B \subseteq A \cup B) \\ &\implies X \in \mathcal{P}(A \cup B). && \text{(definición conjunto potencia)} \end{aligned}$$

Como X es arbitrario, de la transitividad de $\Rightarrow$ y de la definición de inclusión de conjuntos se concluye que $\mathcal{P}(A) \cup \mathcal{P}(B) \subseteq \mathcal{P}(A \cup B)$.

(II) Sea $X \subseteq E$ arbitrario. Notar que

$$\begin{aligned} X \in \mathcal{P}(A) \cap \mathcal{P}(B) &\iff X \in \mathcal{P}(A) \wedge X \in \mathcal{P}(B) && \text{(definición de } \cap) \\ &\iff X \subseteq A \wedge X \subseteq B && \text{(definición de conjunto potencia)} \\ &\iff X \subseteq A \cap B && \text{(Corolario 3.11 parte (I) y (II))} \\ &\iff X \in \mathcal{P}(A \cap B). && \text{(definición de conjunto potencia)} \end{aligned}$$

Como X es arbitrario, de la transitividad de $\iff$ y de la definición de igualdad de conjuntos se concluye que $\mathcal{P}(A) \cap \mathcal{P}(B) = \mathcal{P}(A \cap B)$.

□

Es natural preguntarse si no se tiene la igualdad en la primera propiedad de la proposición anterior. La forma de mostrar que no es el caso es exhibir un contraejemplo. Preferentemente, el contraejemplo más "simple" o más "pequeño" posible. En este caso, corresponde a tomar $A = \{a\}$ y $B = \{b\}$ y observar que $\mathcal{P}(A) = \{\emptyset, A\}$ y $\mathcal{P}(B) = \{\emptyset, B\}$. Como $\mathcal{P}(A \cup B) = \{\emptyset, A, B, A \cup B\}$ y $A \cup B \notin \mathcal{P}(A) \cup \mathcal{P}(B)$, se tiene que $\mathcal{P}(A) \cup \mathcal{P}(B) \neq \mathcal{P}(A \cup B)$.

Es importante resaltar que un subconjunto $\mathcal{C}$ de $\mathcal{P}(A)$ tiene como elementos a subconjuntos de A. Formalmente, si $X \in \mathcal{C}$, entonces $X \subseteq A$. Algunos subconjuntos de $\mathcal{P}(A)$, llamados particiones de A, son particularmente interesantes por, como veremos en un par de semanas, estar en correspondencia con clasificaciones de los elementos de A. Formalmente,

Definición 3.28 (Partición de conjuntos) *Se dice que $\mathcal{C} \subseteq \mathcal{P}(A)$ es **partición** de A si las siguientes tres condiciones se cumplen:*

- $\forall C \in \mathcal{C}$, $C \neq \emptyset$.
- *Los elementos de $\mathcal{C}$ son disjuntos de a pares, es decir, $\forall C, C' \in \mathcal{C}$, si $C \neq C'$, entonces $C \cap C' = \emptyset$.*
- *$\mathcal{C}$ **cubre** A, es decir, $\bigcup_{C \in \mathcal{C}} C = A$.*

*Los elementos de $\mathcal{C}$ se denominan **partes**.*

Ejemplo:

- Sean $\mathbb{P}\mathtt{ar}$ e $\mathbb{I}\mathtt{mp}$ los conjuntos de enteros pares e impares, respectivamente. Notar que $\{\mathbb{P}\mathtt{ar}, \mathbb{I}\mathtt{mp}\}$ es una partición de $\mathbb{Z}$.
- El conjunto $A = \{x, y, z\}$ tiene 5 particiones distintas, a saber,

$$\big\{\{x\},\{y\},\{z\}\big\}, \quad \big\{\{x,y\},\{z\}\big\}, \quad \big\{\{x,z\},\{y\}\big\}, \quad \big\{\{x\},\{y,z\}\big\}, \quad \big\{\{x,y,z\}\big\}.$$

  En la Figura 12 se representan gráficamente cada una de estas particiones.

  Por otro lado, no son particiones de A ni $\big\{\{x\},\{x,y,z\}\big\}$ (porque sus elementos no son disjuntos de a pares), ni $\big\{\{x\},\{y\}\big\}$ (porque no cubre A).

♢

3.7 Cuantificando sobre conjuntos

Dado un conjunto $A \subseteq E$ y una función proposicional $P(x)$ con conjunto de referencia E, podemos escribir cuantificadores en los que sólo nos interese ver lo que ocurre con los elementos de A. Esto da lugar a las siguientes convenciones:

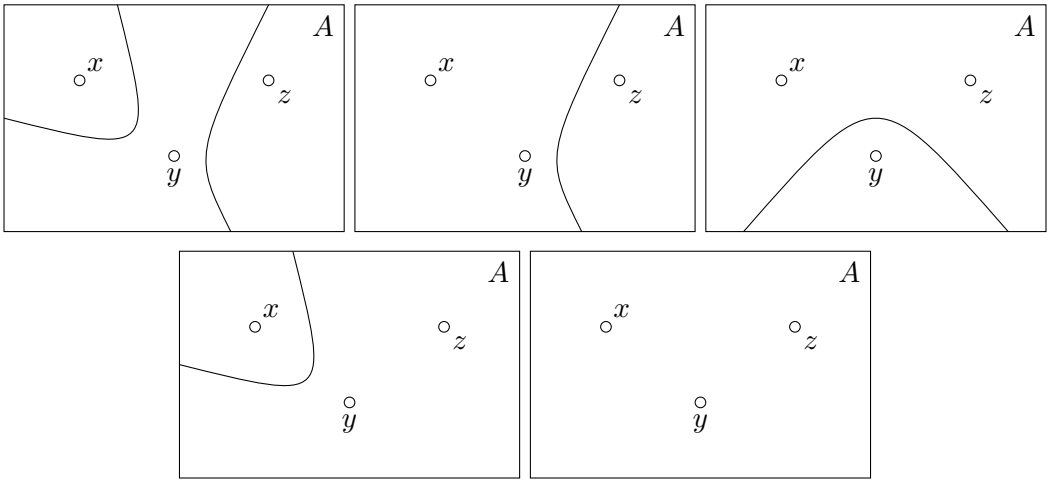


Figura 12: Ilustración de cada una de las 5 particiones de $A = \{x, y, z\}$ (el conjunto A se representa como un rectángulo y sus elementos como círculos).

(I) Para decir que $P(x)$ se cumple para todos los elementos de A, escribimos $\forall x \in A, P(x)$. Formalmente,

$$(\forall x \in A, P(x)) \iff (\forall x \in E, x \in A \implies P(x)).$$

Notar en particular que $x \in \emptyset \implies P(x)$ es siempre verdadera (porque $x \in \emptyset$ es falsa y por definición de $\Rightarrow$). Luego, si $A = \emptyset$, tenemos que $\forall x \in A, P(x)$ resulta ser verdadera independiente de cual sea la función proposicional $P(x)$.

(II) Para decir que $P(x)$ se cumple para algún elemento en A, escribimos $\exists x \in A, P(x)$. Formalmente,

$$(\exists x \in A, P(x)) \iff (\exists x \in E, x \in A \wedge P(x)).$$

Ahora, $x \in \emptyset \wedge P(x)$ es siempre falsa (porque $x \in \emptyset$ es falsa y por definición de $\wedge$). Luego, si $A = \emptyset$, tenemos que $\exists x \in A, P(x)$ resulta ser falsa independiente de cual sea la función proposicional $P(x)$.

(III) Para decir que $P(x)$ se cumple para un único elemento en A, escribimos $\exists! x \in A, P(x)$. Formalmente,

$$(\exists! x \in A, P(x)) \iff (\exists! x \in E, x \in A \wedge P(x)).$$

El lector puede fácilmente verificar que se tienen las siguientes propiedades:

Proposición 3.29

- $\overline{(\forall x \in A, P(x))} \iff \exists x \in A, \overline{P(x)}$.
- $\overline{(\exists x \in A, P(x))} \iff \forall x \in A, \overline{P(x)}$.
- $\overline{(\exists! x \in A, P(x))} \iff (\forall x \in A, \overline{P(x)}) \vee (\exists x, x' \in A, P(x) \wedge P(x') \wedge x \neq x')$.
- $\forall x \in A \cup B, P(x) \iff (\forall x \in A, P(x)) \wedge (\forall x \in B, P(x))$.
- $\exists x \in A \cup B, P(x)) \iff (\exists x \in A, P(x)) \vee (\exists x \in B, P(x))$.

SEMANA 04:

Funciones

Ingeniería Matemática
FACULTAD DE CIENCIAS
FÍSICAS Y MATEMÁTICAS
UNIVERSIDAD DE CHILE

Vamos a comenzar a discutir el concepto de función, que es probablemente la noción matemática más importante. El aspecto central del concepto es el de correspondencia entre los elementos de un conjunto y los de otro conjunto. La noción de función es imprescindible y básica. Es además una parte fundamental del lenguaje usado para la formulación y el estudio de modelos matemáticos.

4.1 Introducción

Ya que conocemos el producto cartesiano $A \times B$ entre dos conjuntos A y B, podemos definir entre ellos algún tipo de correspondencia. Es decir, asociar de algún modo elementos de A con elementos de B. Una de las posibles formas de hacer esto es mediante una **función**. Formalmente:

Definición 4.1 (Función) *Diremos que la 3-tupla $f = (A, B, G)$ es función de A en B si*

- $G \subseteq A \times B$.
- $\forall a \in A, \exists! b \in B, (a, b) \in G$.

A G se le llama el grafo de la función f.

Podemos entender una función como una regla de asociación que, dado un elemento cualquiera de A, le asigna un único elemento de B. Por unicidad, si $f = (A, B, G)$ es función y $(a, b) \in G$, entonces podemos usar sin ambigüedad la notación $b = f(a)$. O sea, llamamos $f(a)$ al (único) elemento $b \in B$ tal que $(a, b) \in G$.

Ejemplo: Si $G = \{(n, p) \in \mathbb{N} \times \mathbb{N} \mid p = 2n\}$, entonces $f = (\mathbb{N}, \mathbb{N}, G)$ resulta ser una función de $\mathbb{N}$ en $\mathbb{N}$, pues a cada natural n estamos asociando un único natural $p = 2n$. $\diamondsuit$

En vez de referirnos a una función f como una tupla (A, B, G), usaremos la notación $f : A \to B$, y daremos la segunda coordenada del par en G cuya primera coordenada es a con una expresión para $f(a)$. Así, la función definida en el ejemplo anterior queda descrita como

> "$f : \mathbb{N} \to \mathbb{N}$ es la función dada por $f(n) = 2n$, para cada $n \in \mathbb{N}$."

Ejemplo:

- Sea $f : \mathbb{R} \to \mathbb{R}$ dada por $f(x) = x^2$, para cada $x \in \mathbb{R}$.

  Sigue que f es función, pues a cada $x \in \mathbb{R}$ le asociamos el número real $x^2 = x \cdot x$. Este valor es único pues la multiplicación de x por sí mismo posee un solo resultado.
- Sea $g : \mathbb{R} \to \mathbb{R}$ dada por $g(x) = p$, donde p es el mayor número entero tal que $p \leq x$.

  Aunque aún no tenemos las herramientas para demostrar que g es efectivamente una función, podemos intuir que sí lo es: a cada número real x le asociamos el número entero más cercano que sea menor o igual a él. Por ejemplo $g(11/2) = 5$; $g(3) = 3$ y $g(-3/2) = -2$.
- Un ejemplo importante, que utilizaremos después, es la llamada función **identidad** de un conjunto A. Ésta es la función $\mathrm{id}_A : A \to A$, que se define por $\mathrm{id}_A(x) = x$, para cada $x \in A$.
- Cuando tenemos conjuntos A y B que tienen pocos elementos, podemos definir una función $f : A \to B$ mediante un diagrama de flechas, como en el ejemplo de la Figura 13. Aquí, lo importante para que f sea efectivamente una función, es que desde cada elemento de A debe partir una única flecha hacia algún elemento de B.

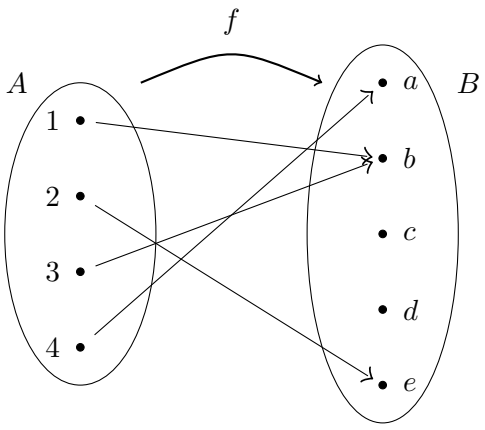


Figura 13: Una función definida mediante diagrama de flechas.

- En una tienda, cada producto tiene asociado un único precio. Así, podemos definir la función $v : X \to \mathbb{N}$, donde denotamos por X el conjunto de productos que la tienda dispone, y $v(x)$ es el precio en pesos del producto x.

  También podemos considerar la función $s : X \to \mathbb{N}$, donde $s(x)$ es la cantidad de unidades disponibles (el stock) del producto x.

$\diamondsuit$

A pesar de que conocemos la definición de función, hay que tener un mínimo de cuidado. Hay objetos que parecen funciones, pero no lo son. Veamos el siguiente ejemplo:

Ejemplo: Considere el conjunto de puntos $G = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x^2 + y^2 = 1\}$ (ver Figura 14). Hay dos razones que impiden que $f = (\mathbb{R}, \mathbb{R}, G)$ constituya una función de $\mathbb{R}$ en $\mathbb{R}$:

- El valor $f(x)$ no está definido para todos los números reales x, es decir, para algunos $x \in \mathbb{R}$ no existe un $y \in \mathbb{R}$ tal que $(x, y) \in G$. A modo de ejemplo, $f(2)$ debiera ser el número real y que cumple que $2^2 + y^2 = 1$. Pero, esto equivale a decir que $y^2 = -3$, lo cual es falso para cualquier $y \in \mathbb{R}$. Por lo tanto, f no está asociando a $x = 2$ ningún número real.

  De la misma forma, se puede demostrar que $f(x)$ no está definido para cualquier $x \in \mathbb{R}$ que cumpla $x < -1$ o $x > 1$.

- Lo más grave, sin embargo, es que existen números reales x a los cuales f les está asociando más de un valor y, es decir, para algunos valores de $x \in \mathbb{R}$ existen $y_1, y_2 \in \mathbb{R}$ tales que $y_1 \neq y_2$ y $(x, y_1), (x, y_2) \in G$. En efecto, basta notar que para $x = \frac{3}{5}$, hay dos valores de $y \in \mathbb{R}$ que cumplen $x^2 + y^2 = 1$: éstos son $y_1 = \frac{4}{5}$ e $y_2 = -\frac{4}{5}$.

  De la misma forma, se demuestra que f está asociando dos valores distintos a todos los reales x que cumplen $-1 < x < 1$.

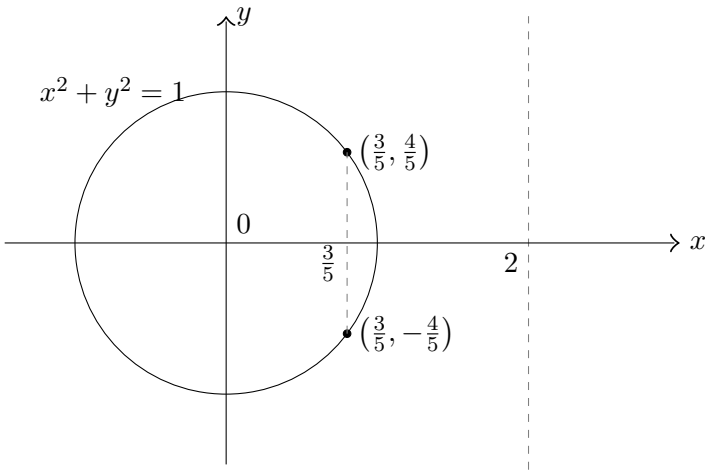


Figura 14: Este diagrama no define una función.

♢

Sea $f : A \to B$ una función. Al conjunto A le llamaremos **dominio** de f, o **conjunto de partida** de f, y lo denotaremos $\mathrm{Dom}(f)$. De igual modo, al conjunto B le llamaremos **codominio** o **conjunto de llegada** de f, y lo denotaremos $\mathrm{Cod}(f)$. Al grafo de la función f, es decir, al conjunto $\{(a, f(a)) \in A \times B : a \in A\}$, lo denotamos por G_f.

Es importante notar que para definir una función es necesario indicar todos sus elementos: dominio, codominio y grafo. Como hemos dicho, este último se suele dar indirectamente mediante la expresión $f(x)$.

Dos funciones $f : A \to B$ y $g : C \to D$ se dirán iguales si vistas como las 3-tuplas (A, B, G_f) y (C, D, G_g) son iguales. Formalmente:

Definición 4.2 (Igualdad de funciones) *Si $f : A \to B$ y $g : C \to D$ son funciones, entonces*

$$f = g \iff \begin{array}{c} \mathrm{Dom}(f) = \mathrm{Dom}(g) \wedge \mathrm{Cod}(f) = \mathrm{Cod}(g) \wedge \\ \forall x \in \mathrm{Dom}(f), f(x) = g(x) \end{array}$$

Ejemplo (Igualdad de funciones): Consideremos las expresiones f y g dadas por

$$f(x) = \frac{(x-1)(x+2)}{(x-1)} \qquad \text{y} \qquad g(x) = (x+2).$$

Aunque a primera vista ambas expresiones nos parecen iguales, por lo que podrían definir funciones iguales, esto no siempre es así, pues los dominios y codominios asociados a estas funciones también deben coincidir.

La expresión g está bien definida para cualquier elemento de $\mathbb{R}$, por lo que podemos considerar $\mathrm{Dom}(g) = \mathbb{R}$. También estaría bien considerar cualquier otro subconjunto de $\mathbb{R}$ (como haremos en lo que sigue).

Para f, sin embargo, observamos que el valor $f(x)$ no está bien definido para $x = 1$. En efecto, no se puede dividir por cero. En ese caso, vemos que $\mathbb{R}$ no puede ser el dominio asociado a f. Sí podría serlo el conjunto $\mathbb{R} \setminus \{1\}$ o cualquiera de sus subconjuntos.

Pero como $\mathbb{R} \neq \mathbb{R} \setminus \{1\}$, sin importar el codominio que definamos para las funciones, éstas serán distintas, pues sus dominios ya lo son.

Es claro que al definir el dominio de g como $\mathbb{R} \setminus \{1\}$ se remedia el problema. Es decir, nos olvidamos que g también puede ser evaluada en $x = 1$.

También es claro que podemos elegir $\mathrm{Cod}(f) = \mathrm{Cod}(g) = \mathbb{R}$. (como ejercicio para el lector, puede mostrar que también se puede considerar $\mathrm{Cod}(f) = \mathrm{Cod}(g) = \mathbb{R} \setminus \{3\}$).

En tal caso, $\mathrm{Dom}(f) = \mathbb{R} \setminus \{1\} = \mathrm{Dom}(g)$, y además $\mathrm{Cod}(f) = \mathbb{R} = \mathrm{Cod}(g)$.

Así, sólo falta ver que las evaluaciones de f y g coinciden. Sea $x \in \mathbb{R} \setminus \{1\}$:

$$f(x) = \frac{(x-1)(x+2)}{(x-1)} = (x+2) = g(x).$$

Esta vez sí podemos realizar la simplificación del factor $(x-1)$ porque estamos suponiendo que $x \neq 1$. Así, las funciones $f : \mathbb{R} \setminus \{1\} \to \mathbb{R}$ y $g : \mathbb{R} \setminus \{1\} \to \mathbb{R}$ son iguales. $\diamondsuit$

Definición 4.3 (Conjunto de funciones) *Sean A y B conjuntos, definimos el conjunto de todas las funciones de A en B por*

$$B^A = \{f : A \to B \mid f \text{ función}\}.$$

Guía Básica

Determinar la veracidad de las siguientes afirmaciones:

1. Dado un conjunto A, siempre es cierto que $A \in \mathcal{P}(A)$.
2. Dados A, B conjuntos, se tiene $\mathcal{P}(A \cap B) \subseteq \mathcal{P}(A) \cap \mathcal{P}(B)$.
3. Se tiene que $\mathcal{P}(\emptyset) = \mathcal{P}(\{\emptyset\})$.
4. Se tiene que $\mathcal{P}(\emptyset) = \{\emptyset\}$.
5. Si $A' \subseteq A$ y $B' \subseteq B$, entonces $A' \times A \subseteq B' \times B$.
6. Si $A' \subseteq A$ y $B' \subseteq B$, entonces $A' \times B' \subseteq A \times B$.
7. Si A y B son conjuntos tales que $A \times B = B \times A$, entonces necesariamente $A = B$.
8. $f \subseteq A \times B$ es función si la proposición $\forall a \in A, \exists b \in B, (a, b) \in f$ es verdadera.
9. $f \subseteq A \times B$ es función si la proposición $\forall a \in A, \exists! b \in B, (a, b) \in f$ es verdadera.
10. $f \subseteq A \times B$ es función si la proposición $\forall a \in A, \forall b \in B, (a, b) \in f$ es verdadera.
11. Según la notación de función, se tiene que para $a \in A$ $(a, f(a)) \in f$.
12. Según la notación de función, $b = f(a)$ equivale a $(f(a), b) \in f$.
13. Según la notación de función $b = f(a)$ equivale a $(f(a), f(b)) \in f$.
14. El conjunto $A = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x^2 + y^2 = 1\}$ es el grafo de una función de $\mathbb{R}$ en $\mathbb{R}$.
15. El conjunto $A = \{(x, y) \in [0, 1) \times (0, \infty) \mid x^2 + y^2 = 1\}$ es el grafo de una función de $[0, 1)$ en $\mathbb{R}$.
16. El conjunto $A = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid y \in \{-1, 1\}\}$ es el grafo de una función de $\mathbb{R}$ en $\mathbb{R}$
17. El conjunto $A = \{(x, y) \in \mathbb{R} \times \mathbb{N} \mid y \in \{-1, 1\}\}$ es el grafo de una función de $\mathbb{R}$ en $\mathbb{N}$
18. Para que dos funciones f y g sean iguales basta que $\forall a \in E, f(a) = g(a)$.
19. Para que dos funciones $f, g : A \to B$ sean iguales basta que $\forall a \in A, f(a) = g(a)$.
20. Para que dos funciones $f : A \to B$ y $g : C \to D$ sean iguales basta que $\forall a \in A \cap C, f(a) = g(a)$.
21. Para que dos funciones $f : A \to B$ y $g : C \to D$ sean iguales se debe cumplir que $\text{Dom}(f) = \text{Dom}(g)$ y que $\forall a \in A, f(a) = g(a)$.
22. Para que dos funciones $f : A \to B$ y $g : C \to D$ sean iguales se debe cumplir que $\text{Dom}(f) = \text{Dom}(g)$, que $\text{Cod}(f) = \text{Cod}(g)$ y que $\forall a \in A, f(a) = g(a)$.

Guía de Ejercicios

1. Sean $A, B, C \subseteq E$ conjuntos. Emplear los teoremas del álgebra de conjuntos para probar las siguientes proposiciones:

   a) $A \subseteq B \iff \mathcal{P}(A) \subseteq \mathcal{P}(B)$.

b) $A \cup B = A \cap C \implies B \subseteq A \wedge A \subseteq C$.
c) $A \cap C = \emptyset \implies (A \setminus B) \setminus C = A \setminus (B \setminus C)$.

2. Dado el conjunto $A = \{a, b\}$, determine los siguentes conjuntos (justifique su respuesta, indicando cómo ésta depende de qué son a y b):

a) $\mathcal{P}(A)$.
b) $\mathcal{P}(\mathcal{P}(A))$.
c) $A \cap \mathcal{P}(A)$.
d) $\mathcal{P}(A) \cap \mathcal{P}(\emptyset)$.
e) $(A \times A) \cap \mathcal{P}(\mathcal{P}(A))$.

3. Sean $A, B \subseteq E$ conjuntos no vacíos. Colocar el signo de inclusión, igualdad o ninguno de ellos, según corresponda entre los conjuntos siguientes (justifique su respuesta). Analice que cambia en los casos $A = \emptyset \neq B$, $A \neq \emptyset = B$ y $A = \emptyset = B$.

a) $A \cap B \ ? \ B$.
b) $A^c \ ? \ B \setminus A$.
c) $\mathcal{P}(A \cup B) \ ? \ \mathcal{P}(A) \cup \mathcal{P}(B)$.
d) $\mathcal{P}(A \cap B) \ ? \ \mathcal{P}(A) \cap \mathcal{P}(B)$.
e) $\mathcal{P}(E \setminus A) \ ? \ \mathcal{P}(E) \setminus \mathcal{P}(A)$.

4. Dar ejemplos de conjuntos A, B, C tales que:

a) $A \times B \neq B \times A$.
b) $A \cup (B \times C) \neq (A \cup B) \times (A \cup C)$.
c) $(A \times B)^c \neq A^c \times B^c$.
d) $(A \neq B) \wedge (A \times C = B \times C)$.

5. Indique cuáles de los siguientes conjuntos son grafos de funciones:

a) $R = \{(a, b) \in \mathbb{N}^2 \mid b = a^p \text{ para algún } p \in N\}$.
b) Sean $a, b, c \in \mathbb{R}\setminus\{0\}$ fijos, $R = \{(x, y) \in \mathbb{R}^2 \mid y = ax^3 + bx + c\}$.
c) $R = \{(x, y) \in \mathbb{R}^2 \mid \ y = ax^3 + bx + c \text{ con } a, b, c \in \mathbb{R}\}$.
d) $R = \{(x, y) \in \mathbb{R}^2 \mid x = y^2 + 2y + 1\}$.
e) $R = \{(y, x) \in \mathbb{R}^2 \mid x = (y + 1)^2\}$.
f) $R = \{(x, y) \in \mathbb{R}^2 \mid x = y^3\}$.

6. Indique cuáles pares de funciones son iguales, si no lo son, explique por qué.

a) $f, g : \mathbb{R} \setminus \{-2\} \to \mathbb{R}$ con $f(x) = (x^2 - 1)/(x^2 + 2x + 2)$ y $g(x) = (x - 1)/(x + 2)$.
b) $f, g : \mathbb{R} \setminus \{-1, 0, 1\} \to \mathbb{R}$ con $f(x) = 1/x, g(x) = (x + 1)(x - 1)/(x^3 - x)$.
c) $f, g : \mathbb{R} \to \mathbb{R}$, con $f(x) = (x + 2)^3$ y $g(x) = x^3 + 6x^2 + 12x + 8$.
d) $f, g : \mathbb{R} \setminus \{-1, 0\} \to \mathbb{R}$ con $f(x) = \text{sen}(x)/(x + 1), g(x) = \text{sen}(x - 1)/x$.
e) $f, g : (0, \infty) \to \mathbb{R}$ con $f(x) = x/\sqrt{x}, g(x) = \sqrt{x}$.

Guía de Problemas

1. (20 min.) Sea E un conjunto no vacío y $A \subseteq E$. Pruebe que si

$$\forall X, Y \in \mathcal{P}(E), A \cup X = A \cup Y \implies X = Y,$$

entonces $A = \emptyset$.

2. (20 min.) Sean A, B subconjuntos de un mismo conjunto de referencia E. Probar que

$$A \cap B = \emptyset \iff \mathcal{P}(A) \cap \mathcal{P}(B) = \{\emptyset\}.$$

3. (40 min.) Sea $\circledast$ la operación entre conjuntos definida por $A \circledast B = A^c \cap B^c$. Considere un conjunto de referencia E y $\mathcal{F} \subseteq \mathcal{P}(E)$ un conjunto no vacío tal que $\forall A, B \in \mathcal{F},\ A \circledast B \in \mathcal{F}$. Si $A, B \in \mathcal{F}$, entonces demuestre que:

   a) $A^c \in \mathcal{F}$
   b) $A \cap B \in \mathcal{F}$
   c) $A \cup B \in \mathcal{F}$
   d) $A \Delta B \in \mathcal{F}$
   e) $\emptyset \in \mathcal{F} \ \wedge \ E \in \mathcal{F}$.

4. Sea $E \neq \emptyset$ un conjunto fijo. Para todo subconjunto A de E se define la función característica de A como:

$$\begin{aligned} \delta_A : E &\longrightarrow \{0,1\} \\ x &\longmapsto \delta_A(x) = \begin{cases} 1, & \text{si } x \in A, \\ 0, & \text{si } x \notin A. \end{cases} \end{aligned}$$

   a) (10 min.) Describa $\delta_E(x)$ y $\delta_\emptyset(x)$ para todo $x \in E$
   b) (10 min.) Demuestre que $\forall x \in E, \delta_{A \cap B}(x) = \delta_A(x)\delta_B(x)$
   c) (10 min.) Si $C, D \subseteq E$, entonces $C \subseteq D \iff \forall x \in E, \delta_C(x) \leq \delta_D(x)$

5. Sea $f : A \to B$ una función. Demuestre que el conjunto $\Omega = \{\{x \in A | f(x) = y\} | y \in B\}$ cubre el conjunto A y que sus elementos son disjuntos de a pares. ¿ Es Ω una partición de A?

4.2 Funciones inyectivas, epiyectivas, y biyectivas

Consideremos el siguiente problema: Dada una función $f : A \to B$, y un elemento $y \in B$, se quiere encontrar un $x \in A$ tal que $y = f(x)$. Por ejemplo consideremos la función $q : \mathbb{R} \to \mathbb{R}$, $q(x) = x^2$. Notemos que:

- Si $y < 0$, entonces no existe $x \in \mathbb{R}$ tal que $y = x^2$.
- Si $y = 0$, entonces hay una única solución: $x = 0$.
- Si $y > 0$, entonces hay dos soluciones: $x_1 = \sqrt{y}$ y $x_2 = -\sqrt{y}$.

Este ejemplo nos basta para darnos cuenta de que no siempre el problema que nos planteamos tiene solución, y que en caso de tenerla, puede tener más de una.

En lo que sigue identificaremos propiedades de la función que nos ayudarán a saber cuándo este problema, para una función $f : A \to B$ dada, posee soluciones para cualquier $y \in B$, y si estas soluciones son únicas.

Inyectividad

Definición 4.4 (Inyectividad) *Diremos que una función $f : A \to B$ es **inyectiva** si se cumple que*

$$\forall x_1, x_2 \in A, x_1 \neq x_2 \implies f(x_1) \neq f(x_2).$$

O, equivalentemente, si se cumple que

$$\forall x_1, x_2 \in A, f(x_1) = f(x_2) \implies x_1 = x_2.$$

Notar que para establecer que una función **no** es inyectiva bastará entonces exhibir dos elementos **distintos** x_1 y x_2, ambos elementos de A, tales que $f(x_1) = f(x_2)$.

Ejemplo:

- La función $l : \mathbb{R} \to \mathbb{R}$ dada por $l(x) = ax + b$ con $a \neq 0$ es inyectiva. En efecto, para $x_1, x_2 \in \mathbb{R}$ arbitrarios.

$$\begin{aligned} l(x_1) = l(x_2) &\iff ax_1 + b = ax_2 + b && \text{(por definición de } l\text{)} \\ &\iff ax_1 = ax_2 && \text{(restando } b \text{ a ambos lados de la igualdad)} \\ &\iff x_1 = x_2 && \text{(dividiendo por } a \neq 0 \text{ a ambos lados de la igualdad)} \end{aligned}$$

  Como x_1 y x_2 eran arbitrarios, concluimos que $\forall x_1, x_2 \in \mathbb{R}, l(x_1) = l(x_2) \implies x_1 = x_2$, por lo que l es inyectiva.

- La función $q : \mathbb{R} \to \mathbb{R}$ tal que $q(x) = x^2$ **no** es inyectiva pues, tomando $x_1 = -1$ y $x_2 = 1$, se tiene que $x_1 \neq x_2$ y $f(x_1) = f(x_2)$.

♢

Epiyectividad

Definición 4.5 (Epiyectividad) *Diremos que $f : A \to B$ es **epiyectiva** si se cumple que*

$$\forall y \in B, \exists x \in A, y = f(x).$$

Observar que para establecer que una función **no** es epiyectiva bastará entonces exhibir un elemento y de su codominio tal que no hay ningún elemento x de su dominio para el cual $f(x) = y$.

Ejemplo:

- La función $q : \mathbb{R} \to \mathbb{R}$ tal que $q(x) = x^2$, **no** es epiyectiva pues para el real $y = -1$ no existe ningún real x tal que $-1 = x^2$.

- Observemos, también, que la función $l : \mathbb{R} \to \mathbb{R}$ que habíamos definido anteriormente es epiyectiva: En efecto, para $y \in \mathbb{R}$ arbitrario, debemos mostrar que es posible encontrar un $x \in \mathbb{R}$ de modo que $y = l(x)$.

  Si elegimos el real $x = \frac{y-b}{a}$ (recordemos que $a \neq 0$), entonces es fácil verificar que $l(x) = y$.

  Como el razonamiento que hicimos es válido para cualquier $y \in \mathbb{R}$, hemos demostrado que l es epiyectiva.

♢

Biyectividad

Definición 4.6 (Biyectividad) *Sea $f : A \to B$ una función. Diremos que f es **biyectiva** si es inyectiva y epiyectiva a la vez.*

Ejemplo: De los ejemplos previos, sigue que q no es biyectiva pero que l sí lo es. Es sencillo verificar que la función identidad $\mathrm{id}_A : A \to A$ también es biyectiva. ♢

Proposición 4.7 *$f : A \to B$ es biyectiva $\iff \forall y \in B, \exists! x \in A, y = f(x)$.*

Dem. (Idea - queda como ejercicio desarrollar el argumento formalmente): Observemos que la epiyectividad de f equivale a la existencia de un $x \in A$ tal que $y = f(x)$ para cualquier $y \in B$. Además, la unicidad del tal x equivale a la inyectividad de f. □

4.3 Función inversa

Dada una función $f : A \to B$, nos gustaría encontrar una función $g : B \to A$ correspondiente al "camino inverso" de f. Es decir $g(y) = x$ cada vez que $f(x) = y$. Es fácil observar que debiéramos al menos pedir que f sea biyectiva para que una tal función g exista. Como vemos en la Figura 15, si f no fuera biyectiva, habría elementos de B a los cuáles no sabríamos asociarle un elemento de A. Recordando que el grafo de f, G_f, es en realidad un

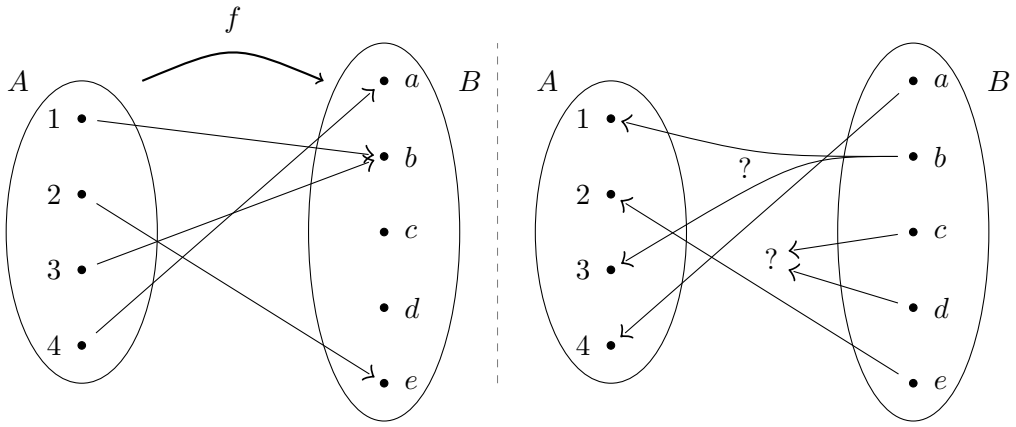


Figura 15: Dificultades para definir la inversa de una función no biyectiva.

subconjunto de $A \times B$, podemos construir un "candidato" a función g usando su grafo G_g.

> Los elementos de $G_g \subseteq B \times A$ serán todos los pares ordenados $(b, a) \in B \times A$ tales que $(a, b) \in G_f$, es decir todos los pares ordenados (b, a) tales que $b = f(a)$.

Ya vimos que esta construcción no siempre hace que g sea función. Sin embargo, tenemos lo siguiente:

Proposición 4.8 *f es biyectiva $\iff$ g es función.*

Dem. En efecto,

$$\begin{aligned} f \text{ es biyectiva} &\iff \forall y \in B, \exists! x \in A, f(x) = y && \text{(por Proposición 4.7)} \\ &\iff \forall y \in B, \exists! x \in A, (y, x) \in G_g && \text{(por definición de } g\text{)} \\ &\iff g \text{ es función.} && \text{(por definición de función)} \end{aligned}$$

La transitividad de $\iff$ nos da la conclusión. □

A la función g que construimos de la manera descrita la llamaremos función inversa. Formalmente:

Definición 4.9 (Función inversa) *Dada $f : A \to B$ biyectiva, se define la función inversa de f, denotada $f^{-1} : B \to A$, como la función de B en A dada por:*

$$\forall x \in A, \forall y \in B, f^{-1}(y) = x \iff y = f(x).$$

Para una función biyectiva $f : A \to B$, y su inversa $f^{-1} : B \to A$, tenemos las siguientes propiedades:

Proposición 4.10 *Si $f : A \to B$ es función biyectiva, entonces su inversa $f^{-1} : B \to A$ es tal que:*

(i) $\forall x \in A, f^{-1}(f(x)) = x.$
(ii) $\forall y \in B, f(f^{-1}(y)) = y.$

Dem. Demostraremos (ii). Consideremos $y \in B$ arbitrario. Luego,

$$\begin{aligned} f(f^{-1}(y)) &= f(x) && \text{(para } x = f^{-1}(y)\text{)} \\ &= y. && \text{(por elección de } x \text{ y definición de función inversa)} \end{aligned}$$

□

4.4 Composición de funciones

Pensemos que tenemos tres conjuntos no vacíos A, B, C, y dos funciones, $f : A \to B$ y $g : B \to C$, como en el diagrama de la figura 16

Es natural asociar a $x \in A$ el elemento $z \in C$ que se obtiene de evaluar f en a, y posteriormente g en $f(a)$. Esto da lugar al siguiente concepto:

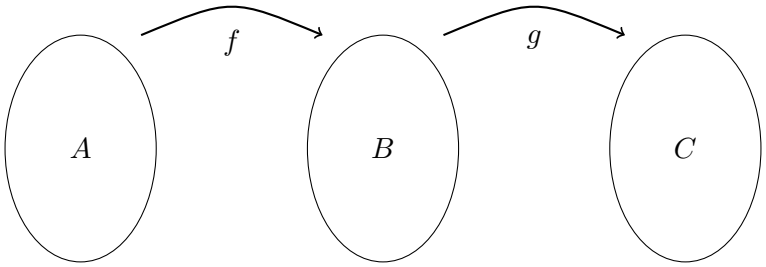


Figura 16: Esquema necesario para poder componer dos funciones f y g.

Definición 4.11 (Función composición) *Sean $f : A \to B$ y $g : B \to C$ funciones, la **composición de f y g**, la cual denotaremos por $g \circ f$, se define como la función de A en C, dada por*

$$\forall x \in A, (g \circ f)(x) = g(f(x)).$$

Notemos que al definir $g \circ f$ hemos impuesto que $\mathrm{Cod}(f) = \mathrm{Dom}(g)$. Esta restricción puede relajarse a $\mathrm{Cod}(f) \subseteq \mathrm{Dom}(g)$, pues esto basta para poder evaluar la función g sobre el elemento $f(a)$. Es decir, la definición puede hacerse de manera más general.

Ejemplo: Consideremos la función $h : \mathbb{R} \setminus \{0\} \to \mathbb{R}$, dada por $h(x) = \frac{1}{x^2}$. Si tomamos las funciones $f : \mathbb{R} \setminus \{0\} \to \mathbb{R}$ tal que $f(x) = \frac{1}{x}$ y $g : \mathbb{R} \to \mathbb{R}$ tal que $g(x) = x^2$, entonces para cualquier $x \in \mathbb{R} \setminus \{0\}$,

$$(g \circ f)(x) = g(f(x)) = g\left(\frac{1}{x}\right) = \left(\frac{1}{x}\right)^2 = h(x).$$

Como además $\mathrm{Dom}(g \circ f) = \mathrm{Dom}(f) = \mathbb{R} \setminus \{0\} = \mathrm{Dom}(h)$ y $\mathrm{Cod}(g \circ f) = \mathrm{Cod}(g) = \mathbb{R} = \mathrm{Cod}(h)$, sigue que $g \circ f = h$. ♢

En lo que sigue estudiamos propiedades de la composición:

Proposición 4.12 *$f : A \to B$ biyectiva $\implies f \circ f^{-1} = \mathrm{id}_B \ \wedge \ f^{-1} \circ f = \mathrm{id}_A$.*

Dem. Veamos primero que $f \circ f^{-1} = \mathrm{id}_B$. Basta observar que $\mathrm{Dom}(f \circ f^{-1}) = \mathrm{Dom}(f^{-1}) = B$, $\mathrm{Cod}(f \circ f^{-1}) = \mathrm{Cod}(f) = B$, y notar que para $y \in B$ arbitrario,

$$\begin{aligned} f \circ f^{-1}(y) &= f(f^{-1}(y)) && \text{(por definición de } \circ) \\ &= y. && \text{(por Proposición 4.10 parte (I))} \end{aligned}$$

La demostración de que $f^{-1} \circ f = \mathrm{id}_A$ es similar. □

El siguiente resultado es directo de la definición de composición de funciones. Su demostración queda como ejercicio.

Proposición 4.13 *Sean $f : A \to B$, $g : B \to C$, y $h : C \to D$ funciones. Se tiene:*

(I) $\circ$ *es asociativa, es decir,* $h \circ (g \circ f) = (h \circ g) \circ f$.

(II) id_B *es neutro por la izquierda para* $\circ$ *en* B^A*, es decir,* $\mathrm{id}_B \circ f = f$.

(III) id_A *es neutro por la derecha para* $\circ$ *en* B^A*, es decir,* $f \circ \mathrm{id}_A = f$.

Observación: Destaca la ausencia, en la proposición anterior, de alguna referencia a la conmutatividad. Esto se debe a que $\circ$ no es conmutativa. Un contraejemplo sencillo está dado por f y g de $\mathbb{R}$ en $\mathbb{R}$ tales que $f(x) = 1$ y $g(x) = 0$ para todo $x \in \mathbb{R}$. Luego, $f \circ g(x) = 1 \neq 0 = g \circ f(x)$, cualquiera sea $x \in \mathbb{R}$. □

Enunciamos ahora algunas propiedades de la composición de funciones con respecto a la inyectividad y epiyectividad:

Proposición 4.14 *Sean* $f : A \to B$ *y* $g : B \to C$ *funciones. Se tiene que:*

(I) f *y* g *son inyectivas* $\implies$ $g \circ f$ *es inyectiva.*

(II) f *y* g *son epiyectivas* $\implies$ $g \circ f$ *es epiyectiva.*

(III) f *y* g *son biyectivas* $\implies$ $g \circ f$ *es biyectiva.*

(IV) $g \circ f$ *es inyectiva* $\implies$ f *es inyectiva (*g *no necesariamente lo es).*

(V) $g \circ f$ *es epiyectiva* $\implies$ g *es epiyectiva (*f *no necesariamente lo es).*

Dem. Demostraremos (II) y (IV). (Notar que (III) es consecuencia directa de (I) y (II).)

Para (II): Por hipótesis tenemos que f y g son epiyectivas. Queremos ver que la función $g \circ f : A \to C$ es epiyectiva. Sea $z \in C$. Buscamos un $x \in A$ tal que $(g \circ f)(x) = z$, es decir, tal que $g(f(x)) = z$.

Como $g : B \to C$ es epiyectiva, sabemos que existe un $y \in B$ tal que $g(y) = z$. Del mismo modo, como $f : A \to B$ es epiyectiva, sabemos que existe $x \in A$ tal que $f(x) = y$. Así

$$(g \circ f)(x) = g(f(x)) = g(y) = z$$

que es lo que queríamos demostrar.

Para (IV): Por hipótesis tenemos que $g \circ f$ es inyectiva. Queremos demostrar que f es inyectiva.

Consideremos $x_1, x_2 \in A$ arbitrarios. Notar que

$$\begin{aligned} f(x_1) = f(x_2) &\implies g \circ f(x_1) = g(f(x_1)) = g(f(x_2)) = g \circ f(x_2) \\ &\qquad \text{(evaluando ambos lados de la = en } g \text{ y por definición de } \circ) \\ &\implies x_1 = x_2. \qquad \text{(porque por hipótesis } g \circ f \text{ es inyectiva)} \end{aligned}$$

Como $x_1, x_2 \in A$ son arbitrarios, se concluye que f es inyectiva.

Veamos ahora, mediante un contraejemplo, que g no tiene porque ser inyectiva. Consideremos $A = \{x\}$, $B = \{1, 2\}$, y $C = \{c\}$. Además, sean $f : A \to B$ tal que $f(x) = 1$ y $g : B \to C$ tal que $g(1) = g(2) = c$. La función f es claramente inyectiva mientras que g no lo es. No obstante, $g \circ f : A \to C$ es trivialmente inyectiva, pues no existen $a, a' \in A$ con $a \neq a'$. □

Corolario 4.15 *Si $f : A \to B$ es biyectiva, entonces f^{-1} es biyectiva y $(f^{-1})^{-1} = f$.*

Dem. Por Proposición 4.12, si f es biyectiva, entonces $f \circ f^{-1} = \mathrm{id}_B$ y $f^{-1} \circ f = \mathrm{id}_A$. Por Proposición 4.14 parte (IV), de $f \circ f^{-1} = \mathrm{id}_B$ sigue que f^{-1} es inyectiva. Por Proposición 4.14 parte (V), de $f^{-1} \circ f = \mathrm{id}_A$ sigue que f^{-1} es epiyectiva. Por lo tanto, se concluye que f^{-1} es biyectiva.

Veamos ahora que $(f^{-1})^{-1} = f$. Primero observamos que $\mathrm{Dom}((f^{-1})^{-1}) = \mathrm{Cod}(f^{-1}) = \mathrm{Dom}(f)$ y que $\mathrm{Cod}((f^{-1})^{-1}) = \mathrm{Dom}(f^{-1}) = \mathrm{Cod}(f)$. Falta probar que $(f^{-1})^{-1}(x) = f(x)$ para todo $x \in A$. En efecto, sea $x \in A$ arbitrario. Notar que

$$\begin{aligned} f(x) = f(x) &\iff x = f^{-1}(f(x)) && \text{(por definición de } f^{-1}) \\ &\iff (f^{-1})^{-1}(x) = f(x). && \text{(por definición de } (f^{-1})^{-1}) \end{aligned}$$

Como $x \in A$ es arbitrario, se obtiene la conclusión que buscábamos. □

Método para cálculo de inversas

Por Corolario 4.15 y Proposición 4.12 sabemos que, si $f : A \to B$ es una función biyectiva, entonces existe $g : B \to A$ inversa de f (es decir, $g = f^{-1}$) que satisface las siguientes tres propiedades:

(a) $g \circ f = \mathrm{id}_A$.
(b) $f \circ g = \mathrm{id}_B$.
(c) g es biyectiva.

El siguiente resultado establece una especie de recíproco.

Proposición 4.16 *Sean $f : A \to B$ y $g : B \to A$. Si de las condiciones (a), (b), (c), las funciones f y g satisfacen dos cualesquiera, entonces f es biyectiva y su inversa es g (es decir, $g = f^{-1}$).*

Dem. Supongamos que se cumplen las condiciones (a) y (c). La primera de estas condiciones garantiza que $g \circ f = \mathrm{id}_A$. La segunda condición y el Corolario 4.15 nos garantizan que g^{-1} existe. Luego,

$$\begin{aligned} g \circ f = \mathrm{id}_A &\iff g^{-1} \circ (g \circ f) = g^{-1} \circ \mathrm{id}_A && \text{(componiendo por la izquierda por } g^{-1}) \\ &\iff (g^{-1} \circ g) \circ f = g^{-1} && \text{(porque } \circ \text{ es asoc. y Proposición 4.13 parte (III))} \\ &\iff \mathrm{id}_B \circ f = g^{-1} && \text{(por Proposición 4.12)} \\ &\iff f = g^{-1}. && \text{(por Proposición 4.13 parte (II))} \end{aligned}$$

Como g es biyectiva, por Corolario 4.15, se tiene que $f = g^{-1}$ es biyectiva y que $g = f^{-1}$.

El caso en que se cumplan las condiciones (b) y (c) se verifica de manera parecida al caso anterior.

Finalmente, supongamos que se cumplen las condiciones (a) y (b). Como $g \circ f = \mathrm{id}_A$ e id_A es epiyectiva, por Proposición 4.14 parte (v), sigue que g es epiyectiva. Como $f \circ g = \mathrm{id}_B$ e id_B es inyectiva, por Proposición 4.14 parte (iv), sigue que g es inyectiva. Luego, g es biyectiva y se cumple la condición (c). La conclusión sigue del caso anterior. □

Como consecuencia, podemos obtener el siguiente resultado:

Proposición 4.17 (Inversa de una composición) *Si $f : A \to B$ y $g : B \to C$ son biyectivas, entonces*

$$(g \circ f)^{-1} = f^{-1} \circ g^{-1}.$$

Dem. Denotemos $F = g \circ f$ y $G = f^{-1} \circ g^{-1}$. Por Proposición 4.16 basta con verificar que

$$G \circ F = \mathrm{id}_A \quad \text{y} \quad F \circ G = \mathrm{id}_C.$$

En efecto,

$$\begin{aligned}
G \circ F &= (f^{-1} \circ g^{-1}) \circ (g \circ f) && \text{(por definición de } F \text{ y } G\text{)} \\
&= f^{-1} \circ ((g^{-1} \circ g) \circ f) && \text{(por asociatividad de } \circ\text{)} \\
&= f^{-1} \circ (\mathrm{id}_B \circ f) && \text{(por Proposición 4.12)} \\
&= f^{-1} \circ f && \text{(por Proposición 4.13 parte (ii))} \\
&= \mathrm{id}_A && \text{(por Proposición 4.12)}
\end{aligned}$$

Análogamente, se verifica que $F \circ G = \mathrm{id}_B$. □

Guía Básica

Determinar la veracidad de las siguientes afirmaciones:

1. El problema de dada una función $f : A \to B$ y $a \in A$, encontrar $x \in B$ tal que $f(a) = x$ siempre tiene una única solución.
2. El problema de dada una función $f : A \to B$ y $a \in A$, encontrar $x \in B$ tal que $f(a) = x$ no siempre tiene una solución.
3. El problema de dada una función $f : A \to B$ y $a \in A$, encontrar $x \in B$ tal que $f(a) = x$ siempre tiene una solución, pero no siempre única.
4. El problema de dada una función $f : A \to B$ y $b \in B$, encontrar $x \in A$ tal que $f(x) = b$ siempre tiene una única solución.
5. El problema de dada una función $f : A \to B$ y $b \in B$, encontrar $x \in A$ tal que $f(x) = b$ no siempre tiene solución.
6. El problema de dada una función $f : A \to B$ y $b \in B$, encontrar $x \in A$ tal que $f(x) = b$, si tiene solución aunque ésta no es siempre única.
7. Una función $f : A \to B$ es inyectiva si satisface que $\forall x_1, x_2 \in A, x_1 \neq x_2 \implies f(x_1) \neq f(x_2)$.
8. Una función $f : A \to B$ es inyectiva si satisface que $\forall x_1, x_2 \in A, x_1 = x_2 \implies f(x_1) = f(x_2)$.
9. Una función $f : A \to B$ es inyectiva si satisface que $\forall x_1, x_2 \in A, f(x_1) = f(x_2) \implies x_1 = x_2$.
10. Una función $f : A \to B$ es inyectiva si satisface que $\forall x_1, x_2 \in A, f(x_1) \neq f(x_2) \implies x_1 \neq x_2$.
11. La función $f : (0, \infty) \to \mathbb{R}$, definida por $f(x) = x^2$, es inyectiva.
12. La función $f : \mathbb{R} \to \mathbb{R}$, definida por $f(x) = x^2$, es inyectiva.
13. La función $f : \mathbb{R} \setminus \{0\} \to (0, \infty)$, definida por $f(x) = x^2$, es inyectiva.
14. La función $f : \mathbb{R} \to (0, \infty)$, definida por $f(x) = |x - 1|$, es inyectiva.
15. La función $f : (0, \infty) \to \mathbb{R}$, definida por $f(x) = |x - 1|$, es inyectiva.
16. La función $f : (1, \infty) \to \mathbb{R}$, definida por $f(x) = |x - 1|$, es inyectiva.
17. Una función $f : A \to B$ es epiyectiva si satisface que $\forall a \in A, \exists b \in B, f(a) = b$.
18. Una función $f : A \to B$ es epiyectiva si satisface que $\forall a \in A, \exists! b \in B, f(a) = b$.
19. Una función $f : A \to B$ es epiyectiva si satisface que $\forall b \in B, \exists a \in A, f(a) = b$.
20. Una función $f : A \to B$ que satisface $\forall b \in B, \exists! a \in A, f(a) = b$, no necesariamente es epiyectiva.
21. Una función $f : A \to B$ que satisface $\forall b \in B, \exists! a \in A, f(a) = b$, es inyectiva.
22. Una función $f : A \to B$ que satisface $\forall b \in B, \exists! a \in A, f(a) = b$, es epiyectiva, pero no necesariamente inyectiva.
23. La función $f : (0, \infty) \to \mathbb{R}$, definida por $f(x) = x^2$, es epiyectiva.

24. La función $f : \mathbb{R} \to \mathbb{R}$, definida por $f(x) = x^2$, no es epiyectiva.
25. La función $f : \mathbb{R} \setminus \{0\} \to (0, \infty)$, definida por $f(x) = x^2$, es epiyectiva.
26. La función $f : (0, \infty) \to (0, \infty)$, definida por $f(x) = x^2$, es epiyectiva.
27. Una función es biyectiva si es inyectiva o epiyectiva.
28. Una función es biyectiva si es inyectiva y epiyectiva.
29. Una función $f : A \to B$ es biyectiva si satisface $(\forall b \in B)(\exists! a \in A)(f(a) = b)$.
30. La función $f : \mathbb{R} \setminus \{0\} \to (0, \infty)$, definida por $f(x) = x^2$, es biyectiva.
31. La función $f : (0, \infty) \to (0, \infty)$, definida por $f(x) = x^2$, es biyectiva.
32. La función $f : (0, \infty) \to \mathbb{R}$, definida por $f(x) = x^2$, es biyectiva.
33. La función $f : \mathbb{R} \to \mathbb{R}$, definida por $f(x) = ax + b$ con $a, b \in \mathbb{R}$, siempre es biyectiva.
34. La función $f : \mathbb{R} \to \mathbb{R}$, definida por $f(x) = ax + b$ con $a, b \in \mathbb{R}$, es biyectiva si $b \neq 0$.
35. La función $f : \mathbb{R} \to \mathbb{R}$, definida por $f(x) = ax + b$ con $a, b \in \mathbb{R}$, es biyectiva si $a \neq 0$.
36. Dada una función $f : A \to B$ cualquiera, su inversa existe y se denota f^{-1}.
37. Existen funciones que no son inyectivas y que tienen una inversa.
38. La inversa de una función biyectiva, es biyectiva.
39. Existe una función $f : A \to A$ biyectiva, tal que para algún $a \in A$ se tiene que $f(f^{-1}(a)) \neq f^{-1}(f(a))$.
40. Si $f : A \to B, g : C \to D$ y $B \subseteq C$, entonces $g \circ f$ existe.
41. Si $f : A \to B, g : C \to D$ y $C \subseteq B$, entonces $g \circ f$ existe.
42. Si $f : A \to B, g : C \to D$ y $g \circ f$ existe, entonces $B = C$.
43. Si $f : A \to B, g : B \to A$, entonces $f \circ g = g \circ f$.
44. Si $f : A \to A, g : A \to A$, entonces $f \circ g = g \circ f$.
45. Si $f : A \to B, g : B \to A$ y f es la función identidad, entonces $f \circ g = g \circ f$.
46. Si $f : A \to B, g : B \to C$ y f es inyectiva, entonces $g \circ f$ también lo es.
47. Si $f : A \to B, g : B \to C$ y f es epiyectiva, $g \circ f$ también lo es.
48. Si $f : A \to B, g : B \to C$ son tales que f y g son epiyectivas, $g \circ f$ también lo es.
49. Si $f : A \to B, g : B \to C$ y f es biyectiva, $g \circ f$ es inyectiva.
50. Si $f : A \to B, g : B \to C$ y f es biyectiva, $g \circ f$ es epiyectiva.
51. Si $f : A \to B, g : B \to C$ y g es biyectiva, $g \circ f$ también lo es.
52. Si $f : A \to B, g : B \to C$ y g es biyectiva, $g \circ f$ es epiyectiva.
53. Si $f : A \to B, g : B \to C$ son tales que f y g son biyectivas, $g \circ f$ también lo es.
54. Si $f : A \to B, g : B \to C$ y $g \circ f$ es inyectiva, g también lo es.
55. Si $f : A \to B, g : B \to C$ y $g \circ f$ es epiyectiva, g también lo es.
56. Si $f : A \to B, g : B \to C$ y $g \circ f$ es biyectiva, g también lo es.
57. Si $f : A \to B, g : B \to C$ y $g \circ f$ es biyectiva, g es inyectiva.
58. Si $f : A \to B, g : B \to C$ y $g \circ f$ es biyectiva, f también lo es.

59. Si $f : A \to B, g : B \to C$ y $g \circ f$ es biyectiva, f es inyectiva.
60. Si $f : A \to B, g : B \to A$ son biyectivas, entonces si $g = f^{-1}$, luego $g \circ f = \mathrm{id}_A$.
61. Si $f : A \to B, g : B \to A$ son biyectivas, entonces si $g = f^{-1}$, luego $f \circ g = \mathrm{id}_A$.
62. Si $f : A \to B, g : B \to A$ son biyectivas, entonces si $g = f^{-1}$, luego $f \circ g = \mathrm{id}_B$.
63. Si $f : A \to B, g : B \to A$ son biyectivas, entonces si $f = g^{-1}$, luego $g = f^{-1}$.
64. Si f es biyectiva, $(f^{-1})^{-1} = f$.
65. Si f es biyectiva, $(f^{-1})^{-1} = f^{-1}$.
66. Si $f : A \to B, g : B \to C$ son biyectivas, luego $(f \circ g)^{-1} = f^{-1} \circ g^{-1}$.
67. Si $f : A \to B, g : B \to C$ son biyectivas, luego $(f \circ g)^{-1} = g^{-1} \circ f^{-1}$.
68. Si $f : A \to B, g : B \to C$ son biyectivas, luego $((f \circ g)^{-1})^{-1} = f^{-1} \circ g^{-1}$.
69. Si $f : A \to B, g : B \to C$ son biyectivas, luego $((f \circ g)^{-1})^{-1} = f \circ g$.

Guía de Ejercicios

1. Dado un conjunto $E \neq \emptyset$ y $B \subseteq$ fijo, determine si cada una de las siguientes es función y, en caso de serlo, si es inyectiva, epiyectiva y biyectiva. Considere a E como el universo. Encuentre la función inversa en el caso que corresponda.

   a) $f : \mathcal{P}(E) \to \mathcal{P}(E)$, dada por $\forall X \subseteq E,\ f(X) = X^c$.
   b) $g : \mathcal{P}(E) \to \mathcal{P}(E)$, dada por $\forall X \subseteq E,\ g(X) = X \setminus (X^c)$.
   c) $h_1 : \mathcal{P}(E) \to \mathcal{P}(E)$, dada por $\forall X \subseteq E,\ h_1(X) = X \cap B$.
   d) $h_2 : \mathcal{P}(E) \setminus \{\emptyset\} \to \mathcal{P}(E)$, dada por $\forall X \subseteq E, h_2(X) = X \cup B$.
   e) $h_3 : \mathcal{P}(E) \to \mathcal{P}(E)$, dada por $\forall X \subseteq E,\ h_3(X) = X \triangle B$.

2. Comente sobre la inyectividad, epiyectividad y biyectividad de las siguientes funciones. Considere $f : \mathbb{R} \to \mathbb{R}$

   a) $f(x) = \sqrt{x^2 + 1}$
   b) $f(x) = x^3$
   c) $f(x) = \mathrm{sen}(x)$
   d) $f(x) = \frac{x^2+3x-1}{2x^2-5x+4}$

   ¿Se puede redefinir el dominio o el codominio de f de modo que la función logre ser inyectiva o epiyectiva?

3. Encuentre la función inversa de las siguientes funciones, verificando previamente si son biyectivas.

   a) $f : \mathbb{R} \setminus \{0\} \to \mathbb{R}$, con $f(x) = \frac{1}{x^3}$
   b) Sea $a \neq 0$. $f : \mathbb{R} \to \mathbb{R}$, con $f(x) = ax + b$
   c) $f : [0, 2\pi] \to \mathbb{R}, \quad f(x) = \mathrm{sen}(x^2)$
   d) $f : (0, \infty) \to \mathbb{R}, \quad f(x) = \frac{x}{\sqrt{x}}$

4. Dadas $f : A \to B$, $g : B \to C$ funciones, demuestre las siguientes propiedades enunciadas en el texto del apunte:

   a) Si f y g son inyectivas, entonces $g \circ f$ es inyectiva.
   b) Si f y g son biyectivas, entonces $g \circ f$ es biyectiva.
   c) Si $g \circ f$ es epiyectiva, entonces g es epiyectiva (f no necesariamente lo es).

5. Sean $f : \mathbb{Z} \to \mathbb{Z}$, $g : \mathbb{Z} \to \mathbb{Z}$ y $h : \mathbb{Z} \to \mathbb{Z}$ tres funciones dadas por $f(x) = 1 - x$, $g(x) = -x - 1$ y $h(x) = x + 2$.

   a) Verificar que cualquier composición entre estas tres funciones (por ejemplo, $f \circ (h \circ g)$, $f \circ g$, $(h \circ h) \circ g$, etc.), resulta ser una función biyectiva.
   b) Pruebe que $h \circ g \circ f = g \circ f \circ h = \mathrm{id}_{\mathbb{Z}}$, en donde $\mathrm{id}_{\mathbb{Z}}$ es la función identidad.
   c) Deducir de lo anterior que $f^{-1} \circ g^{-1} = h$.

6. Dados dos conjuntos A y B, determine si las siguientes son funciones y si son inyectivas, epiyectivas y biyectivas. Encuentre la función inversa en el caso que corresponda.

   a) $\pi_A : A \times B \to A$, dada por $\forall (a, b) \in A \times B,\ \pi_A((a, b)) = a$.
   b) $\pi_B : A \times B \to B$, dada por $\forall (a, b) \in A \times B,\ \pi_B((a, b)) = b$.
   c) $d_A : A \to A \times B$, dada por $\forall a \in A,\ d_A(a) = (a, a)$.
   d) $\tau : A \times B \to B \times A$, dada por $\forall (a, b) \in A \times B,\ \tau((a, b)) = (b, a)$.
   e) Dado $b_0 \in B$ fijo. $f : A \to A \times B$, dada por $\forall a \in A,\ f(a) = (a, b_0)$.

7. Considere las mismas funciones del ejercicio anterior, pero suponiendo $A = B$. Indique si se pueden o no definir las siguientes funciones. En los casos afirmativos, determínelas.

   a) $\pi_A \circ \pi_B$.
   b) $\pi_B \circ d_A \circ \pi_A$.
   c) $\pi_B \circ \tau$.
   d) $\pi_A \circ \tau \circ f$.
   e) $d_A \circ f \circ \pi_A$.

Guía de Problemas

1. (20 min.) Considere las funciones $f : \mathbb{N} \setminus \{0\} \to \mathbb{Q}$ definida en cada $n \in \mathbb{N} \setminus \{0\}$ por $f(n) = \frac{1}{2n}$ y $g : \mathbb{Q} \to \mathbb{Q}$ definida en cada $q \in \mathbb{Q}$ por $g(q) = \frac{q}{2}$. Determine si f, g son inyectivas, epiyectivas y biyectivas.
2. Sea $f : \mathbb{R} \setminus \{2\} \to \mathbb{R}$ la función definida en cada $x \in \mathbb{R} \setminus \{2\}$ por $f(x) = \frac{2x+1}{x-2}$.

   a) (10 min.) Demostrar que $\{f(x) \mid x \in \mathbb{R} \setminus \{2\}\} = \mathbb{R} \setminus \{2\}$.
   b) (10 min.) Demostrar que f es inyectiva.
   c) (10 min.) Se define una nueva funcion $g : \mathbb{R} \setminus \{2\} \to \mathbb{R} \setminus \{2\}$ tal que en cada $x \in \mathbb{R} \setminus \{2\}$ se tiene que $g(x) = f(x)$. Pruebe que g es biyectiva y calcule su inversa.

3. (30 min.) Para $a, b \in \mathbb{R}$ considere la recta $L_{a,b} = \{(x, y) \in \mathbb{R}^2 \mid y = ax + b\}$ y la colección de rectas $\mathcal{L} = \{L_{a,b} \subseteq \mathbb{R}^2 \mid a, b \in \mathbb{R}\}$. Se define el conjunto de pares de rectas no paralelas

$$\mathcal{H} = \{(L, L') \in \mathcal{L}^2 \mid L \cap L' \neq \emptyset, L \neq L'\}$$

y la función $\psi : \mathcal{H} \to \mathbb{R}^2$ tal que $\psi((L, L')) = (x_0, y_0)$, donde (x_0, y_0) es el único punto de intersección de L y L'. Pruebe que ψ es epiyectiva.

4. Sea E el conjunto universo y $A, B \subseteq E$. Se define

$$\begin{aligned} f : \mathcal{P}(E) &\longrightarrow \mathcal{P}(E) \\ X &\longmapsto f(X) = A \cap (B \cup X) \end{aligned}$$

   a) (15 min.) Pruebe que $f(f(X)) = f(X)$ para todo $X \in \mathcal{P}(E)$.
   b) (15 min.) Si $A \neq E \vee B \neq \emptyset$, pruebe que f no es inyectiva.
   c) (10 min.) Si $A \neq E$ pruebe que f no es epiyectiva.

5. Sea Ω una partición de un conjunto A y sea $f : A \to \Omega$ la función que a $a \in A$ asocia $f(a)$, con $a \in f(a)$. Determine qué condiciones debe cumplir Ω para que f sea inyectiva y cuáles para que sea epiyectiva. En las situaciones en las que f es invertible determine cuál es su inversa.

6. Sea $f : A \to A$ una función y $a \in A$ tal que $(f \circ f)(x) = a, \forall x \in A$. Determine el conjunto A cuando se sabe que f es inyectiva y cuando se sabe que f es epiyectiva.

4.5 Conjuntos imagen y preimagen

Si $f : A \to B$ es una función, y si $y = f(x)$, decimos que y es **imagen** de x a través de f, y que x es **preimagen** de y a través de f.

Como f es una función, tenemos que $\forall x \in A, \exists! y \in B, y = f(x)$.

Esto nos dice que cada $x \in A$ posee una única imagen $y \in B$. Sin embargo, los elementos $y \in B$ pueden tener varias preimágenes distintas, como veremos en el siguiente ejemplo.

Ejemplo: Tomemos la función $f : \mathbb{N} \to \mathbb{N}$ dada por $f(n) = (n-10)^2$. Se tiene que 36 es la imagen por f de 4, pues $f(4) = 36$. A su vez, tenemos que 4 es preimagen de 36. Pero también $f(16) = 36$, por lo que 16 también es preimagen de 36. Es fácil observar que 36 no tiene más preimágenes que estas dos, así que podemos decir que $\{4, 16\}$ es el conjunto de preimágenes de 36. Del mismo modo, $\{5, 15\}$ es el conjunto de preimágenes de 25, y $\{10\}$ es el conjunto de preimágenes de 0. Podemos reunir estos conjuntos de preimágenes:

> $\{4, 5, 10, 15, 16\}$ es la unión de las preimágenes de los elementos de $\{0, 25, 36\}$.

También está el caso del natural 2, el cual no tiene preimágenes por f (esto se observa dado que $f(n)$ siempre es un cuadrado perfecto, y 2 no lo es). En este caso decimos que el conjunto de preimágenes de 2 es $\emptyset$ (el conjunto vacío).

Así como obtuvimos el conjunto de todas las preimágenes de ciertos elementos, podemos formar el conjunto de todas las imágenes de una colección de elementos. Como sabemos que 9, 4, 1, 0, 1 y 4 son respectivamente las imágenes de 7, 8, 9, 10, 11 y 12, escribimos:

> $\{0, 1, 4, 9\}$ es el conjunto obtenido al reunir las imágenes de $\{7, 8, 9, 10, 11, 12\}$ (observar que en el primer conjunto hemos eliminado los elementos repetidos, como corresponde en los conjuntos).

$\diamondsuit$

Definición 4.18 (Conjunto imagen) *Sea $f : A \to B$ una función, y sea $A' \subseteq A$. Definimos el conjunto imagen de A' por f como*

$$f(A') = \{f(x) \in B | x \in A'\}$$

o, equivalentemente

$$\forall y \in B, (y \in f(A') \iff \exists x \in A', f(x) = y).$$

Notemos que $f(A')$ siempre es un subconjunto de B. Es el obtenido al reunir todas las imágenes de los elementos de A'.

Proposición 4.19 *$f : A \to B$ es epiyectiva $\iff$ $f(A) = B$*

Dem. En efecto,

$$\begin{aligned}
f(A) = B &\iff B \subseteq f(A) && \text{(porque } f(A) \subseteq B \text{ por definición de función)} \\
&\iff \forall y \in B, y \in f(A) && \text{(definición de } \subseteq) \\
&\iff \forall y \in B, \exists x \in A, y = f(x) && \text{(definición de conjunto imagen)} \\
&\iff f \text{ es epiyectiva.} && \text{(definición de epiyectividad)}
\end{aligned}$$

□

Proposición 4.20 *Sea $f : A \to B$ función. Sean $A_1, A_2 \subseteq A$. Se tiene:*

(I) $A_1 \subseteq A_2 \implies f(A_1) \subseteq f(A_2)$.

(II) $f(A_1 \cap A_2) \subseteq f(A_1) \cap f(A_2)$.

(III) $f(A_1 \cup A_2) = f(A_1) \cup f(A_2)$.

Dem. Demostraremos (I) y (II).

Veamos que se cumple (I). Por hipótesis, se tiene que $A_1 \subseteq A_2$. Luego,

$$\begin{aligned}
f(A_1) &= \{f(x) | x \in A_1\} && \text{(definición de conjunto imagen)} \\
&\subseteq \{f(x) | x \in A_2\} && \text{(porque } A_1 \subseteq A_2) \\
&= f(A_2). && \text{(definición de conjunto imagen)}
\end{aligned}$$

Veamos que se cumple (II). En efecto, sea $y \in B$ arbitrario,

$$\begin{aligned}
y \in f(A_1 \cap A_2) &\iff \exists x \in A_1 \cap A_2, y = f(x) && \text{(definición de conjunto imagen)} \\
&\iff \exists x \in E, x \in A_1 \cap A_2 \wedge y = f(x) \\
& && \text{(convención sobre cuantificación sobre conjuntos)} \\
&\iff \exists x \in E, (x \in A_1 \wedge y = f(x)) \wedge (x \in A_2 \wedge y = f(x)) \\
& && \text{(Idempotencia y asociatividad del } \wedge) \\
&\implies (\exists x \in E, x \in A_1 \wedge y = f(x)) \wedge (\exists x \in E, x \in A_2 \wedge y = f(x)) \\
& && \text{(por Proposicion 1.21(IV))} \\
&\implies (\exists x \in A_1, y = f(x)) \wedge (\exists x \in A_2, y = f(x)) \\
& && \text{(convención de cuantificación sobre conjuntos)} \\
&\iff y \in f(A_1) \wedge y \in f(A_2) && \text{(definición de conjunto imagen)} \\
&\iff y \in f(A_1) \cap f(A_2). && \text{(definición de } \cap)
\end{aligned}$$

Como y es arbitrario, se concluye que $f(A_1 \cap A_2) \subseteq f(A_1) \cap f(A_2)$. □

Ejercicio: Queda propuesto mostrar que no se cumple el recíproco. Es decir, mostrar con un contraejemplo que, en general, no se cumple que $f(A_1 \cap A_2) = f(A_1) \cap f(A_2)$. △

Definición 4.21 (Conjunto preimagen) *Sea $f : A \to B$ función y sea $B' \subseteq B$. Definimos el conjunto preimagen de B' por f como*

$$f^{-1}(B') = \{x \in A \ : \ f(x) \in B'\}$$

o, equivalentemente

$$\forall x \in A, \big(x \in f^{-1}(B') \iff f(x) \in B'\big).$$

Notar que $f^{-1}(B')$ es siempre un subconjunto de A. Es el obtenido al reunir todas las preimágenes de los elementos de B'. Más aún, $f^{-1}(B')$ queda bien definido siempre, inclusive si f no es biyectiva (en cuyo caso f no sería invertible).

Proposición 4.22 *Sea $f : A \to B$ función y sean $B_1, B_2 \subseteq B$. Se tiene:*

(I) $B_1 \subseteq B_2 \implies f^{-1}(B_1) \subseteq f^{-1}(B_2)$.
(II) $f^{-1}(B_1 \cap B_2) = f^{-1}(B_1) \cap f^{-1}(B_2)$.
(III) $f^{-1}(B_1 \cup B_2) = f^{-1}(B_1) \cup f^{-1}(B_2)$.

Dem. Demostraremos (I) y (II).

Veamos que se cumple (I). Por hipótesis, se tiene que $B_1 \subseteq B_2$. Luego,

$$\begin{aligned}
f^{-1}(B_1) &= \{x \in A : f(x) \in B_1\} && \text{(definición de conjunto preimagen)} \\
&\subseteq \{x \in A : f(x) \in B_2\} && \text{(porque } B_1 \subseteq B_2) \\
&= f^{-1}(B_2). && \text{(definición de conjunto preimagen)}
\end{aligned}$$

Veamos que se cumple (II). Notar que si $x \in A$ es arbitrario, entonces

$$\begin{aligned} x \in f^{-1}(B_1 \cap B_2) &\iff f(x) \in B_1 \cap B_2 && \text{(definición de conjunto preimagen)} \\ &\iff f(x) \in B_1 \wedge f(x) \in B_2 && \text{(definición de } \cap) \\ &\iff x \in f^{-1}(B_1) \wedge x \in f^{-1}(B_2) && \text{(definición de conjunto preimagen)} \\ &\iff x \in f^{-1}(B_1) \cap f^{-1}(B_2). && \text{(definición de } \cap) \end{aligned}$$

Como x es arbitrario, se concluye que $f(B_1 \cap B_2) = f(B_1) \cap f(B_2)$. □

A continuación enunciaremos un par de resultados que reunen los conceptos vistos en esta sección y las anteriores. Posteriormente, resolveremos ejercicios relacionados.

Proposición 4.23 *Sea $f : A \to B$ función, $A' \subseteq A$ y $B' \subseteq B$. Se tiene:*

(I) $A' \subseteq f^{-1}(f(A'))$.

(II) $f(f^{-1}(B')) = B' \cap f(A)$.

Proposición 4.24 *Sea $f : A \to B$ función. Se tiene:*

(I) *f es inyectiva si cada elemento del codominio tiene a lo más una preimagen, es decir,*

$$f \text{ es inyectiva} \iff \forall y \in B, f^{-1}(\{y\}) = \emptyset. \vee (\exists! x \in A, f^{-1}(\{y\}) = \{x\}).$$

(II) *f es epiyectiva si cada elemento del codominio tiene al menos una preimagen, es decir*

$$f \text{ es epiyectiva} \iff \forall y \in B, f^{-1}(\{y\}) \neq \emptyset.$$

(III) *f es biyectiva si cada elemento del codominio tiene exactamente una preimagen, es decir,*

$$f \text{ es biyectiva} \implies \forall y \in B, \exists! x \in A, f^{-1}(\{y\}) = \{x\}.$$

En general, si f es biyectiva y denotamos su inversa por h, entonces se tiene que

$$\forall B' \subseteq B, f^{-1}(B') = h(B').$$

Es decir, la preimagen de B' por f y la imagen de B' por h coinciden, para cualquier $B' \subseteq B$.

Ejemplo: Primero veamos que f es inyectiva $\iff \forall A' \subseteq A, A' = f^{-1}(f(A'))$.

Haremos la demostración por Equivalencia dividida.

$\Rightarrow$) Debemos probar que $\forall A' \subseteq A, A' = f^{-1}(f(A'))$.

Sea entonces $A' \subseteq A$ y $x \in A$ arbitrario. Notar que,

$$\begin{aligned} x \in f^{-1}(f(A')) &\iff f(x) \in f(A') && \text{(definición de conjunto preimagen)} \\ &\iff \exists x' \in A', f(x) = f(x') && \text{(definición de conjunto imagen)} \\ &\iff \exists x' \in A', x = x' && \text{(porque } f \text{ es inyectiva por hipótesis)} \\ &\iff x \in A' && \text{(definición de } \in) \end{aligned}$$

Como x es arbitrario, se concluye que $A' = f^{-1}(f(A'))$.

$\Leftarrow$) Por hipótesis $\forall A' \subseteq A, A' = f^{-1}(f(A'))$. Debemos probar que $\forall x_1, x_2 \in A, f(x_1) = f(x_2) \Rightarrow x_1 = x_2$. En efecto, si $x_1, x_2 \in A$ arbitrarios, entonces

$$\begin{aligned} f(x_1) = f(x_2) &\iff \{f(x_1)\} = \{f(x_2)\} && \text{(definición de = de conjuntos)} \\ &\iff f(\{x_1\}) = f(\{x_2\}) && \text{(definición de conjunto imagen)} \\ &\implies f^{-1}(f(\{x_1\})) = f^{-1}(f(\{x_2\})) \\ & && \text{(tomando preimágenes de ambos lados de la =)} \\ &\iff \{x_1\} = \{x_2\} && \text{(hipótesis)} \\ &\iff x_1 = x_2. && \text{(definición de = de conjuntos)} \end{aligned}$$

Ahora veamos que: f es epiyectiva $\iff \forall B' \subseteq B, f(f^{-1}(B')) = B'$.

Haremos la demostración por Equivalencia dividida.

$\Rightarrow$) Por hipótesis, f es epiyectiva. Debemos probar que $\forall B' \subseteq B, f(f^{-1}(B')) = B'$.

Sea entonces $B' \subseteq B$ e $y \in B'$ arbitrario. Como f es epiyectiva, $\exists x \in A$ tal que $y = f(x)$. Notar que,

$$\begin{aligned} y = f(x) \in B' &\iff x \in f^{-1}(B') && \text{(definición de conjunto preimagen)} \\ &\implies y = f(x) \in f(f^{-1}(B')). \\ & && \text{(porque } y = f(x) \text{ y definición de conjunto imagen)} \end{aligned}$$

Como y es arbitrario, se concluye que $B' \subseteq f(f^{-1}(B'))$. La inclusión reversa se tiene por Proposición 4.23 parte (II).

$\Leftarrow$) Por hipótesis $\forall B' \subseteq B, B' = f(f^{-1}(B'))$. Debemos probar que f es epiyectiva, o lo que es equivalente, por Proposición 4.19, que $f(A) = B$. En efecto, tomando $B' = B$ en la hipótesis, tenemos que

$$\begin{aligned} B = f(f^{-1}(B)) &\implies B \subseteq f(A) && \text{(porque } f^{-1}(B) \subseteq A \text{ y Proposición 4.20 parte (I))} \\ &\iff B = f(A). && \text{(porque } f(A) \subseteq B \text{ y definición de = de conjuntos)} \end{aligned}$$

$\diamondsuit$

SEMANA 06:

Relaciones

El siguiente concepto que vamos a estudiar es el de relación, en particular las relaciones binarias. Estas nos permitirán modelar conceptos como "es mayor que", "es adyacente a", "es divisible por", "precede a", etc. En general, las relaciones son la manera de formalizar matemáticamente que objetos de interés comparten cierta vinculación. Un caso muy particular de las relaciones son las funciones.

Aunque no lo estudiaremos, las relaciones (no necesariamente binarias) también constituyen la principal forma de describir la estructura de las bases de datos en que se almacena información en los sistemas informáticos modernos.

5.1 Definiciones y propiedades generales

Definición 5.1 (Relación) *Una tripleta de conjuntos $(A, B, \mathcal{R})$ es una* ***relación*** *si cumple $\mathcal{R} \subseteq A \times B$.*

Para $(a, b) \in A \times B$, denotaremos $a\mathcal{R}b$ cuando $(a, b) \in \mathcal{R}$, y $a \not\mathcal{R}\ b$ cuando $(a, b) \notin \mathcal{R}$.

El conjunto A se llama el ***dominio*** *de la relación y el conjunto B el* ***codominio****.*

En lugar de $(A, B, \mathcal{R})$ **es una relación**, diremos que $\mathcal{R}$ **es una relación en** $A \times B$.

En este apunte, el estudio de relaciones en $A \times B$, cuando A y B son arbitrarios, se restringe a lo ya hecho en el capítulo de las funciones, que por cierto son un tipo de relaciones.

En lo que sigue consideraremos sólo relaciones donde $A = B$. En este caso, diremos que $\mathcal{R}$ **es una relación en** A, en lugar de decir que $\mathcal{R}$ **es una relación en** $A \times A$**.**

Ejemplo:

- Cualquiera sea el conjunto A la relación $\mathcal{R} = \emptyset$ es relación en A.
- Para $A = \{a\}$ sólo hay una relación no vacia en A, a saber $\mathcal{R} = \{(a, a)\} = A \times A$.

  Diremos que una relación $\mathcal{Q}$ en un conjunto Ω es **trivial** si Ω tiene un solo elemento y $\mathcal{Q} = \Omega \times \Omega$.
- El orden de los números reales, $\leq$, es una relación en $\mathbb{R}$, interpretando $\leq$ como el conjunto $\{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x \leq y\}$.

- Para $A \neq \emptyset$ no vacío y $f : A \to B$ una función dada, el conjunto $\{(a, b) \in A \times A \mid f(a) = f(b)\}$ es una relación en A.

$\diamondsuit$

Ejemplo: Si $E \neq \emptyset$ y $\mathcal{P}(E)^* = \mathcal{P}(E) \setminus \{\emptyset\}$, entonces las siguientes son relaciones:

- Inclusión de conjuntos ($\subseteq$) en $\mathcal{P}(E)$, es decir, $\{(A, B) \in \mathcal{P}(E) \times \mathcal{P}(E) \mid A \subseteq B\}$.
- Menor o igual cardinal en $\mathcal{P}(E)^*$, es decir,

$$\mathcal{M} = \{(A, B) \in \mathcal{P}(E)^* \times \mathcal{P}(E)^* \mid \exists f : A \to B \text{ inyectiva }\}.$$

- Igual cardinal en $\mathcal{P}(E)^*$, es decir,

$$\mathcal{I} = \{(A, B) \in \mathcal{P}(E)^* \times \mathcal{P}(E)^* \mid \exists f : A \to B \text{ biyectiva }\}.$$

$\diamondsuit$

Ejemplo: También se suele definir una relación de manera menos formal mediante una descripción con palabras.

- Congruencia módulo 3: $p \equiv_3 q$ si p y q son enteros tales que $p - q = 3k$, para algún $k \in \mathbb{Z}$. Es decir, $\equiv_3$ es una relación en $\mathbb{Z}$ dada por $\{(p, q) \in \mathbb{Z}^2 | \exists k \in \mathbb{Z}, p - q = 3k\}$.
- $a\mathcal{R}b$ si a y b son personas cuyos RUT tienen el mismo símbolo verificador. Es claro del contexto que la relación es en el conjunto de las personas que poseen RUT.
- $a\mathcal{R}b$ si a y b son palabras de un libro que comienzan con la misma letra.
- Orden alfabético: $a\mathcal{R}b$ si a y b son palabras de un diccionario de español donde a aparece antes que b o bien $a = b$.

$\diamondsuit$

Dada una relación en un conjunto, definimos las siguientes propiedades (al igual que con la inyectividad, epiyectividad y biyectividad de funciones, estas propiedades pueden ser o no cumplidas por cada relación):

Definición 5.2 (Propiedades de relaciones) *Se dice que la relación $\mathcal{R}$ en A es*

- ***refleja**, si $\forall x \in A,\ x\mathcal{R}x$.*
- ***simétrica**, si $\forall x, y \in A,\ x\mathcal{R}y \Rightarrow y\mathcal{R}x$.*
- ***antisimétrica**, si $\forall x, y \in A,\ x\mathcal{R}y \wedge y\mathcal{R}x \Rightarrow x = y$.*
- ***transitiva**, si $\forall x, y, z \in A,\ x\mathcal{R}y \wedge y\mathcal{R}z \Rightarrow x\mathcal{R}z$.*

Estudiemos qué propiedades cumplen algunas de las relaciones de los ejemplos anteriores y otros adicionales.

Ejemplo:

- Una relación trivial es refleja, simétrica, antisimétrica y transitiva.

- Si $E = \emptyset$, entonces $\mathcal{P}(E) = \{\emptyset\}$. Por lo tanto, hay sólo una relación en $\mathcal{P}(\emptyset)$, que es una relación trivial y cuyas propiedades son las señaladas en el punto anterior.
- De lo que sabemos de la teoría de conjuntos, la relación de inclusión de conjuntos ($\subseteq$) en $\mathcal{P}(E)$ es refleja, no es simétrica, es antisimétrica y transitiva cuando $E \neq \emptyset$.
- Para $A \neq \emptyset$ no vacío y $f : A \to B$ una función dada, la relación $\{(a, b) \in A \times A : f(a) = f(b)\}$:
  - es refleja, porque $f(a) = f(a)$ para todo $a \in A$..
  - es simétrica, porque para todo $a, b \in A$, $f(a) = f(b)$ equivale a $f(b) = f(a)$.
  - no es antisimétrica si f no es inyectiva pues entonces existen $a \neq b$ tales que $f(a) = f(b)$ y $f(b) = f(a)$.
  - es antisimétrica si f es inyectiva puesto que si $f(a) = f(b)$ y $f(b) = f(a)$, entonces $a = b$.
  - es transitiva ya que si $f(a) = f(b)$ y $f(b) = f(c)$, entonces $f(a) = f(c)$.

$\diamondsuit$

Ejemplo (menor o igual cardinal): Si $E \neq \emptyset$ y $\mathcal{M} = \{(A, B) \in \mathcal{P}(E)^* \times \mathcal{P}(E)^* \mid \exists f : A \to B \text{ inyectiva}\}$, entonces

- cuando $E = \{a\}$, se tiene que $\mathcal{P}(E) = \{\emptyset, \{a\}\}$ por lo que $\mathcal{P}(E)^* = \{a\}$ y la relación $\mathcal{M}$ es trivial.
- cuando E tiene al menos dos elementos a y b, la relación $\mathcal{M}$:
  - es refleja: la función identidad $\mathrm{id}_A : A \to A$ muestra que $A\mathcal{M}A$.
  - no es simétrica: La función $g : \{a\} \to \{a, b\}$ dada por $g(a) = a$ es inyectiva, pero no hay función inyectiva $f : \{a, b\} \to \{a\}$ pues $f(a) = f(b) = a$. De este modo, $\{a\}\mathcal{M}\{a, b\}$ pero $\{a, b\} \not\mathcal{M} \{a\}$.
  - No es antisimétrica: $f : \{a\} \to \{b\}$ y $g : \{b\} \to \{a\}$ dadas por $f(a) = b$ y $g(b) = a$ son inyectivas, y entonces $\{a\}\mathcal{M}\{b\}$ y $\{b\}\mathcal{M}\{a\}$, pero $\{a\} \neq \{b\}$.
  - Es transitiva: pues la composición de funciones inyectivas es inyectiva.

$\diamondsuit$

Ejemplo (relación diagonal): Consideremos $\mathcal{R}_= = \{(a, b) \in A \times A : a = b\}$ que es un caso especial de la relación del ejemplo anterior con $f = \mathrm{id}_A$. Se tiene que $\mathcal{R}_=$ es:

- refleja, ya que por definición $a\mathcal{R}_=a$.
- simétrica, puesto que si $a\mathcal{R}_=b$, entonces $a = b$, luego $b\mathcal{R}_=a$.
- es antisimétrica, dado que $a\mathcal{R}_=b$ y $b\mathcal{R}_=a$ implican que $a = b$.
- es transitiva, ya que si $a, b, c \in A$ son tales que $a\mathcal{R}_=b$ y $b\mathcal{R}_=c$, entonces $a = b$ y $b = c$ con lo cual $a = c$, luego $a\mathcal{R}_=c$.

$\diamondsuit$

El último de los ejemplos, $\mathcal{R}_=$, muestra que hay relaciones que pueden ser simétricas y antisimétricas. Relaciones que cumplen con esto son escasas y están caracterizadas por ser un subconjunto de $\mathcal{R}_=$. En efecto, sea $\mathcal{R}$ es una relación en A simétrica y antisimétrica. Si $a\mathcal{R}b$, entonces por simetría, $b\mathcal{R}a$ y, por antisimetría, $a = b$. Es decir, $\mathcal{R} \subseteq \mathcal{R}_=$.

Ejemplo (congruencia): La relación $\equiv_3$ cumple lo siguiente:

- Es refleja puesto que $p - p = 0 = 3 \cdot 0$.
- Es simétrica ya que $p - q = 3k$ implica que $q - p = 3(-k)$.
- No es antisimétrica pues $0 \equiv_3 3$ y $3 \equiv_3 0$, sin embargo $0 \neq 3$.
- Es transitiva porque si $p \equiv_3 q$ y $q \equiv_3 s$, entonces existen k y ℓ tales que $p - q = 3k$ y $q - s = 3\ell$. Por lo tanto, $p - s = 3k + 3\ell = 3(k + \ell)$.

$\diamondsuit$

Divisibilidad en $\mathbb{Z}$ y en $\mathbb{N}$

Definición 5.3 (Divisibilidad) *En $\mathbb{Z}$ se define la relación **divisibilidad**, que se anota $|$, por $a|b$ si existe $q \in \mathbb{Z}$ tal que $b = qa$.*

*Cuando $a|b$, se dice que a **divide a** b, o que b **es divisible por** a, o que b **es múltiplo de** a.*

Notar que todo entero es divisible por -1 y $+1$ y que 0 es divisible por cualquier entero.

La relación divisibilidad en $\mathbb{Z}$ tiene las siguientes propiedades:

- Es refleja: para todo $p \in \mathbb{Z}$ existe $k = 1 \in \mathbb{Z}$ tal que $p = 1p$.
- No es simétrica: 2 divide a 4 pero 4 no divide a 2.
- No es antisimétrica: 2 divide a -2 y -2 divide a 2, pero $2 \neq -2$.
- Es transitiva: si $p|q$ y $q|t$, entonces existen k y ℓ en $\mathbb{Z}$ tales que $pk = q$ y $q\ell = t$. Luego, $pk\ell = t$ y como $k\ell \in \mathbb{Z}$, se concluye que $p|t$.

Consideremos ahora la relación que se obtiene de la divisibilidad en $\mathbb{Z}$ al restringir el dominio y codominio a $\mathbb{N}$. ¿Qué cambia?.

Es importante observar que como en $\mathbb{Z}$ la divisibilidad es refleja y transitiva, entonces lo seguirá siendo en $\mathbb{N}$. Esto se debe a que para que una relación sea refleja, simétrica, antisimétrica o transitiva, ciertos predicados deben ser verdaderos para todo entero, pares de enteros o tripletas de enteros, según corresponda. Como $\mathbb{N} \subseteq \mathbb{Z}$, cualquiera de estos predicados que sea verdadero para números enteros lo seguirá siendo para números naturales.

Por su parte, cuando estos predicados son falsos en $\mathbb{Z}$, no sabemos si seguirán siendo falsos en $\mathbb{N}$. Esto es así pues la falsedad de ellos se demuestra usando un contraejemplo. En el caso de la simetría el contraejemplo es $(2, 4)$ y $(4, 2)$, y en el caso de la antisimetría el contraejemplo es $(2, -2)$ y $(-2, 2)$. Como $2, 4 \in \mathbb{N}$, los pares $(2, 4)$ y $(4, 2)$ también son un contraejemplo para la simetría de la divisibilidad en $\mathbb{N}$. Por lo tanto, la divisibilidad en $\mathbb{N}$ no es simétrica. Sin embargo, como $-2 \notin \mathbb{N}$, el contraejemplo de la antisimetría en $\mathbb{Z}$ ya no es un contraejemplo en $\mathbb{N}$.

En cambio, podemos probar que divisibilidad en $\mathbb{N}$ es antisimétrica. En efecto, si $p|q$ y $q|p$, entonces $\exists k, \ell \in \mathbb{N}$ tales que $q = kp$ y $p = \ell q$. Luego, $p = \ell kp$ lo que, para $p \neq 0$, nos dice que $\ell k = 1$. Pero como $k, \ell \in \mathbb{N}$ esto ocurre sólo si $k = \ell = 1$. Por lo tanto, si $p \neq 0$, entonces $p = q$. Por otro lado, si $p = 0$, entonces $q = k0$ y, nuevamente, $p = q$. Concluimos que la relación de divisibilidad en $\mathbb{N}$ es antisimétrica.

Tipos de relaciones

Hay dos grandes familias de relaciones que ocurren con frecuencia en matemáticas: las relaciones de orden y las de equivalencia.

Definición 5.4 (Relación de orden) *$\mathcal{R}$ es una **relación de orden** en A, o simplemente un **orden en** A, si es una relación en A que es refleja, antisimétrica y transitiva.*

Para $x, y \in A$ decimos que:

- *x **precede** a y si $x\mathcal{R}y$.*
- *$x, y \in A$ son **comparables** si se cumple que $x\mathcal{R}y$ o $y\mathcal{R}x$. Es decir, si x precede a y, o y precede a x.*

*Decimos que $\mathcal{R}$ es un **orden total** si para todo $x, y \in A$, x e y son comparables.*

Definición 5.5 (Relación de equivalencia) *$\mathcal{R}$ es una **relación de equivalencia** en A si es una relación en A que es refleja, simétrica y transitiva.*

Retomamos los ejemplos para ver si corresponden a relaciones de orden, de equivalencia o de ningún tipo. Cuando sean de orden también discutiremos si son órdenes totales.

Ejemplo:

- Una relación trivial es refleja, simétrica, antisimétrica y transitiva por lo que es de orden y de equivalencia. Lo mismo ocurre con la relación $\mathcal{R}_=$. Una relación trivial es un orden total pero $R_=$ no lo es a menos que sea trivial.
- La divisibilidad en $\mathbb{Z}$ es refleja y transitiva y no es ni simétrica, ni antisimétrica.

  Por lo tanto no es de orden ni de equivalencia.
- La divisibilidad en $\mathbb{N}$ es refleja, antisimétrica y transitiva, pero no es simétrica.

  Por lo tanto es de orden pero no de equivalencia. No es un orden total pues los números 3 y 5 (claramente) no son comparables.
- La relación $\equiv_3$ es refleja, simétrica y transitiva, y no es antisimétrica.

  Por lo tanto, es una relación de equivalencia y no de orden.
- Ya vimos que $\{(A, B) \in \mathcal{P}(E)^* \times \mathcal{P}(E)^* \mid \exists f : A \to B \text{ inyectiva } \}$ es refleja y transitiva pero que no es ni simétrica ni antisimétrica.

  Por lo tanto, no es de orden ni de equivalencia.
- La relación inclusión de conjuntos ($\subseteq$) en $\mathcal{P}(E)$, si $E \neq \emptyset$, entonces $\subseteq$ es refleja, antisimétrica y transitiva. Pero no es simétrica.

  Por lo tanto es de orden pero no de equivalencia.

  Si $E = \{a\}$, entonces $\mathcal{P}(E) = \{\emptyset, \{a\}\}$ y $\subseteq$ es un orden total. Si E tiene al menos dos elementos a y b, entonces los subconjuntos $\{a\}$ y $\{b\}$ no son comparables lo que hace que, en este caso, $\subseteq$ no sea un orden total.

- Consideremos de nuevo $\mathcal{I} = \{(A, B) \in \mathcal{P}(E)^* \times \mathcal{P}(E)^* \mid \exists f : A \to B \text{ biyectiva }\}$. Como en el ejemplo anterior, si E tiene un sólo elemento, la relación es trivial. Veamos qué propiedades se tienen cuando en E hay al menos dos elementos a y b, $a \neq b$.
  - Es refleja: la función identidad $\mathrm{id}_A : A \to A$ muestra que $A\mathcal{I}A$.
  - Es simétrica: Si $f : A \to B$ es biyectiva entonces f tiene función inversa f^{-1} y $f^{-1} : B \to A$ es una biyección. Entonces, $\mathcal{I}$ es simétrica.
  - No es antisimétrica. El mismo ejemplo que dimos para la relación $\mathcal{M}$ funciona aquí pues las funciones $f : \{a\} \to \{b\}$ y $g : \{b\} \to \{a\}$ dadas por $f(a) = b$ y $g(b) = a$ son biyectivas.
  - Es transitiva: pues la composición de funciones biyectivas es biyectiva.

  Entonces, $\mathcal{I}$ es una relación de equivalencia pero no es una relación de orden.
- Para $A \neq \emptyset$ no vacío y $f : A \to B$ una función dada, la relación $\{(a, b) \in A \times A | f(a) = f(b)\}$ cumple lo siguiente:
  - Si f no es inyectiva, entonces la relación es refleja, simétrica y transitiva pero no antisimétrica.

    Por lo tanto, es una relación de equivalencia pero no de orden.
  - Si f es inyectiva, entonces corresponde a la relación $\mathcal{R}_=$, por lo que es de orden y de equivalencia.

  La relación tener el mismo símbolo verificador en el R.U.T., definida en el conjunto de las persona con R.U.T, y comenzar con la misma letra, definida en el conjunto de las palabras de un libro, son casos particulares del ejemplo anterior.

  En efecto, para la primera relación podemos tomar f como la función que dada una persona le asigna el símbolo verificador de su R.U.T.

  Lo mismo ocurre con la segunda relación al definir la función f que a cada palabra de un libro le asocia su primera letra.

  En ambos casos la función no es inyectiva por lo que las relaciones son relaciones de equivalencia pero no relaciones de orden.
- La relación $\mathcal{R}$ dada por $a\mathcal{R}b$ si a y b son palabras de un diccionario de Español donde a aparece antes que b o bien $a = b$ es un orden total.

  En efecto, al permitir que $a = b$ se logra que sea refleja.

  Como no puede ocurrir que una palabra a aparezca antes que una palabra b y que la palabra b aparezca antes que la palabra a, la única forma que $a\mathcal{R}b$ y $b\mathcal{R}a$ es que $a = b$, con lo que $\mathcal{R}$ es antisimétrica.

  Suponiendo que las palabras *estudio* y *trabajo* aparecen en el diccionario, entonces *estudio*$\mathcal{R}$*trabajo* y *trabajo*$\not\mathcal{R}$ *estudio*, lo que muestra que $\mathcal{R}$ no es simétrica.

  Si una palabra a aparece antes que una palabra b y la palabra b aparece antes que una palabra c, se tendrá que la palabra a aparece antes que la palabra c.

  Luego, $\mathcal{R}$ no es una relación de equivalencia pero sí es una relación de orden.

  Dos palabras que aparecen en un diccionario de Español siempre son comparables por lo que $\mathcal{R}$ es una relación de orden total.

$\diamondsuit$

Guía Básica

Determinar la veracidad de las siguientes afirmaciones:

1. Sea $f : A \to B$, se tiene que f es inyectiva $\iff f(A) = B$.
2. Sea $f : A \to B$, se tiene que f es inyectiva $\implies f(A) = B$.
3. Sea $f : A \to B$, se tiene que f es epiyectiva $\iff f(A) = B$.
4. Sea $f : A \to B$, se tiene que f es epiyectiva $\implies f(A) = B$.
5. Sea $f : A \to B$ y $A_1, A_2 \subseteq A$, si $f(A_1) \subseteq f(A_2) \implies A_1 \subseteq A_2$.
6. Sea $f : A \to B$ y $A_1, A_2 \subseteq A$, si $A_1 \subseteq A_2 \implies f(A_1) \subseteq f(A_2)$.
7. Sea $f : A \to B$ y $A_1, A_2 \subseteq A$, entonces $f(A_1 \cap A_2) \subseteq f(A_1) \cap f(A_2)$.
8. Sea $f : A \to B$ inyectiva y $A_1, A_2 \subseteq A$, entonces $f(A_1 \cap A_2) = f(A_1) \cap f(A_2)$.
9. Sea $f : A \to B$ y $A_1, A_2 \subseteq A$, entonces $f(A_1 \cup A_2) = f(A_1) \cup f(A_2)$.
10. Sea $f : A \to B$ y $B_1, B_2 \subseteq B$, si $B_1 \subseteq B_2 \implies f^{-1}(B_1) \subseteq f^{-1}(B_2)$.
11. Sea $f : A \to B$ y $B_1, B_2 \subseteq B$, $f^{-1}(B_1 \cap B_2) = f^{-1}(B_1) \cap f^{-1}(B_2)$.
12. Sea $f : A \to B$ y $B_1, B_2 \subseteq B$, $f^{-1}(B_1 \cup B_2) = f^{-1}(B_1) \cup f^{-1}(B_2)$.
13. Sea $f : A \to B$, entonces si $A' \subseteq A \implies A' \subseteq f^{-1}(f(A'))$.
14. Sea $f : A \to B$, entonces si $B' \subseteq B \implies f(f^{-1}(B')) \subseteq B'$.
15. Sea $f : A \to B$, entonces si $B' \subseteq B \implies B' \subseteq f(f^{-1}(B'))$.
16. Sea $f : A \to B$ inyectiva, entonces si $A' \subseteq A \implies A' = f^{-1}(f(A'))$.
17. Sea $f : A \to B$ epiyectiva, entonces si $A' \subseteq A \implies A' = f^{-1}(f(A'))$.
18. Sea $f : A \to B$ inyectiva, $B' \subseteq B \implies f(f^{-1}(B')) = B'$.
19. Sea $f : A \to B$ epiyectiva, $B' \subseteq B \implies f(f^{-1}(B')) = B'$.
20. Una relación $\mathcal{R} \subseteq A \times A, \mathcal{R} \neq \emptyset$ siempre cumple alguna de las siguientes propiedades: $\mathcal{R}$ es refleja, $\mathcal{R}$ es simétrica, $\mathcal{R}$ es antisimétrica, $\mathcal{R}$ es transitiva.
21. $\mathcal{R} = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x = 2y\}$ es una relación refleja.
22. $\mathcal{R} = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x = 2y\}$ es una relación simétrica.
23. $\mathcal{R} = \{(x, y) \in \mathbb{R} \setminus \{0\} \times \mathbb{R} \setminus \{0\} \mid \exists k \in \mathbb{N}, \frac{x}{y} = 2k\}$ es una relación refleja.
24. $\mathcal{R} = \{(x, y) \in \mathbb{R} \setminus \{0\} \times \mathbb{R} \setminus \{0\} \mid \exists k \in \mathbb{N}, \frac{x}{y} = 2k\}$ es una relación simétrica.
25. $\mathcal{R} = \{(x, y) \in \mathbb{R} \setminus \{0\} \times \mathbb{R} \setminus \{0\} \mid \exists k \in \mathbb{N}, \frac{x}{y} = 2k\}$ es una relación transitiva.
26. $\mathcal{R} = \{(x, y) \in \mathbb{N} \setminus \{0\} \times \mathbb{N} \setminus \{0\} \mid \exists k \in \mathbb{N}, \frac{x}{y} \leq 3k\}$ es una relación simétrica.
27. Sea $r \in \mathbb{R}$, $\mathcal{R} = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x^2 + y^2 = r^2\}$ es una relación simétrica.
28. Sea $r \in \mathbb{R}$, $\mathcal{R} = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x^2 + y^2 = r^2\}$ es una relación antisimétrica.
29. Sea $r \in \mathbb{R}$, $\mathcal{R} = \{(x, y) \in [-r, r] \times [-r, r] \mid x^2 + y^2 = r^2\}$ es una relación refleja.
30. Sea $r \in \mathbb{R}$, $\mathcal{R} = \{(x, y) \in [-r, r] \times [-r, r] \mid x^2 + y^2 = r^2\}$ es una relación simétrica.
31. $\mathcal{R} = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x^2 + y^2 = r^2, r \in \mathbb{R}\}$ es una relación antisimétrica.

32. $\mathcal{R} = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x^2 + y^2 = r^2, r \in \mathbb{R}\}$ es una relación transitiva.
33. Una relación simétrica nunca es antisimétrica.
34. Una relación antisimétrica nunca es simétrica.
35. La $=$ es una relación que es simétrica y antisimétrica a la vez.
36. La única relación simétrica y antisimétrica a la vez es la igualdad.
37. No existen relaciones que sean de equivalencia y de orden a la vez.
38. $\mathcal{R} = \{(x, y) \in \mathbb{Z} \setminus \{0\} \times \mathbb{Z} \setminus \{0\} \mid xy \leq 0\}$ es una relación refleja.
39. $\mathcal{R} = \{(x, y) \in \mathbb{Z} \setminus \{0\} \times \mathbb{Z} \setminus \{0\} \mid xy \leq 0\}$ es una relación antisimétrica.
40. $\mathcal{R} = \{(x, y) \in \mathbb{Z} \setminus \{0\} \times \mathbb{Z} \setminus \{0\} \mid xy > 0\}$ es una relación transitiva.
41. $\mathcal{R} = \{(x, y) \in \mathbb{Z} \setminus \{0\} \times \mathbb{Z} \setminus \{0\} \mid xy < 0\}$ es una relación transitiva.
42. $\mathcal{R} = \{(x, y) \in [0, \infty) \times [0, \infty) \mid x \geq 0\}$ es una relación refleja.
43. $\mathcal{R} = \{(x, y) \in [0, \infty) \times [0, \infty) \mid x \geq 0\}$ es una relación simétrica.
44. $\mathcal{R} = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x \leq 0\}$ es una relación antisimétrica.
45. $\mathcal{R} = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x \leq 0\}$ es una relación transitiva.
46. Sea A el conjunto de alumnos de primer año. La relación en A, dada por $a_1 \mathcal{R} a_2 \iff$ a_1 tiene mejor nota que a_2, es una relación de orden.
47. Sea A el conjunto de alumnos de primer año. La relación en A, dada por $a_1 \mathcal{R} a_2 \iff$ a_1 tiene mejor o igual nota que a_2, es una relación de orden total.
48. Sea A el conjunto de alumnos de primer año. La relación en A, dada por $a_1 \mathcal{R} a_2 \iff$ a_1 tiene mejor o igual nota que a_2, es una relación de orden que no es total.
49. $\mathcal{R} = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x < y\}$ es una relación de orden total.
50. $\mathcal{R} = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x < y\}$ es una relación de orden que no es total.

Guía de Ejercicios

1. Dados dos conjuntos A y B, determine el conjunto imagen de las siguientes funciones.

   a) $\pi_A : A \times B \to A$, dada por $\forall (a, b) \in A \times B,\ \pi_A((a, b)) = a$.
   b) $\pi_B : A \times B \to B$, dada por $\forall (a, b) \in A \times B,\ \pi_B((a, b)) = b$.
   c) $d_A : A \to A \times B$, dada por $\forall a \in A,\ d_A(a) = (a, a)$.
   d) $\tau : A \times B \to B \times A$, dada por $\forall (a, b) \in A \times B, \tau((a, b)) = (b, a)$.
   e) Dado $b_0 \in B$ fijo. $f : A \to A \times B$, dada por $\forall a \in A,\ f(a) = (a, b_0)$.

2. Dado un conjunto $A \neq \emptyset$ y $B \subseteq A$ fijo, determine el conjunto imagen de las siguientes funciones. Además, determine la preimagen de los conjuntos $\mathcal{C}_1 = \{B\}$, $\mathcal{C}_2 = \{A\}$ y $\mathcal{C}_3 = \{A, \emptyset\}$.

   a) $f : \mathcal{P}(A) \to \mathcal{P}(A)$, dada por $\forall X \subseteq A,\ f(X) = A \setminus X$.
   b) $g : \mathcal{P}(A) \to \mathcal{P}(A)$, dada por $\forall X \subseteq A,\ g(X) = X \setminus (A \setminus X)$.

c) $h_1 : \mathcal{P}(A) \to \mathcal{P}(A)$, dada por $\forall X \subseteq A,\ h_1(X) = X \cap B$.
d) $h_2 : \mathcal{P}(A) \setminus \{\emptyset\} \to \mathcal{P}(A)$, dada por $\forall X \subseteq A,\ h_2(X) = X \cup B$.
e) $h_3 : \mathcal{P}(A) \to \mathcal{P}(A)$, dada por $\forall X \subseteq A,\ h_3(X) = X \triangle B$.

3. Dadas $f : A \to B$, función y $A_1, A_2 \subseteq A$, demuestre las siguientes propiedades enunciadas en el texto del apunte:

a) f es sobreyectiva $\iff f(A) = B$.
b) $f(A_1 \cap A_2) \subseteq f(A_1) \cap f(A_2)$.
c) $f(A_1 \cup A_2) = f(A_1) \cup f(A_2)$.
d) $A_1 \subseteq f^{-1}(f(A_1))$

4. Dadas $f : A \to B$, función y $B_1, B_2 \subseteq B$, demuestre las siguientes propiedades:

a) $B_1 \subseteq B_2 \implies f^{-1}(B_1) \subseteq f^{-1}(B_2)$.
b) $f^{-1}(B_1 \cup B_2) = f^{-1}(B_1) \cup f^{-1}(B_2)$.
c) $f(f^{-1}(B_1)) \subseteq B_1$.
d) $f^{-1}(B_1^c) = (f^{-1}(B_1))^c$.
e) $f^{-1}(B_1 \triangle B_2) = f^{-1}(B_1) \triangle f^{-1}(B_2)$.

5. Estudie si las siguientes relaciones son o no reflejas. En caso que no lo sean, para demostrarlo, enuncie un contraejemplo.

a) $\mathcal{R} = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid y = ax + b\}$, con $a \neq 0$.
b) $\mathcal{R} = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid y = ax + b \wedge y = ax + d\}$, con $a \neq 0, b \neq d$.
c) $\mathcal{R} = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid y = ax + b \wedge y = cx + d\}$, con $ac = -1$.
d) $\mathcal{R} = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid y \leq ax + b \wedge y \leq cx + d\}$, con $b, d > 0$.
e) $\mathcal{R} = \{(x, y) \in [-r, r] \times [-r, r] \mid y^2 + x^2 \leq r^2 \wedge |y| \leq \frac{r}{2}\}$, con $r > 0$.
f) $\mathcal{R} = \{(x, y) \in [-\frac{r}{2}, \frac{r}{2}] \times [-r, r] \mid y^2 + x^2 \leq r^2 \wedge |y| \leq \frac{r}{2}\}$, con $r > 0$.
g) $\mathcal{R} = \{(x, y) \in [-\frac{r}{2}, \frac{r}{2}] \times [-r, r] \mid y^2 + x^2 \leq r^2\}$, con $r > 0$.

6. Estudie si las siguientes relaciones son o no simétricas. En caso que no lo sean, para demostrarlo, enuncie un contraejemplo.

a) $\mathcal{R} = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid y \neq x\}$
b) $\mathcal{R} = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid y = x\}$
c) $\mathcal{R} = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid y^2 = x^2\}$
d) $\mathcal{R} = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid |y| = x\}$
e) $\mathcal{R} = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid xy = 2k, k \in \mathbb{Z}\}$
f) $\mathcal{R} = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid xy < 0\}$

7. Estudie si las siguientes relaciones son o no antisimétricas. En caso que no lo sean, para demostrarlo, enuncie un contraejemplo.

a) $\mathcal{R} = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid y \neq x\}$
b) $\mathcal{R} = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid y < x\}$
c) $\mathcal{R} = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid y \geq x\}$

d) $\mathcal{R} = \{(x,y) \in \mathbb{R} \times \mathbb{R} \mid |y| = x\}$
e) $\mathcal{R} = \{(x,y) \in \mathbb{R} \times \mathbb{R} \mid xy = 2k, \text{ para algún } k \in \mathbb{N}\}$

8. Estudie si las siguientes relaciones son o no transitivas. En caso que no lo sean, para demostrarlo, enuncie un contraejemplo.

a) $\mathcal{R} = \{(x,y) \in \mathbb{R} \times \mathbb{R} \mid y \neq x\}$.
b) $\mathcal{R} = \{(x,y) \in \mathbb{R} \times \mathbb{R} \mid |y| \geq x\}$
c) $\mathcal{R} = \{(x,y) \in \mathbb{R} \times \mathbb{R} \mid y^2 < x^3\}$
d) $\mathcal{R} = \{(x,y) \in \mathbb{R} \times \mathbb{R} \mid xy = 1\}$
e) $\mathcal{R} = \{(x,y) \in \mathbb{R} \times \mathbb{R} \mid x^y \in \mathbb{Q}\}$
f) $\mathcal{R} = \{(x,y) \in \mathbb{R} \times \mathbb{R} \mid x - y = pk, \text{ para algún } k \in \mathbb{Q}\}$

Guía de Problemas

1. (10 min.) Considere las funciones $f : \mathbb{N} \setminus \{0\} \to \mathbb{Q}$ definida en cada $n \in \mathbb{N} \setminus \{0\}$ por $f(n) = \frac{1}{2n}$ y $g : \mathbb{Q} \to \mathbb{Q}$ definida en cada $q \in \mathbb{Q}$ por $g(q) = \frac{q}{2}$. Determine los conjuntos preimagenes $g^{-1}(\mathbb{Z})$ y $(g \circ f)^{-1}(\mathbb{Z})$
2. (30 min.) Sea $f : X \to Y$ una función. Pruebe que $\forall A, B \subseteq X$

$$f(A) \triangle f(B) \subseteq f(A \triangle B).$$

Muestre ademas que si f es inyectiva, entonces

$$f(A) \triangle f(B) = f(A \triangle B).$$

3. (20 min.) Sea $f : E \to F$ una función y $A, B \subseteq E$. Pruebe que

$$f(B) \backslash f(A) = \phi \implies f(A \cup B) = f(A).$$

4. Sobre un conjunto de proposiciones $\mathcal{P}$ lógicas se define la relación $\mathcal{R}$ por

$$p \mathcal{R} q \iff (p \wedge q \iff q).$$

Además, para $p, q \in \mathcal{P}$ se dice que $p = q$ si y solo si $p \iff q$.

a) (20 min.) Demuestre que $\mathcal{R}$ es una relación de orden sobre $\mathcal{P}$.
b) (10 min.) Pruebe que $\mathcal{R}$ es una relacion de orden total.

5. (30 min.) Sea A el conjunto de todas las relaciones binarias en $\mathbb{R}$. Sobre A definamos la relación binaria Ω siguiente:
Sean $\mathcal{R}_1, \mathcal{R}_2 \in A$, entonces

$$\mathcal{R}_1 \Omega \mathcal{R}_2 \iff (\forall x, y \in \mathbb{R}, x \mathcal{R}_1 y \implies x \mathcal{R}_2 y).$$

Pruebe que Ω es una relación de orden. Muestre además que Ω no es un orden total en A.

SEMANA 07:

Relaciones

5.2 Relaciones de equivalencia

Nos concentraremos ahora en el estudio más detallado de las relaciones de equivalencia, o sea, las relaciones que son reflejas, simétricas y transitivas.

Lo que se pretende con una relación de equivalencia $\mathcal{R}$ en A es definir un criterio de semejanza entre los elementos de A que permita clasificarlos. Los elementos semejantes a un elemento dado $a \in A$, son todos aquellos que se relacionan con a.

Definición 5.6 (Clase de equivalencia) *Dado un elemento $a \in A$, definimos la* ***clase de equivalencia de*** *a* ***asociada a*** *$\mathcal{R}$ como el conjunto*

$$[a]_{\mathcal{R}} = \{x \in A \mid a\mathcal{R}x\} \subseteq A.$$

Ejemplo: Veamos cuáles son las clases de equivalencia de algunas de las relaciones de equivalencia que hemos estudiado en ejemplos anteriores.

- $\mathcal{R}_{=} = \{(a,b) \in A \times A \mid f(a) = f(b)\}$ en $A \neq \emptyset$: La clase de equivalencia de $a \in A$ es $[a]_{\mathcal{R}} = \{b \in A \mid f(b) = f(a)\}$. Es decir, $[a]_{\mathcal{R}}$ es la pre-imagen por f de $\{f(a)\}$.

  Para hacerlo más concreto, consideremos la relación $\mathcal{R}$ en el conjunto de las palabras de un libro donde a y b están relacionadas si comienzan con la misma letra.

  Calculemos en este caso las clases de equivalencia de algunas palabras: la clase $[hola]_{\mathcal{R}}$ es el conjunto de todas las palabras del libro que comienzan con h, mientras que $[casa]_{\mathcal{R}}$ es el conjunto de todas las palabras que comienzan con c.

  En este ejemplo, notemos que podemos escribir

  $$A = [ahora]_{\mathcal{R}} \cup [bote]_{\mathcal{R}} \cup [casa]_{\mathcal{R}} \cup \ldots \cup [zorro]_{\mathcal{R}}.$$

  Además, se tiene que $[tapa]_{\mathcal{R}} \cap [velero]_{\mathcal{R}} = \emptyset$, y que $[manzana]_{\mathcal{R}} = [menos]_{\mathcal{R}}$.
- Veamos ahora cuáles son las clases de equivalencia de la relación $\equiv_3$. Recordemos que ésta está dada por $p \equiv_3 q$ si $p - q = 3k$, para algún $k \in \mathbb{Z}$.

  La clase de equivalencia de 0 es el conjunto $\{q \in \mathbb{Z} \mid \exists k \in \mathbb{Z}, q = 3k\}$. Es decir, el conjunto de los múltiplos de 3 en $\mathbb{Z}$.

La clase de equivalencia de 1 es el conjunto $\{q \in \mathbb{Z} \mid \exists k \in \mathbb{Z}, q-1=3k\}$. Éste es el conjunto de los múltiplos de 3 más 1. Notemos que las clases de equivalencia del 0 y del 1 no tienen elementos en común pues no hay ningún entero que sea múltiplo de 3 y a la vez múltiplo de 3 más 1.

Debiese ser claro ahora que si tomamos $p \in \{0,1,2\}$, entonces la clase de equivalencia de p es el conjunto de los múltiplos de 3 más p.

¿Cuál es la clase de equivalencia de 3? Si leemos con cuidado la definición de la relación $\equiv_3$ nos daremos cuenta que esta clase es la misma que la del 0, es decir, el conjunto de los múltiplos de 3.

De aquí podemos ver que esta relación tiene sólo 3 clases de equivalencia: $[0]_{\equiv_3}, [1]_{\equiv_3}$ y $[2]_{\equiv_3}$, y éstas son disjuntas de a pares. Más aún, como cada entero pertenece a (sólo) una de ellas, el conjunto $\{[0]_{\equiv_3}, [1]_{\equiv_3}, [2]_{\equiv_3}\}$ es una partición de $\mathbb{Z}$.

$\diamondsuit$

Los ejemplos anteriores sugieren que el conjunto de las clases de equivalencia tiene propiedades relevantes que es deseable destacar.

Definición 5.7 (Conjunto cuociente) *Al conjunto de las clases de equivalencia de una relación de equivalencia $\mathcal{R}$ se le llama **conjunto cuociente**, y se denota $A/\mathcal{R}$.*

Esto es $A/\mathcal{R} = \{[a]_{\mathcal{R}} \mid a \in A\}$.

Notemos que los conceptos de clase de equivalencia y conjunto cuociente tienen perfecto sentido para cualquier relación. En el contexto de las relaciones de equivalencia, el conjunto cuociente posee una propiedad destacable que ha aparecido en los ejemplos anteriores y que demostraremos a continuación: el conjunto $A/\mathcal{R}$ es una partición de A.

Proposición 5.8 *Sea $\mathcal{R}$ una relación de equivalencia en A. Para todo $x, y \in A$, las siguientes afirmaciones son equivalentes.*

(I) $[x]_{\mathcal{R}} \subseteq [y]_{\mathcal{R}}$.

(II) $[x]_{\mathcal{R}} \cap [y]_{\mathcal{R}} \neq \emptyset$

(III) $x\mathcal{R}y$.

En particular: $[x]_{\mathcal{R}} \cap [y]_{\mathcal{R}} \neq \emptyset \iff [x]_{\mathcal{R}} = [y]_{\mathcal{R}}$.

Dem. Demostraremos que (I) $\Rightarrow$ (II) $\Rightarrow$ (III) $\Rightarrow$ (I) que, por la transitividad del $\Rightarrow$, implicará la equivalencia de las tres propiedades. Sean $x, y \in A$ arbitrarios.

Como $\mathcal{R}$ es refleja se tiene que $x \in [x]_{\mathcal{R}}$. Así, es claro que (I) $\Rightarrow$ (II): .

Veamos que (II) $\Rightarrow$ (III): Sea $z \in [x]_{\mathcal{R}} \cap [y]_{\mathcal{R}}$. Entonces, $x\mathcal{R}z$ y $y\mathcal{R}z$. Por la simetría de $\mathcal{R}$ se obtiene que $z\mathcal{R}y$. Por la transitividad de $\mathcal{R}$ se concluye que $x\mathcal{R}y$.

Ahora, probemos que (III) $\Rightarrow$ (I): Por la simetría tenemos que $y\mathcal{R}x$. Sea $z \in [x]_{\mathcal{R}}$ y probemos que $z \in [y]_{\mathcal{R}}$. Por la definición de $[x]_{\mathcal{R}}$ se cumple que $x\mathcal{R}z$. Como ya sabemos que $y\mathcal{R}x$

podemos invocar la transitividad de $\mathcal{R}$ para concluir que $y\mathcal{R}z$, lo que muestra que $z \in [y]_\mathcal{R}$. Por lo tanto, $[x]_\mathcal{R} \subseteq [y]_\mathcal{R}$.

Con lo que ya se demostró se tiene que $[x]_\mathcal{R} \cap [y]_\mathcal{R} \neq \emptyset$ equivale a $[x]_\mathcal{R} \subseteq [y]_\mathcal{R}$ y $[y]_\mathcal{R} \subseteq [x]_\mathcal{R}$. Como esto último equivale a $[x]_\mathcal{R} = [y]_\mathcal{R}$, se termina la demostración. □

Usaremos la propiedad anterior para demostrar que el conjunto $A/\mathcal{R}$ es una partición de A. Recordemos que esto quiere decir que:

- Cada $C \in A/\mathcal{R}$ es no vacío.
- Si $C, C' \in A/\mathcal{R}$, $C \neq C'$, entonces $C \cap C' = \emptyset$.
- $A/\mathcal{R}$ cubre A. Es decir, para todo $x \in A$, existe $C \in A/\mathcal{R}$ con $x \in C$.

Proposición 5.9 *Para toda relación de equivalencia $\mathcal{R}$ en un conjunto A, el conjunto $A/\mathcal{R}$ es una partición de A.*

Dem. Como $\mathcal{R}$ es refleja, todo $x \in A$ es tal que $x \in [x]_\mathcal{R}$. De aquí obtenemos dos conclusiones: cada elemento de $A/\mathcal{R}$ es no vacío y el conjunto $A/\mathcal{R}$ cubre el conjunto A.

Por su parte, la Propiedad 5.8 nos dice que los conjuntos en $A/\mathcal{R}$ son disjuntos de a pares pues $[x]_\mathcal{R} \cap [y]_\mathcal{R} \neq \emptyset$ equivale a $[x]_\mathcal{R} = [y]_\mathcal{R}$. □

Relación congruencia módulo n

Un tipo de relaciones de equivalencia importantes son las relaciones **de congruencia módulo** n, de las cuales ya conocemos el caso $n = 3$, desarrollado en la pág. 90.

Sea $n \in \mathbb{N}$. Se define en $\mathbb{Z}$ la relación $\equiv_n$ por

$$a \equiv_n b \iff (\exists q \in \mathbb{Z},\ a - b = qn).$$

Si $a \equiv_n b$, diremos que a y b son **congruentes módulo** n. También es habitual, anotar $a = b \mod n$, que se lee "a es igual a be módulo ene", para decir que $a \equiv_n b$.

El caso $n = 0$ es especial pues corresponde a la igualdad en $\mathbb{Z}$. Es decir, $a \equiv_0 b$ si y sólo si $a = b$. Por su parte, para $n = 1$, $\forall a, b \in Z, a \equiv_1 b$ pues para $a, b \in \mathbb{Z}$ siempre $a - b \in \mathbb{Z}$.

Como ejemplo, tenemos que $13 \equiv_3 7$ pues $13 - 7 = 6 = 2 \cdot 3$, y que $12 \equiv_5 27$, pues $12 - 27 = -15 = -3 \cdot 5$. Alternativamente, podemos decir que $13 = 7 \mod 3$ y que $12 = 27 \mod 5$; también podemos decir que $13 = 7 \mod 2$ y que $12 = 27 \mod 3$.

Con los mismos argumentos que se usaron para demostrar que $\equiv_3$ era relación de equivalencia, se puede ver que $\equiv_n$ es una relación de equivalencia en $\mathbb{Z}$.

Queremos ver ahora cómo es el conjunto cuociente $\mathbb{Z}/\equiv_n$ que anotaremos $\mathbb{Z}_n$. Para facilitar la lectura, anotaremos $[a]_n$ la clase de equivalencia de a por la relación $\equiv_n$ (en lugar de la notación genérica $[a]_{\equiv_n}$).

Con esta notación tenemos que $\mathbb{Z}_n = \{[a]_n \mid a \in \mathbb{Z}\}$.

Nos preguntamos entonces cuáles son las clases distintas de la relación $\equiv_n$.

Para $n = 0$ cada clase de equivalencia es un singleton, es decir $\mathbb{Z}_0 = \{\{x\} : x \in \mathbb{Z}\}$. Por lo recién dicho, para $n = 1$, hay sólo una clase de equivalencia $[0]_1 = \mathbb{Z}$. Para $n = 3$ se llegó a la conclusión que $\mathbb{Z}_3 = \{[0]_3, [1]_3, [2]_3\}$.

Para obtener una descripción similar en el caso general haremos uso de la división de enteros. Es decir, dados dos enteros a y m queremos calcular la así llamada división entera de a por m que consiste en encontrar dos enteros q y r, el cuociente y el resto, respectivamente, tales que $a = qm + r$ y $0 \leq r < |m|$. La existencia y unicidad de q y r, para a y m dados, se establece en el siguiente teorema.

Teorema 5.10 (Teorema de la División Entera) *Sean $a, m \in \mathbb{Z}$, $m \neq 0$. Existe un único par $q, r \in \mathbb{Z}$ tal que $a = q \cdot m + r$ y $0 \leq r < |m|$.*

En términos de la relación $\equiv_n$, el teorema anterior aplicado a enteros a y n dice que existe un único par (r, q) con $0 \leq r < n$ y $a - r = qn$. Por definición de $\equiv_n$, esto equivale a que para todo entero a existe un único r con $0 \leq r < n$ tal que $a \equiv_n r$.

Proposición 5.11 *Si $n \geq 1$, entonces $\mathbb{Z}_n$ tiene n elementos. Más aún, $\mathbb{Z}_n = \{[r]_n \mid 0 \leq r < n\}$.*

Dem. Llamemos $C = \{[r]_n \mid 0 \leq r < n\}$. Por definición de $\mathbb{Z}_n$ tenemos que $C \subseteq \mathbb{Z}_n$. Para probar que $\mathbb{Z}_n = C$ basta entonces ver que $\mathbb{Z}_n \subseteq C$.

En efecto, sea $a \in \mathbb{Z}$. Por el Teorema de la División Entera sabemos que existe r con $a \equiv_n r$ y $0 \leq r < n$. Luego, $[a]_n = [r]_n \in C$.

Más aún, supongamos que $[r]_n = [r']_n$ y $0 \leq r < r' < n$. Como $r \in [r]_n = [r']_n$, existirá un entero k tal que $r' = r + kn$. Luego, $kn = r' - r \geq 1$. Sigue que $k \geq 1$ y que $r' \geq r + n \geq n$, contradicción. Se concluye que $[0]_n, \ldots, [n-1]_n$ son elementos distintos de $\mathbb{Z}_n$. □

Ejemplo: Sea $a > 0$ un número real y consideremos la relación $\mathcal{R}$ en $\mathbb{R}$ dada por $x\mathcal{R}y$ si existe $k \in \mathbb{Z}$ con $x - y = ak$. Notemos que mirado con atención esto es muy similar a lo hecho con las congruencias módulo n. En realidad, corresponde a extender esta definición desde $\mathbb{Z}$ a $\mathbb{R}$, reemplazando $n \in \mathbb{N}$ por $a > 0$.

No es difícil ver que $\mathcal{R}$ es una relación de equivalencia. La demostración es idéntica a lo ya hecho sólo que cambiamos $\mathbb{Z}$ por $\mathbb{R}$ y n por $a > 0$.

También es cierto que dado $x \in \mathbb{R}$ existe un único $y \in [0, a)$ tal que $x\mathcal{R}y$. En efecto, el conjunto $\{[ka, (k+1)a) \mid k \in \mathbb{Z}\}$ es una partición de $\mathbb{R}$ por lo que para cada x existe un único k tal que $x \in [ka, (k+1)a)$. Entonces, $y = x - ka \in [0, a)$ y, obviamente, cumple que $x - y = ka$.

Además, dos elementos distintos $x, y \in [0, a)$ no pueden estar relacionados pues $0 < |x - y| < a$ y, si lo estuvieran, entonces $x - y = ka$, para algún $k \in \mathbb{Z} \setminus \{0\}$, lo que implicaría que $|x - y| \geq a$.

Podemos concluir que el conjunto cuociente de $\mathcal{R}$ está dado por $\{[x]_{\mathcal{R}} \mid x \in [0, a)\}$.

Llamaremos a esta relación **congruencia módulo** a **en** $\mathbb{R}$ y anotaremos $x = y \mod a$ en lugar de decir $\exists k \in \mathbb{Z}$ tal que $x = y + ka$.

Un caso que aparece con frecuencia cuando se usan las funciones trigonométricas es la relación $\mod 2\pi$. Así, sabemos que

$$\cos\theta = \cos\alpha \ \wedge \ \operatorname{sen}\theta = \operatorname{sen}\alpha \iff \theta = \alpha \mod 2\pi.$$

$\diamondsuit$

SEMANA 07:

Sumatorias

Ingeniería Matemática
FACULTAD DE CIENCIAS
FÍSICAS Y MATEMÁTICAS
UNIVERSIDAD DE CHILE

En esta sección formalizaremos el significado de calcular la suma: $a_0+a_1+\cdots+a_n$, donde a_i son números reales. Veremos que este formalismo recupera todos los manejos intuitivos y nos entrega una herramienta muy eficaz para manipular estas sumas. En cierto modo, veremos que el referido formalismo puede ser considerado como simple notación, y posteriormente veremos como trabajar y manipular esta útil nueva notación.

6.1 Definiciones y propiedades básicas

Definición 6.1 (Secuencia de números reales) *Una* ***secuencia de números reales*** *es una función $a : I \to \mathbb{R}$, donde $I \subseteq \mathbb{N}$.*

Por comodidad, una secuencia también se anotará $a = (a_i)_{i\in I}$, donde $a_i = a(i)$, para todo $i \in I$.

Si el conjunto de índices $I = \{i \in \mathbb{N} \mid i \geq m\}$, denotaremos la secuencia $(a_i)_{i\in I}$ por $(a_i)_{i\geq m}$. Cuando trabajemos con una secuencia $(a_i)_{i\in I}$, asumiremos $a_i = 0$ si $i \notin I$.

Es importante notar que $a = (a_i)_{i\in I} = (a_j)_{j\in I} = (a_x)_{x\in I}$. Es decir, i, j y x son índices mudos.

Sea $(a_i)_{i\in I}$ una secuencia de números reales. Como acabamos de decir, en esta sección estudiaremos propiedades y métodos de cálculo para las sumas de los elementos a_i con $i \in I$.

Introduciremos para este efecto una notación especial: $\sum_{i\in I} a_i$. Al símbolo $\sum$ lo llamaremos **sumatoria**. Partiremos considerando $I = [m..n] = \{m, \ldots, n\}$.[7] Formalmente,

Definición 6.2 (Sumatoria) *Sea $(a_i)_{i\geq m}$ una secuencia de números reales.*

Para $n \geq m$, definimos la sumatoria de los términos $a_m, a_{m+1}, \ldots, a_n$, por la siguiente recurrencia:

$$\sum_{k=m}^{n} a_k = \begin{cases} a_m, & \text{si } n = m, \\ a_n + \sum_{k=m}^{n-1} a_k, & \text{si } n > m. \end{cases}$$

[7] Si $n < m$, entonces $[m..n] = \emptyset$.

Tomaremos como convención que $\sum_{k=m}^{n} a_k = 0$ para $n < m$.

Ejemplo: El segundo ejemplo que dimos del principio de inducción nos mostró que

$$1 + 2 + \cdots + n = n(n+1)/2.$$

Considerando la secuencia $(k)_{k\geq 1}$, lo podemos escribir como $\sum_{k=1}^{n} k = n(n+1)/2$. $\diamondsuit$

La sumatoria cumple la siguiente lista de propiedades:

Proposición 6.3 *Sea $\lambda \in \mathbb{R}$, y sean $(a_k)_{k\geq m}$, $(b_k)_{k\geq m}$ dos secuencias. Para todo $n \geq m$ se tiene:*

(1) $\displaystyle\sum_{k=m}^{n} 1 = n - m + 1.$ (Secuencia constante igual a 1)

(2) $\displaystyle\sum_{k=m}^{n} \lambda \cdot a_k = \lambda \cdot \sum_{k=m}^{n} a_k.$ (Factorización de constantes)

(3) $\displaystyle\sum_{k=m}^{n} (a_k \pm b_k) = \sum_{k=m}^{n} a_k \pm \sum_{k=m}^{n} b_k$ (Sumatoria de dos secuencias)

(4) $\displaystyle\sum_{k=m}^{n} a_k = \sum_{k=m+s}^{n+s} a_{k-s} = \sum_{k=m-s}^{n-s} a_{k+s}.$ (Traslación de índices, para $s \in \mathbb{N}$)

(5) $\displaystyle\sum_{k=m}^{n} a_k = \sum_{k=m}^{s} a_k + \sum_{k=s+1}^{n} a_k.$ (Separación del conjunto de índices, para $m \leq s < n$)

(6) $\displaystyle\sum_{k=m}^{n} (a_k - a_{k+1}) = a_m - a_{n+1}.$ (Propiedad telescópica.)

Dem. Demostraremos (1) y (6).

Para (1): Lo haremos usando el principio de inducción sobre $n \geq m$.

El caso base ($n = m$) corresponde a $\sum_{k=m}^{m} 1 = (m - m + 1)$. Esto es directo, pues ambos lados valen 1.

Supongamos ahora que $\sum_{k=m}^{n} 1 = (n - m + 1)$. Entonces

$$\sum_{k=m}^{n+1} 1 = 1 + \sum_{k=m}^{n} 1 = 1 + (n - m + 1) = (n + 1) - m + 1.$$

Para (6): Nuevamente aplicaremos el principio de inducción sobre $n \geq m$.

Si $n = m$, el resultado se reduce a demostrar que

$$\sum_{k=m}^{m} (a_k - a_{k+1}) = a_m - a_{m+1},$$

lo cual es directo gracias a la definición de sumatoria.

Supongamos ahora que $\sum_{k=m}^{n}(a_k - a_{k+1}) = a_m - a_{n+1}$. Entonces

$$\sum_{k=m}^{n+1}(a_k - a_{k+1}) = (a_{n+1} - a_{n+2}) + \sum_{k=m}^{n}(a_k - a_{k+1}) = (a_{n+1} - a_{n+2}) + (a_m - a_{n+1}) = a_m - a_{n+2},$$

donde la segunda igualdad es válida por la hipótesis de inducción. □

En los siguientes ejemplos veremos cómo las propiedades anteriores nos ayudan a calcular sumatorias.

Ejemplo: Verifiquemos que $\sum_{k=0}^{n} k^2 = n(n+1)(2n+1)/6$.

Aquí lo haremos directamente, notando que para cualquier $k \in [0..n]$ se tiene que

$$(k+1)^3 = k^3 + 3k^2 + 3k + 1 \Leftrightarrow k^2 = \left((k+1)^3 - k^3 - (3k+1)\right)/3.$$

Por lo que, en lugar de calcular la sumatoria $\sum_{k=0}^{n} k^2$, calcularemos

$$\sum_{k=0}^{n}((k+1)^3 - k^3 - (3k+1))/3.$$

A primera vista esto parece un despropósito. Sin embargo, veremos que es una manera simple de calcular la sumatoria pedida. La razón es que la nueva sumatoria se separa en dos sumas fáciles de calcular. La primera, $\sum_{k=0}^{n}(3k+1)/3$, se puede calcular de inmediato usando las propiedades de la sumatoria y sumatorias conocidas.

$$\sum_{k=0}^{n}(3k+1)/3 = \sum_{k=0}^{n} k + \sum_{k=0}^{n}(1/3) = n(n+1)/2 + (n+1)/3.$$

Por otra parte, $\sum_{k=0}^{n}((k+1)^3 - k^3)$ es un ejemplo de suma telescópica cuyo valor es $(n+1)^3$.

Factorizando adecuadamente se obtiene que

$$\begin{aligned}\sum_{k=0}^{n} k^2 &= (n+1)^3/3 - (n+1)n/2 - (n+1)/3 = (2(n+1)^2 - 3n - 2)(n+1)/6 \\ &= (2n^2 + n)(n+1)/6 = n(2n+1)(n+1)/6.\end{aligned}$$

Verifique como ejercicio que $\sum_{k=0}^{n} k^3 = \left(\frac{n(n+1)}{2}\right)^2$. ♢

Ejemplo (sumatoria de una progresión geométrica): Verifiquemos que $\sum_{i=0}^{n} r^i = (r^{n+1} - 1)/(r-1)$, para $r \neq 1$.

Tenemos que para todo $i \geq 0$, $r^{i+1} - r^i = r^i(r-1)$. Para $r \neq 1$, lo anterior implica que $(r^{i+1} - r^i)/(r-1) = r^i \quad (*)$. Por lo tanto,

$$\begin{aligned}
\sum_{i=0}^{n} r^i &= \sum_{i=0}^{n} (r^{i+1} - r^i)/(r-1) && \text{(igualdad (*))} \\
&= (\sum_{i=0}^{n} (r^{i+1} - r^i))/(r-1) && \text{(constantes salen de una sumatoria)} \\
&= (r^{n+1} - r^0)/(r-1) && \text{(propiedad telescópica)} \\
&= (r^{n+1} - 1)/(r-1) && (r^0 = 1)
\end{aligned}$$

♢

Ejemplo: Para $a, b \in \mathbb{R}$, $a \neq b$, verifiquemos que $\sum_{k=0}^{n} a^k b^{n-k} = (a^{n+1} - b^{n+1})/(a-b)$. Para esto la reduciremos al caso de una progresión geométrica. Si $b = 0$, entonces el valor de la sumatoria es a^n. Para $b \neq 0$, sea $r = a/b$. Entonces, $r \neq 1$ y $a^k b^{n-k} = b^n (a/b)^k = b^n r^k$ y con esto:

$$\begin{aligned}
\sum_{k=0}^{n} a^k b^{n-k} &= \sum_{k=0}^{n} r^k b^n && \text{(definición de } r\text{)} \\
&= b^n \sum_{k=0}^{n} r^k && (b^n \text{ es constante para la sumatoria)} \\
&= b^n (r^{n+1} - 1)/(r-1) && (r \neq 1 \text{ y sumatoria de un progresión geométrica)} \\
&= (a^{n+1} - b^{n+1})/(a-b). && \text{(definición de } r \text{ y reacomodo)}
\end{aligned}$$

♢

Ejemplo: Calculemos $\sum_{k=1}^{n} \frac{1}{k(k+1)}$. Podemos hacer el siguiente cálculo

$$\begin{aligned}
\sum_{k=1}^{n} \frac{1}{k(k+1)} &= \sum_{k=1}^{n} \left(\frac{1}{k} - \frac{1}{k+1} \right) && \text{(uso de la igualdad } \tfrac{1}{k(k+1)} = \tfrac{1}{k} - \tfrac{1}{k+1}\text{)} \\
&= \frac{1}{1} - \frac{1}{n+1} = 1 - \frac{1}{n+1}. && \text{(propiedad telescópica)}
\end{aligned}$$

♢

Ejemplo: Calculemos $\sum_{k=0}^{n} k \cdot k!$. Consideremos la igualdad $(k+1)! = (k+1)k! = k \cdot k! + k!$, con la que obtenemos que

$$k \cdot k! = (k+1)! - k!$$

Sumando ambos lados de la igualdad de $k = 0$ a $k = n$, llegamos a

$$\sum_{k=0}^{n} k \cdot k! = \sum_{k=0}^{n} ((k+1)! - k!) = (n+1)! - 0! = (n+1)! - 1,$$

donde la segunda igualdad es por propiedad telescópica. ♢

Guía Básica

Determinar la veracidad de las siguientes afirmaciones:

1. Sea A un conjunto de un elemento. Sea $\mathcal{R}$ una relación de equivalencia definida en A. Independiente de la forma de $\mathcal{R}$, $A/\mathcal{R}$ siempre tendrá dos elementos.
2. Sea A un conjunto de un elemento. Sea $\mathcal{R}$ una relación de equivalencia definida en A. Independiente de la forma de $\mathcal{R}$, $A/\mathcal{R}$ siempre tendrá un elemento.
3. $(-\infty, 0)$ y $[0, \infty)$ son las clases de equivalencia de $R = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid xy \geq 0\}$
4. $(-\infty, 0)$ y $(0, \infty)$ son las clases de equivalencia de $R = \{(x, y) \in (\mathbb{R} \setminus \{0\}) \times (\mathbb{R} \setminus \{0\}) \mid xy > 0\}$
5. $(-\infty, 0)$ y $[0, \infty)$ son las clases de equivalencia de $R = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x + y \geq 0\}$
6. Dos clases de equivalencia siempre tienen al menos un elemento en común.
7. $\{x \in \mathbb{N} \mid \exists n \in \mathbb{N}, x = 2n\}$ y $\{x \in \mathbb{N} \mid \exists n \in \mathbb{N}, x = 2n + 1\}$, son las clases de equivalencia de $\mathcal{R} = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x = 2y\}$.
8. $\{x \in \mathbb{N} \mid \exists n \in \mathbb{N}, x = 2n\}$ y $\{x \in \mathbb{N} \mid \exists n \in \mathbb{N}, x = 2n + 1\}$, son las clases de equivalencia de $\mathcal{R} = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid \frac{x}{y} = 2\}$.
9. $\{x \in \mathbb{N} \mid \exists n \in \mathbb{N}, x = 2n\}$ y $\{x \in \mathbb{N} \mid \exists n \in \mathbb{N}, x = 2n + 1\}$, son las clases de equivalencia de $\mathcal{R} = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid \exists n \in \mathbb{N}, \frac{x}{y} = 2n\}$.
10. $\{x \in \mathbb{N} \mid \exists n \in \mathbb{N}, x = 2n\}$ y $\{x \in \mathbb{N} \mid \exists n \in \mathbb{N}, x = 2n + 1\}$, son las clases de equivalencia de $\mathcal{R} = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid \exists n \in \mathbb{N}, x - y = 2n\}$.
11. Sea $(a_n)_{n\geq 0}$ una secuencia de reales y $\lambda \in \mathbb{R}$, se tiene que $\sum_{i=0}^{N} \lambda a_i = \lambda \sum_{i=0}^{N} a_i$.
12. Sea $(a_n)_{n\geq 0}$ una secuencia de reales y $\lambda \in \mathbb{R}$, se tiene que $\sum_{i=0}^{N} \lambda + a_i = \lambda + \sum_{i=0}^{N} a_i$.
13. Sea $(a_n)_{n\geq 0}$ una secuencia de reales y $\lambda \in \mathbb{R}$, se tiene que $\sum_{i=0}^{N} \lambda + a_i = (N + 1)\lambda + \sum_{i=0}^{N} a_i$.
14. Sea $(a_n)_{n\geq 0}$ una secuencia de reales y $\lambda \in \mathbb{R}$, se tiene que $\sum_{i=0}^{N} \lambda + a_i = N\lambda + 1 + \sum_{i=0}^{N} a_i$.
15. Sea $(a_n)_{n\geq 0}$ una secuencia de reales, se tiene que $\sum_{i=0}^{N} a_i = \sum_{i=1}^{N+1} a_{i-1}$.
16. Sea $(a_n)_{n\geq 0}$ una secuencia de reales, se tiene que $\sum_{i=0}^{N} a_i = \sum_{i=2}^{N+3} a_{i-2}$.
17. Sea $(a_n)_{n\geq 0}$ una secuencia de reales y $N \geq 1$ par, se tiene que $\sum_{i=0}^{N} a_i = \sum_{i=0}^{N/2} a_{2i} + \sum_{i=0}^{\frac{N}{2}-1} a_{2i+1}$.
18. Sea $(a_n)_{n\geq 0}$ y $(b_n)_{n\geq 0}$ secuencias de reales, se tiene que $\sum_{i=1}^{N}(a_i + b_i) = \sum_{i=1}^{N} a_i + \sum_{j=1}^{N} b_j$.
19. Sean $(a_n)_{n\geq 0}$ y $(b_n)_{n\geq 0}$ secuencias de reales, se tiene que $\sum_{i=1}^{N}(a_i + b_i) = \sum_{i=1}^{N} \left(a_i + \sum_{j=1}^{N} b_j\right)$.
20. Sea $(a_n)_{n\geq 0}$ una secuencia de reales, se tiene que $\sum_{i=j}^{N} a_i = \sum_{j=i}^{N} a_j$.
21. Sea $(a_n)_{n\geq 0}$ una secuencia de reales, se tiene que $\sum_{i=0}^{N} a_i = \sum_{j=0}^{N} a_j$.

22. Sea $(a_n)_{n\geq 0}$ una secuencia de reales, se tiene que $\sum_{i=0}^{N} a_i = \sum_{j=0}^{N-1}(a_j - a_N)$.
23. Sea $(a_n)_{n\geq 0}$ una secuencia de reales, se tiene que $\sum_{i=0}^{N} a_i = \sum_{j=0}^{N-1}(a_j + a_N)$.
24. Sea $(a_n)_{n\geq 0}$ una secuencia de reales, se tiene que $\sum_{i=0}^{N} a_i = \left(\sum_{j=0}^{N-1} a_j\right) + a_N$.
25. Sea $(a_n)_{n\geq 0}$ una secuencia de reales, se tiene que $\sum_{i=0}^{N} a_i = \left(\sum_{j=0}^{N-1} a_j\right) - a_N$.
26. Sea $(a_n)_{n\geq 0}$ una secuencia de reales, se tiene que $\sum_{i=1}^{N} a_i - a_{i-1} = a_N - a_0$.
27. Sea $(a_n)_{n\geq 0}$ una secuencia de reales, se tiene que $\sum_{i=1}^{N} a_i - a_{i-1} = a_0 - a_N$.
28. Sea $(a_n)_{n\geq 0}$ una secuencia de reales, se tiene que $\sum_{i=1}^{N} a_i - (a_i - 1) = a_N - a_0$.
29. Sea $(a_n)_{n\geq 0}$ una secuencia de reales, se tiene que $\sum_{i=1}^{N} (a_i + 1) - a_i = a_{N+1} - a_1$.
30. Sea $(a_n)_{n\geq 0}$ una secuencia de reales, se tiene que $\sum_{i=1}^{N} a_{i-1} - a_i = a_N - a_0$.
31. Sea $(a_n)_{n\geq 0}$ una secuencia de reales, se tiene que $\sum_{i=1}^{N} a_{i-1} - a_i = a_0 - a_N$.
32. Sea $(a_n)_{n\geq 0}$ una secuencia de reales, se tiene que $\sum_{i=5}^{N} a_{i-1} - a_i = a_5 - a_N$.
33. Sea $(a_n)_{n\geq 0}$ una secuencia de reales, se tiene que $\sum_{i=5}^{N} a_{i-1} - a_i = a_4 - a_N$.
34. Si $n \geq 1$ y $q \neq 1$, entonces $\sum_{i=0}^{n-1} q^i = \frac{1-q^n}{1-q}$.
35. Si $n \geq 1$ y $q \neq 1$, entonces $\sum_{i=0}^{n-1} q^i = \frac{1-q^{n+1}}{1-q}$.
36. Si $n \geq 1$ y $q \neq 1$, entonces $\sum_{i=0}^{n-1} q^i = \frac{1}{1-q}$.
37. Si $n \geq 1$ y $q \neq 1$, entonces $\sum_{i=k}^{n-1} q^i = q^k \frac{1-q^{n-k}}{1-q}$.
38. Si $n \geq 1$ y $q \neq 1$, entonces $\sum_{i=k}^{n-1} q^i = q^k \frac{1-q^n}{1-q}$.
39. Si $n \geq 1$, entonces $\sum_{i=0}^{n-1} i = \frac{1}{2}n(n+1)$.
40. Si $n \geq 1$, entonces $\sum_{i=0}^{n-1} i = \frac{1}{2}n(n-1)$.
41. Si $n \geq 0$, entonces $\sum_{i=0}^{n} i = \frac{1}{2}n(n+1)$.
42. Si $n \geq 0$, entonces $\sum_{i=0}^{n} i^2 = \frac{1}{6}n(n+1)(2n+1)$.
43. Si $n \geq 0$, entonces $\sum_{i=0}^{n-1} i^2 = \frac{1}{6}n(n-1)(2n-1)$.
44. Si $n \geq 0$, entonces $\sum_{i=0}^{n-1} i^2 = \frac{1}{6}n(n-1)(2n+1)$.
45. Si $n \geq 1$, entonces $\sum_{i=0}^{n-1} \operatorname{sen}(i) \leq n$.
46. $\sum_{i=0}^{n}(a_i + b_i) = \sum_{i=0}^{n}(a_i + \sum_{j=0}^{n} b_j)$.
47. $\sum_{i=0}^{n}(a_i + b_i) = \sum_{i=0}^{n}(a_i + \sum_{j=i}^{n} b_i)$.
48. $\sum_{i=0}^{n}(a_i + b_i) = \sum_{i=0}^{n} a_i + \sum_{i=0}^{n} b_i$.

Guía de Ejercicios

1. Sea H el conjunto de todos los hombres y M el conjunto de todas las mujeres. Se define $E \subseteq H \times M$ por

$$E = \{(h, m) \in H \times M \mid h \text{ está casado con } m\}.$$

Es decir, E es el conjunto de todos los matrimonios.

Estudie las siguientes relaciones. Indique si son de orden, o de equivalencia, si es el primer caso determine si son de orden total o parcial, si es el segundo, encuentre las clases de equivalencia.

Indicación: Haga los supuestos que estime convenientes y vea qué pasa si los cambia (por ejemplo, si se permite que uno sea hermano de si mismo, o no). Además, no se preocupe en ser demasiado formal, lo importante es que comprenda qué verificar para una relación de orden y para una de equivalencia.

a) Sea $\mathcal{R}_1$ la relación definida en E por:
$(h_1, m_1)\mathcal{R}_1(h_2, m_2) \iff$ Algún miembro del matrimonio 1 es hermano(a) de algún miembro del matrimonio 2.

b) Sea $\mathcal{R}_2$ la relación definida en E por:
$(h_1, m_1)\mathcal{R}_2(h_2, m_2) \iff h_1$ es hermano(a) de h_2.

c) Sea $\mathcal{R}_3$ la relación definida en E por:
$(h_1, m_1)\mathcal{R}_3(h_2, m_2) \iff$ Algún miembro del matrimonio 1 es de mayor o igual estatura que algún miembro del matrimonio 2.

d) Sea $\mathcal{R}_4$ la relación definida en E por:
$(h_1, m_1)\mathcal{R}_4(h_2, m_2) \iff m_1$ es de menor estatura que m_2.

e) Sea $\mathcal{R}_5$ la relación definida en E por:
$(h_1, m_1)\mathcal{R}_5(h_2, m_2) \iff$ Las edades del matrimonio 1 suman mas que las edades del matrimonio 2.

f) Sea $\mathcal{R}_6$ la relación definida en E por:
$(h_1, m_1)\mathcal{R}_6(h_2, m_2) \iff$ Las edades del matrimonio 1 suman a lo menos la suma de las edades del matrimonio 2.

g) Sea $\mathcal{R}_7$ la relación definida en E por:
$(h_1, m_1)\mathcal{R}_7(h_2, m_2) \iff$ Las edades del matrimonio 1 suman lo mismo que las edades del matrimonio 2.

2. Estudie las siguientes relaciones. Indique si son de orden, o de equivalencia, si es el primer caso determine si son de orden total o parcial, si es el segundo, encuentre las clases de equivalencia.

a) $x\mathcal{R}y \iff x^2 + y = y^2 + x$.

b) $(x, y)\mathcal{R}(z, w) \iff (\exists k \in \mathbb{N},\ x < z \wedge y + w = 2k)$.

c) $(x, y)\mathcal{R}(z, w) \iff x + z = y + w$.

d) $(x, y)\mathcal{R}(z, w) \iff x \leq z \wedge y \geq w$.

e) $(x, y)\mathcal{R}(z, w) \iff xw \leq zy$.

3. Encuentre el valor de las siguientes sumas, usando sumas conocidas:

a) $\displaystyle\sum_{k=1}^{n-1} k(k+1)$.

b) $\displaystyle\sum_{k=3}^{n-1} (k-2)(k+1)$.

c) $\displaystyle\sum_{k=4}^{n-2}\Big(2k^3-\tfrac{1}{3}k+2\Big)$.

d) $\displaystyle\sum_{k=1}^{n}\frac{(k+1)!(1-k)}{k^2+k}$.

4. Encuentre el valor de las siguientes sumatorias. (Sin usar inducción).

a) $\displaystyle\sum_{i=0}^{n}(i+i^2)$.

b) $\displaystyle\sum_{i=0}^{n}\big((i-1)^2-i^2\big)$.

c) $\displaystyle\sum_{i=1}^{n}\big(\operatorname{sen}(i)-\operatorname{sen}(i+1)\big)$.

d) $\displaystyle\sum_{i=1}^{n}\big(\cos(i+2)+\cos(i)-\cos(i+1)-\cos(i-1)\big)$.

e) $\displaystyle\sum_{i=1}^{n}\Big(\frac{i}{i^2+2i+1}-\frac{i-1}{i^2}\Big)$.

5. Sea $(a_n)_{n\in\mathbb{N}}$ una progresión aritmética.

a) Si $a_i=x$, $a_j=y$, $a_k=z$ para $i,j,k\in\mathbb{N}$. Pruebe que

$$(j-k)x+(k-i)y+(i-j)z=0.$$

b) Pruebe que $\dfrac{1}{\sqrt{a_0}+\sqrt{a_1}}+\dfrac{1}{\sqrt{a_1}+\sqrt{a_2}}+...+\dfrac{1}{\sqrt{a_{n-1}}+\sqrt{a_n}}=\dfrac{n}{\sqrt{a_0}+\sqrt{a_n}}$.

Guía de Problemas

1. Sea A un conjunto no vacío y $f:A\to A$ una función que satisface la condicion siguiente:

$$\exists n\in\mathbb{N}\setminus\{0\}\text{ tal que }f^{(n)}=\mathrm{id}_A.$$

Se define en A la relación R por:

$$x\mathcal{R}y\iff\exists k\in\{1,2,...,n\}\text{ tal que }f^{(k)}(x)=y.$$

a) (30 min.) Demuestre que $\mathcal{R}$ es relación de equivalencia.

b) Considere $A=\{0,1\}^3$ y $f:A\to A$ definida por $f(x_1,x_2,x_3)=(x_2,x_3,x_1)$

1) (10 min.) Pruebe que f satisface la propiedad enunciada.
2) (20 min.) Determine y escriba todas las clases de equivalencia inducidas por $\mathcal{R}$ en A.

2. Sea E un conjunto y $A \neq \emptyset$ un subconjunto fijo de E. Se define en $\mathcal{P}(E)$ la relación $\mathcal{R}$ por:

$$X\mathcal{R}Y \iff A \cap X = A \cap Y$$

   a) (10 min.) Demuestre que $\mathcal{R}$ es relación de equivalencia.
   b) (15 min.) Demuestre que el conjunto cuociente $\mathcal{P}(E)/\mathcal{R} = \{[X] \mid X \in \mathcal{P}(A)\}$.
   c) (15 min.) Demuestre que para $X, Y \in \mathcal{P}(A)$ se tiene que $X \neq Y \implies [X] \neq [Y]$.

3. Considere el conjunto $A = \mathbb{Z} \times \mathbb{Z}$. Se define la relación $\mathcal{R}$ en A por:

$$(a_1, a_2)\ \mathcal{R}\ (b_1, b_2) \iff a_1 + a_2 - b_1 - b_2 = 2k \text{ para un cierto } k \in \mathbb{Z}.$$

   a) (30 min.) Pruebe que $\mathcal{R}$ es una relación de equivalencia.
   b) (10 min.) Calcular explícitamente $[(0,0)]_{\mathcal{R}}$ y $[(1,0)]_{\mathcal{R}}$.
   c) (10 min.) Pruebe que $A = [(0,0)]_{\mathcal{R}} \cup [(1,0)]_{\mathcal{R}}$.
   d) (10 min.) Pruebe que existe una biyección $f : [(1,0)]_{\mathcal{R}} \to [(0,0)]_{\mathcal{R}}$.

4. Sea $p \in \mathbb{Z}, p \geq 2$. Se define en $\mathbb{Q}^+ = \{q \in \mathbb{Q} \mid q > 0\}$ la relación Ω_p por:

$$x\Omega_p y \iff \exists \alpha \in \mathbb{Z},\ \frac{x}{y} = p^{\alpha}.$$

   a) (20 min.) Demostrar que Ω_p es relación de equivalencia en $\mathbb{Q}^+$.
   b) (10 min.) Describa por extensión $[1]_{\Omega_2}$.

5. (20 min.) Calcular las siguientes sumatorias

   a) $\displaystyle\sum_{k=n}^{m} \log\left(1 + \frac{1}{k}\right)$, donde $n \leq m$.
   b) $\displaystyle\sum_{i=\frac{1}{2}m(m-1)+1}^{\frac{1}{2}m(m+1)} (2i-1)$.
   c) $\displaystyle\sum_{k=1}^{n} \frac{1}{\sqrt{k(k+1)}(\sqrt{k+1}+\sqrt{k})}$.

6. (30 min.) Probar que para todo natural mayor o igual que 1 se tiene $\displaystyle\sum_{k=1}^{n+1} \frac{1}{n+k} \leq \frac{5}{6}$.

7. Dadas $f, g : \mathbb{N} \to \mathbb{R}$, se define $(f * g) : \mathbb{N} \to \mathbb{R}$ por:

$$(f * g)(n) = \sum_{k=0}^{n} f(k)g(n-k).$$

   a) (20 min.) Si $f(u) = 1$ y $g(u) = u$, $\forall u \in \mathbb{N}$, calcule, en función de n:

$$(f * f)(n), \qquad (f * g)(n) \qquad \text{y} \qquad (g * g)(n).$$

b) (20 min.) Si $f(u) = \frac{a^u}{u!}$ y $g(u) = \frac{b^u}{u!}$, con $a, b \in \mathbb{R}$, $u \in \mathbb{N}$. Calcule, en función de a, b y n, el valor de

$$n!(f * g)(n)$$

8. Se define $H_n = \sum_{i=1}^{n} \frac{1}{i}$, para todo $n \geq 1$. Demuestre usando inducción que:

a) (10 min.) $H_{2^k} \leq 1 + k$ para todo $k \in \mathbb{N}$.

b) (20 min.) $\sum_{i=1}^{n} H_i = (n+1)H_n - n$ para todo $n \geq 1$.

SEMANA 08:

Sumatorias

Ingeniería Matemática
FACULTAD DE CIENCIAS
FÍSICAS Y MATEMÁTICAS
UNIVERSIDAD DE CHILE

6.2 Sumatorias generales

Para motivar la discusión de esta parte comencemos preguntándonos si la siguiente igualdad es válida para una secuencia $(a_k)_{k\in[1..n]}$:

$$¿\sum_{k=1}^{n} a_k = \sum_{k=1}^{n} a_{n+1-k}?$$

La respuesta es que sí lo es, ya que estamos sumando la misma secuencia de números reales, sólo que en un orden diferente. Más aún, en cualquier orden en que se haga la suma se obtendrá el mismo valor, por lo que en lugar de escribir $\sum_{k=1}^{n} a_k$, podemos simplemente escribir $\sum_{k\in[1..n]} a_k$.

Cuando expresamos una sumatoria de dos formas distintas mediante un reordenamiento de la secuencia de números reales, diremos que se está haciendo un **cambio de índices**.

Ejemplo: Calculemos la sumatoria $\sum_{i=1}^{n}(n-i)^2$. Al hacer el cambio de índices $k = n - i$ obtenemos el reordenamiento $\sum_{k=0}^{n-1} k^2$ que ya vimos es igual a $(n-1)n(2(n-1)+1)/6$. $\diamondsuit$

Proposición 6.4 *Sea $(a_k)_{k\in[1..n]}$ una secuencia de números reales y sean $I, J \subseteq [1..n]$ disjuntos. Entonces*

$$\sum_{k\in I\cup J} a_k = \sum_{k\in I} a_k + \sum_{k\in J} a_k.$$

Ejemplo: Verifiquemos que $\sum_{i=0}^{2n}(-1)^i i = n$. En efecto, el conjunto de índices se puede separar en los índices pares y los índices impares. Por una parte:

$$\sum_{i,\text{ par en } [0..(2n)]} (-1)^i i = \sum_{i,\text{ par en } [0..(2n)]} i$$

y

$$\sum_{i,\text{ impar en } [0..(2n)]} (-1)^i i = -\sum_{i,\text{ impar en } [0..(2n)]} i.$$

La primera sumatoria mediante una traslación de índices $i \to i+1$ es igual a

$$\sum_{i,\text{ par en } [0..(2n)]} i = \sum_{i,\text{ impar en } [1..(2n+1)]} (i-1) = 2n + \sum_{i,\text{ impar en } [1..(2n)]} (i-1).$$

Entonces,

$$\begin{aligned}\sum_{i=0}^{2n}(-1)^i i &= 2n + \sum_{i,\text{ impar en } [1..(2n)]}(i-1) - \sum_{i,\text{ impar en } [1..(2n)]} i \\ &= 2n + \sum_{i,\text{ impar en } [1..(2n)]}(-1) \\ &= 2n - n = n \qquad \text{(hay } n \text{ impares en } [1..(2n)])\end{aligned}$$

♢

Sumatorias dobles

Dadas dos secuencias de números reales $(a_k)_{k\in[1..n]}$ y $(b_j)_{j\in[1..m]}$, nos interesa obtener fórmulas para el producto de sus respectivas sumatorias. Por las propiedades de $\mathbb{R}$ y de las sumatorias, si $c_k = \sum_{j\in[1..m]} a_k b_j$, para $k \in [1..n]$, podemos reescribir este producto como sigue:

$$(\sum_{k\in[1..n]} a_k)(\sum_{j\in[1..m]} b_j) = \sum_{k\in[1..n]}(\sum_{j\in[1..m]} a_k b_j) = \sum_{k\in[1..n]} c_k.$$

Es decir, el producto de dos sumatorias es una sumatoria cuya secuencia de números reales es a su vez una sumatoria. A la inversa, si tenemos una sumatoria con la estructura anterior sabemos que es el producto de dos sumatorias.

Ejemplo: En la sumatoria $\sum_{i=1}^{n}(\sum_{j=1}^{m} ij)$, podemos identificar $a_i = i$, para $i \in [1..n]$ y $b_j = j$, para $j \in [1..m]$. Entonces, esta sumatoria es el producto de dos sumatorias conocidas.

$$\sum_{i=1}^{n}(\sum_{j=1}^{m} ij) = (\sum_{i=1}^{n} i)(\sum_{j=1}^{m} j) = \frac{n(n+1)}{2}\frac{m(m+1)}{2}.$$

♢

En general, podemos estudiar cada sumatoria $\sum_{k=s}^{t} b_k$, donde $(b_k)_{k\geq m}$ es a su vez una sumatoria.

Es decir, para cada k existe una secuencia $(a_{k,j})_{j\in[m(k)..n(k)]}$ y $b_k = \sum_{j=m(k)}^{n(k)} a_{k,j}$.

Reescribiendo: $\sum_{k=s}^{t} b_k = \sum_{k=s}^{t}\sum_{j=m(k)}^{n(k)} a_{k,j}$.

Este tipo de sumatorias se llaman **sumatorias dobles**. Notar que, a diferencia de lo recién hecho para el producto de dos sumatorias, las sumatorias dobles permiten:

- Que la sucesión que define el término b_k varíe con k. Esto se explicita en el uso de dos índices en $a_{k,j}$.
- Los límites inferior y superior de $\sum_{j=m(k)}^{n(k)} a_{k,j}$ son funciones del índice k.

Esta idea se puede repetir dando lugar a sumatorias triples, cuádruples, etc. En este apunte nos contentaremos con las sumatorias dobles.

La evaluación de una sumatoria doble a menudo requiere una herramienta adicional a las que conocemos que se llama **intercambio de sumatorias.** Para ver esto, supongamos que para todo k tenemos que $m(k) = 1$ y $n(k) = m$ donde $m \in \mathbb{N}$ es fijo. Notemos que los términos que estamos sumando son:

$$\begin{matrix} a_{1,1} & a_{1,2} & \cdots & a_{1,m} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n,1} & a_{n,2} & \cdots & a_{n,m} \end{matrix}$$

y que, por ende, la sumatoria doble representa la sumatoria de los resultados de sumar cada **fila** a la vez. Es claro que esto es equivalente a sumar los resultados de sumar cada **columna** a la vez. De donde tenemos la siguiente propiedad:

Proposición 6.5 (Intercambio de sumatorias) *Para una sumatoria doble* $\sum_{k=1}^{n}\sum_{j=1}^{m} a_{k,j}$ *cuyos límites inferiores y superiores no dependen de los índices, se tiene:*

$$\sum_{k=1}^{n}\sum_{j=1}^{m} a_{k,j} = \sum_{j=1}^{m}\sum_{k=1}^{n} a_{k,j}.$$

Dem. Queda propuesta como ejercicio, usando el principio de inducción en $n \in \mathbb{N}$. □

6.3 Coeficientes binomiales

A continuación vamos a estudiar una familia de número que se conocen con el nombre de coeficientes binomiales que tienen propiedades e interpretaciones interesantes (por razones de tiempo, no discutiremos estas últimas).

Definición 6.6 (Coeficiente binomial) *Para dos enteros n y k, $0 \leq k \leq n$, se define*

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

(se lee "ene sobre ka").

Adoptaremos la siguiente convención: Si $k < 0$ o $k > n$, entonces $\binom{n}{k} = 0$.

Proposición 6.7 *Para n y k enteros, $n \geq 0$,*

(I) $\binom{n}{k} = \binom{n}{n-k}$.

(II) *Identidad de Pascal:* $\binom{n+1}{k+1} = \binom{n}{k} + \binom{n}{k+1}$.

Dem.

(I) Verifique este punto como ejercicio.

(II) Si $k < -1$, entonces $\binom{n+1}{k+1} = \binom{n}{k} = \binom{n}{k+1} = 0$. Si $k = -1$, entonces $\binom{n+1}{0} = \binom{n}{0} = 1$ y $\binom{n}{-1} = 0$. De manera análoga, si $k > n$, entonces $\binom{n+1}{k+1} = \binom{n}{k} = \binom{n}{k+1} = 0$. Si $k = n$, entonces, $\binom{n+1}{k+1} = \binom{n}{k} = 1$ y $\binom{n}{n+1} = 0$.

Analicemos ahora el caso $0 \leq k < n$:

$$\begin{aligned}
\binom{n}{k} + \binom{n}{k+1} &= \frac{n!}{k!(n-k)!} + \frac{n!}{(k+1)!(n-(k+1))!} && \text{(por definición de } \tbinom{n}{i}) \\
&= \frac{n!}{k!(n-k)(n-k-1)!} + \frac{n!}{(k+1)k!(n-k-1)!} && (m! = (m-1)!m) \\
&= \frac{n!}{k!(n-k-1)!}\left(\frac{1}{n-k} + \frac{1}{k+1}\right) && \text{(factorizando)} \\
&= \frac{n!}{k!(n-k-1)!} \cdot \frac{n+1}{(n-k)(k+1)} && \text{(suma de fracciones)} \\
&= \frac{(n+1)n!}{(k+1)k!\ (n-k)(n-k-1)!} && \text{(reacomodo)} \\
&= \binom{n+1}{k+1}. && \text{(por definición de } \tbinom{n}{i})
\end{aligned}$$

□

La parte (II) de la Proposición 6.7 permite utilizar un método iterativo para calcular $\binom{n}{k}$. Éste consiste en construir un triángulo, donde las filas están etiquetadas con valores de n, y las columnas con valores de k. Los bordes de este triángulo los rellenamos con unos, como muestra la tabla:

	$k=0$	$k=1$	$k=2$	$k=3$	$k=4$	$k=5$
$n=0$	1					
$n=1$	1	1				
$n=2$	1		1			
$n=3$	1			1		
$n=4$	1				1	
$n=5$	1					1

En esta estructura, el término $\binom{n}{k}$ es el que aparece en la fila n y la columna k. Para calcularlo, entonces, como $0 < k < n$:

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1},$$

es decir, cada término es la suma del que se encuentra sobre él, y el que se encuentra en su diagonal superior-izquierda. Rellenando, obtenemos el triángulo:

	$k=0$	$k=1$	$k=2$	$k=3$	$k=4$	$k=5$
$n=0$	1					
$n=1$	1	1				
$n=2$	1	2	1			
$n=3$	1	3	3	1		
$n=4$	1	4	6	4	1	
$n=5$	1	...				1

Este triángulo es llamado **Triángulo de Pascal**.

Binomio de Newton

En esta sección encontraremos una fórmula para $(x+y)^n$ que generaliza la fórmula del **cuadrado de binomio**: $(x+y)^2 = x^2 + 2xy + y^2$. Una forma de entender este resultado es codificar expresiones de la forma $\sum_{k=0}^{n} a_k x^k y^{n-k}$ por sus coeficientes $(a_k)_{k=0}^{n}$. Por ejemplo, para $n=2$ y $n=3$ tenemos

$n=2$		x^2	xy	y^2
$x(x+y) = x^2 + xy$		1	1	0
$(x+y)y = xy + y^2$		0	1	1
$x^2 + 2xy + y^2$		1	2	1

$n=3$	x^3	x^2y	xy^2	y^3
$x(x^2 + \mathbf{2xy} + y^2) = x^3 + \mathbf{2x^2y} + xy^2$	$\binom{2}{2}$	$\binom{\mathbf{2}}{\mathbf{1}}$	$\binom{2}{0}$	0
$(\mathbf{x^2} + 2xy + y^2)y = \mathbf{x^2y} + 2xy^2 + y^3$	0	$\binom{\mathbf{2}}{\mathbf{2}}$	$\binom{2}{1}$	$\binom{2}{0}$
$x^3 + \mathbf{3x^2y} + 3xy^2 + y^3$	$\binom{3}{3}$	$\binom{\mathbf{3}}{\mathbf{2}}$	$\binom{3}{1}$	$\binom{3}{0}$

Los dos casos anteriores tienen un claro patrón. Por ejemplo, el coeficiente que acompaña al producto x^2y en $(x+y)^3$ es la suma de 2 con 1, que son el coeficiente que acompaña a xy y el coeficiente que acompaña a x^2 en $(x+y)^2$, respectivamente. De esta forma no es demasiado sorprendente que la fórmula general quede expresada en términos de los coeficientes binomiales que en el caso que estamos discutiendo es $\binom{3}{0}x^3 + \binom{3}{1}x^2y^+\binom{3}{2}xy^2 + \binom{3}{3}y^3$.

Teorema 6.8 (Binomio de Newton) *Sean $x, y \in \mathbb{R}, n \in \mathbb{N}$. Entonces*

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k.$$

Dem. Probémoslo por inducción en $n \in \mathbb{N}$.

Primero analicemos el caso base, $n = 0$. Por un lado $\sum_{k=0}^{0} \binom{0}{k} x^k y^{0-k} = \binom{0}{0} x^0 y^0 = 1$ (Aquí suponemos que $\forall x \in \mathbb{R},\ x^0 = 1$) y por otro $(x+y)^0 = 1$. Es decir, la propiedad se cumple para $n = 0$.

Sea entonces $n \geq 0$ tal que se tiene que $(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k$ (H.I.). Probemos que se tiene el teorema para $n+1$:

$$\begin{aligned}
(x+y)^{n+1} &= (x+y)(x+y)^n && \text{(definición de potencia)} \\
&= (x+y) \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k && \text{(hipótesis de inducción)} \\
&= \sum_{k=0}^{n} \binom{n}{k} (x+y) x^{n-k} y^k && \text{(constantes salen y entran de una sumatoria)} \\
&= \sum_{k=0}^{n} \binom{n}{k} x^{n-k+1} y^k + \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^{k+1} && \text{(distributividad en } \mathbb{R} \text{ y aditividad)} \\
&= \sum_{k=0}^{n} \binom{n}{k} x^{n-k+1} y^k + \sum_{k=1}^{n+1} \binom{n}{k-1} x^{n-(k-1)} y^k && \text{(cambio de índices: } k+1 \to k) \\
&= \sum_{k=0}^{n+1} \binom{n}{k} x^{n-k+1} y^k + \sum_{k=0}^{n+1} \binom{n}{k-1} x^{n-k+1} y^k && \text{(agregamos } 0 = \tbinom{n}{-1} = \tbinom{n}{n+1}) \\
&= \sum_{k=0}^{n+1} \left[\binom{n}{k} + \binom{n}{k-1} \right] x^{n+1-k} y^k && \text{(aditividad)} \\
&= \sum_{k=0}^{n+1} \binom{n+1}{k} x^{n+1-k} y^k. && \text{(identidad de Pascal)}
\end{aligned}$$

De donde se concluye el teorema. □

A continuación veremos algunos ejemplos donde el teorema del Binomio de Newton es útil.

Ejemplo: Calculemos $\sum_{k=0}^{n} \binom{n}{k}$. Esta suma resulta ser una aplicación directa del teorema del Binomio de Newton. Utilizando que $1^m = 1$ para cualquier $m \geq 1$,

$$\sum_{k=0}^{n} \binom{n}{k} = \sum_{k=0}^{n} \binom{n}{k} 1^k 1^{n-k}.$$

Así, por teorema del Binomio de Newton, se tiene que $\sum_{k=0}^{n} \binom{n}{k} = (1+1)^n = 2^n$. ♢

Ejemplo: Calculemos $\sum_{k=0}^{n} \binom{n}{k} \frac{1}{k+1}$. Podemos relacionar este tipo de sumatorias con la forma del teorema del Binomio de Newton, típicamente, ingresando los factores que "sobran" al coeficiente binomial. Reescribamos el término de la sumatoria:

$$\binom{n}{k} \frac{1}{k+1} = \frac{n!}{k!(n-k)!} \cdot \frac{1}{k+1} = \frac{n!}{(k+1)!(n-k)!}.$$

Para formar un nuevo coeficiente binomial, debemos procurar que los dos valores de abajo (en este caso $k+1$ y $n-k$) sumen el de arriba (en este caso n). Para arreglarlo, amplifiquemos numerador y denominador por $(n+1)$, obteniendo

$$\frac{n!}{(k+1)!(n-k)!} = \frac{1}{n+1} \cdot \frac{(n+1)n!}{(k+1)!(n-k!)} = \frac{1}{n+1} \cdot \frac{(n+1)!}{(k+1)!(n-k)!} = \frac{1}{n+1}\binom{n+1}{k+1}.$$

Ahora tenemos un factor $\frac{1}{n+1}$ en lugar de $\frac{1}{k+1}$. ¿Hemos ganado algo? Sí, pues $\frac{1}{n+1}$ es un término independiente de k, por lo que

$$\sum_{k=0}^{n} \binom{n}{k} \frac{1}{k+1} = \frac{1}{n+1} \sum_{k=0}^{n} \binom{n+1}{k+1}.$$

El término de la derecha es muy parecido a lo recién calculado $\sum_{k=0}^{n} \binom{n}{k} = 2^n$. Mediante una traslación de índices podemos escribir

$$\sum_{k=0}^{n} \binom{n+1}{k+1} = \sum_{k=1}^{n+1} \binom{n+1}{k} = \sum_{k=0}^{n+1} \binom{n+1}{k} - \binom{n+1}{0} = 2^{n+1} - 1,$$

y por lo tanto,

$$\sum_{k=0}^{n} \binom{n}{k} \frac{1}{k+1} = (2^{n+1} - 1)/(n+1).$$

♢

Ejemplo: Verifiquemos que

$$\sum_{k \in \{[n] | k \text{ es par}\}} \binom{n}{k} = \sum_{k \in \{[n] | k \text{ es impar}\}} \binom{n}{k}.$$

Por el teorema del Binomio de Newton sabemos que

$$0 = (1-1)^n = \sum_{k=0}^{n} \binom{n}{k} (-1)^k.$$

Usando la separación de los índices en una sumatoria se deduce que:

$$0 = \sum_{k=0}^{n} \binom{n}{k} (-1)^k = \sum_{k \text{ par}} \binom{n}{k} - \sum_{k \text{ impar}} \binom{n}{k},$$

de donde se obtiene la igualdad deseada. ♢

SEMANA 08:

Conjuntos finitos

En esta sección queremos definir formalmente qué es un conjunto finito y establecer algunos resultados básicos que nos permitan comparar sus tamaños y contar la cantidad de sus elementos.

Antes de proceder recordemos que si $n \in \mathbb{N}$, denotabamos por $[1..n]$ el conjunto $\{1, ..., n\}$, y convenimos que $[1..0] = \emptyset$.

Definición 7.1 *Un conjunto A es **finito** si existe $n \in \mathbb{N}$ y $a_1, a_2, ..., a_n$ distintos entre si (i.e., $a_i \neq a_j$ si $i \neq j$) tales que $A = \{a_1, ..., a_n\}$. En este caso diremos $a_1, a_2, ..., a_n$ es una enumeración de A, que el cardinal de A es n y lo denotaremos por $|A| = n$.*

En particular, se tiene:

Proposición 7.2 *Para todo conjunto A, $|A| = 0$ si y sólo si $A = \emptyset$.*

Las siguientes propiedades son particularmente útiles para establecer que ciertos conjuntos tienen cardinalidad finita a partir de otros conjuntos cuya cardinalidad se sabe es finita.

Proposición 7.3 *Si A es un conjunto finito y $f : A \to B$ es biyectiva, entonces B es un conjunto finito y $|A| = |B|$.*

Dem. Basta notar que si $a_1, ..., a_n$ es una enumeración de A, entonces $b_1 = f(a_1)$, ..., $b_n = f(a_n)$ es una enumeración de B. Por definición de conjunto finito sigue que B es conjunto finito y $|B| = n = |A|$. □

Proposición 7.4 *Sea B un conjunto finito. Si $A \subseteq B$, entonces A es finito y $|A| \leq |B|$.*

Dem. Sea $n \in \mathbb{N}$ tal que $|B| = n$ y $b_1, ..., b_n$ una enumeración de B. Si $A = \emptyset$, el resultado es obvio. Supongamos entonces que $A \neq \emptyset$. Si $A \subseteq B$, entonces existen $k \in [1..n]$ y $1 \leq i_1 < i_2 < ... < i_k \leq n$ tales que $A = \{b_{i_1}, ..., b_{i_k}\}$. Luego, $a_1, a_2, ..., a_k$ tales que $a_j = b_{i_j}$ es una enumeración de A y $|A| = k \leq n = |B|$. □

Ahora podemos deducir fácilmente propiedades intuitivas que cumplen los conjuntos finitos.

Proposición 7.5 (Cardinal de la unión disjunta) *Si A y B son conjuntos finitos disjuntos, entonces $|A \cup B| = |A| + |B|$.*

Dem. Por definición de cardinalidad sabemos que existen $a_1, ..., a_n$ y $b_1, ..., b_m$ enumeraciones de A y B, respectivamente. Para $i \in \{1, ..., n+m\}$ definimos,

$$c_i = \begin{cases} a_i, & \text{si } i \leq n, \\ b_{i-n}, & \text{si } i > n. \end{cases}$$

Como A y B son disjuntos, sigue que $c_1, ..., c_{n+m}$ son distintos entre sí, por lo que forman una enumeración de $A \cup B$. Luego, concluimos que $|A \cup B| = n + m = |A| + |B|$. □

Corolario 7.6 (Cardinal de la diferencia) *Si $B \subseteq A$ y A es finito, entonces $|A \setminus B| = |A| - |B|$. En particular, $|B| \leq |A|$ y, si $|A| = |B|$, entonces $B = A$.*

Dem. Sabemos que $A = (A \setminus B) \cup B$ y de la Proposición 7.4 que $A \setminus B$ es finito. Entonces, de la Proposición 7.5 obtenemos que $|A| = |(A \setminus B) \cup B| = |A \setminus B| + |B|$.

La segunda afirmación es inmediata pues $|B| + |A \setminus B| = |A|$ y $|A \setminus B| \geq 0$. La tercera sigue de lo anterior pues si $|A| = |B|$, entonces $|A \setminus B| = 0$. Por lo tanto, de la Proposición 7.2 sabemos que $A \setminus B = \emptyset$ con lo que $A = B$. □

La siguiente fórmula permite calcular el cardinal de una unión cualquiera de dos conjuntos finitos. Su generalización a n conjuntos escapa del alcance de este curso.

Proposición 7.7 (Cardinal de la unión) *Si A y B son conjuntos finitos, entonces $|A \cup B| = |A| + |B| - |A \cap B|$.*

Dem. Usamos las igualdades $A \cup B = A \cup (B \setminus A)$ y $B \setminus A = B \setminus (A \cap B)$. Como $A \setminus B$ es subconjunto de B, de la Proposición 7.4 sabemos que $A \cap B$ y $B \setminus (A \cap B)$ son finitos. Entonces,

$$|A \cup B| = |A| + |B \setminus (A \cap B)| = |A| + |B| - |A \cap B|,$$

donde la primera igualdad es por la Proposición 7.5 y la segunda igualdad es el corolario anterior. □

Terminamos esta sección con un par de relaciones interesantes entre inyectividad y epiyectividad de funciones entre conjuntos finitos y sus cardinales.

Proposición 7.8 *Sean A y B conjuntos finitos con $|A| = |B|$ y sea $f : A \to B$ función. Las siguientes afirmaciones son todas equivalentes:*

(I) f es inyectiva.

(II) f es epiyectiva.

(III) f es biyectiva.

Dem. Basta demostrar que se tiene (I) si y sólo si se tiene (II), pues ello implica que (III) es equivalente a cualquiera de las otras partes.

Supongamos primero que f es inyectiva. Observar que $h : A \to f(A)$ tal que $h(a) = f(a)$ es biyección. Luego, por Proposición 7.3 e hipótesis, $|f(A)| = |A| = |B|$. Como $f(A) \subseteq B$, por el Corolario 7.6, se concluye que $f(A) = B$. De la Proposición 4.19 se concluye que f es epiyectiva.

Recíprocamente, nuevamente por Proposición 4.19, si f es epiyectiva, entonces $f(A) = B$. Sea $g : B \to A$ definida como sigue: para cada $b \in B$ sea $g(b)$ cualquier elemento de A tal que $f(g(b)) = b$. La función $g : B \to A$ cumple que $f \circ g = \mathrm{id}_B$. Esto y la parte (IV) de la Proposición 4.14 nos permite concluir que g es inyectiva. Aplicamos lo demostrado en el párrafo anterior a $g : B \to A$ y obtenemos que g es epiyectiva, por lo tanto, es biyectiva. Así, g posee inversa. Como $f \circ g = \mathrm{id}_B$, parte (V) de la Proposición 4.14, sabemos que esta inversa es f. De esta forma f es biyectiva, en particular es inyectiva. □

Proposición 7.9 *Sean A y B conjuntos, donde B es conjunto finito. Se cumple que:*

(I) A es finito y $|A| \leq |B|$ si y sólo si existe $f : A \to B$ inyectiva.

(II) A es finito y $|A| = |B|$ si y sólo si existe $f : A \to B$ biyectiva.

Dem. Para probar (I), supongamos primero que A es finito y $|A| \leq |B|$. Por definición de conjunto finito, existen $n, m \in \mathbb{N}$, tales que $a_1, ..., a_n$ y $b_1, ..., b_m$ son enumeraciones de A y B, respectivamente. Como $n = |A| \leq |B| = m$, sigue que $h : A \to B$ tal que $h(a_i) = b_i$ está bien definida y es inyectiva. Supongamos ahora que existe $f : A \to B$ inyectiva. Como B es finito y $f(A) \subseteq B$, por Proposición 7.4, sigue que $f(A)$ es finito y $|f(A)| \leq |B|$. Dado que f es inyectiva, tenemos que $f : A \to f(A)$ es biyectiva y por lo tanto $f^{-1} : f(A) \to A$ es biyectiva también. Por Proposición 7.3 concluimos que $|A| = |f(A)|$ y por lo tanto $|A| \leq |B|$.

La segunda parte se propone como ejercicio. □

La primera parte del resultado anterior es particularmente útil cuando uno quiere probar que un conjunto, digamos A, es finito, puesto que nos dice que basta encontrar otro conjunto B que sepamos es finito y establecer una inyección de A en B. Más aún, la segunda parte del referido resultado nos da una forma de inclusive determinar el cardinal de A si podemos establecer una biyección con B.

7.1 Uniones y productos cartesianos finitos de conjuntos finitos

Con la ayuda de la noción de sumatoria de una sucesión de números reales podemos extender lo que sabemos de cardinales de conjuntos finitos.

Proposición 7.10 (Cardinal de la unión finita de conjuntos disjuntos) *Si los conjuntos $A_1, \ldots, A_n$ son disjuntos de a pares, entonces*

$$|\bigcup_{i=1}^{n} A_i| = \sum_{i=1}^{n} |A_i|.$$

Dem. Por inducción y la Proposición 7.5 (propuesta como ejercicio). □

Proposición 7.11 (Cardinal del producto cartesiano) *Para A y B conjuntos finitos se tiene que $|A \times B| = |A| \cdot |B|$.*

Dem. Sean n y m los cardinales de A y B, respectivamente. Sean $a_1, ..., a_n$ y $b_1, ..., b_m$ enumeraciones de A y B, respectivamente. Definimos $c_k = (a_i, b_j)$ si $k = (i-1)m + j$ con $i \in [1..n]$ y $j \in [1..m]$. Claramente $k \in [1..nm]$ y $A \times B = \{c_1, ..., c_{nm}\}$. Más aún, si $k \neq k'$, $k = (i-1)m+j$ y $k' = (i'-1)m+j'$, entonces $i \neq i'$ o $j \neq j'$, por lo que $a_i \neq a_{i'}$ o $b_j \neq b_{j'}$, de donde se concluye que $c_k \neq c_{k'}$, es decir, $c_1, ..., c_{nm}$ es una enumeración de $A \times B$. Por definición de cardinalidad se concluye el resultado deseado. □

Por lo anterior, es claro que si $A_1, \dots A_n$ son conjuntos finitos, entonces su producto cartesiano también lo es y

$$|A_1 \times \cdots \times A_n| = |A_1| \cdots |A_n|.$$

En particular, si A es finito, A^n es finito y $|A^n| = |A|^n$.

Definición 7.12 (Conjunto de funciones) *Sean A y B conjuntos, definimos el conjunto de todas las funciones de A en B por*

$$B^A = \{f : A \to B \mid f \text{ función}\}.$$

Intuitivamente, para construir una función, para cada elemento de A se debe elegir un elemento de B. En esta elección, para cada elemento de A hay $|B|$ opciones. Como hay $|A|$ elementos en A las funciones posibles son $|B|^{|A|}$. Formalmente:

Proposición 7.13 (Cardinal de las funciones) *Para A y B finitos el conjunto B^A tiene cardinal $|B|^{|A|}$.*

Dem. Basta demostrar que existe una biyección φ entre B^A y $B^{|A|}$. Sea $A = \{a_1, \dots, a_n\}$, $B = \{b_1, \dots, b_m\}$ y $\varphi(f)$ la n-tupla cuya coordenada i-ésima es $f(a_i)$, para $i \in [1..n]$. Dejamos como ejercicio verificar que φ así definida es una biyección. □

Recordemos que $\mathcal{P}(A)$, el conjunto potencia de un conjunto A, consiste en el conjunto cuyos elementos son los subconjuntos de A. Tenemos, por ejemplo, que $\mathcal{P}(\{a, b\})$ es $\{\emptyset, \{a\}, \{b\}, \{a, b\}\}$ o $\mathcal{P}(\emptyset) = \{\emptyset\}$. ¿Qué podemos decir del cardinal de $\mathcal{P}(A)$ en términos del cardinal de A?. Lo primero que notamos es que si A es finito entonces $\mathcal{P}(A)$ también lo es. En la siguiente propiedad daremos su valor exacto.

Ejercicio (Cardinal del conjunto potencia): Si A es un conjunto finito, entonces el conjunto de sus partes, $\mathcal{P}(A)$, tiene cardinal finito dado por $|\mathcal{P}(A)| = 2^{|A|}$.

Indicación: Muestre que $|\mathcal{P}(A)| = |\{0,1\}^{|A|}|$. Para ello, considere una enumeración $a_1, ..., a_n$ de A y $\varphi : \{0,1\}^n \to \mathcal{P}(A)$ donde $\varphi((x_1, ..., x_n)) = \{a_i : x_i = 1\}$. Considere además $\xi : \mathcal{P}(A) \to \{0,1\}^n$ tal que $\xi(C) = (x_1, \dots, x_n)$ donde $x_i = 1$ si y sólo si $a_i \in C$. Pruebe que ξ es inversa de φ. △

Guía Básica

Determinar la veracidad de las siguientes afirmaciones:

1. $\sum_{k=0}^{n}\sum_{j=0}^{m} a_{kj} = \sum_{i=0}^{m}\sum_{j=0}^{n} a_{kj}$.
2. $\sum_{k=0}^{n}\sum_{j=0}^{m} a_{kj} = \sum_{j=0}^{m}\sum_{k=0}^{n} a_{kj}$.
3. $\sum_{k=0}^{n}\sum_{j=0}^{m} a_{kj} = \sum_{j=0}^{m}\sum_{k=0}^{n} a_{jk}$.
4. $\sum_{k=0}^{n}\sum_{j=0}^{m} c_k d_j = \sum_{k=0}^{n} c_k \sum_{j=0}^{m} d_j$.
5. $\sum_{i=0}^{n}\sum_{j=0}^{m} ij = (n+1)(m+1)$.
6. $\sum_{i=0}^{n}\sum_{j=0}^{m} ij = nm$.
7. $\sum_{i=0}^{n}\sum_{j=0}^{m} ij = \frac{1}{4}n(n+1)m(m+1)$.
8. $\sum_{i=0}^{n}\sum_{j=0}^{m} 2 = 2nm$.
9. $\sum_{i=0}^{n}\sum_{j=0}^{m} 2 = 2(n+1)(m+1)$.
10. $\sum_{i=0}^{n}\sum_{j=0}^{m} i = \frac{1}{2}n(n+1)(m+1)$.
11. $\sum_{i=0}^{n}\sum_{j=0}^{m} i = \frac{1}{2}n(n+1)$.
12. $\sum_{i=0}^{n}\sum_{j=0}^{m} i = \frac{1}{2}m(m+1)(n+1)$.
13. $\sum_{i=0}^{N}\sum_{j=0}^{M}\sum_{k=0}^{L} a_k = \sum_{j=0}^{N}\sum_{k=0}^{M}\sum_{i=0}^{L} a_i$.
14. $\sum_{i=0}^{N}\sum_{j=0}^{i} a_i = \sum_{j=0}^{N}\sum_{i=0}^{j} a_j$.
15. $\sum_{i=0}^{N}\sum_{j=0}^{i} a_j = \sum_{j=0}^{N}\sum_{i=0}^{j} a_i$.
16. Si $k \leq n$, entonces $\binom{n}{k} + \binom{n+1}{k+1} = \binom{n+1}{k+1}$.
17. Si $1 \leq k \leq n$, entonces $\binom{n-1}{k} + \binom{n}{k+1} = \binom{n+1}{k+1}$.
18. Si $k \leq n$, entonces $\binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1}$.
19. Si $1 \leq k \leq n$, entonces $\binom{n}{k-1} + \binom{n}{k} = \binom{n+1}{k+1}$.
20. Si $1 \leq k \leq n$, entonces $\binom{n-1}{k-1} + \binom{n}{k} = \binom{n+1}{k+1}$.
21. Dados $x, y \in \mathbb{R}$ y $n \geq 0$, se tiene que $(x+y)^n = \sum_{k=0}^{n}\binom{n}{k}x^k y^{n-k}$.
22. Dados $x, y \in \mathbb{R}$ y $n \geq 0$, se tiene que $(x-y)^n = \sum_{k=0}^{n}\binom{n}{k}x^k y^{n-k}$.
23. Dados $x, y \in \mathbb{R}$ y $n \geq 0$, se tiene que $(x-y)^n = -\sum_{k=0}^{n}\binom{n}{k}x^k y^{n-k}$.
24. Dados $x, y \in \mathbb{R}$ y $n \geq 0$, se tiene que $(x-y)^n = \sum_{k=0}^{n}\binom{n}{k}(-1)^{n-k}x^k y^{n-k}$.
25. Dados $x, y \in \mathbb{R}$ y $n \geq 0$, se tiene que $(x+y)^{2n} = \sum_{k=0}^{n}\binom{n}{2k}x^{2k} y^{n-2k}$.
26. Dados $x, y \in \mathbb{R}$ y $n \geq 0$, se tiene que $(x+y)^{2n} = \sum_{k=0}^{2n}\binom{2n}{k}x^k y^{2n-k}$.
27. Dados $x, y \in \mathbb{R}$ y $n \geq 0$, se tiene que $(x+y)^n = \sum_{k=0}^{n}\binom{n}{n-k}x^k y^{n-k}$.
28. Dados $x, y \in \mathbb{R}$ y $n \geq 0$, se tiene que $(x+y)^n = \sum_{k=0}^{n}\binom{n}{k}y^k x^{n-k}$.
29. Dados $x, y \in \mathbb{R}$ y $n \geq 0$, se tiene que $(x+y)^n = \sum_{k=1}^{n}\binom{n}{k-1}y^{k-1} x^{n-k+1}$.
30. Dados $x \in \mathbb{R}$ y $n \geq 0$, se tiene que $x^n = \sum_{k=0}^{n}\binom{n}{k}x^k$.
31. Dados $x \in \mathbb{R}$ y $n \geq 0$, se tiene que $(x+1)^n = \sum_{k=0}^{n}\binom{n}{k}x^k$.

32. Dados $x \in \mathbb{R}$ y $n \geq 0$, se tiene que $(x-1)^n = \sum_{k=0}^{n} \binom{n}{k} x^k$.
33. Dado $n \geq 0$, se tiene que $1^n = \sum_{k=0}^{n} \binom{n}{k}$.
34. Dado $n \geq 0$, se tiene que $2^n = \sum_{k=0}^{n} \binom{n}{k}$.
35. Dado $n \geq 0$, se tiene que $(-1)^n = \sum_{k=0}^{n} \binom{n}{k}(-1)^k$.
36. Dado $n \geq 0$, se tiene que $0 = \sum_{k=0}^{n} \binom{n}{k}(-1)^k$.
37. Dados $0 \leq k \leq n$, el término multiplicando a x^k en la expansión de $(x+y)^n$ es y^{n-k}.
38. Dados $0 \leq k \leq n$, el término multiplicando a x^k en la expansión de $(x+y)^n$ es $\binom{n-k}{k} y^{n-k}$.
39. Dados $0 \leq k \leq n$, el término multiplicando a x^k en la expansión de $(x+y)^n$ es $\binom{n}{k} y^{n-k}$.
40. Dados $0 \leq k \leq n$, el término multiplicando a x^k en la expansión de $(x+y)^n$ es $\binom{n}{n-k} y^{n-k}$.
41. Dados $0 \leq k \leq n$, el término multiplicando a x^k en la expansión de $(x+y)^n$ es $\binom{n}{k} y^k$.
42. Dados $0 \leq k \leq n$, el término multiplicando a x^k en la expansión de $(x+y)^n$ es $\binom{n}{k} y$.
43. Para todo conjunto finito A, $|A| < |A|$.
44. Para todo conjunto finito A, $|A| \leq |A|$.
45. Dados A y B conjuntos finitos, $A \subseteq B \implies |A| \leq |B|$.
46. Dados A y B conjuntos finitos, $A \subseteq B \implies |B| \leq |A|$.
47. Dados A y B conjuntos finitos, $A \subseteq B \implies |A| < |B|$.
48. Dados A, B y C conjuntos finitos, $|A| \leq |B| \wedge |B| \leq |C| \implies |A| \leq |C|$.
49. Dados A y B conjuntos finitos, $|A| \leq |B| \wedge |B| \leq |A| \iff |A| = |B|$.
50. Dados A y B conjuntos finitos, $|A \setminus B| = |A| - |B|$.
51. Dados A y B conjuntos finitos, $|A \setminus B| = |A| - |B| + |B \setminus A|$.
52. Dados A y B conjuntos finitos, $|A \cup B| = |A| + |B|$.
53. Dados A y B conjuntos finitos, $|A \times B| = |A||B|$.

Guía de Ejercicios

1. Escriba con notación de sumatoria las siguientes sumas y calcúlelas cuando pueda:

   a) $1+1+x+1+x+x^2+1+x+x^2+x^3+1+x+x^2+x^3+x^4+1+x+x^2+x^3+x^4+x^5$.
   b) $a+b+(a+b)^2+(a+b)^3+(a+b)^4+(a+b)^5$.
   c) $1+1+\frac{1}{2}+1+\frac{1}{2}+\frac{1}{4}+1+\frac{1}{2}+\frac{1}{4}+\frac{1}{8}+1+\frac{1}{2}+\frac{1}{4}+\frac{1}{8}+\frac{1}{16}$.
   d) $1+1+2+1+2+3+1+2+3+4+1+2+3+4+5+1+2+3+4+5+6$.
   e) $1+1+4+1+4+9+1+4+9+16+1+4+9+16+25+1+4+9+16+25+36$.
   f) $1+x+x^2+x^3+x^4+x^5+x+x^2+x^3+x^4+x^5+x^2+x^3+x^4+x^5+x^3+x^4+x^5+x^4+x^5+x^5$.

2. Desarrolle las siguientes sumas, hasta donde le sea posible (puede que no obtenga resultados demasiado explícitos)

a) $\sum_{i=0}^{N}\sum_{j=0}^{i}(a_i - a_{i+1})$.
b) $\sum_{i=0}^{N}\sum_{j=0}^{i}(a_j - a_{j+1})$.
c) $\sum_{i=1}^{N}\sum_{j=i-1}^{i+1}(a_j - a_{j+1})$.
d) $\sum_{i=0}^{N}\sum_{j=0}^{i} q^j$.
e) $\sum_{i=0}^{N}\sum_{j=i}^{N} q^j$.

3. Desarrolle las siguientes sumas, hasta donde le sea posible (puede que no obtenga resultados demasiado explícitos)

a) $\sum_{k=1}^{n}\binom{n}{k} - \sum_{k=0}^{n-1}\binom{n+1}{k}$.
b) $\sum_{i=0}^{n-1} x^{n-1-i}y^i$ para $x \neq y$.
c) $\sum_{i=0}^{N}\sum_{k=0}^{N}\binom{N}{k}$
d) $\sum_{i=0}^{N}\sum_{k=i}^{N}\binom{N}{k}$
e) $\sum_{i=0}^{N}\sum_{k=0}^{i}\binom{i}{k}a^k b^{i-k}$
f) $\sum_{i=0}^{N}\sum_{k=0}^{i}\binom{i}{k}a^k b^{N-k}$

4. Encuentre el valor de las siguientes sumas, usando el teorema del Binomio:

a) $\sum_{k=0}^{n}\binom{n}{k}$.
b) $\sum_{k=1}^{n}\frac{1}{k!(n-k)!}$.
c) $\sum_{k=3}^{n-2}\binom{n}{k}a^k b^{n-k}$.
d) $\sum_{k=0}^{r}\binom{r}{k}a^k b^{n-k}$.
e) $\sum_{k=0}^{n}\binom{r}{k}2^k(-1)^{n-k}$.
f) $\sum_{k=1}^{n}\frac{n-1}{k!(n-k)!}$.
g) $\sum_{k=1}^{n}\frac{(n-1)!}{k!(n-k)!}$.
h) $\sum_{k=2}^{n+1}\binom{k}{2}$.
i) $\sum_{i=1}^{n}\binom{i+j-1}{j}$.
j) $\sum_{k=2}^{n+1}\binom{k}{2}$.
k) $\sum_{k=0}^{n}\binom{n}{k}\frac{1}{k+1}$.

5. Sean k, p, n naturales tales que $0 \leq k \leq p \leq n$. Pruebe las siguientes igualdades:

a) $\binom{n}{k}\binom{n-k}{p-k} = \binom{n}{p}\binom{p}{k}$.
b) $\binom{n}{0}\binom{n}{p} + \binom{n}{1}\binom{n-1}{p-1} + ... + \binom{n}{p}\binom{n-p}{0} = 2^p\binom{n}{p}$.
c) $\binom{n}{k} = \binom{n+1}{k+1} - \binom{n}{k+1}$.

6. Encuentre el valor de los coeficientes pedidos:

a) El coeficiente de x^{50} en el desarrollo de $(x-a)^{100}$, con $a \in \mathbb{R}$.
b) El coeficiente de x^{10} en el desarrollo de $(x+2a)^{50}$, con $a \in \mathbb{R}$.
c) El coeficiente de x^3 en el desarrollo de $(x^3 + x^2 + x + 1)^3$.
d) El coeficiente de x^n en el desarrollo de $(x^n - a^n)^n$, con $a \in \mathbb{R}$.
e) El coeficiente de x^4 en el desarrollo de $(1 + 2x + 3x^2)^5$.

7. Muestre que los siguientes conjuntos son finitos.

   a) $A = \{f : [1..n] \to [1..n] \mid f \text{ es biyectiva }\}$.
   b) $C = \{f : \mathbb{R} \to \mathbb{N} \mid f \text{ es biyectiva}\}$.
   c) $D = \{$*todas las estaturas (en cms) de los habitantes del planeta tierra*$\}$.
   d) Dados $a < b \in \mathbb{R}$, $E = (-\infty, b] \cap [a, \infty) \cap \mathbb{N}$.

8. Demuestre que para A, B y C conjuntos finitos

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|.$$

9. Calcule $|(A \cup C) \times (B \cup C)|$ en términos del cardinal de A, B y C y/o sus intersecciones.
10. Sean p y q primos distintos. Calcule en función de p y q la cardinalidad de

$$C = \{n \in \mathbb{N} \mid n < (pq)^2 \text{ tal que } p \text{ o } q \text{ dividen a } n\}.$$

11. Calcule la cardinalidad de $S = \{(a, b, c) \in \mathbb{N}^3 : a + b + c = 50\}$.
12. Sea $\mathcal{C}$ una partición de un conjunto finito A de modo que para todo $X, Y \in \mathcal{C}$, $|X| = |Y|$. Demuestre que $|\mathcal{C}|$ divide a $|A|$.
13. Determine cuántas particiones con dos partes hay en un conjunto finito de cardinal n. ¿Cuántas hay con tres partes?.

Guía de Problemas

1. (20 min.) Demuestre, sin usar inducción, que:

$$\sum_{k=1}^{n} (1 + 4 + 4^2 + \cdots + 4^{k-1}) \binom{n}{k} = \frac{5^n - 2^n}{3}.$$

2. (20 min.) Calcule, sin usar inducción: $\displaystyle\sum_{j=1}^{n} \sum_{i=1}^{j} \sum_{k=0}^{i} \binom{i}{k} \frac{8^{k+1}}{3^i}$.
3. (20 min.) Demuestre que $\forall n \in \mathbb{N}$, $\displaystyle\sum_{k=0}^{n} (1 - x)^k = \sum_{k=0}^{n} (-1)^k \binom{n+1}{k+1} x^k$.
4. (20 min.) Calcule la suma $\displaystyle\sum_{k=0}^{n} k 7^k \binom{n}{k}$.
5. a) (15 min.) Demuestre que $\forall n, i, k \in \mathbb{N}$ con $k \leq i \leq n$, $\binom{n}{i}\binom{i}{k} = \binom{n}{k}\binom{n-k}{i-k}$.
   b) (15 min.) Use lo anterior para probar sin uso de inducción que:

$$\sum_{i=k}^{n} \binom{n}{i} \binom{i}{k} = \binom{n}{k} 2^{n-k}$$

6. Demuestre que:

   a) $|\{2i+1 \mid i \in \mathbb{N}, 0 \leq i < 2^{n-1}, n \in \{1,\ldots,m\}\}| = 2^{m-1}$.
   b) $|\{\frac{2i+1}{2^n} \mid i \in \mathbb{N}, 0 \leq i < 2^{n-1}, n \in \{9,10\}\}| = 2^8 + 2^9$.
   c) $|\{\frac{2i+1}{2^n} \mid i \in \mathbb{N}, 0 \leq i < 2^{n-1}, n \in \{1,\ldots,m\}\}| = 2^m - 1$.

7. Sea $\mathcal{C}$ una partición de un conjunto finito A. Demuestre que el cardinal de A es igual a la suma de los cardinales de las partes de $\mathcal{C}$, es decir, $|A| = \sum_{C \in \mathcal{C}} |C|$.

8. Sea $A_1, \ldots A_n$ conjuntos finitos.

   a) Demuestre que $|\bigcup_{i=1}^n A_i| \leq \sum_{i=1}^n |A_i|$.
   b) Demuestre que $|\bigcup_{i=1}^n A_i| = \sum_{i=1}^n |A_i|$ si y sólo si para todo $i, j \in [1..n]$, $i \neq j$ implica $A_i \cap A_j = \emptyset$.

9. (30 min) Sea $A = [1..n]$ y considere la secuencia $(x_0, x_1, x_2, x_3, ...)$ de elementos en A (es decir, $x_i \in A$ para cada $i \in \mathbb{N}$). Probar que existen $\ell, j \in \mathbb{N}$, $\ell \neq j$, tales que $x_\ell = x_j$.

10. Sea S_n el conjunto de las funciones biyectivas en $[1..n]^{[1..n]}$.

    a) Determine cuántas funciones f en S_n cumplen que $f(1) = 1$.
    b) Determine cuántas funciones f en S_n cumplen que $\exists x \in [1..n], f(x) = x$, para $n = 3$.
    c) Determine cuántas funciones f en S_n cumplen que $\forall x \in [1..n], f(x) \neq x$, para $n = 4$.
    d) Determine cuántas funciones f en S_n cumplen que $\exists! x \in [1..n], f(x) = x$, para $n = 5$.

SEMANA 09:

Conjuntos infinitos

En lo que sigue anotaremos $|A| = |B|$ para indicar que existe $f : A \to B$ biyectiva. Es decir, $|A| = |B|$ si A tiene igual cardinal que B. También anotaremos $|A| \leq |B|$ para indicar que existe $f : A \to B$ inyectiva. Es decir, $|A| \leq |B|$ si A tiene cardinal menor o igual que B. Por último, escribiremos $|A| < |B|$ cuando $|A| \leq |B|$ y $|A| \neq |B|$. Notar que estas convenciones son consistentes con la ya adoptada de denotar por enteros no-negativos el cardinal de un conjunto finito.

Partamos con las siguientes propiedades básicas acerca de $|\cdot|$:

Proposición 8.1 *Para A y B conjuntos no vacíos se tienen las siguientes propiedades.*

(i) $|A| \leq |A|$ *(reflexividad de menor o igual cardinal)*

(ii) *Si $A \subseteq B$, entonces* $|A| \leq |B|$

(iii) *Si* $|A| \leq |B|$ *y* $|B| \leq |C|$, *entonces* $|A| \leq |C|$ *(transitividad de menor o igual cardinal)*

(iv) $|A| \leq |B| \wedge |B| \leq |A| \iff |A| = |B|$

Dem. Las dos primeras propiedades se justifican por la existencia de la función $\mathrm{id}_A : A \to A$ y la función $f : A \to B$ con $f(x) = x$, ambas inyectivas. La tercera es consecuencia de que la composición de funciones inyectivas es inyectiva. La última propiedad, cuya demostración escapa del alcance de este curso, es conocida como el Teorema de Cantor-Berstein-Schröder. □

En la próxima propiedad damos una relación entre el cardinal de la imagen de una función y el de su domino.

Proposición 8.2 (Cardinal de la imagen de un conjunto) *Si $f : A \to B$ es función, entonces* $|f(A)| \leq |A|$.

Dem. Consideremos la función $g : f(A) \to A$ tal que $g(b) = a$ donde a es un elemento cualquiera perteneciente a $f^{-1}(b)$ (observar que $f^{-1}(b) \neq \emptyset$ porque $b \in f(A)$). Con esta definición se cumple que $f(g(b)) = b$.

Entonces g es un función inyectiva pues si $g(b) = g(c)$ entonces $b = f(g(b)) = f(g(c)) = c$. Por definición, se obtiene que $|f(A)| \leq |A|$. □

Claramente no todo conjunto es finito.

Definición 8.3 (Conjunto infinito) *Un conjunto que no es finito se dice* ***infinito****.*

Proposición 8.4 $\mathbb{N}$ *es infinito.*

Dem. Supongamos que $\mathbb{N}$ fuese finito. Entonces, existiría un $k \in \mathbb{N}$ tal que $|\mathbb{N}| = k$. Es decir, existiría una función biyectiva g entre $\mathbb{N}$ y $[1..k]$.

Como $[1..k+1] \subseteq \mathbb{N}$ sabemos que existe una función inyectiva $f : [1..k+1] \to \mathbb{N}$ y, por lo tanto, $g \circ f : [1..k+1] \to [1..k]$ es una función inyectiva. Esto contradice lo que hemos probado para los conjuntos finitos $[1..k]$ y $[1..k+1]$. □

8.1 Conjuntos numerables

Definición 8.5 (Conjuntos Numerables) *Llamaremos conjunto* ***numerable*** *a cualquier conjunto que tenga la misma cardinalidad que* $\mathbb{N}$*.*

Proposición 8.6 $\mathbb{Z}$ *es numerable.*

Dem. Listemos ordenadamente los elementos de $\mathbb{Z}$:

$\mathbb{Z}$	...	-6	-5	-4	-3	-2	-1	0	1	2	3	4	5	6	...

Construiremos una función de $\mathbb{N}$ a $\mathbb{Z}$ simplemente asignando a cada natural un entero. Notemos que de esta forma estaremos **enumerando** los elementos de $\mathbb{Z}$. Es decir, iremos "contando" $0, 1, 2, 3, 4, \ldots$ en la medida que recorremos $\mathbb{Z}$. Una posible forma de hacerlo es la siguiente:

$\mathbb{Z}$	...	-6	-5	-4	-3	-2	-1	0	1	2	3	4	5	6	...
$\mathbb{N}$	...	11	9	7	5	3	1	0	2	4	6	8	10	12	...

Observemos que ésta es una forma sencilla de construir una $f : \mathbb{N} \to \mathbb{Z}$, que en nuestro caso posee una forma explícita:

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

Queda como ejercicio para el lector demostrar que esta f es efectivamente biyectiva, con lo que se concluye que $|\mathbb{N}| = |\mathbb{Z}|$, lo que buscábamos. □

Al igual que lo hecho para conjuntos finitos, podemos nombrar los elementos de un conjunto numerable A aprovechando una biyección f entre $\mathbb{N}$ y A. Así, llamamos a_i al elemento de A tal que $f(i) = a_i$ y a $(a_i)_{i\in\mathbb{N}}$ una numeración de A. De esta forma, no sólo podemos escribir un conconjunto finito A, como $A = \{a_1, ..., a_n\}$ para algún n, sino que también, si A es numerable, lo podemos escribir como $A = \{a_1, a_2, ...\}$ (o $A = \{a_0, a_1, ...\}$ según sea más conveniente). Esta flexibilidad adicional resulta muy útil.

Proposición 8.7 ($|\mathbb{N}|$ es el menor cardinal infinito) *Sea A un conjunto infinito cualquiera. Entonces, para todo $a_1 \in A$ y para todo $k \in \mathbb{N}$, $k \geq 1$, se cumplen las siguientes afirmaciones.*

- *A tiene un subconjunto finito B_k de cardinal k con $a_1 \in B_k$.*
- *A tiene un subconjunto numerable H, con $a_1 \in H$. En particular, $|A| \geq |\mathbb{N}|$.*

Dem. Para demostrar la primera parte, aplicamos inducción en k. Para $k = 1$ consideramos $B_1 = \{a_1\}$. Aceptamos que para $k \geq 1$ existe un subconjunto B_k de A de cardinal k. Como A no es finito, $B_k \neq A$. Luego, existe $a_{k+1} \in A \setminus B_k$ que junto a B_k forma el subconjunto $B_{k+1} = B_k \cup \{a_{k+1}\}$ de A de cardinal $k + 1$.

Para la segunda parte, sea $H = \bigcup_{k\in\mathbb{N},k\geq 1} B_k$. Veamos que H es infinito. Si no lo fuera, entonces $|H| = \ell$ para algún $\ell \in \mathbb{N}$. Pero para $k > \ell$, $B_k \subseteq H$ lo que produce la contradicción $|H| \geq k$.

Notemos que por la construcción de H la función $f : \mathbb{N} \to H$, dada por $f(k) = a_{k+1}$, es una biyección. Con esto concluimos que H es numerable. □

Corolario 8.8 *Todo conjunto infinito A con $|A| \leq |\mathbb{N}|$ es numerable.*

Dem. Por hipótesis $|A| \leq |\mathbb{N}|$. Por la Proposición 8.7, sabemos que $|A| \geq |\mathbb{N}|$. Luego, de la parte (IV) de la Proposición 8.1, sigue que $|A| = |\mathbb{N}|$. □

Intuitivamente, al agregar o quitar una cantidad finita de elementos a un conjunto infinito este sigue siendo infinito. La siguiente propiedad permite formalizar esta intuición.

Proposición 8.9 (Perturbación de un conjunto infinito por uno finito) *Sea A infinito y B finito. Entonces $|A \cup B| = |A \setminus B| = |A|$*

Dem. Probaremos la propiedad usando inducción en el cardinal del conjunto B. Por lo antes hecho sabemos que existe H numerable contenido en A. Sea $(a_i)_{i\in\mathbb{N}}$ una numeración de H.

Caso base $|B| = 1$. Digamos $B = \{a\}$. Supongamos primero que $a \notin A$. Definimos $f : A \cup B \to A$ como sigue: $f(x) = x$ si $x \notin H$, $f(a_i) = a_{i+1}$ y $f(a) = a_0$. Se verifica que f es biyección (propuesto). Luego, $|A \cup B| = |A|$. Por nuestro supuesto $a \notin A$, tenemos que $A \setminus B = A$ con lo que $|A \setminus B| = |A|$.

Supongamos ahora que $a \in A$. Por la Proposición 8.7 podemos suponer que $a \in H$ y que $a_0 = a$. De esta forma, la función $g : A \setminus B \to A$ definida por $g(x) = x$, si $x \notin H$, y $g(a_i) = a_{i-1}$, para $i \in \mathbb{N}, i \geq 1$, es una biyección (propuesto). Luego, $|A \setminus B| = |A|$. Por nuestro supuesto $a \in A$, tenemos que $A \cup B = A$ con lo que $|A \cup B| = |A|$.

Paso inductivo: Si $|B| = k + 1$, $k \geq 0$ entonces tomamos $a \in B$ y consideramos $B' = B \setminus \{a\}$ con cardinal $|B'| = k$. Por hipótesis de inducción, $|A \cup B'| = |A \setminus B'| = |A|$. Por el caso base, $|(A \cup B') \cup \{a\}| = |A \cup B'| = |A|$ y $|(A \setminus B') \setminus \{a\}| = |(A \setminus B')|$. Poniendo todo junto se obtienen las conclusiones. □

Proposición 8.10 (Unión finita de numerables) *Si A y B son conjuntos numerables, entonces $A \cup B$ también lo es. En general, si $A_1, \ldots, A_n$ es una familia de n conjuntos numerables, entonces $\bigcup_{i=1}^{n} A_i$ también lo es.*

Dem. Sea $(a_i)_{i \in \mathbb{N}}$ una numeración de A y $(b_j)_{j \in \mathbb{N}}$ una numeración de B.

Consideramos dos situaciones. La primera, cuando $A \cap B = \emptyset$. Entonces, la función $f : A \cup B \to \mathbb{N}$, dada por $f(a_i) = 2i$ y $f(b_j) = 2j + 1$, define una biyección entre $A \cup B$ y $\mathbb{N}$. Concluimos que $A \cup B$ es numerable. De aquí es fácil probar por inducción que la propiedad se tiene para una familia finita de n conjuntos numerables cuando los conjuntos son disjuntos de a pares.

Cuando A y B tienen elementos en común consideramos $A \cup B = (A \setminus B) \cup B$. En el lado derecho de la igualdad los conjuntos involucrados son disjuntos. Al menos uno de ellos debe ser numerable pues $A \cup B$ es infinito. Hemos visto que el cardinal de un conjunto infinito no varía al perturbarlo con un conjunto finito. De esta forma, el cardinal de $A \cup B$ será el cardinal de la unión disjunta de conjuntos numerables (potencialmente uno solo) y, por ende, será numerable.

Nuevamente, aplicando inducción, la conclusión se obtiene para una familia finita de conjuntos numerables. □

Es importante que nos detengamos en el siguiente punto: cuando construimos la asociación entre $\mathbb{N}$ y $\mathbb{Z}$ mediante el diagrama

$\mathbb{Z}$	...	-6	-5	-4	-3	-2	-1	0	1	2	3	4	5	6	...
$\mathbb{N}$	...	11	9	7	5	3	1	0	2	4	6	8	10	12	...

ya hemos establecido una función f de $\mathbb{N}$ a $\mathbb{Z}$, a pesar de que su forma explícita la damos después. A través del diagrama estamos dando el valor de $f(n)$ sólo para los naturales $n \leq 12$. Sin embargo, también estamos dejando en claro la forma de calcular $f(n)$ para los naturales $n > 12$.

Por ejemplo, es claro gracias al proceso que seguimos, que $f(13) = -7$ y que $f(20) = 10$. Y para esto no hace falta conocer la forma explícita de la función f. Es más, veremos casos

donde no es fácil mostrar explícitamente la función f que corresponda, por lo que no nos preocuparemos de ella. Simplemente, mostraremos la enumeración que hay que hacer en cada caso.

Proposición 8.11 $\mathbb{N} \times \mathbb{N}$ *es numerable.*

Dem. Para este caso, ordenaremos los elementos de $\mathbb{N} \times \mathbb{N}$ en una tabla de doble entrada:

$\mathbb{N} \times \mathbb{N}$	0	1	2	3	4	5	...
0	(0,0)	(0,1)	(0,2)	(0,3)	(0,4)	(0,5)	...
1	(1,0)	(1,1)	(1,2)	(1,3)	(1,4)	(1,5)	...
2	(2,0)	(2,1)	(2,2)	(2,3)	(2,4)	(2,5)	...
3	(3,0)	(3,1)	(3,2)	(3,3)	(3,4)	(3,5)	...
4	(4,0)	(4,1)	(4,2)	(4,3)	(4,4)	(4,5)	...
5	(5,0)	(5,1)	(5,2)	(5,3)	(5,4)	(5,5)	...
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋱

Y ahora, para enumerar $\mathbb{N} \times \mathbb{N}$, asociaremos a cada casilla de la tabla un número natural distinto:

$\mathbb{N} \times \mathbb{N}$	0	1	2	3	4	5	...
0	0	1	3	6	10	15	...
1	2	4	7	11	16		...
2	5	8	12	17			...
3	9	13	18				...
4	14	19					...
5	20						...
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋱

Observar que es crucial el que las casillas se enumeren siguiendo las "diagonales" – si se procede por filas (respectivamente, por columnas), el argumento falla, pues nunca "terminamos" de enumerar las casillas de la primera fila (respectivamente, columna).

De esta manera hemos establecido un proceso que enumera $\mathbb{N} \times \mathbb{N}$. Por lo tanto, sabemos que hay una función biyectiva entre $\mathbb{N}$ y $\mathbb{N} \times \mathbb{N}$, y así concluimos lo que deseábamos demostrar.

Como ejercicio, demuestre que la función $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ definida por $f(i, j) = (i + j)(i + j + 1)/2 + i$, que corresponde a la enumeración de la tabla usada arriba, es una biyección. □

Proposición 8.12 *Si A y B son conjuntos numerables, entonces $A \times B$ también lo es. En general, si $A_1, \ldots, A_n$ son n conjuntos numerables, entonces $A_1 \times \cdots \times A_n$ también lo es.*

Dem. La demostración anterior se extiende casi idéntica para probar que el producto cartesiano de dos conjuntos numerables es numerable. Otra forma de ver esto es como sigue. Sean $(a_i)_{i\in\mathbb{N}}$ y $(b_j)_{j\in\mathbb{N}}$ numeraciones para A y B, respectivamente. Entonces la función $f(a_i, b_j) = (i, j)$ es una biyección entre $A \times B$ y $\mathbb{N} \times \mathbb{N}$ que muestra que $A \times B$ es numerable. Aplicando un argumento de inducción se obtiene la propiedad para una familia de n conjuntos numerables. □

Corolario 8.13 $\mathbb{Q}$ *es numerable.*

Dem. Como $\mathbb{Q}$ es un conjunto infinito, sabemos inmediatamente que $|\mathbb{N}| \leq |\mathbb{Q}|$. Basta demostrar entonces que $|\mathbb{Q}| \leq |\mathbb{N}|$. Consideremos la función $f : \mathbb{Z} \times (\mathbb{N} \setminus \{0\}) \to \mathbb{Q}$ dada por $f(k, n) = k/n$. Entonces, f es epiyectiva, pues todo racional r se puede escribir de la forma $r = k/n$, con $k \in \mathbb{Z}$ y $n \in \mathbb{N} \setminus \{0\}$.

De la Proposición 8.2 sabemos que $|f(\mathbb{Z} \times (\mathbb{N} \setminus \{0\})| \leq |\mathbb{Z} \times (\mathbb{N} \setminus \{0\})|$. Como f es epiyectiva se concluye que $|\mathbb{Q}| \leq |\mathbb{Z} \times (\mathbb{N} \setminus \{0\})| = |\mathbb{N}|$, pues $\mathbb{Z}$ y $\mathbb{N} \setminus \{0\}$ son conjuntos numerables. □

Proposición 8.14 (Unión numerable de numerables) *La unión de una familia numerable de conjuntos numerables es numerable.*

Dem. Sean $(A_i)_{i\in\mathbb{N}}$ una numeración de la familia y sea $H = \bigcup_{i\in\mathbb{N}} A_i$. Queremos ver que $|H| = |\mathbb{N}|$.

Cada uno de los conjuntos A_i es un conjunto numerable, entonces para cada uno de ellos existe una numeración $A_i = (a^i_j)_{j\in\mathbb{N}}$.

Sea $f : \mathbb{N} \times \mathbb{N} \to H$ la función que a (i, j) asocia a^i_j. Esta es una función epiyectiva pudiendo no ser inyectiva. Sabemos que $|f(\mathbb{N} \times \mathbb{N})| \leq |\mathbb{N} \times \mathbb{N}|$. Luego, $|H| \leq |\mathbb{N}|$. Como H es infinito sabemos que $|H| \geq |\mathbb{N}|$ y con esto se obtiene la conclusión. □

De manera análoga se establece lo siguiente:

Proposición 8.15 (Unión finita o numerable de finitos o numerables) *La unión de una familia finita o numerable de conjuntos finitos o numerables es finita o numerable, es decir, si* $(A_i)_{i\in I}$, $I \subseteq \mathbb{N}$, *es tal que* $|A_i| \leq |\mathbb{N}|$ *para todo* $i \in I$, *entonces* $\left|\bigcup_{i\in I} A_i\right| \leq |\mathbb{N}|$.

Ejemplo: Veamos que el conjunto de palabras, digamos Σ^*, que se pueden formar con las letras de un alfabeto Σ finito no vacío es un conjunto numerable. En efecto, las palabras de largo n que podemos formar son el conjunto de n-tuplas de elementos en Σ, o sea, el conjunto Σ^n. Luego, $\Sigma^* = \bigcup_{n\in\mathbb{N}} \Sigma^n$. Sabemos que Σ^n tiene cardinal finito (de hecho, igual a $|\Sigma|^n$), por lo que Σ^* es una unión numerable de conjuntos finitos. Por la Proposición 8.15, concluimos que Σ^* es finito o numerable. Pero, Σ^* no es finito, porque dado $\sigma \in \Sigma$, las palabras $\sigma, \sigma\sigma, \sigma\sigma\sigma, ...$ son distintas y estan en Σ^*, o sea, Σ^* contiene una infinidad de palabras. Sigue que Σ^* no es finito y se concluye que es numerable. ♢

8.2 Conjuntos no numerables

En la sección anterior, estudiamos los conjuntos numerables, una serie de propiedades acerca de ellos, y conocimos varios conjuntos numerables, como $\mathbb{Z}$, $\mathbb{N} \times \mathbb{N}$ y $\mathbb{Q}$. También hemos estudiado los conjuntos finitos. Queda, así, la pregunta:

¿Hay conjuntos infinitos no numerables? ¿Cuáles son?

Proposición 8.16 (Cardinal del conjunto potencia) *El cardinal del conjunto potencia de un conjunto es mayor que el cardinal del conjunto. Es decir, si A es un conjunto, entonces $|A| < |\mathcal{P}(A)|$.*

Dem. Sea A un conjunto. Lo primero que podemos justificar fácilmente es que existe una función inyectiva entre A y $\mathcal{P}(A)$ que podemos elegir como $f(a) = \{a\}$, para todo $a \in A$. Luego, $|A| \leq \mathcal{P}(A)$.

Para ver que no puede haber una función biyectiva entre A y $\mathcal{P}(A)$ procedemos por contradicción, suponiendo que sí existe una función biyectiva f entre A y $\mathcal{P}(A)$.

Consideramos el conjunto $B = \{x \in A : x \notin f(x)\}$, que es un subconjunto de A. Como tal, debe ser la imagen de algún elemento de A. Es decir, existe $a \in A$ con $f(a) = B$. Veamos que esto es una contradicción.

En efecto, si $a \in B$, entonces, por definición de B, se cumple que $a \notin f(a) = B$. Además, si $a \notin B = f(a)$ entonces, nuevamente por la definición de B, $a \in B$. Hemos probado de esta forma que $(x \in B) \Rightarrow (x \notin B)$ y que $(x \notin B) \Rightarrow (x \in B)$. Esto es $(x \in B) \Leftrightarrow (x \notin B)$, que sabemos es una contradicción. Por lo tanto $|A| \neq |\mathcal{P}(A)|$. $\square$

Las propiedades anteriores muestran que hay conjuntos con cardinal mayor que el de $\mathbb{N}$. Por ejemplo, $\mathcal{P}(\mathbb{N})$.

En lo que resta de esta sección nos dedicaremos a estudiar conjuntos no numerables con el cardinal de $\mathbb{R}$.

Del curso de Introducción al Cálculo se sabe que la función $\tan : (-\pi/2, \pi/2) \to \mathbb{R}$ es una función biyectiva. Entonces $|(-\pi/2, \pi/2)| = |\mathbb{R}|$.

También sabemos que el cardinal de un conjunto infinito no varía si se le agrega o se le quita un conjunto finito de elementos. Así, para todo $a, b \in \mathbb{R}$, $a < b$, se tiene que

$$|(a, b)| = |(a, b]| = |[a, b]|.$$

Por otra parte, la función lineal $f(x) = (x - a)/(b - a)$ es una biyección entre $[a, b]$ y $[0, 1]$. Así,

$$|\mathbb{R}| = |(-\pi/2, \pi/2)| = |[-\pi/2, \pi/2]| = |[0, 1]|.$$

Veamos que es posible definir una función inyectiva entre el conjunto potencia de $\mathbb{N}$ y el intervalo $[0,1]$. Esta construcción es similar a la que se suele hacer para demostrar que $|\mathcal{P}(A)| = 2^{|A|}$, cuando A es finito.

Proposición 8.17 $|\mathcal{P}(\mathbb{N})| \leq |[0,1]|$.

Dem. Vamos a construir una función inyectiva $f : \mathcal{P}(\mathbb{N}) \to [0,1]$. A cada $S \subseteq \mathbb{N}$ asociamos el número real $0.a_0a_1 \cdots a_i \cdots$, donde $a_i \in \{0,1\}$ y $a_i = 1$ si y sólo si $i \in S$.

Por ejemplo, si S es el conjunto finito $\{0,3,6\}$, entonces el número real asociado es 0,1001001. Por su parte, si S es el conjunto de los números pares, entonces el número real asociado es $0{,}101010\cdots 10\cdots = 10/99$.

Para dos subconjuntos distintos S y T de $\mathbb{N}$, existe $i \in \mathbb{N}$ tal que $i \in (S \setminus T) \cup (T \setminus S)$. Luego, $f(T)_i \neq f(S)_i$ lo que muestra que f es inyectiva. De esta forma $|\mathcal{P}(\mathbb{N})| \leq |[0,1]|$. □

Como sabemos que $|A| < |\mathcal{P}(A)|$ se concluye lo siguiente.

Corolario 8.18 $|\mathbb{N}| = |\mathbb{Z}| = |\mathbb{Q}| < |[0,1]| = |\mathbb{R}|$. *En particular,* $\mathbb{R}$ *no es numerable.*

Las preguntas inocentes pueden tener respuestas muy, pero muy, interesantes. Es natural preguntarse si existe un conjunto X con $|\mathbb{N}| < |X| < |\mathbb{R}|$. Se sabe que esta es una pregunta sin respuesta.

Podemos suponer que no existe un conjunto X con $|\mathbb{N}| < |X| < |\mathbb{R}|$ y no hay ninguna contradicción con la teoría de conjuntos generalmente aceptada, ¡y lo mismo ocurre si suponemos lo contrario!. El primer supuesto se conoce como la Hipótesis del Continuo.

Guía Básica

Determinar la veracidad de las siguientes afirmaciones:

1. $|\mathbb{N}| < |\mathbb{Z}|$.
2. $|\mathbb{N}| < |\mathbb{Z} \times \mathbb{Z}|$.
3. $|\mathbb{N}| = |\mathbb{Z} \times \mathbb{Z}|$.
4. $|\mathbb{N}| = |\mathbb{Q} \times \mathbb{Z}|$.
5. No todo conjunto infinito A cumple que $|\mathbb{N}| \leq |A|$.
6. Unión finita de conjuntos numerables es numerable.
7. Unión numerable de conjuntos numerables es numerable.
8. Producto cartesiano finito de conjuntos numerables es numerable.
9. Producto cartesiano finito de conjuntos finitos es finito.
10. El producto cartesiano de un conjunto finito no vacío con uno numerable es finito.
11. El producto cartesiano de un conjunto finito no vacío con uno numerable es numerable.
12. Todo subconjunto no vacío de un conjunto numerable es numerable.
13. Todo subconjunto de un conjunto numerable es numerable.
14. Todo subconjunto infinito de un conjunto numerable es numerable.
15. Todo subconjunto de un conjunto finito es numerable.
16. Todo subconjunto de un conjunto finito es finito.
17. $|[0,1)| \leq |\mathbb{R}|$
18. $|\mathbb{R}| < |[0,1)|$
19. $|[0,1)| < |\mathbb{N}|$
20. $|[0,1)| = |\mathbb{N}|$
21. $|\mathbb{N}| < |[0,1)|$
22. $|\mathbb{Q}| = |[0,1)|$
23. $|\mathbb{Q}| < |[0,1)|$
24. $|\mathbb{N}| = |\mathbb{R}|$
25. $|\mathbb{N}| = |\mathbb{Q}|$
26. $|\mathbb{N}| = |\mathbb{Z}|$
27. $|\mathbb{Z}| < |\mathbb{N}|$
28. $|\mathbb{Q}| < |\mathbb{N}|$
29. $|\mathbb{N}| < |\mathbb{N} \times \mathbb{N}|$
30. $|\mathbb{N}| = |\mathbb{N} \times \mathbb{N} \times \mathbb{N}|$
31. $|\mathbb{N}| < |\mathbb{R}|$
32. Dado $p \in \mathbb{N} \setminus \{1\}$, $|\mathbb{Z}| = |\mathbb{Z}_p|$
33. $|\mathbb{N}| = |\mathbb{Q} \times \mathbb{Z}|$

34. $|\mathbb{N}| < |\mathbb{Q} \times \mathbb{Z}|$

Guía de Ejercicios

1. Pruebe que los siguientes conjuntos son numerables. Señale cuál es la función utilizada para probarlo en cada parte.

   a) $A = \{2k \in \mathbb{Z} \mid k \in \mathbb{Z}\}$.
   b) $A = \{p^k \in \mathbb{Z} \mid k \in \mathbb{Z}\}$, dado $p \in \mathbb{Z}$ fijo.
   c) $A = \{(x, 0) \in \mathbb{N} \times \mathbb{N} \mid x \in \mathbb{N}\}$.
   d) $A = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} \mid x - y = -3\}$.
   e) $A = \{a^n + b^m \in \mathbb{R} \mid n, m \in \mathbb{Z}\}$, con $a, b \in \mathbb{R}$ fijos.
   f) $A = \{C_r \subseteq \mathbb{R}^2 \mid C_r$ es una circunferencia centrada en $(0, 0)$ y de radio $r \in \mathbb{N}\}$.

2. Sean $A, B \subseteq \mathbb{R}$ conjuntos numerables. Refiérase a la cardinalidad de los siguientes conjuntos, es decir indique si son o no numerables y por qué.

   a) $(A \times A) \times B$.
   b) $A + B = \{x \mid x = a + b, a \in A,\ b \in B\}$.
   Indicación: Escriba $A + B$ como $\bigcup_{b \in B} C_b$, con C_b adecuado.
   c) $AB = \{x \mid x = ab, a \in A,\ b \in B\}$.
   Indicación: Escriba AB como $\bigcup_{b \in B} C_b$, con C_b adecuado.
   d) $A \cap B$.
   e) $A \cup B$.

3. Demuestre que:

   a) $|\mathbb{N} \times \mathbb{Z}| = |\mathbb{N}|$.
   b) $|\mathbb{Q} \times \mathbb{Z}| = |\mathbb{N}|$.
   c) $|\mathbb{N}| < |\mathbb{R} \times \mathbb{Z}|$.
   Indicación: Pruebe que $|\mathbb{R}| \leq |\mathbb{R} \times \mathbb{Z}|$.
   d) $|\mathbb{N}| < |\mathbb{R} \setminus (\mathbb{N} \setminus \{0\})|$.
   Indicación: Use la demostración de $|\mathbb{N}| < |\mathbb{R}|$.

4. Muestre que los siguientes conjuntos son numerables. Recuerde que puede probar primero que el conjunto es infinito y luego que su cardinal es menor o igual al de uno numerable.

   a) $A = \{(m, n) \in \mathbb{Z}^2 \mid m \leq n\}$.
   b) $C = \{x \in \mathbb{R} \mid \exists k \in \mathbb{Z}, \exists i \in \mathbb{N}, x = k/3^i\}$.
   c) $D = \{x = (x_1, x_2, x_3) \in \mathbb{Z}^3 \mid x_1 < x_2 < x_3\}$.
   d) $G = \{$*circunferencias de radio y centro racional*$\}$.

5. Muestre que los siguientes conjuntos son no numerables. Recuerde que aquí basta probar que el cardinal del conjunto es mayor o igual al de uno no numerable.

a) $B = \{(x, y) \in \mathbb{R}^2 \mid x + y = 1\}$.
b) Sea $r \in \mathbb{Q} \setminus \{0\}$, $C = \{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 = r^2\}$.
c) Sean $a, b \in \mathbb{Q}$ con $a < b$, $E = (-\infty, b] \cap [a, \infty)$.

Guía de Problemas

1. Pruebe que los siguientes conjuntos son numerables.

   a) (30 min) $C = \{x \in [0, +\infty) \mid \exists n \in \mathbb{N} \setminus \{0\},\ x^n \in \mathbb{N}\}$.
   b) (20 min.) $A = \{x \in \mathbb{R} \mid \exists k \in \mathbb{Z}, \exists i \in \mathbb{N}, x = \frac{k}{3^i}\}$.
   c) (20 min.) El conjunto de todas las rectas no verticales que pasan por el punto $(0, 1)$ y cortan al eje OX en una coordenada racional.
   d) (20 min.) El conjunto de todas las rectas no verticales que no pasan por el origen y cortan a los ejes OX y OY en coordenadas racionales.
   e) (15 min.) $A = \{\frac{p}{q} \in \mathbb{Q} \mid (\exists n \in \mathbb{N}, q = 2^n) \wedge (p \in \mathbb{N}, p < q)\}$.
   f) (15 min.) $E = \{(a_1, ..., a_n) \in \{-1, 1\}^n \mid n \in \mathbb{N}, n \geq 2, \sum_{i=1}^{n} a_i = 0\}$.
   g) (15 min.) $E = \{x = (x_1, x_2, x_3) \in \mathbb{R} \times \mathbb{N} \times \mathbb{N} \mid \exists n \in \mathbb{N},\ x_1 + x_2 + x_3 = n\}$.

2. Pruebe que los siguientes conjuntos no son numerables:

   a) (15 min.) $A = \{x \in \mathbb{R}^3 \mid \exists n \in \mathbb{N},\ x_1 + x_2 + x_3 = n\}$.
   b) (15 min.) $\mathcal{T} = \{T \subseteq \mathbb{R}^2 \mid T \text{ es un triángulo}\}$.

3. (20 min.) Pruebe que el conjunto de todas las rectas no verticales que pasan por el punto $(0, 1)$ no es numerable.

4. a) (20 min.) Sea A un conjunto no numerable y sea $B \subseteq A$ un conjunto numerable. Pruebe que el conjunto $A \setminus B$ es no numerable.
   b) (10 min.) Demuestre, usando lo anterior, que el conjunto $\mathbb{I}$ de los números irracionales es no numerable.

SEMANA 10:

Estructuras algebraicas

Hemos estudiado conjuntos, como operar con ellos, como establecer relaciones y asociaciones entre sus elementos, etc. No obstante, algo que hacemos con mucha frecuencia es operar con los elementos de un conjunto. Por ejemplo, sumar y multiplicar números, ya sea enteros o reales, componer funciones, operamos con conjuntos (uniéndolos, intersectándolos, ...), etc. Lo siguiente que haremos es abocarnos al estudio de los conjunto dotados de una o más operaciones, es decir, a estudiar las estructuras algebraicas. Un objetivo importante de nuestro esfuerzo es identificar propiedades comúnes a clases de estructuras algebraicas y entender que sifnifica que dos estructuras aparentemente distintas son "matemáticamente equivalentes".

9.1 Definiciones generales

Nuestra primera definición captura la noción operador entre elementos de un conjunto.

Definición 9.1 (Ley de composición interna) *Dado A un conjunto no vacío. Una* ***ley de composición interna*** *en A (l.c.i.) es una función*

$$\begin{array}{rccc} * : & A \times A & \to & A \\ & (x, y) & \to & x * y \end{array}$$

Ejemplo:

- $+$ en $\mathbb{R}$.
- $\cdot$ en $\mathbb{Q}$.
- $\cup$ en $\mathcal{P}(A)$, donde A es un conjunto.
- La división **no** es una ley de composición interna en $\mathbb{Z}$, pues $1/3$ no es un entero.

$\diamondsuit$

Para estudiar estas operaciones entre elementos de un conjunto, definimos:

Definición 9.2 (Estructura algebraica) *Si $*$ es una l.c.i. (es decir, una operación) definida en el conjunto A, al par $(A, *)$ le llamaremos* ***estructura algebraica****.*

Si sobre A tenemos definida una segunda operación $\triangle$, entonces denotamos por $(A, *, \triangle)$ la estructura algebraica que considera ambas leyes de composición interna en A.

Notemos que conocemos ya varias estructuras algebraicas:

Ejemplo:

- $(\mathbb{N}, +, \cdot)$, $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$ y $(\mathbb{R}, +, \cdot)$.
- $(\{V, F\}, \wedge, \vee)$.
- Para E conjunto, $(\mathcal{P}(E), \cup, \cap)$.
- Para A conjunto no vacío, $(A^A, \circ)$, donde $\circ$ es la composición de funciones.

$\diamondsuit$

Como vemos, hay una enorme cantidad de estructuras algebraicas posibles. En este capítulo estudiaremos propiedades que muchas de ellas comparten. Veremos que las estructuras de distintos tipos pueden comportarse de manera muy similar. Es decir, tener propiedades muy parecidas, cuando las llevamos a un nivel de abstracción mayor.

Nombres especiales y propiedades básicas

Definición 9.3 *Sea $(A, *)$ una estructura algebraica.*

- *Diremos que $*$ es* ***asociativa*** *si*

$$\forall x, y, z \in A,\ (x * y) * z = x * (y * z).$$

- *Sea $e \in A$. Diremos que e es elemento* ***neutro*** *para $*$ si*

$$\forall x \in A,\ e * x = x * e = x.$$

- *Si $e \in A$ es el neutro para $*$ y $x \in A$, diremos que x tiene* ***inverso*** *si existe un $y \in A$ tal que*

$$x * y = y * x = e.$$

  En tal caso, y será un inverso de x, y viceversa.
- *Diremos que $*$ es* ***conmutativa*** *si*

$$\forall x, y \in A,\ x * y = y * x.$$

- *Un elemento $a \in A$ es **cancelable** si para todo $y, z \in A$, se tienen:*

$$a * y = a * z \Rightarrow y = z,$$
$$y * a = z * a \Rightarrow y = z.$$

- *Si $(A, *, \triangle)$ es un estructura algebraica con dos operaciones, diremos que $\triangle$ **distribuye** con respecto a $*$ si para todo $x, y, z \in A$, se tienen:*

$$x\triangle(y * z) = (x\triangle y) * (x\triangle z),$$
$$(y * z)\triangle x = (y\triangle x) * (z\triangle x).$$

Ejemplo: En lo que se refiere a los ejemplos $(\mathbb{N}, +, \cdot)$, $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$ y $(\mathbb{R}, +, \cdot)$ ya discutidos, se tiene lo siguiente:

- En todos los casos las operaciones $+$ y $\cdot$ son asociativas y conmutativas y $\cdot$ distribuye con respecto a $+$.
- 0 es el neutro de $(\mathbb{R}, +)$.
- 1 es el neutro de $(\mathbb{R}, \cdot)$.
- Los inversos existen en $(Z, +)$, $(\mathbb{Q}, +)$ y $(\mathbb{R}, +)$, pero no en $(\mathbb{N}, +)$ donde ningún elemento, salvo el 0, tiene inverso.
- En $(\mathbb{Q}^*, \cdot)$ y en $(\mathbb{R}^*, \cdot)$ todo elemento es invertible. En $(\mathbb{Z}, \cdot)$ sólo -1 y $+1$ son invertibles y en $(\mathbb{N}, \cdot)$ sólo el $+1$ lo es.

$\diamondsuit$

Para los restantes ejemplos haga el ejercicio de dar una descripción similar a la recién hecha.

Es importante notar que:

Proposición 9.4 (Unicidad del neutro) *Una estructura algebraica $(A, *)$ posee a lo más un elemento neutro.*

Dem. Supongamos que $(A, *)$ posee dos neutros e y e'. Como e es neutro, entonces $e * e' = e'$. A su vez, como e' es neutro, entonces $e * e' = e$. Juntando ambas igualdades, concluimos que $e = e'$. $\square$

Sea $(A, *)$ una estructura algebraica. Ya sabemos que si $e \in A$ es neutro, entonces es único. Supongamos ahora que un elemento $x \in A$ tiene inverso. ¿Será único este inverso? La respuesta es no necesariamente. Observemos el siguiente ejemplo, donde $A = \{a, b, c, d\}$.

Ejemplo: Estructura sin unicidad de los inversos

$*$	a	b	c	d
a	a	**c**	a	**c**
b	**c**	b	b	a
c	a	b	c	d
d	**c**	b	d	a

La tabla nos indica el valor de $z = x * y$ buscando el símbolo x en la primera columna, a la izquierda de la barra vertical, y el símbolo y en la primera fila, sobre la barra horizontal. Si x está en la fila i e y está en la columna j, z aparece en la fila i y la columna j. Así, $a * b = c$ pues a está en la primera fila de la primera columna, b está en la segunda columna de la primera fila y c está en la primera fila y en la segunda columna.

En la estructura $(A, *)$ donde $*$ está dada por la tabla, tenemos que c es el neutro. El elemento a, en tanto, posee dos inversos: b y d, pues $a * b = b * a = c$ y $a * d = d * a = c$. $\diamondsuit$

En el ejemplo anterior, $(A, *)$ no es asociativa. En efecto, $(a*b)*d = c*d = d \neq a*(b*d) = a * a = a$. Al eliminar este inconveniente se tiene la siguiente propiedad.

Proposición 9.5 (Unicidad de inversos) *Si la estructura algebraica $(A, *)$ tiene neutro e y $*$ es asociativa, entonces los inversos (en el caso en que existan) son únicos.*

Así, si $x \in A$ posee inverso, lo podemos denotar sin ambigüedad como x^{-1}.

Dem. Sea $x \in A$, y supongamos que x posee dos inversos: y y z. Demostraremos que $y = z$.

Como y es inverso de x, entonces $x * y = y * x = e$. Análogamente, como z también es inverso de x, entonces $z * x = x * z = e$. Así,

$$\begin{aligned} y &= y * e && (e \text{ es neutro}) \\ &= y * (x * z) && (x * z = e) \\ &= (y * x) * z && (\text{asociatividad}) \\ &= e * z && (y * x = e) \\ &= z. && (e \text{ es neutro}) \end{aligned}$$

$\square$

Proposición 9.6 *Si $(A, *)$ es una estructura algebraica asociativa y con neutro $e \in A$, entonces también cumple las siguientes propiedades:*

(I) Si $x \in A$ posee inverso, entonces x^{-1} también. Más aún, $(x^{-1})^{-1} = x$.

(II) Si $x, y \in A$ poseen inversos, entonces $x*y$ también posee inverso que cumple $(x*y)^{-1} = y^{-1} * x^{-1}$.

(III) Si $x \in A$ posee inverso, entonces x es cancelable.

Dem. Demostraremos (II).

Sea $w = y^{-1} * x^{-1}$. Queremos probar que $w = (x * y)^{-1}$. Puesto que los inversos son únicos, bastará con mostrar que $w * (x * y) = e = (x * y) * w$. Verifiquemos la primera igualdad.

$$\begin{aligned} w * (x * y) &= (w * x) * y && (\text{asociatividad}) \\ &= ((y^{-1} * x^{-1}) * x) * y && (\text{def. de } w) \\ &= (y^{-1} * (x^{-1} * x)) * y && (\text{asociatividad}) \\ &= (y^{-1} * e) * y && (x \text{ y } x^{-1} \text{ son inversos}) \\ &= y^{-1} * y = e. && (e \text{ es neutro; } y \text{ e } y^{-1} \text{ son inversos}) \end{aligned}$$

Queda propuesto mostrar que también $(x*y)*w = e$. Así, concluimos que $w = (x*y)^{-1}$. $\square$

La estructura $(\mathbb{Z}_n, +_n, \cdot_n)$

Definimos anteriormente la relación $\equiv_n$ (congruencia módulo n) en $\mathbb{Z}$, denotamos su conjunto de clases de equivalencia por $\mathbb{Z}_n = \mathbb{Z}/\equiv_n$, y vimos que $\mathbb{Z}_0 = \{\{x\} : x \in \mathbb{Z}\}$ y que $\mathbb{Z}_n = \{[0]_n, [1]_n, \ldots, [n-1]_n\}$ si $n \geq 1$.

Ahora vamos a definir operaciones de suma $+_n$ y producto $\cdot_n$ para que $(\mathbb{Z}_n, +_n, \cdot_n)$ sea una estructura algebraica con buenas propiedades. Lo haremos como sigue: Para $[x]_n, [y]_n \in \mathbb{Z}_n$

$$[x]_n +_n [y]_n = [x+y]_n \qquad \text{y} \qquad [x]_n \cdot_n [y]_n = [x \cdot y]_n.$$

Sin embargo, estas definiciones podrían acarrearnos problemas. Pensemos en el siguiente ejemplo, tomando $n = 7$:

$$[5]_7 +_7 [3]_7 = [8]_7.$$

Notemos que $[8]_7 = [1]_7$, pues $8 \equiv_7 1$. Sin embargo, como $5 \equiv_7 19$ y $3 \equiv_7 38$, entonces

$$[5]_7 +_7 [3]_7 = [19]_7 +_7 [38]_7 = [57]_7.$$

Si queremos que $+_7$ quede bien definida, entonces debería cumplirse que $[57]_7 = [1]_7$, y así para todas las posibles reescrituras de $[5]_7$ y $[3]_7$.

Afortunadamente, esto no representa un problema gracias al siguiente resultado.

Proposición 9.7 *Sean $x_1, x_2, y_1, y_2 \in \mathbb{Z}$ tales que $x_1 \equiv_n x_2$ e $y_1 \equiv_n y_2$. Entonces*

$$(x_1 + y_1) \equiv_n (x_2 + y_2) \quad y \quad (x_1 \cdot y_1) \equiv_n (x_2 \cdot y_2).$$

Es decir, si $[x_1]_n = [x_2]_n$ y $[y_1]_n = [y_2]_n$, entonces

$$[x_1 + y_1]_n = [x_2 + y_2]_n \quad y \quad [x_1 \cdot y_1]_n = [x_2 \cdot y_2]_n.$$

Dem. Sabemos que $x_1 \equiv_n x_2$ e $y_1 \equiv_n y_2$. Entonces existen $k_x, k_y \in \mathbb{Z}$ tales que $x_1 - x_2 = k_x n$ e $y_1 - y_2 = k_y n$. Sumando ambas igualdades, obtenemos que

$$(x_1 + y_1) - (x_2 + y_2) = (k_x + k_y) \cdot n$$

y por lo tanto $(x_1 + y_1) \equiv_n (x_2 + y_2)$.

Para la multiplicación, calculamos

$$\begin{aligned} x_1 \cdot y_1 &= (x_2 + k_x n)(y_2 + k_y n) \\ &= x_2 \cdot y_2 + (x_2 k_y + y_2 k_x + k_x k_y n) \cdot n \end{aligned}$$

y entonces $(x_1 \cdot y_1) \equiv_n (x_2 \cdot y_2)$. □

Así, $+_n$ y $\cdot_n$ son leyes de composición interna en $\mathbb{Z}_n$ dadas por $[x]_n +_n [y]_n = [x+y]_n$ y $[x]_n \cdot [y]_n = [xy]_n$, para todo $x, y \in \mathbb{Z}$.

Notemos que $(\mathbb{Z}_0, +_0, \cdot_0)$ es esencialmente lo mismo que $(\mathbb{Z}, +, \cdot)$ mientras que $(\mathbb{Z}_1, +_1, \cdot_1)$ es trivial pues tiene sólo un elemento: $\mathbb{Z}$.

Recordemos que hemos expresado $x \equiv_n y$ de manera equivalente como $x = y \mod n$. En estos términos lo anterior nos dice que si $x_1 = y_1 \mod n$ y $x_2 = y_2 \mod n$, entonces $x_1 + x_2 = y_1 + y_2 \mod n$ y $x_1 \cdot x_2 = y_1 \cdot y_2 \mod n$. Preferiremos esta escritura para alivianar la notación.

Ejemplo: La estructura $(\mathbb{Z}_n, +_n, \cdot_n)$ suele ser apropiada al tratar con problemas de divisibilidad.

Veamos que si a y b son enteros, con $a < b$, entonces para todo $m \in \mathbb{N}$, $a^m - b^m$ es divisible por $a - b$.

Sea $n = b - a$ y consideremos la estructura $(\mathbb{Z}_n, +_n, \cdot_n)$. Es claro que por la elección de n, $a = b \mod n$. Por la definición del producto $\cdot_n$ se tiene que $a^2 = b^2 \mod n$. Inductivamente, para $m \geq 2$ se tiene que $a^m = b^m \mod n$. Por la definición de n, esto quiere decir que existe un entero q tal que $a^m - b^m = qn = q(a - b)$, lo que concluye lo prometido. $\diamondsuit$

9.2 Homomorfismos

Hemos visto que las operaciones $+_n$ y $\cdot_n$ en $\mathbb{Z}_n$ quedan definidas en términos de las operaciones $+$ y $\cdot$ en $\mathbb{Z}$. Por esta razón, es fácil conocer otras propiedades de estas estructuras haciendo uso de propiedades de $\mathbb{Z}$.

Por ejemplo, la asociatividad y la conmutatividad de $(\mathbb{Z}, +)$ son heredadas por $(\mathbb{Z}_n, +_n)$, y lo mismo pasa con la relación entre $(\mathbb{Z}, \cdot)$ y $(\mathbb{Z}_n, \cdot_n)$. También es cierto que la distributividad de $\cdot$ con respecto a $+$ en $\mathbb{Z}$ se transfiere a la propiedad análoga en $\mathbb{Z}_n$ con $+_n$ y $\cdot_n$.

Además, sabiendo que 0 en neutro de $(\mathbb{Z}, +)$ y que 1 es neutro de $(\mathbb{Z}, \cdot)$ se deduce directamente que el neutro de $(\mathbb{Z}_n, +_n)$ es $[0]_n$ y que el neutro de $(\mathbb{Z}_n, \cdot_n)$ es $[1]_n$.

Todo lo anterior proviene del hecho que la función $f : \mathbb{Z} \to \mathbb{Z}_n$ definida por $f(x) = [x]_n$ cumple que $f(x + y) = f(x) +_n f(y)$ y $f(x \cdot y) = f(x) \cdot_n f(y)$, para todo $x, y \in \mathbb{Z}$. Esto motiva la siguiente definición.

Definición 9.8 (Homomorfismos de estructuras) *Para dos estructuras $(A, *)$, $(B, \triangle)$ una función $f : A \to B$ es un **homomorfismo** de $(A, *)$ en $(B, \triangle)$ si*

$$\forall x, y \in A, f(x * y) = f(x) \triangle f(y).$$

*Cuando f es inyectiva, se llama un **monomorfismo**, cuando f es epiyectiva se llama un **epimorfismo** y cuando f es biyectiva se llama un **isomorfismo**. En este último caso decimos que f es un isomorfismo entre $(A, *)$ y $(B, \triangle)$.*

*Cuando $(A, *) = (B, \triangle)$, los homomorfismos se llaman **endomorfismos** y, si son biyectivos, se llaman **automorfismos**. En estos casos decimos que f es un endomorfismo o automorfismo en $(A, *)$.*

Ejemplo:

- El primer ejemplo es, por supuesto, $f : \mathbb{Z} \to \mathbb{Z}_n$ dada por $f(x) = [x]_n$, que es un epimorfismo de $(\mathbb{Z}, +)$ en $(\mathbb{Z}_n, +_n)$, así como un epimorfismo de $(\mathbb{Z}, \cdot)$ en $(\mathbb{Z}_n, \cdot_n)$. Sin embargo, para $n \geq 1$, no es un isomorfismo en ninguno de los casos, pues no es inyectiva: $f(0) = f(n) = [0]_n$. Por su parte, para $n = 0$, f es un isomorfismo entre $(\mathbb{Z}, +)$ y $(\mathbb{Z}_0, +_0)$, y entre $(\mathbb{Z}, \cdot)$ y $(\mathbb{Z}_0, \cdot_0)$.
- La función $f : \mathbb{Z} \to \mathbb{Z}$ dada por $f(x) = x^2$, es un endomorfismo de $(\mathbb{Z}, \cdot)$ y no es un automorfismo pues $1^2 = (-1)^2$ lo que nos dice que no es inyectiva.
- Por su parte, la función lineal $f : \mathbb{R} \to \mathbb{R}$ dada por $f(x) = 2x$ es un automorfismo en $(\mathbb{R}, +)$, pero no en $(\mathbb{R}, \cdot)$ pues $f(4) = 8 \neq f(2)^2 = 16$.
- También, la función 2^x es un isomorfismo entre $(\mathbb{R}, +)$ y $((0, \infty), \cdot)$.
- Recordando las Leyes de Morgan tanto para las operaciones lógicas como para las operaciones de conjuntos, podemos ver que la función negación definida en $\{V, F\}$ es un isomorfismo entre $(\{V, F\}, \wedge)$ y $(\{V, F\}, \vee)$. Por su parte, la función complemento definida en $\mathcal{P}(A)$ es un isomorfismo entre $(\mathcal{P}(A), \cup)$ y $(\mathcal{P}(A), \cap)$.

$\diamondsuit$

Proposición 9.9 *Si $f : A \to B$ es un epimorfismo de $(A, *)$ en $(B, \triangle)$, entonces se tienen las siguientes propiedades:*

(I) Si $(A, *)$ es asociativa, entonces $(B, \triangle)$ también lo es.

(II) Si $(A, *)$ es conmutativa, entonces $(B, \triangle)$ también lo es.

(III) Si e es neutro de $(A, *)$, entonces $f(e)$ es neutro de $(B, \triangle)$.

(IV) Si $a \in A$ tiene inverso b para $(A, *)$, entonces $f(a)$ tiene inverso $f(b)$ para $(B, \triangle)$.

Dem. Verifiquemos que se tiene (I). Para $u, v, w \in B$ existen $a, b, c \in A$ tales que $f(a) = u, f(b) = v, f(c) = w$. Entonces,

$$(u \triangle v) \triangle w = (f(a) \triangle f(b)) \triangle f(c) = f(a * b) \triangle f(c) = f((a * b) * c)$$

y

$$u \triangle (v \triangle w) = f(a) \triangle (f(b) \triangle f(c)) = f(a) \triangle f(b * c) = f(a * (b * c)).$$

Por ser $(A, *)$ asociativa se tiene que $(a * b) * c = a * (b * c)$. Entonces $(B, \triangle)$ también es asociativa.

Dejamos la parte (II) como ejercicio y damos una demostración de la parte (III). Sea e neutro de $(A, *)$. Entonces,

$$u \triangle f(e) = f(a) \triangle f(e) = f(a * e) = f(a) = u = f(e * a) = f(e) \triangle f(a) = f(e) \triangle u,$$

lo que muestra que $f(e)$ es neutro de $(B, \triangle)$.

Para la parte (IV), como ya sabemos que $f(e)$ es neutro de $(B, \triangle)$, es suficiente demostrar que $f(a) \triangle f(b) = f(e)$ y $f(b) \triangle f(a) = f(e)$.

Esto se cumple pues $f(a)\triangle f(b) = f(a*b)$ y $f(b)\triangle f(a) = f(b*a)$. Si b es el inverso de a en $(A,*)$, entonces $a*b = b*a = e$. De esta forma, $f(a)\triangle f(b) = f(b)\triangle f(a) = f(e)$. □

Ejemplo: Sean $(\mathbb{Z},\cdot)$ los enteros con el producto usual, y $(\mathbb{Z}\times\mathbb{Z},\odot)$, con $\odot$ dado por $(a,b)\odot(c,d) = (ac,bd)$. Entonces, $(1,1)$ es neutro de $(\mathbb{Z}\times\mathbb{Z},\odot)$.

Sea $f:\mathbb{Z}\to\mathbb{Z}\times\mathbb{Z}$ dada por $f(a) = (a,0)$. Entonces f es un homomorfismo de $(\mathbb{Z},\cdot)$ en $(\mathbb{Z}\times\mathbb{Z},\odot)$. Sin embargo, $f(1) = (1,0) \neq (1,1)$. Es decir, la proposición anterior no es cierta si f no es un epimorfismo, lo que se refleja en este ejemplo en $(1,1)\notin f(\mathbb{Z})$.

Notemos que $f(1) = (1,0)$ sí es neutro de la estructura $(\mathbb{Z}\times\{0\},\odot)$ pues $f:\mathbb{Z}\to\mathbb{Z}\times\{0\}$ es un isomorfismo, en particular, un epimorfismo. ♢

Veremos a continuación que las partes (III) y (IV) de la Proposición 9.9 son válidas, a condición que el neutro de $(B,\triangle)$ esté en la imagen de f.

Proposición 9.10 *Sea f un homomorfismo, no necesariamente epiyectivo, de $(A,*)$ en $(B,\triangle)$, con neutros e_A y e_B, respectivamente.*

(I) Si $e_B\in f(A)$, entonces $e_B = f(e_A)$.

(II) Si $e_B\in f(A)$ y $a\in A$ tiene inverso b para $(A,*)$, entonces $f(a)$ tiene inverso $f(b)$ para $(B,\triangle)$.

Dem. Sea $u\in A$ tal que $f(u) = e_B$. Entonces, $e_B = f(u) = f(u*e_A) = f(u)\triangle f(e_A) = e_B\triangle f(e_A)$. Por lo tanto, $e_B = f(e_A)$.

Si $a\in A$ tiene inverso b para $(A,*)$, entonces $f(e_A) = f(a*b) = f(a)\triangle f(b)$ y $f(e_A) = f(b*a) = f(b)\triangle f(a)$. Como $e_B\in f(A)$, por la parte (I), $f(e_A) = e_B$, lo que permite concluir. □

Para finalizar esta sección, estudiemos que se obtiene al componer dos homomorfismos.

Proposición 9.11 *Si $f:A\to B$ un homomorfismo de $(A,*)$ en $(B,\triangle)$ y $g:B\to C$ un homomorfismo de $(B,\triangle)$ en $(C,\bullet)$, entonces la composición de f con g, $g\circ f:A\to C$, es un homomorfismo de $(A,*)$ en $(C,\bullet)$.*

Dem. Supongamos que $x,y\in A$. Usando que f es homomorfismo se tiene que $f(x*y) = f(x)\triangle f(y)$. Ahora, como $f(x),f(y)\in B$, usando que g es homomorfismo, se obtiene que $g(f(x)\triangle f(y)) = g(f(x))\bullet g(f(y))$. Con lo que $(g\circ f)(x*y) = (g\circ f)(x)\bullet(g\circ f)(y)$. Es decir, $g\circ f$ es homomorfismo. □

Estructuras isomorfas

Hemos definido un isomorfismo entre estructuras algebraicas $(A,*)$ y $(B,\triangle)$ como una función biyectiva $f:A\to B$ que cumple $\forall x,y\in A, f(x*y) = f(x)\triangle f(y)$. Esta noción corresponde a un refinamiento de la noción de cardinalidad; no sólo pide que A y B tengan el mismo cardinal –lo que corresponde a la condición en f de ser una biyección– sino que también dice que los elementos de A se comportan respecto de la operación $*$ de la misma forma que lo hacen sus elementos asociados por f en B, respecto de la operación $\triangle$.

Definición 9.12 (Estructuras isomorfas) *Dos estructuras $(A, *)$ y $(B, \triangle)$ son isomorfas, denotado $(A, *) \cong (B, \triangle)$, si existe una función $f : A \to B$ que es un isomorfismo entre $(A, *)$ y $(B, \triangle)$.*

Ejemplo: De los ejemplos discutidos en las secciones precedentes, podemos deducir lo siguiente.

- $(\mathbb{R}, +)$ y $((0, \infty), \cdot)$ son isomorfas.
- $(\{V, F\}, \wedge)$ y $(\{V, F\}, \vee)$ son isomorfas.
- $(\mathcal{P}(E), \cup)$ y $(\mathcal{P}(E), \cap)$ son isomorfas.
- $(\mathbb{Z}_0, +_0, \cdot_0)$ y $(\mathbb{Z}, +, \cdot)$ son isomorfas.

$\diamondsuit$

Proposición 9.13 *Si $f : A \to B$ es un isomorfismo entre $(A, *)$ y $(B, \triangle)$, entonces $f^{-1} : B \to A$ es isomorfismo entre $(B, \triangle)$ y $(A, *)$.*

Dem. Como f es biyectiva, f^{-1} también lo es, por lo que sólo hay que mostrar que es un homomorfismo. Sean $u, v \in B$ y sean $x, y \in A$ con $f(x) = u$ y $f(y) = v$. Entonces,

$$f^{-1}(u \triangle v) = f^{-1}(f(x) \triangle f(y)) = f^{-1}(f(x * y)) = x * y = f^{-1}(u) * f^{-1}(v).$$

$\square$

Teorema 9.14 *La relación $\cong$ entre estructuras algebraicas es relación de equivalencia.*

Dem. Es claro que toda estructura es isomorfa a sí misma pues la función identidad es un isomorfismo. Luego, $\cong$ es refleja.

Si $f : A \to B$ es isomorfismo entre $(A, *)$ y $(B, \triangle)$, entonces $f^{-1} : B \to A$ es isomorfismo de $(B, \triangle)$ y $(A, *)$. Luego, $\cong$ es simétrica.

Sea $f : A \to B$ isomorfismo de $(A, *)$ y $(B, \triangle)$, y $g : B \to C$ un isomorfismo entre $(B, \triangle)$ y $(C, \bullet)$. Como $g \circ f$ es composición de funciones biyectivas, entonces ella misma lo es. Como $g \circ f$ es composición de homomorfismos, también es homomorfismo. Sigue que $\cong$ es transitiva.

Concluimos que $\cong$ es relación de equivalencia. $\square$

Guía Básica

Determinar la veracidad de las siguientes afirmaciones:

1. La suma en $\mathbb{R}$ es una ley de composición interna.
2. La suma en $\mathbb{N}$ es una ley de composición interna.
3. La suma en $\mathbb{Z}$ es una ley de composición interna.
4. La suma en $\mathbb{Z} \setminus \{0\}$ es una ley de composición interna.
5. La suma en $\{n \in \mathbb{N} \mid n \text{ es par}\}$ es una ley de composición interna.
6. La suma en $\{n \in \mathbb{N} \mid n \text{ es impar}\}$ es una ley de composición interna.
7. La multiplicación en $\mathbb{R}$ es una ley de composición interna.
8. La multiplicación en $\mathbb{N}$ es una ley de composición interna.
9. La multiplicación en $\mathbb{Z}$ es una ley de composición interna.
10. La multiplicación en $\mathbb{Q}$ es una ley de composición interna.
11. La multiplicación en $\mathbb{Q} \setminus \{1\}$ es una ley de composición interna.
12. Una operación $*$ sobre un conjunto A, es conmutativa si $\forall x, y \in A,\ x * y = y$.
13. Una operación $*$ sobre un conjunto A, es conmutativa si $\forall x, y \in A,\ x * y = y * x$.
14. Una operación $*$ sobre un conjunto A, es asociativa si $\forall x, y \in A,\ x * y = y * x$.
15. Una operación $*$ sobre un conjunto A, es asociativa si $\forall x, y, z \in A,\ (x * y) * z = (y * z) * (x * z)$.
16. Sea una operación $*$ sobre un conjunto A, con neutro e. $x \in A$ es invertible si $\exists y \in A,\ x * y = e = y * x$.
17. El neutro en una estructura algebraica es único.
18. El inverso de un elemento en una estructura algebraica es siempre único.
19. El inverso de un elemento en una estructura algebraica es único, si la operación es conmutativa.
20. El inverso de un elemento en una estructura algebraica es único, si la operación es asociativa.
21. El 0 es un elemento cancelable en $(\mathbb{N}, +)$.
22. El 0 es un elemento cancelable en $(\mathbb{R}, \cdot)$.
23. Un homomorfismo entre estructuras se dice isohomomorfismo si es inyectivo.
24. $(\mathbb{R}, \cdot) \cong (\mathbb{R}, +)$.
25. $(\mathbb{R}_+, \cdot) \cong (\mathbb{R}, +)$.
26. Un homomorfismo f de $(A, *)$ en $(B, \triangle)$ satisface que $(\forall x, y \in A, f(x) \triangle f(y) = f(x * y))$.

Guía de Ejercicios

1. Señale si las siguientes operaciones son o no leyes de composición interna. Justifique por qué.

   a) $+$ en $\mathbb{Z}$.
   b) $+$ en $\mathbb{Z} \setminus \{0\}$.
   c) $+$ en $\mathbb{N}$.
   d) $\cdot$ en $\mathbb{R}$.
   e) $/$ (división) en $\mathbb{Q}$.
   f) Dado $A \neq \emptyset$, la $\circ$ (composición de funciones) en el conjunto de las funciones de A en A.
   g) $\cap$ en $\mathcal{P}(A)$, para cierto $A \neq \emptyset$.

2. Considerando las operaciones del ejercicio anterior, en los casos que corresponda:

   a) Estudie si la operación es asociativa.
   b) Estudie si la operación es conmutativa.
   c) Determine la existencia de neutros.
   d) Determine la existencia de inversos. Dé condiciones sobre un elemento para que posea inverso.

3. Demuestre las siguientes propiedades, enunciadas en el texto del apunte, para una estructura algebraica asociativa $(A, *)$:

   a) Si $x \in A$ posee inverso, entonces x^{-1} también. Más aun, $(x^{-1})^{-1} = x$.
   b) Si $x \in A$ posee inverso, entonces es cancelable.

Guía de Problemas

1. Dado un conjunto no vacío A, sea $\mathcal{F} = \{f : A \to A \mid f \text{ es biyectiva}\}$. Se define la operación $\star$ dada por:

$$\forall f, g \in \mathcal{F},\ f \star g = (f \circ g)^{-1}.$$

   a) (5 min.) Pruebe que $(\mathcal{F}, \star)$ es una estructura algebraica.
   b) (10 min.) Estudie la asociatividad de $\star$.
   c) (10 min.) Estudie la conmutatividad de $\star$.
   d) (10 min.) Encuentre el neutro en $(\mathcal{F}, \star)$.
   e) (10 min.) Determine si todo elemento $f \in \mathcal{F}$ admite un inverso para $\star$. En caso afirmativo, determínelo.

2. Sea $(E, *)$ una estructura algebraica y $\mathcal{R}$ una relación de equivalencia en E que satisface la siguiente propiedad:

$$\forall x_1, x_2, y_1, y_2,\ x_1 \mathcal{R} x_2 \wedge y_1 \mathcal{R} y_2 \implies (x_1 * y_1) \mathcal{R} (x_2 * y_2).$$

   Definimos una nueva l.c.i. $\otimes$ sobre el conjunto cuociente $E/\mathcal{R}$ mediante:

$$[x]_{\mathcal{R}} \otimes [y]_{\mathcal{R}} = [x * y]_{\mathcal{R}}.$$

a) (15 min.) Pruebe que $\otimes$ está bien definida, es decir, si $[x]_{\mathcal{R}} = [x']_{\mathcal{R}}$ y $[y]_{\mathcal{R}} = [y']_{\mathcal{R}}$, entonces $[x * y]_{\mathcal{R}} = [x' * y']_{\mathcal{R}}$.

b) (10 min.) Suponiendo que $(E, *)$ posee un neutro e, encuentre el neutro de $(E/\mathcal{R}, \otimes)$.

c) (15 min.) Dado un elemento $x \in E$ que posee inverso en $(E, *)$, determine el inverso de $[x]_{\mathcal{R}} \in E/\mathcal{R}$ en $(E/\mathcal{R}, \otimes)$.

SEMANA 11:

Estructuras Algebraicas

9.3 Grupos

Un **grupo** es un caso particular de estructura algebraica. Veremos que esta noción rescata ampliamente las propiedades de estructuras tales como $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$ y $(\mathbb{R}, +)$.

Dedicaremos una sección especial a grupos, debido a que las particularidades que poseen nos permiten conocer muy bien sus propiedades, que son bastantes.

Definición 9.15 (Grupo) *Sea $(G, *)$ una estructura algebraica. Diremos que $(G, *)$ es*

- ***grupo**, si $*$ es asociativa, admite neutro en G y todo elemento $x \in G$ posee inverso $x^{-1} \in G$.*
- ***grupo abeliano** si es un grupo y $*$ es conmutativa.*

A modo de ejemplo, notemos que $(\mathbb{R}, \cdot)$ no es un grupo pues 0 no posee inverso. Sin embargo, $(\mathbb{R} \setminus \{0\}, \cdot)$ sí es un grupo.

Si $(G, *)$ es un grupo, entonces cumple (por Proposición 9.6) las siguientes propiedades:

- El inverso de cada elemento es único
- $\forall x \in G,\ (x^{-1})^{-1} = x$.
- $\forall x, y \in G,\ (x * y)^{-1} = y^{-1} * x^{-1}$.
- Todo elemento $x \in G$ es cancelable.

Las siguientes propiedades se agregan a las recién mencionadas:

Proposición 9.16 *Dado $(G, *)$ grupo, entonces:*

(i) Para todo $a, b \in G$, las siguientes ecuaciones tienen solución única:

$$a * x_1 = b$$
$$x_2 * a = b$$

Ellas son $x_1 = a^{-1} * b$ y $x_2 = b * a^{-1}$

(II) *Para todo $a \in G$, las funciones I_a y D_a, dadas por $I_a(x) = a * x$ y $D_a(x) = x * a$, para todo $x \in G$, son biyecciones.*

(III) *Si $(K, \triangle)$ es una estructura y $f : G \to K$ es homomorfismo, entonces $(f(G), \triangle)$ es un grupo.*

(IV) *Sea $(K, \triangle)$ una estructura algebraica y $f : G \to K$ un homomorfismo. Sea $e_K = f(e_G)$ el neutro del grupo $(f(G), \triangle)$. Entonces, f es inyectiva si y sólo si $f^{-1}(\{e_K\}) = \{e_G\}$*

Dem.

(I) Consideremos sólo el caso de la primera ecuación. Sean $a, b \in G$. Como G es grupo, tiene neutro, digamos e, y a posee inverso a^{-1}. Luego,

$$\begin{aligned} a^{-1} * (a * x_1) = a^{-1} * b &\Leftrightarrow (a^{-1} * a) * x_1 = a^{-1} * b && \text{(asociatividad.)} \\ &\Leftrightarrow e * x_1 = a^{-1} * b && \text{(definición de inverso.)} \\ &\Leftrightarrow x_1 = a^{-1} * b. && \text{(definición de neutro.)} \end{aligned}$$

Y esta última expresión es única, pues a^{-1} es único.

(II) La demostración se propone como ejercicio.

(III) Por Proposición 9.9, un homomorfismo de G en K hace que $(f(G), \triangle)$ herede la asociatividad de G, que $f(e)$ sea el neutro de $(f(G), \triangle)$ y que todo elemento $f(x)$ tenga inverso pues $f(x)^{-1} = f(x^{-1}) \in f(G)$.

(IV) Supongamos que f es inyectiva, es decir, si $x, y \in G$ y $f(x) = f(y)$, entonces $x = y$. Si $x \in f^{-1}(\{e_K\})$, entonces $e_K = f(x)$. Como f es homomorfismo, de la parte (I) de la Proposición 9.10, tenemos que $f(x) = e_K = f(e_G)$ y $\{e_G\} \subseteq f^{-1}(\{e_K\})$. Como f es inyectivo, $x = e_G$. Con esto, $f^{-1}(\{e_K\}) = \{e_G\}$.

Recíprocamente, supongamos que $f^{-1}(\{e_K\}) = \{e_G\}$ y sean $x, y \in G$ tales que $f(x) = f(y)$. Como G es grupo, sabemos que x e y tienen inversos y de la parte (II) de la Proposición 9.10, sabemos que $f(x)^{-1} = f(x^{-1})$ y que $f(y)^{-1} = f(y^{-1})$. Entonces, como f es homomorfismo, $e_K = f(x) \triangle f(y)^{-1} = f(x * y^{-1})$. Así, $x * y^{-1} = e_G$ y, por lo tanto, $x = y$.

□

Ejemplo:

- $(\mathbb{Z}_n, +_n)$ es grupo abeliano. Esto es directo del hecho que $(\mathbb{Z}, +)$ es grupo abeliano y que la función $f : \mathbb{Z} \to \mathbb{Z}_n$ dada por $f(x) = [x]_n$ es un epimorfismo de $(\mathbb{Z}, +)$ en $(\mathbb{Z}_n, +_n)$ pues, de la Proposición 9.16 parte (III), sabemos que $(f(\mathbb{Z}), +_n) = (\mathbb{Z}_n, +_n)$ es un grupo.
- $(\mathbb{Z}_n, \cdot_n)$ es estrucutra algebraica donde $\cdot_n$ es asociativa, conmutativa y admite neutro. Al igual que antes, esto es directo del hecho que en $(\mathbb{Z}, \cdot)$ el producto $\cdot$ es asociativo y admite neutro y que la función $f : \mathbb{Z} \to \mathbb{Z}_n$ dada por $f(x) = [x]_n$ es un epimorfismo de $(\mathbb{Z}, \cdot)$ en $(\mathbb{Z}_n, \cdot_n)$.

- Diferencia simétrica en el conjunto potencia. Sea A un conjunto no vacío. Veamos que $(\mathcal{P}(A), \Delta)$ es un grupo abeliano, donde Δ denota la diferencia simétrica que como se recordará es tal que

$$X\Delta Y = (X \setminus Y) \cup (Y \setminus X) = (X \cup Y) \setminus (X \cap Y)$$

  En efecto, es claro que Δ es una ley de composición interna en $\mathcal{P}(A)$. De nuestro estudio de teoría de conjuntos, sabemos que Δ es asociativa y conmutativa.

  Si $X \subseteq A$, entonces $X\Delta\emptyset = (X \cup \emptyset) \setminus (X \cap \emptyset) = X \setminus \emptyset = X$. Concluimos así que $\emptyset$ es el neutro de Δ.

  Además, como $X\Delta X = (X \setminus X) \cup (X \setminus X) = \emptyset \cup \emptyset = \emptyset$, sigue que todo $X \in \mathcal{P}(A)$ es invertible, y que $X^{-1} = X$ (es decir, cada elemento es su propio inverso).
- Sea A el intervalo $[0, a)$ para algún número real $a > 0$. Definimos en A la operación $+_a$ por $x +_a y = x + y$ si $x + y < a$ y $x + y - a$ si $x + y \geq a$, para todo $x, y \in A$, donde $+$ es la suma en $\mathbb{R}$.

  Está bien definida pues $x +_a y \in [0, a)$ para todo $x, y \in [0, a)$. En efecto, esto es inmediato cuando $x + y < a$. Como $x + y < 2a$, cuando $x + y \geq a$ también se tiene que $x + y - a < a$ y $x + y - a \geq 0$.

  Dejamos como ejercicio demostrar que $(A, +_a)$ es asociativa y conmutativa.

  Vemos que 0 es el neutro en $(A, +_a)$ pues, como $x + 0 = x < a$, $x +_a 0 = x + 0 = x$, para todo $x \in A$.

  Finalmente, el inverso de x es $a - x$ pues $x + (a - x) = a \geq a$ por lo tanto $x +_a (a - x) = a - a = 0$.

  Concluimos que $([0, a), +_a)$ es un grupo abeliano.

$\diamondsuit$

Subgrupos

A menudo, cuando trabajamos en alguna estructura algebraica, por ejemplo en un grupo, identificamos subestructuras que son de interés. Para no tener que rehacer el estudio de propiedades que ya hemos comprobado en la estructura original, es útil establecer condiciones bajo las cuales la subestructura hereda propiedades de la estructura de partida. También interesa determinar características de las subestructuras que puedan existir. A continuación abordamos estas preguntas para el caso en que la estructura algebraica de partida es un grupo.

Definición 9.17 (Subgrupo) *Sea $(G, *)$ un grupo, y sea $H \subseteq G$, $H \neq \emptyset$. Diremos que H es **subgrupo** de G si $(H, *)$ también es grupo.*

Si consideramos el grupo $(\mathbb{R}, +)$, entonces un posible subgrupo es $(\mathbb{Q}, +)$. También tenemos a $(\{-1, 1\}, \cdot)$ como subgrupo de $(\mathbb{R} \setminus \{0\}, \cdot)$.

Todo grupo $(G, *)$ tiene dos subgrupos que llamaremos **triviales**:

$$(G, *) \quad \text{y} \quad (\{e\}, *)$$

donde e es el neutro de $(G, *)$.

Proposición 9.18 *Sea $(G, *)$ un grupo, y $(H, *)$ un subgrupo de él. Un par de propiedades básicas que resultan de ver los elementos de H como elementos de G:*

(I) Si $e \in G$ es el neutro de G y $e_H \in H$ es el neutro de H, entonces $e = e_H$.

(II) Además, sea $x \in H$. Si $x^{-1} \in G$ es el inverso de x en $(G, *)$ y $\widetilde{x} \in H$ es el inverso de x en $(H, *)$, entonces $x^{-1} = \widetilde{x}$.

Dem. Sólo demostraremos la primera La otra propiedad queda propuesta como ejercicio.

Como $H \subseteq G$, tenemos que $e_H \in G$. Luego, $e_H = e_H * e$ (porque e es neutro de G y $e_H \in G$) y existe $e_H^{-1} \in G$ inverso de e_H tal que $e = e_H * e_H^{-1}$. Sigue que $e_H = e_H * (e_H * e_H^{-1}) = (e_H * e_H) * e_H^{-1} = e_H * e_H^{-1} = e$, donde hemos usado que $*$ es asociativa y e_H es neutro en H. □

En principio, si uno quisiera demostrar que un conjunto $H \subseteq G$, $H \neq \emptyset$, forma un subgrupo de $(G, *)$, tendría que demostrar que $(H, *)$ cumple todas las propiedades de la definición de grupo, además de mostrar (el cual es el punto de partida) que

$$\forall x, y \in H,\ x * y \in H.$$

A esta propiedad se le conoce como **cerradura**, y es lo que nos permite decir que $*$ es una ley de composición interna también en H.

La siguiente es una forma compacta para determinar si $(H, *)$ es subgrupo de $(G, *)$.

Teorema 9.19 (Caracterización de subgrupos) *Sea $H \neq \emptyset$. Entonces*

$$(H, *) \text{ es subgrupo de } (G, *) \iff H \subseteq G \wedge \forall x, y \in H,\ x * y^{-1} \in H.$$

Dem. La implicancia $\Rightarrow$ se verifica directamente. Sin embargo, la propiedad fuerte es la implicancia $\Leftarrow$. Para demostrarla, supongamos que $\forall x, y \in H,\ x * y^{-1} \in H$. Debemos probar que $(H, *)$ es grupo.

Notemos que la asociatividad se hereda automáticamente del hecho que $(G, *)$ sea grupo. Nos basta entonces probar que:

- $(H, *)$ es una estructura algebraica (cerradura de $*$ en H).
- $(H, *)$ admite un neutro (que por las propiedades anteriores, sabemos debe ser el neutro de G).
- Todo elemento en H tiene inverso **en** H.

Probaremos estas afirmaciones en un orden distinto:

- Veamos primero que, si $e \in G$ es el neutro de $(G, *)$, entonces $e \in H$. Con esto e será el neutro de H.

  En efecto, como $H \neq \emptyset$, tomando $h \in H$, por hipótesis se tiene que

  $$h * h^{-1} = e \in H.$$

- Ahora probemos que dado $h \in H$, éste admite un inverso en H.

  Sabemos que h^{-1} es inverso de h, pero sólo para $(G, *)$. O sea, no sabemos si pertenece a H.

  Pero usando la hipótesis con $x = e$ e $y = h$, tenemos que:

  $$e * h^{-1} \in H \;\Leftrightarrow\; h^{-1} \in H.$$

- Finalmente, probamos la cerradura de $*$ en H.

  Dados $x, y \in H$. Por lo que establecimos recién, $y^{-1} \in H$. Así que aplicando la hipótesis para x e y^{-1}, tenemos que:

  $$x * (y^{-1})^{-1} \in H \;\Leftrightarrow\; x * y \in H.$$

Concluimos de esta manera que $(H, *)$ es subgrupo de $(G, *)$. □

Ejemplo: Subgrupos de $(\mathbb{Z}, +)$

Sea $S \subseteq \mathbb{Z}$ y veamos que debe ocurrir con S para que sea subgrupo de $(\mathbb{Z}, +)$. Primero $0 \in S$. Supongamos que $1 \in S$. Entonces, $2 = 1 + 1$, $3 = 2 + 1$, etc. deben estar en S pues S debe ser cerrado para $+$. También, $-1 \in S$ y por lo tanto, $-2, -3, \ldots$ deben estar en S. Así, informalmente, vemos que, si $1 \in S$ y S es un subgrupo de $\mathbb{Z}$, entonces $S = \mathbb{Z}$. Notemos que lo mismo va a ocurrir si $-1 \in S$.

Supongamos ahora que ni 1 ni -1 están en S y que $2 \in S$. Entonces, $0, 2, 4, 6, 8, \ldots$ deben estar y también $-2, -4, -6, \ldots$. Entonces S contiene a todos los pares. ¿Puede tener a un impar? No. Si lo tuviese, digamos $11 \in S$, entonces, $11 - 10 = 1 \in S$ lo que es contrario a nuestro supuesto. Así, si $2k + 1 \in S$ entonces como $2k \in S$ se tendría que $1 \in S$. Concluimos así que un subgrupo de $\mathbb{Z}$ que no tiene a 1 ni -1 y sí tiene a 2 debe ser el conjunto de números pares.

Queda como ejercicio decir cómo debe ser un subgrupo S de $(\mathbb{Z}, +)$ cuyo elemento positivo más pequeño es k. ♢

Proposición 9.20 *Sea $(G, *)$ grupo, $(K, \triangle)$ una estructura algebraica y $f : G \to K$ un homomorfismo. Si H es subgrupo de $(G, *)$, entonces $f(H)$ es un subgrupo de $(f(G), \triangle)$.*

Dem. Usando la caracterización de subgrupos recién vista, bastará con demostrar que para $x, y \in H$, $f(x) \triangle f(y)^{-1} \in f(H)$.

De la definición de homomorfismo se tiene que $f(x * y^{-1}) = f(x) \triangle f(y^{-1})$. De la Proposición 9.10 parte (II) sabemos que $f(y^{-1}) = f(y)^{-1}$. Por lo tanto,

$$f(x * y^{-1}) = f(x) \triangle f(y^{-1}) = f(x) \triangle f(y)^{-1}.$$

Usando la caracterización de subgrupo para H, se tiene que $x * y^{-1} \in H$. Así, $f(x * y^{-1}) \in f(H)$. Ahora, usando la caracterización de subgrupos para $f(H)$ concluimos que $f(H)$ es un subgrupo de $(f(G), \triangle)$. □

9.4 Anillos y cuerpos

Comenzamos ahora el estudio de estructuras algebraicas que tengan definidas dos operaciones, y las clasificaremos en anillos y en cuerpos. El mejor ejemplo que conocemos de un anillo es $(\mathbb{Z}, +, \cdot)$, y de un cuerpo es $(\mathbb{R}, +, \cdot)$. Sin embargo, hay muchas más posibilidades. Culminaremos este capítulo mostrando que $(\mathbb{Z}_n, +_n, \cdot_n)$ es cuerpo si n cumple una condición especial.

Definición 9.21 (Anillo) *Una estructura $(A, +, \cdot)$ se llamará **anillo** si:*

- *$(A, +)$ es grupo abeliano cuyo neutro se denota por 0.*
- *$\cdot$ es asociativa.*
- *existe un elemento neutro en $A \setminus \{0\}$ para $\cdot$ que se denota 1.*
- *$\cdot$ distribuye con respecto a $+$.*

*Si $\cdot$ es conmutativa, entonces $(A, +, \cdot)$ se llamará **anillo conmutativo**.*

Observación (Importante): Hay varios textos matemáticos, usualmente los más especializados, en lo cuales no se pide como parte de la definición de anillos que éstos tengan elemento neutro para $\cdot$ (en cuyo caso, anillos como el que hemos definido se denominan anillos con unidad). De hecho, la exigencia de contar con neutro multiplicativo tampoco era parte de la definición de anillo en las versiones de este apunte anteriores a la del 2019. Los ejemplos más comunes de anillos así como casi todos los casos de anillos que se discuten en los cursos siguientes admiten neutro multiplicativo y es por ello que en adelante optamos por trabajar con la definición de anillo dada.

Algunos textos tampoco exigen que el neutro multiplicativo 1 (en caso de existir) tenga que ser distinto del neutro aditivo 0. Como hay esencialmente un único anillo (y que consta de un único elemento) en que ambos neutros coinciden, nosotros excluimos esta rareza de nuestra definición de anillos. □

Convención: Usualmente, cuando trabajemos con con una estructura de anillo $(A, +, \cdot)$,

- Al neutro de $(A, +)$ lo denotaremos 0, y para todo $x \in A$, a su inverso para la operación $+$, que es único pues $+$ es asociativa, se le denotará $-x$, y se le llamará **opuesto** o **inverso aditivo**.

- Si $x \in A$ posee inverso para la operación $\cdot$, entonces éste es único pues la operación es asociativa y se denotará por x^{-1}.

Ejemplo:

- $(\mathbb{Z}, +, \cdot)$ es un anillo conmutativo.
- $(\mathbb{Z}_n, +_n, \cdot_n)$ es anillo para $n \geq 2$. Sea $n \geq 2$. Recordemos que $(\mathbb{Z}_n, +_n)$ es un grupo abeliano y que $(\mathbb{Z}_n, \cdot_n)$ es una estructura algebraica donde $\cdot_n$ es asociativa y admite neutro.

  Nuevamente, el epimorfismo $f : \mathbb{Z} \to \mathbb{Z}_n$ dado por $f(x) = [x]_n$ traslada la distributividad de $\cdot$ con respecto a $+$ de $\mathbb{Z}$ a la distributividad de $\cdot_n$ con respecto a $+_n$ de $\mathbb{Z}_n$. En efecto, como f es epimorfismo entre $(\mathbb{Z}, +)$ y $(\mathbb{Z}_n, +_n)$, así como entre $(\mathbb{Z}, \cdot)$ y $(\mathbb{Z}_n, \cdot_n)$, dados $x, y, z \in \mathbb{Z}$, tenemos que

$$f(x(y+z)) = f(xy + xz) = f(xy) +_n f(xz) = f(x) \cdot_n f(y) +_n f(x) \cdot_n f(z)$$

  y

$$f(x(y+z)) = f(x) \cdot_n f(y+z) = f(x) \cdot_n (f(y) +_n f(z)).$$

  Luego,

$$[x]_n \cdot_n ([y]_n +_n [z]_n) = [x]_n \cdot_n [y]_n + [x]_n \cdot_n [z]_n.$$

  Se verifica además que $(\mathbb{Z}_n, +_n, \cdot_n)$ es anillo conmutativo.

$\diamondsuit$

Definición 9.22 (Homomorfismo de anillos) *Sean $(A, +_A, \cdot_A)$ y $(B, +_B, \cdot_B)$ dos anillos. Un homomorfismo de $(A, +_A, \cdot_A)$ en $(B, +_B, \cdot_B)$ es una función $f : A \to B$ tal que para todo $x, y \in A$,*

$$\begin{aligned} f(x +_A y) &= f(x) +_B f(y), \\ f(x \cdot_A y) &= f(x) \cdot_B f(y), \\ f(1_A) &= 1_B. \end{aligned}$$

Proposición 9.23 *Si $(A, +, \cdot)$ es un anillo, entonces $\forall x, y \in A$ se cumple que:*

(I) $0 \cdot x = x \cdot 0 = 0$

(II) $-(x \cdot y) = (-x) \cdot y = x \cdot (-y)$

(III) $(-x) \cdot (-y) = x \cdot y$

(IV) $-x = (-1) \cdot x = x \cdot (-1)$.

Dem. Probaremos (I), (II) y (IV).

Para (I) tenemos que:

$$\begin{aligned} 0 \cdot x &= (0+0) \cdot x && \text{(0 es neutro para } (A,+)) \\ &= 0 \cdot x + 0 \cdot x. && \text{(distributividad)} \end{aligned}$$

Sigue que

$$\begin{aligned} 0 &= -(0 \cdot x) + 0 \cdot x && \text{(definición y existencia de inverso aditivo)} \\ &= -(0 \cdot x) + (0 \cdot x + 0 \cdot x) && \text{(identidad recién demostrada)} \\ &= \big(-(0 \cdot x) + 0 \cdot x\big) + 0 \cdot x && \text{(asociatividad)} \\ &= 0 + 0 \cdot x && \text{(definición de inverso aditivo)} \\ &= 0 \cdot x. && \text{(definición de neutro aditivo)} \end{aligned}$$

La demostración es análoga para $x \cdot 0$.

Para (II), tenemos que $(-x) \cdot y + x \cdot y = (-x + x) \cdot y = 0 \cdot y = 0$. Entonces, por la unicidad de los inversos en $(A,+)$, $(-x) \cdot y = -(x \cdot y)$.

Para (IV), debemos verificar que $x + (-1) \cdot x = 0$ (gracias a que A es abeliano).

Esto es cierto pues:

$$\begin{aligned} x + (-1) \cdot x &= 1 \cdot x + (-1) \cdot x && \text{(1 es neutro para } (A,\cdot)) \\ &= (1 + (-1)) \cdot x && \text{(distributividad)} \\ &= 0 \cdot x && \text{(inversos en } (A,+)) \\ &= 0. && \text{(propiedad (1))} \end{aligned}$$

Luego $(-1) \cdot x$ es el opuesto de x y se concluye.

La demostración es también análoga para $x \cdot (-1)$. □

Si bien los ejemplos de anillos mencionados hasta ahora, así como otros que veremos, son todos anillos conmutativos, existen importantes anillos no conmutativos, entre los cuales destaca el anillo de matrices a coeficientes en $\mathbb{R}$ o $\mathbb{C}$ que será definido y estudiado en profundidad en un próximo curso.

Operación iterada en una estructura

En $\mathbb{R}$ podemos definir la suma iterada y el producto iterado de sus elementos. Por ejemplo, para π, su suma iterada 16 veces es 16π y su producto iterado 20 veces es π^{20}. Lo mismo puede hacerse en estructuras abstractas.

Definición 9.24 *Sea $(A,+,\cdot)$ un anillo. Para $a \in A$ y $n \in \mathbb{N}$, se definen recursivamente potencias y múltiplos de a que se anotan a^n y $n \cdot a$, respectivamente.*

- *$a^0 = 1$ y $a^{n+1} = a^n \cdot a, n \in \mathbb{N}, n \geq 0$. Si a posee inverso a^{-1}, entonces $a^{-n} = (a^{-1})^n$.*
- *$0 \cdot a = 0$, $(n+1) \cdot a = n \cdot a + a$, y $(-n) \cdot a = n \cdot (-a), n \in \mathbb{N}, n \geq 0$*

Muchas más nociones y propiedades que conocemos de los números reales tienen sentido y son verdaderas en estructuras más abstractas. En particular, la noción de sumatoria y sus propiedades son válidas en un anillo. Destacaremos a continuación algunas de ellas.

Hay que notar que, sin embargo, cálculos que involucren inversos multiplicativos no tendrán sentido en general. Por ejemplo, si bien la fórmula $\sum_{k=1}^{n} k$ tiene sentido en un anillo $(A, +, \cdot)$ ($k = k \cdot 1$, ver Definición 9.24), la fórmula $n(n+1)/2$ no lo tiene. Usualmente, en estos casos, uno puede obtener una fórmula válida evitando las divisiones. En nuestro caso, $2\sum_{k=1}^{n} k = n(n+1)$ sí es verdadera en un anillo.

Proposición 9.25 *Sea $(A, +, \cdot)$ un anillo.*

(i) $\forall k, \ell \in \mathbb{Z}, \forall a, b \in A$, $k(a+b) = ka + kb$, $(k+\ell)a = ka + \ell a$ *y* $(ka)(\ell b) = (k\ell)(ab)$.

(ii) $\forall x \in A$, $\forall n \in \mathbb{N}$, $x^{n+1} - 1 = (x-1)\sum_{k=0}^{n} x^k$.

(iii) Cuando el anillo es conmutativo, $\forall x, y \in A$, $\forall n \in \mathbb{N}$, $(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k$.

Divisores de cero y dominios de integridad

Definición 9.26 (Divisores de cero) *Sea $(A, +, \cdot)$ un anillo. Un elemento $a \in A$, $a \neq 0$, es un **divisor de cero** si existe un elemento $y \in A \setminus \{0\}$ tal que $a \cdot y = 0$ o $y \cdot a = 0$. (Notamos que cuando esto ocurre, el elemento y también es un divisor de cero).*

La definición anterior no nos es muy familiar, debido a que en los anillos que nos resultan más conocidos no aparece. Sin embargo, en $\mathbb{Z}_6$ podemos dar un sencillo ejemplo. En efecto, $[2]_6$ y $[3]_6$ son divisores de 0 porque $[2]_6 \cdot_6 [3]_6 = [6]_6 = [0]_6$.

Definición 9.27 (Dominio de integridad) *Un anillo conmutativo y sin divisores de cero se llama **dominio de integridad**.*

Cuerpos

Definición 9.28 (Cuerpo) *Una estructura $(K, +, \cdot)$ se llamará **cuerpo** si:*

- *$(K, +, \cdot)$ es anillo conmutativo.*
- *Todo elemento $x \in K \setminus \{0\}$ es invertible para $\cdot$.*

Equivalentemente, $(K, +, \cdot)$ es un cuerpo si y sólo si

- $(K, +)$ es grupo abeliano.

- $(K \setminus \{0\}, \cdot)$ es grupo abeliano.
- $\cdot$ distribuye con respecto a $+$.

Como ejemplos conocidos tenemos que $(\mathbb{Q}, +, \cdot)$ y $(\mathbb{R}, +, \cdot)$ son cuerpos. Pero $(\mathbb{Z}, +, \cdot)$ no lo es, pues para todo $k \in \mathbb{Z} \setminus \{-1, 1\}$, $k\ell$ es mayor o igual a k o menor o igual a $-k$ y, por ende, k no tiene inverso para $(\mathbb{Z}, \cdot)$.

Convención: En el caso de un cuerpo, digamos $(\mathbb{K}, +, \cdot)$, el inverso de un elemento $x \neq 0$ con respecto a la operación $\cdot$, además de escribirse x^{-1} suele también escribirse $1/x$ o $\frac{1}{x}$. También podemos escribir $x^{-1} \cdot y$ o $y \cdot x^{-1}$ o $\frac{1}{x} \cdot y$ o $y \cdot \frac{1}{x}$ como y/x.

Proposición 9.29 *Si $(K, +, \cdot)$ es un cuerpo, entonces K no tiene divisores de cero. Es decir, K es un dominio de integridad.*

Dem. Supongamos que $a \neq 0$ es un divisor de cero. Es un ejercicio que un divisor de cero en un anillo no puede ser invertible. Esto no puede ocurrir en un cuerpo a menos que $a = 0$, por lo que tenemos una contradicción. Para la segunda afirmación basta notar que todo cuerpo es un anillo conmutativo. □

Lamentablemente, no todo anillo conmutativo y sin divisores de cero (es decir un dominio de integridad) es un cuerpo. Un ejemplo es $(\mathbb{Z}, +, \cdot)$: ya vimos que no tiene divisores de cero y que no es cuerpo.

Ejemplo: $(\mathbb{Z}_n, +_n, \cdot_n)$ es cuerpo si y sólo si n es primo. En efecto, si n no es primo, entonces $n = pq$ para $p, q \notin \{1, n\}$. De aquí, $[p]_n \cdot_n [q]_n = [n]_n = [0]_n$. Pero, $1 < p, q < n$, lo que nos dice que $[p]_n, [q]_n \neq [0]_n$. Por lo tanto, ambos son divisores de cero en $(\mathbb{Z}_n, +_n, \cdot_n)$ y por ende $(\mathbb{Z}_n, +_n, \cdot_n)$ no es cuerpo. Esto muestra que si $(\mathbb{Z}_n, +_n, \cdot_n)$ es cuerpo, entonces n es primo.

Recíprocamente, para todo $n \geq 2$, sabemos que $(\mathbb{Z}_n, +_n, \cdot_n)$ es un anillo conmutativo. Para concluir que es cuerpo falta establecer que si $[a]_n \in \mathbb{Z}_n$ y $[a]_n \neq 0$, entonces $[a]_n$ es invertible. En efecto, como $\mathbb{Z}_n$ es finito, existen k y r, $k > r > 0$, tales que $[a]_n^k = [a]_n^r$, luego $[a]_n^r * ([a]_n^{k-r} - [1]) = [0]_n$. Como $[a]_n$ no es un divisor de cero, entonces $[a]_n^r$ no puede ser $[0]_n$, de lo que se concluiye que $[a]_n^{k-r-1} * [a]_n = [1]_n$. Luego, $[a]_n$ es invertible. ♢

Guía Básica

Determinar la veracidad de las siguientes afirmaciones:

1. En un grupo $(G, *)$, $*$ es conmutativa.
2. En un grupo $(G, *)$, $*$ es asociativa.
3. En un grupo $(G, *)$ pueden haber elementos que no admiten inverso.
4. En un grupo $(G, *)$ el neutro es el único elemento que no admite inverso.
5. La estructura $(\mathbb{R}, \cdot)$, es un grupo.
6. La estructura $(\mathbb{R} \setminus \{1\}, \cdot)$, es un grupo.
7. La estructura $(\mathbb{R} \setminus \{0\}, \cdot)$, es un grupo.
8. En un grupo pueden existir elementos con dos inversos.
9. En un grupo no existen elementos cancelables.
10. En un grupo hay elementos cancelables.
11. El neutro de un grupo es el único elemento con más de un inverso.
12. En un grupo $(G, *)$, el inverso de $x^{-1} * y$ es $y^{-1} * x$.
13. En un grupo $(G, *)$, el inverso de $x^{-1} * y$ es $y * x$.
14. En un grupo abeliano $(G, *)$, el inverso de $x * y$ es $x^{-1} * y^{-1}$.
15. En un grupo $(G, *)$, con $a, b \in G$, la ecuación $a * x = b$ siempre tiene solución.
16. En un grupo $(G, *)$, con $a, b \in G$, la ecuación $a * x = b$ siempre tiene más de una solución.
17. En un grupo $(G, *)$, con $a, b \in G$, la ecuación $x * a = b$ tiene como solución a $a^{-1} * b$.
18. En un grupo abeliano $(G, *)$, con $a, b \in G$, la ecuación $x * a = b$ tiene como solución a $a^{-1} * b$.
19. En un grupo abeliano $(G, *)$, con $a, b \in G$, las ecuaciones $x * a = b$ y $a * x = b$ tienen la misma solución.
20. Dado $n \geq 2$, $(\mathbb{Z}_n, +_n)$ es un grupo.
21. Dado $n \geq 2$, $(\mathbb{Z}_n \setminus \{[0]_n\}, +_n)$ es un grupo.
22. Dado un homomorfismo entre dos grupos $(A, *)$ y $(B, \triangle)$, la preimagen del neutro de B contiene al neutro de A.
23. Existen homomorfismos no epiyectivos entre dos grupos $(A, *)$ y $(B, \triangle)$ tales que la preimagen del neutro de B es vacía.
24. Dado un homomorfismo epiyectivo f, entre los grupos $(A, *)$ y $(B, \triangle)$, se tiene que para $x \in A$, $(f(x^{-1}))^{-1} = f(x)$.
25. Dado un homomorfismo epiyectivo f, entre los grupos $(A, *)$ y $(B, \triangle)$, se tiene que para todo $x \in A$, $(f(x^{-1}))^{-1} = f(e)$, con e neutro de A.
26. Dado un grupo $(G, *)$, un subconjunto no vacío $H \subseteq G$ se dice subgrupo de G si $*$ es cerrada en H.

27. Dado un grupo $(G, *)$, un subconjunto no vacío $H \subseteq G$ se dice subgrupo de G si $(H, *)$ es también grupo.
28. Dado un grupo $(G, *)$, un ejemplo de subgrupo de G es $(\emptyset, *)$.
29. G es siempre subgrupo de sí mismo (para la misma operación).
30. G es subgrupo de sí mismo sólo cuando $(G, *)$ es abeliano.
31. Dado un grupo $(G, *)$ y H un subgrupo, el neutro de H es a veces distinto del de G.
32. Dado un grupo $(G, *)$ y H un subgrupo, el inverso de un elemento $x \in H$ pertenece a $G \setminus H$.
33. Dado un grupo $(G, *)$ y H un subgrupo, el inverso de un elemento $x \in H$ pertenece a H.
34. Dado un grupo $(G, *)$, para probar que $H \subseteq G$ es subgrupo basta verificar que $\forall x, y \in H,\ x * y \in H$.
35. Dado un grupo $(G, *)$, para probar que $H \subseteq G$ es subgrupo basta verificar que $\forall x, y \in H,\ x * y^{-1} \in H$.
36. Dado un grupo finito $(G, *)$ y cualquier subgrupo $H \subseteq G$, $|G|$ es múltiplo de $|H|$.
37. Dado un grupo finito $(G, *)$ y cualquier subgrupo $H \subseteq G$, existe $k \in \mathbb{N}$ tal que $|G| = k|H|$.
38. Si un grupo G tiene un subgrupo con 16 elementos, entonces $|G|$ es par.
39. $(\mathbb{Z}_7, +_7)$ tiene subgrupos de tamaño 5.
40. Dado $p > 1$ primo, $(\mathbb{Z}_p, +_p)$ tiene al menos tres subgrupos distintos.
41. $(A, +, \cdot)$ es un anillo si y sólo si $(A, +)$ es un grupo abeliano.
42. $(A, +, \cdot)$ es un anillo si y sólo si $(A, +)$ es un grupo abeliano y $\cdot$ es asociativa.
43. $(A, +, \cdot)$ es un anillo si y sólo si $(A, +)$ es un grupo abeliano, $\cdot$ es asociativa y distribuye con respecto a $+$.
44. $(\mathbb{Z}, +, \cdot)$ es un anillo.
45. Todo anillo $(A, +, \cdot)$ tiene neutro para la operación $\cdot$.
46. En todo anillo $(A, +, \cdot)$ la operación $\cdot$ es conmutativa.
47. Todo anillo $(A, +, \cdot)$ tiene neutro para la operación $+$.
48. En todo anillo $(A, +, \cdot)$ la operación $+$ es conmutativa.
49. $(\mathbb{Z}, +, \cdot)$ es un anillo conmutativo con unidad.
50. En todo anillo $(A, +, \cdot)$, el neutro para $\cdot$ y para $+$ son elementos distintos.
51. En todo anillo $(A, +, \cdot)$, con más de un elemento, el neutro para $\cdot$ y para $+$ son elementos distintos.
52. Si $(A, +, \cdot)$ es un anillo, se cumple que $(\forall x \in A,\ 0 \cdot x = x \cdot 0 = 0)$.
53. Si $(A, +, \cdot)$ es un anillo, $x, y \in A$, entonces $x \cdot y = 0 \implies x = 0 \vee y = 0$.
54. $(\mathbb{Z}_9, +, \cdot)$ es un anillo.
55. $(\mathbb{Z}_9, +, \cdot)$ es un anillo conmutativo con unidad.
56. $(\mathbb{Z}_9, +, \cdot)$ es un anillo conmutativo con unidad sin divisores del cero.

57. $(\mathbb{Z}_7, +, \cdot)$ es un anillo conmutativo con unidad sin divisores del cero.
58. $(\mathbb{Z}_{17}, +, \cdot)$ es un anillo conmutativo con unidad sin divisores del cero.
59. $[1]_p$ es el neutro para $\cdot_p$ en el anillo $(\mathbb{Z}_p, +, \cdot)$.
60. En $(\mathbb{Z}_9, +, \cdot)$ se cumple que $[3]_9 \cdot_9 [3]_9 = [0]_9$.
61. Todo cuerpo es un anillo.
62. $(\mathbb{Z}_9, +, \cdot)$ es un cuerpo.
63. $(\mathbb{R}, +, \cdot)$ es un anillo.
64. $(\mathbb{R}, +, \cdot)$ es un cuerpo.
65. En todo cuerpo, $x \cdot y = 0 \implies x = 0 \vee y = 0$.
66. Todo anillo finito sin divisores del cero es un cuerpo.
67. Todo anillo finito conmutativo con unidad sin divisores del cero es un cuerpo.
68. Para p primo, $(\mathbb{Z}_p, +, \cdot)$ es un cuerpo.

Guía de Ejercicios

1. Señale cuáles de las siguientes estructuras algebraicas no son grupos. Explique por qué:

   a) $(\mathbb{R}, +)$.
   b) $(\mathbb{R}, \cdot)$.
   c) Dado $A \neq \emptyset$, $(\mathcal{P}(A), \cup)$.
   d) Dado $A \neq \emptyset$, $(\mathcal{P}(A), \cap)$.
   e) $(\mathbb{N}, \cdot)$.
   f) $(\mathbb{Z} \setminus \{0\}, \cdot)$.
   g) $(\mathbb{Z} \setminus \{0\}, +)$.

2. En la demostración de que $(\mathbb{Z}_n, +_n)$, para $n \geq 2$ es grupo, falto demostrar la existencia de inversos. Pruebelo, es decir, verifique que cualquier $x \in \mathbb{Z}_n$, x admite un inverso para $+_n$.
3. Sea $G = \{f : \mathbb{R} \to \mathbb{R} \mid \exists a, b \in \mathbb{R},\ a \neq 0 \wedge f(x) = ax + b\}$.

   a) Pruebe que $(G, \circ)$ es un grupo, en donde $\circ$ es la composición de funciones. ¿Es abeliano?
   b) Sea $G_1 = \{f : \mathbb{R} \to \mathbb{R} \mid \exists b \in \mathbb{R},\ f(x) = x + b\}$. Probar que $(G_1, \circ)$ es subgrupo de $(G, \circ)$.
   c) Sea $G_2 = \{f : \mathbb{R} \to \mathbb{R} \mid \exists b \in \mathbb{R},\ f(x) = 2x + b\}$. Pruebe que $(G_2, \circ)$ **no** es subgrupo de $(G, \circ)$.

4. Sean $(G_1, *)$ y $(G_2, \triangle)$ grupos con e_2 el neutro de G_2 y sea $f : (G_1, *) \to (G_2, \triangle)$ un homomorfismo. Demuestre las siguientes afirmaciones:

   a) Dado un subgrupo $H_1 \subseteq G_1$, entonces $f(H_1)$ es subgrupo de $(G_2, \triangle)$.

b) Dado un subgrupo $H_2 \subseteq G_2$, entonces $f^{-1}(H_2)$ es subgrupo de $(G_1, *)$.
c) $\text{Im}(f)$ es un subgrupo de $(G_2, \triangle)$.
d) El conjunto $\{x \in G_1 \mid f(x) = e_2\}$ es un subgrupo de $(G_1, *)$.

5. a) Considere el conjunto de los números pares $\mathcal{P}$, dotado con la multiplicación y suma usual en $\mathbb{R}$. Determine si la estructura $(\mathcal{P}, +, \cdot)$ es un anillo.
   b) Si la respuesta de la parte anterior es negativa, señale qué propiedad falla.
6. Demuestre, para un anillo $(A, +, \cdot)$, la siguiente propiedad enunciada en el texto del apunte: $\forall x, y \in A,\ (-x) \cdot (-y) = x \cdot y$.
7. Sean $(A, +, \cdot)$ y $(A', \oplus, \odot)$ dos anillos con neutros aditivos 0 y $0'$ respectivamente y $f : A \longrightarrow A'$ un homomorfismo de anillos. Se define $I = \{x \in A \mid f(x) = 0'\}$.
   (a) Demuestre que $(I, +)$ es subgrupo de $(A, +)$.
   (b) Demuestre que $\forall a \in A, \forall b \in I,\ a \cdot b \in I \wedge b \cdot a \in I$.
   (c) Si $(A, +, \cdot)$ tiene unidad u (neutro para $\cdot$) y $\exists x \in I$ tal que x es invertible, pruebe que $f(u) = 0'$ y utilícelo para demostrar que $\forall a \in A, a \in I$, es decir $A = I$.
8. Pruebe que si $(\mathbb{Z}_n, +_n, \cdot_n)$ no tiene divisores de cero, entonces n es un número primo.

Guía de Problemas

1. (20 min.) Sea $(G, *)$ un grupo que satisface la propiedad $a * a = e$ (el neutro del grupo) en cada $a \in G$, es decir, el inverso de cada elemento del grupo es el mismo elemento. Pruebe que G es un grupo abeliano. (Indicación: calcule $(a * b) * (b * a)$).
2. (20 min.) Sea $(G, *)$ un grupo tal que $G = \{e, a, b\}$ con e neutro en G. Pruebe que $a^{-1} = b$.
3. Sea $(G \times H, \otimes)$ el producto cartesiano de los grupos $(G, *)$ y $(H, \circ)$ con neutros e_G y e_H, respectivamente.
   a) (20 min.) Demuestre que las funciones φ y ψ definidas por
   $$\begin{array}{rcl} \varphi : G \times H & \longrightarrow & G \\ (g, h) & \longmapsto & \varphi((g, h)) = g \end{array} \quad y \quad \begin{array}{rcl} \psi : G \times H & \longrightarrow & H \\ (g, h) & \longmapsto & \psi((g, h)) = h \end{array}$$
   son epimorfismos.
   b) (20 min.) Considere $G = H$, $* = \circ$, y la función $f : G \times G \to G$ definida por
   $$f((a, b)) = (a * b)^{-1}.$$
   Pruebe que f es homomorfismos entre $(G \times G, \otimes)$ y $(G, *)$ si y sólo si el grupo $(G, *)$ es abeliano.
4. (30 min.) Sea $(G, *)$ un grupo. Demuestre que la función $f : G \to G$, dada por $f(x) = x^{-1}$, es un automorfismo de $(G, *)$ si y sólo si $(G, *)$ es un grupo abeliano.

5. En $\mathbb{Q}^2$ se define la operacion $*$ por $(a,b)*(c,d) = (a\cdot d + b\cdot c, a\cdot c - b\cdot d)$, donde $+$ y $\cdot$ son la suma y el producto en $\mathbb{Q}$, respectivamente. Determine si $(\mathbb{Q}^2 \setminus \{(0,0)\}, *)$ es un grupo abeliano, indicando neutro e inversos, cuando existan.

6. Sea $(G,*)$ un grupo con neutro $e \in G$ y

$$A = \{F : G \to G \mid \ F \text{ es un isomorfismo de } (G,*) \text{ en } (G,*)\}.$$

   a) (20 min.) Probar que $(A, \circ)$ es un grupo
   b) (20 min.) Para cada $g \in G$ se define la función $F_g : G \to G$ tal que $F_g(x) = g * x * g^{-1}$ en cada $x \in G$. Pruebe que:
      - F_g es un homomorfismo de $(G,*)$ en $(G,*)$.
      - $F_{g*h} = F_g \circ F_h$, para todo $g, h \in G$.
      - $F_e = \mathrm{id}_G$.

      Concluya que F_g es un isomorfismo y que $(F_g)^{-1} = F_{g^{-1}}$ para todo $g \in G$.
   c) (20 min.) Pruebe que $B = \{F_g \mid g \in G\}$ es un subgrupo de $(A, \circ)$.

7. Las siguientes tablas incompletas corresponden a las operaciones en el anillo $(A, \oplus, \odot)$, para $A = \{a, b, c, d\}$

$\oplus$	a	b	c	d
a	a	b		d
b		a		
c			a	
d				

$\odot$	a	b	c	d
a	a	a	a	a
b	a			a
c	a		c	
d	a	b	c	

   a) (30 min.) Considerando las propiedades generales del anillo, complete las tablas anteriores justificando cada relleno. (Indicación: complete primero la tabla para $\oplus$ y para $\odot$ utilice adecuadamente la distributividad.)
   b) (10 min.) ¿Es $(A, \oplus, \odot)$ conmutativo? ¿Posee $(A, \oplus, \odot)$ unidad? ¿Tiene divisores del cero?

8. (30 min.) Si $(A, +, \cdot)$ es un anillo tal que $x \cdot x = x$ para todo $x \in A$. Pruebe que

   a) $x = -x$ para todo $x \in A$.
   b) $(A, +, \cdot)$ es anillo conmutativo.
   c) $(x \cdot y) \cdot (x + y) = 0$, para todo $x, y \in A$.

SEMANA 12:

Ingeniería Matemática
FACULTAD DE CIENCIAS
FÍSICAS Y MATEMÁTICAS
UNIVERSIDAD DE CHILE

Números complejos

10.1 Introducción

Consideremos la ecuación $x^2 = 2$.

Ésta no tiene soluciones en $\mathbb{Q}$, pero sí en $\mathbb{R}$ ($\sqrt{2}$ y $-\sqrt{2}$). Podemos pensar en los reales como una extensión de los racionales, donde esta ecuación sí tiene solución.

Del mismo modo, sabemos que en $\mathbb{R}$ la siguiente ecuación **no** tiene solución: $x^2 = -4$.

Debido a esta carencia, se "crea" el conjunto de los números complejos, el cual será una extensión de $\mathbb{R}$, donde esta ecuación sí tiene solución.

Definición 10.1 (Números complejos) *Sea $\mathbb{C} = \mathbb{R}^2$. Llamaremos a $\mathbb{C}$ conjunto de los **números complejos**, y lo dotaremos de las operaciones $+$ y $\cdot$ definidas a continuación: para $z = (a, b), w = (c, d) \in \mathbb{C}$*

$$z + w = (a + c, b + d),$$
$$z \cdot w = (ac - bd, ad + bc).$$

Es fácil verificar que:

- El neutro en $(\mathbb{C}, +)$ es $(0, 0)$ y el neutro en $(\mathbb{C}, \cdot)$ es $(1, 0)$.
- El inverso en $(\mathbb{C}, +)$ de (a, b) es $(-a, -b)$.
- El inverso en $(\mathbb{C}, \cdot)$ para $(a, b) \neq (0, 0)$ es $\left(\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2}\right)$.

Además, como $(\mathbb{C}, +, \cdot)$ es un anillo conmutativo también son ciertas las identidades de la Proposición 9.25.

¿Tiene solución la ecuación $z^2 = -4$ en $\mathbb{C}$? Antes de responder esta pregunta notemos que la igualdad involucra a -4 que no es un elemento de $\mathbb{C}$. Así, primero que todo es necesario decir como vamos a representar -4 como un complejo y en general cualquier número real.

10.2 Forma cartesiana y módulo de un complejo

En Geometría Analítica se considera al subconjunto de $\mathbb{C} = \mathbb{R}^2$ de las abscisas dado por $OX = \{(a, 0) : a \in \mathbb{R}\}$ como correspondiente al conjunto de números reales $\mathbb{R}$. Esta correspondencia se ha tratado hasta ahora de manera intuitiva. Con el lenguaje que hemos desarrollado podemos expresar esto de manera más precisa.

Proposición 10.2 *La función $f : \mathbb{R} \to OX$ dada por $f(a) = (a, 0)$ es un isomorfismo de anillos entre $(\mathbb{R}, +, \cdot)$ y $(OX, +, \cdot)$, donde las operaciones en OX son las de $\mathbb{C}$.*

Dem. Es claro que en $\mathbb{C}$ se tiene que $(a + b, 0) = (a, 0) + (b, 0)$ y que $(a, 0) \cdot (b, 0) = (a \cdot b - 0, a \cdot 0 + 0 \cdot b) = (a \cdot b, 0)$. Además, $f(1) = (1, 0)$ que es el neutro de $(\mathbb{C}, \cdot)$. De esta forma, f es un homomorfismo de anillo. Por otra parte, f es biyectiva con inversa $g : OX \to \mathbb{R}$ dada por $g(a, 0) = a$. □

Desde ahora en adelante, pensaremos que $\mathbb{R}$ es el subconjunto OX de $\mathbb{C}$. En lugar de anotar $(a, 0)$ los elementos de OX los anotaremos, simplemente, a.

Sea $z = (a, b) \in \mathbb{C}$. Entonces, $(a, 0) + (0, b) = (a, b)$, pues la suma en $\mathbb{C}$ es coordenada por coordenada. De este modo, (ver Figura 17) geométricamente z queda representado como un punto en el plano cartesiano cuyo desplazamiento en el **eje real** (eje horizontal) es a y en el **eje imaginario** (eje vertical) es b. (También el complejo z se representa como un **vector** que se dibuja como una flecha que parte del origen O del plano cartesiano y termina en z.)

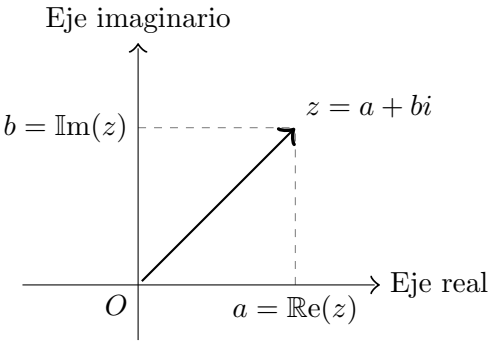


Figura 17: Representación del "plano" complejo.

Además, $(0, 1) \cdot (b, 0) = (0 \cdot b - 1 \cdot 0, 0 \cdot 0 + 1 \cdot b) = (0, b)$. Entonces, $z = (a, b) = (a, 0) + (0, 1) \cdot (b, 0)$. Es decir, el complejo z se puede escribir en términos de los dos elementos $(a, 0)$ y $(b, 0)$ de OX, los cuales hemos dicho se anotarán a y b, respectivamente.

El elemento $(0, 1)$ juega un rol destacado en el estudio del conjunto $\mathbb{C}$.

Definición 10.3 *La **unidad imaginaria** es el complejo $(0, 1)$. Se anota i.*

Usando la unidad imaginaria, el complejo z se puede escribir como $a + ib$, $a, b \in \mathbb{R}$.

Definición 10.4 (Forma cartesiana) *La expresión $a+ib$, $a, b \in \mathbb{R}$ se llama la **forma cartesiana** del complejo $z = (a, b) \in \mathbb{C}$.*

*Se dice que la **parte real de** z es a y se anota $\mathbb{R}e(z)$. La **parte imaginaria de** z es b y se anota $\mathbb{I}m(z)$.*

Una propiedad importante de la unidad imaginaria i es que su cuadrado es -1. En efecto,

$$i^2 = (0, 1) \cdot (0, 1) = (0 - 1, 0) = -1.$$

Proposición 10.5 *Las funciones $\mathbb{R}e(\cdot)$ e $\mathbb{I}m(\cdot)$ son endomorfismos en $(\mathbb{C}, +)$. Además, para $z \in \mathbb{C}$ y $a \in \mathbb{R}$:*

(I) $\mathbb{R}e(az) = a\mathbb{R}e(z)$

(II) $\mathbb{I}m(az) = a\mathbb{I}m(z)$.

(III) $z = w$ *si y solo si* $\mathbb{R}e(z) = \mathbb{R}e(w)$ *y* $\mathbb{I}m(z) = \mathbb{I}m(w)$.

Estas propiedades quedan propuestas como ejercicio.

Ejemplo: Volvamos a la pregunta original. ¿La ecuación $z^2 = -4$, tiene solución en $\mathbb{C}$?

Ahora podemos formular la pregunta en $\mathbb{C}$. Buscamos $z = a+ib$ tal que $(a+ib)^2 = -4+i\cdot 0$. Esto ocurre si y sólo si $\mathbb{R}\text{e}((a+ib)^2) = -4$ y $\mathbb{I}\text{m}((a+ib)^2) = 0$. Como $(a+ib)^2 = a^2-b^2+2abi$, de lo anterior se obtienen dos ecuaciones para a y b: $a^2 - b^2 = -4$ y $2ab = 0$. Cuando $b = 0$, la primera se reduce a $a^2 = -4$, que sabemos no tiene solución. Así, podemos suponer que $b \neq 0$ y entonces $a = 0$, lo que implica que $b^2 = 4$. De esta forma, $b = 2$ o $b = -2$, con lo que encontramos dos soluciones a la pregunta $z^2 = -4$: $2i$ y $-2i$.

Más generalmente, veamos que toda ecuación $z^2 = w$ tiene solución en $\mathbb{C}$, para $w \in \mathbb{C}$ dado. Procediendo como antes vemos que si $z = a + ib$ y $w = c + id$, entonces $a^2 - b^2 = c$ y $2ab = d$.

Si $d = 0$, entonces se procede como antes, definiendo $b = 0$ y $a = \sqrt{c}$, si $c \geq 0$, y $a = 0$ y $b = \sqrt{-c}$, si $c < 0$.

Para $d \neq 0$, tenemos que $a, b \neq 0$ y podemos despejar $a = d/(2b)$. Al reemplazarlo en $a^2 - b^2 = c$ nos queda $d^2/4b^2 - b^2 = c$. Ésta es una ecuación cuadrática en b^2 que tiene como solución $b^2 = (-c + \sqrt{c^2 + d^2})/2$. De aquí es claro como obtener el valor de a. Por lo tanto, siempre tenemos solución. ♢

La conclusión del ejemplo anterior es que la ecuación $z^2 = w$, para $w \in C$ dado, siempre tiene al menos una solución y nunca más de dos soluciones.

Veremos pronto una segunda manera de representar los elementos de $\mathbb{C}$, que será muy útil para entender geométricamente las soluciones de la ecuación $z^2 = w$, para w dado, y en general las ecuaciones $z^n = w$, para $n \in \mathbb{N}$ y $w \in \mathbb{C}$ dados.

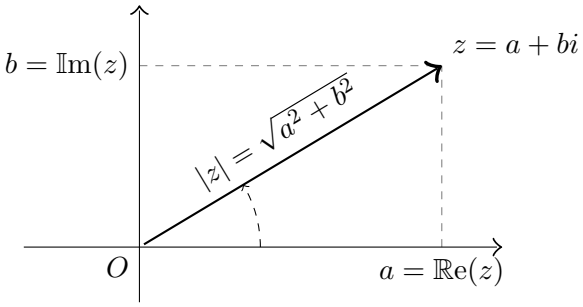


Figura 18: Representación del módulo de un complejo.

Definición 10.6 (Módulo de un complejo) *El módulo de $z \in \mathbb{C}$ es su distancia al origen O. Se anota $|z|$. Según el Teorema de Pitágoras tenemos que si $z = a + ib$, entonces*

$$|z| = \sqrt{a^2 + b^2}.$$

Algunas propiedades relevantes del módulo de un complejo son las siguientes.

Recordemos que las potencias z^k, para $z \in \mathbb{C}$ y $k \in \mathbb{Z}$, se definen como $z^0 = 1$, $z^{k+1} = z^k \cdot z$, para $k \geq 0$ y $z^k = (z^{-1})^{-k}$, si $k < 0$.

Proposición 10.7 *Para $z \in \mathbb{C}$, con $z = a + ib$ se tiene que:*

(I) $|z| \geq 0$ *y vale cero si y sólo si* $z = 0$.

(II) $|z| \geq |a|$ *y* $|z| \geq |b|$ *con lo que* $|z| \geq |\mathbb{R}e(z)|, |\mathbb{I}m(z)|$.

(III) Además, para $w \in \mathbb{C}$, $|zw| = |z| \cdot |w|$.

(IV) $|z^k| = |z|^k$, *para* $k \in \mathbb{Z}$.

Dem. Lo primero es consecuencia de que $\sqrt{x} \geq 0$ y vale cero si y sólo si $x = 0$. Lo segundo viene de la desigualdad $\sqrt{a^2 + b^2} \geq \max\{a, b\}$. Lo tercero queda como ejercicio y lo último se obtiene aplicando recursivamente la tercera parte a $z = w$. □

Conjugación en $\mathbb{C}$

Definición 10.8 (Conjugado) *La función $\boldsymbol{C}\colon \mathbb{C} \to \mathbb{C}$ dada por $f(a + ib) = a - ib$ se llama la conjugación de un complejo. Al complejo $a - bi$ se le llama el* ***conjugado*** *de $a + bi$ y se anota $\overline{a + ib}$.*

En la Figura 19 se ilustra la acción de la función conjugación.

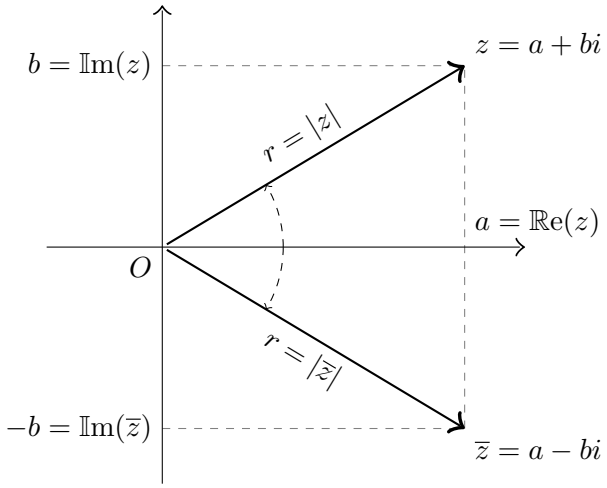


Figura 19: Representación gráfica de z y $\overline{z}$.

Proposición 10.9 *Sean $z, w \in \mathbb{C}$. Se tiene:*

(I) Propiedades simples de la conjugación:

a) $\overline{\overline{z}} = z$. *(es autoinversa)*
b) $z \in \mathbb{R} \iff z = \overline{z}$. *(es la identidad cuando se restringe a $\mathbb{R}$)*
c) $\overline{z \pm w} = \overline{z} \pm \overline{w}$. *(es endomorfismo de $(\mathbb{C}, +)$)*
d) $\overline{z \cdot w} = \overline{z} \cdot \overline{w}$. *(es endomorfismo de $(\mathbb{C}, \cdot)$)*

(II) Relación con $\mathbb{R}e(\cdot)$ e $\mathbb{I}m(\cdot)$.

a) $\mathbb{R}e(\overline{z}) = \mathbb{R}e(z)$ *e* $\mathbb{I}m(\overline{z}) = -\mathbb{I}m(z)$.
b) $\mathbb{R}e(z) = \frac{1}{2}(z + \overline{z})$ *e* $\mathbb{I}m(z) = \frac{1}{2i}(z - \overline{z})$.

(III) Relación con módulo.

a) $|\overline{z}| = |z|$.
b) $z \cdot \overline{z} = |z|^2$.
c) $z^{-1} = \overline{z}/|z|^2$ *si* $z \neq 0$.
d) Si $w \neq 0$, *entonces* $|z/w| = |z|/|w|$ *y* $\overline{z/w} = \overline{z}/\overline{w}$.

Dem. Sean $z = (a, b)$ y $w = (c, d)$.

(I) Que la conjugación sea autoinversa es, simplemente porque $\overline{a - bi} = a - (-bi) = a + bi$.

La segunda afirmación hay que entenderla en el sentido que $a + 0i$ es considerado un elemento de $\mathbb{R}$. De esta manera, $\overline{a + 0i} = a - 0i = a$, para todo $a \in \mathbb{R}$.

Para la tercera se tiene que:

$$\overline{z + w} = \overline{a + bi + c + di} = \overline{(a + c) + (b + d)i} = a + c - (b + d)i = a - bi + c - di = \overline{z} + \overline{w}.$$

Similarmente, tenemos la fórmula $z \cdot w = (ac - bd) + i(ad + bc)$ por lo que

$$\overline{z \cdot w} = (ac - bd) - i(ad + bc) = (a - ib)(c - id) = \overline{z} \cdot \overline{w}.$$

(II) Es claro que $\mathbb{R}\mathrm{e}(a-ib) = a = \mathbb{R}\mathrm{e}(z)$ y que $\mathbb{I}\mathrm{m}(a-ib) = -b = -\mathbb{I}\mathrm{m}(z)$. Además, $a+ib+a-ib = 2a$ y $a+ib-(a-ib) = 2ib$.

(III) Tenemos que $z \cdot \overline{z} = (a+ib)(a-ib) = a^2+b^2 = |z|^2$.

Para $z \neq 0$, podemos dividir por $|z|^2$ y obtener $z(\overline{z}/|z|^2) = 1$. Lo que significa que $\overline{z}/|z|^2$ es el inverso de z en $(\mathbb{C}, \cdot)$.

Usamos que $w^{-1} = \overline{w}/|w|^2$ y que $\overline{w}^{-1} = w/|w|^2$. De aquí, $z/w = z\overline{w}/|w|^2$ y es directo que $|z/w| = |z|/|w|$. Además, $\overline{z/w} = \overline{z}w/|w|^2 = \overline{z}/\overline{w}$.

□

Obtenemos el siguiente resultado:

Corolario 10.10 *La conjugación es un automorfismo en* $(\mathbb{C}, +, \cdot)$*, autoinversa y restringida a* $\mathbb{R}$ *es la identidad.*

Dem. Directa de las proposiciones anteriores. □

El siguiente resultado resalta una importante propiedad geométrica que relaciona el "largo" de la suma de dos complejos con los "largos" de los sumandos (ver Figura 20).

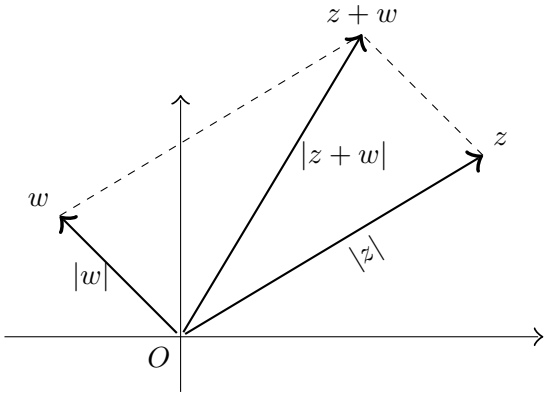


Figura 20: Ilustración de la Desigualdad Triangular.

Proposición 10.11 (Desigualdad triangular) *Si* $z, w \in \mathbb{C}$*, entonces* $|z+w| \leq |z|+|w|$.

Dem. En efecto, $|z+w|^2 = (z+w)\overline{(z+w)} = (z+w)(\overline{z}+\overline{w}) = |z|^2 + w\overline{z} + \overline{w}z + |w|^2$.

Notemos que el conjugado de $w\overline{z}$ es $\overline{w}z$, con lo que la suma $w\overline{z} + \overline{w}z = 2\mathbb{R}\mathrm{e}(w\overline{z})$. Pero, $\mathbb{R}\mathrm{e}(w\overline{z}) \leq |w\overline{z}| = |w| \cdot |z|$. Así, $|z|^2 + w\overline{z} + \overline{w}z + |w|^2 \leq |z|^2 + 2|z| \cdot |w| + |w|^2 = (|z|+|w|)^2$. Esto permite concluir que $|z+w| \leq |z| + |w|$. □

Damos ahora una nueva representación de un complejo. En ésta, un complejo z no nulo se describe por su distancia r al origen $O = (0,0)$ junto con el ángulo θ que se forma entre el eje OX y el segmento que une O y z, medido en el sentido antihorario (ver Figura 21). En este caso, para evitar repeticiones, el ángulo θ se elige en $[0, 2\pi)$.

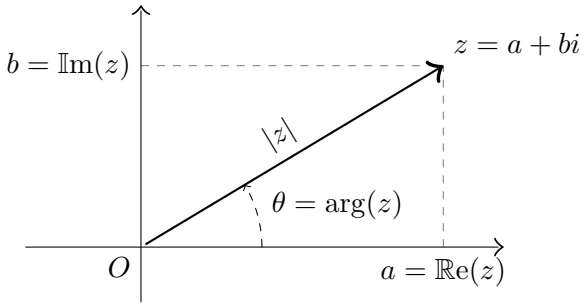


Figura 21: Representación del argumento de un complejo.

Definición 10.12 (Argumento y Coordenadas Polares) *Las coordenadas polares de $z \in \mathbb{C} \setminus \{O\}$ son el par $(r, \theta) \in (0, \infty) \times [0, 2\pi)$ donde:*

- *r es el módulo de z, $|z|$.*
- *θ es el ángulo que se forma entre el eje OX y el segmento que une z con el origen O. Se llama el **argumento** de z y se anota $\arg(z)$.*

Destacamos que, para $z, w \neq 0$, $z = w$ si y sólo si $|z| = |w|$ y $\arg(z) = \arg(w)$.

La relación entre las coordenadas polares y las usuales, las cartesianas, es la siguiente. Sean (a, b) las coordenadas cartesianas de z y (r, θ) sus coordenadas polares. Entonces,

$$a = r\cos\theta \quad \text{y} \quad b = r\,\mathrm{sen}\,\theta.$$

La razón de manipular dos sistemas de coordenadas para $\mathbb{R}^2$ es que en el primero, las coordenadas cartesianas, son más amigables para operar con la adición $+$, mientras que en el segundo, las coordenadas polares, son más cómodas para operar con $\cdot$ y calcular inversos multiplicativos.

Definición 10.13 (Forma polar) *Para $\theta \in \mathbb{R}$ anotamos $e^{i\theta} = \cos\theta + i\,\mathrm{sen}\,\theta$.*

*La expresión $|z|e^{i\arg(z)}$ se llama la **forma polar** de z.*

Ejemplo: Veamos la forma polar de algunos complejos.

- Para $\theta \in [0, 2\pi)$, sea $z = (\cos\theta, \mathrm{sen}\,\theta)$. Entonces, $|z|^2 = \cos^2\theta + \mathrm{sen}^2\,\theta = 1$, por lo que $|z| = 1$. Claramente, su argumento es θ. Luego, $z = e^{i\theta}$.
- Calculemos la forma polar del complejo $z = 2 + 2i$. Primero observamos que $|z| = \sqrt{2^2 + 2^2} = \sqrt{8}$. Luego, $z = 2\sqrt{2}\big(\frac{1}{\sqrt{2}} + i\frac{1}{\sqrt{2}}\big)$ de modo que el argumento es $\pi/4$. Así, $2 + 2i = 2\sqrt{2}\ e^{i\pi/4}$.

$\diamondsuit$

La utilidad de la forma polar se debe en gran medida a la propiedad siguiente:

Proposición 10.14 *Para todo $\alpha, \beta \in \mathbb{R}$ se cumple que $e^{i\alpha} \cdot e^{i\beta} = e^{i(\alpha+\beta)}$.*

Dem. Por definición del producto en $\mathbb{C}$,

$$e^{i\alpha} \cdot e^{i\beta} = (\cos\alpha, \operatorname{sen}\alpha) \cdot (\cos\beta, \operatorname{sen}\beta) = (\cos\alpha\cos\beta - \operatorname{sen}\alpha\operatorname{sen}\beta, \cos\alpha\operatorname{sen}\beta + \cos\beta\operatorname{sen}\alpha).$$

Al lado derecho aparecen las fórmulas trigonométricas para la suma de ángulos: $\cos\alpha\cos\beta - \operatorname{sen}\alpha\operatorname{sen}\beta = \cos(\alpha+\beta)$ y $\cos\alpha\operatorname{sen}\beta + \cos\beta\operatorname{sen}\alpha = \operatorname{sen}(\alpha+\beta)$. De este modo, el lado derecho es $e^{i(\alpha+\beta)}$. □

¿Hay alguna relación entre $\arg(z)$, $\arg(w)$ y $\arg(z \cdot w)$, para $z, w \in \mathbb{C}$? Lo anterior sugiere que sí pues nos dice que al multiplicar los complejos $z = e^{i\alpha}$ y $w = e^{i\beta}$ el resultado es el complejo $zw = e^{i(\alpha+\beta)}$. De aquí, podemos concluir que si $\alpha + \beta \in [0, 2\pi)$ entonces $\arg(zw) = \arg(z) + \arg(w)$. Pero, puede ocurrir que $\alpha + \beta \notin [0, 2\pi)$ cuando $\alpha, \beta \in [0, 2\pi)$. De modo que, para z y w arbitrarios, lo que se cumple es: $\arg(zw) = \arg(z) + \arg(w)$ mód 2π.

Proposición 10.15 *Para $z, w \in \mathbb{C} \setminus \{0\}$, $k \in \mathbb{Z}$ y $\theta \in \mathbb{R}$, se tiene que:*

(I) $\arg(zw) = \arg(z) + \arg(w)$ mód 2π.

(II) $\arg z^k = k \cdot \arg z$ mód 2π.

(III) Fórmula de De Moivre: $(e^{i\theta})^k = e^{i(k\theta)}$.

(IV) $\arg(\overline{z}) = 2\pi - \arg(z)$.

(V) $z^{-1} = (1/|z|)e^{i\arg(\overline{z})} = (1/|z|)e^{-i\arg(z)}$.

Dem. Ya vimos que la primera afirmación es correcta. La segunda se obtiene al aplicar la primera de manera iterada. La tercera es consecuencia de las anteriores, pues $|e^{i\theta}| = 1$ y $\arg\left((e^{i\theta})^k\right) = k\theta$ mód 2π. La justificación de las dos restantes se propone como ejercicio. □

Del resultado anterior, es fácil ver que para todo $n \in \mathbb{Z}$,

$$i^n = \begin{cases} +1, & \text{si } n \equiv_4 0, \\ +i, & \text{si } n \equiv_4 1, \\ -1, & \text{si } n \equiv_4 2, \\ -i, & \text{si } n \equiv_4 3, \end{cases}$$

Interpretación geométrica del producto

Ahora estamos en pie de dar una interpretación geométrica al producto de complejos. Sean $z = re^{i\theta}, w \in \mathbb{C} \setminus \{0\}$:

- Si $w = \alpha \in \mathbb{R}$, $w > 0$, entonces $z \cdot w = (\alpha r)e^{i\theta}$, es decir $z \cdot w$ es un estiramiento $(w > 1)$ o contracción $(w < 1)$ de z en un factor α.

- Si $w = e^{i\varphi}$, entonces $z \cdot w = re^{i(\theta+\varphi)}$, es decir $z \cdot w$ es una rotación de z en un ángulo $\varphi = \arg(w)$.
- De este modo, si $w = |w|e^{i\arg(w)}$, entonces $z \cdot w$ representa un estiramiento o contracción de z en un factor $|w|$, además de rotarlo en un ángulo $\arg(w)$.

La Figura 22 muestra gráficamente el efecto de distintas combinaciones de rotaciones, estiramientos y contracciones de un complejo z por otro w.

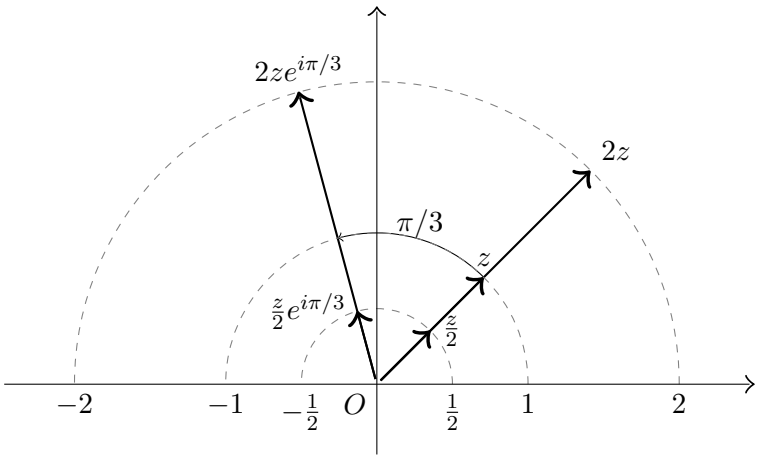


Figura 22: Efecto de multiplicar $z = \frac{1}{\sqrt{2}}(1+i)$ por $w \in \left\{2, \frac{1}{2}, 2e^{i\pi/3}, \frac{1}{2}e^{i\pi/3}\right\}$.

La interpretación geométrica de los complejos y las operaciones entre ellos nos permiten manipularlos y pensar de manera gráfica. Esto nos ayuda a desarrollar intuición que nos oriente sobre como desarrollar argumentos formales con los complejos. Aunque más frívolo, podemos generar hermosas imágenes por medio de esta relación entre los complejos y la geometría del plano cartesiano. Por ejemplo, considere la Figura 23.

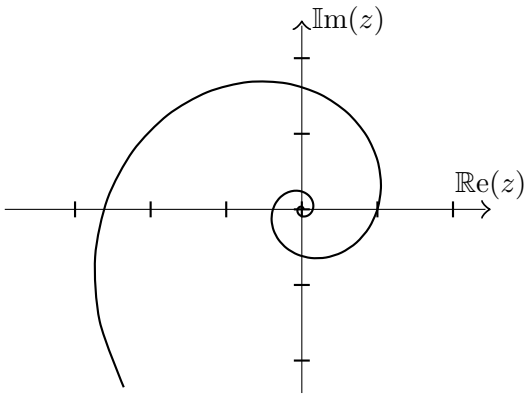


Figura 23: Representación parcial de la Espiral Áurea, específicamente, de $\{f(\theta) \in \mathbb{C} \mid \theta \leq \pi\}$ con $f : \mathbb{C} \to \mathbb{C}$ tal que $f(\theta) = e^{i\theta} \cdot e^{\frac{2}{\pi}\ln\varphi}$, donde $\varphi = \frac{1}{2}(1+\sqrt{5})$ es la razón áurea.

10.3 Raíces de un complejo

Definición 10.16 (Raíces de un complejo) *Sean $w \in \mathbb{C}\setminus\{0\}$ y $n \geq 2$. Diremos que z es una raíz n-ésima de w si $z^n = w$.*

Definición 10.17 (Raíces n-ésimas de la unidad) *Las raíces n-ésimas de 1, se llaman* ***las raíces n-ésimas de la unidad***

Proposición 10.18 *Sean $w \in \mathbb{C} \setminus \{0\}$ y $n \geq 2$. Entonces, la ecuación $z^n = w$ tiene exactamente n soluciones $w_0, \ldots, w_{n-1} \in \mathbb{C}$ donde $w_k = \sqrt[n]{|w|}e^{i(\arg(w)+2k\pi)/n}$.*

Dem. Para encontrar las soluciones z, escribimos $z = re^{i\theta}$ y $w = r_0e^{i\theta_0}$, con $r, r_0 > 0$ y $\theta, \theta_0 \in [0, 2\pi)$. Con esto la ecuación queda: $r^n(e^{i\theta})^n = r_0e^{i\theta_0}$.

Sabemos que $(e^{i\theta})^n = e^{in\theta}$ y que la igualdad se tiene si y sólo si $r^n = r_0$ y $e^{in\theta} = e^{i\theta_0}$.

Entonces, z es solución si y sólo si $r^n = r_0$ y $e^{in\theta} = e^{i\theta_0}$. La primera ecuación define $r = \sqrt[n]{r_0}$.

La segunda ecuación se cumple cada vez que $n\theta = \theta_0 \mod 2\pi$. Es decir, cada vez que exista $k \in \mathbb{Z}$ tal que $n\theta = \theta_0 + 2k\pi$. Luego, el conjunto de soluciones es

$$\{\theta_0/n + 2k\pi/n | k \in \mathbb{Z}\}.$$

De esta forma, las soluciones distintas son $\theta_0/n, \theta_0/n + 2\pi/n, \ldots, \theta_0/n + 2(n-1)\pi/n$.

Así, la ecuación $z^n = w$ tiene exactamente n soluciones dadas por

$$w_0 = \sqrt[n]{r_0}e^{i\theta_0/n}, w_1, \ldots, w_{n-1},$$

donde $w_k = w_0e^{i2\pi k/n}$, para $k \in [0..(n-1)]$. □

Con la interpretación geométrica del producto, las raíces n-ésimas de un complejo w se pueden entender de la siguiente forma: La primera raíz w_0 tiene módulo $\sqrt[n]{|w|}$ y argumento $\arg(w)/n$. Es decir, el argumento original de w se divide en n partes. Para obtener la solución w_k, simplemente se debe rotar w_0 en un ángulo de $2k\pi/n$ radianes. (Para un ejemplo, ver Figura 24.)

Una consecuencia inmediata del último resultado demostrado es la siguiente:

Corolario 10.19 *Las raíces n-ésimas de la* **unidad** *son $w_k = e^{i2k\pi/n}$, para $k \in [0..(n-1)]$. Además, se tiene que $w_k = w_0^k$ para todo $k \in [0..(n-1)]$.*

También es fácil deducir que:

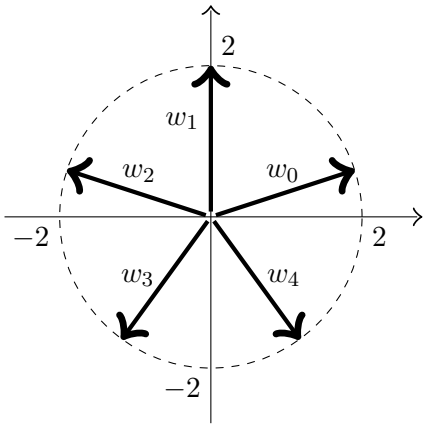


Figura 24: Raíces de $z^5 = w$ con $w = 32i$.

Corolario 10.20 *Si U es el conjunto de las raíces n-ísimas de la unidad, entonces $(U, \cdot)$ es subgrupo de $(\mathbb{C}, \cdot)$.*

Proposición 10.21 *Sea $n \geq 2$ y $w \in \mathbb{C}$. La suma de las raíces n-ésimas de w vale cero, es decir, si $w_0, \ldots, w_{n-1}$ son las raíces n-ésimas de w, entonces $\sum_{k=0}^{n-1} w_k = 0$.*

Dem. Sabemos que las raíces n-ésimas de $w \in \mathbb{C}$ están dadas por $w_k = w_0 e^{i2\pi k/n}$ para $k \in [0..(n-1)]$ donde $w_0 = \sqrt[n]{|w|}e^{i\theta_0/n}$.

Como $e^{i2\pi k/n} = (e^{i2\pi/n})^k$ se tiene que $\sum_{k=0}^{n-1} w_k = w_0 \sum_{k=0}^{n-1} (e^{i2\pi/n})^k$. La segunda sumatoria es la suma de una progresión geométrica. Como para $n \geq 2$, se tiene que $e^{i2\pi/n} \neq 1$, de la parte (II) de la Proposición 9.25, la referida sumatoria vale $((e^{i2\pi/n})^n - 1)/(e^{i2\pi/n} - 1)$. Pero, $(e^{i2\pi/n})^n = e^{i2\pi} = 1$.

De este modo, $\sum_{k=0}^{n-1} w_k = w_0((e^{i2\pi/n})^n - 1)/(e^{i2\pi/n} - 1) = 0$. □

Para concluir nuestro estudio de las raíces de los complejos. Intentemos entender como se comporta la función que a $w \in \mathbb{C}$, $0 < |w| \leq 1$, le asocia $w_k = w_0 e^{i2\pi k/n}$, donde $w_0 = \sqrt[n]{|w|}e^{i \arg(w)/n}$, $n \geq 2$ y $k \in [0..(n-1)]$. En particular, consideremos el caso $n = 2$ y $k = 0$ y grafiquemos $\mathbb{R}\mathrm{e}(w_0)$ e $\mathbb{I}\mathrm{m}(w_0)$ – ver Figura 25 y Figura 26. ¿Porqué $\mathbb{I}\mathrm{m}(w_0)$ es siempre positiva? ¿Cuál es la intersección de $\mathbb{R}\mathrm{e}(w_0)$ e $\mathbb{I}\mathrm{m}(w_0)$ con el plano $\mathbb{I}\mathrm{m}(z) = 0$? ¿cómo se interpreta? ¿Cuál es la curva que se obtiene al restringir w de forma que $|w| = 1$? ¿Qué se obtendría si se superpone a $\mathbb{R}\mathrm{e}(w_0)$ el gráfico de $\mathbb{R}\mathrm{e}(w_1)$? y, ¿si se superpone a $\mathbb{I}\mathrm{m}(w_0)$ el gráfico de $\mathbb{I}\mathrm{m}(w_1)$?

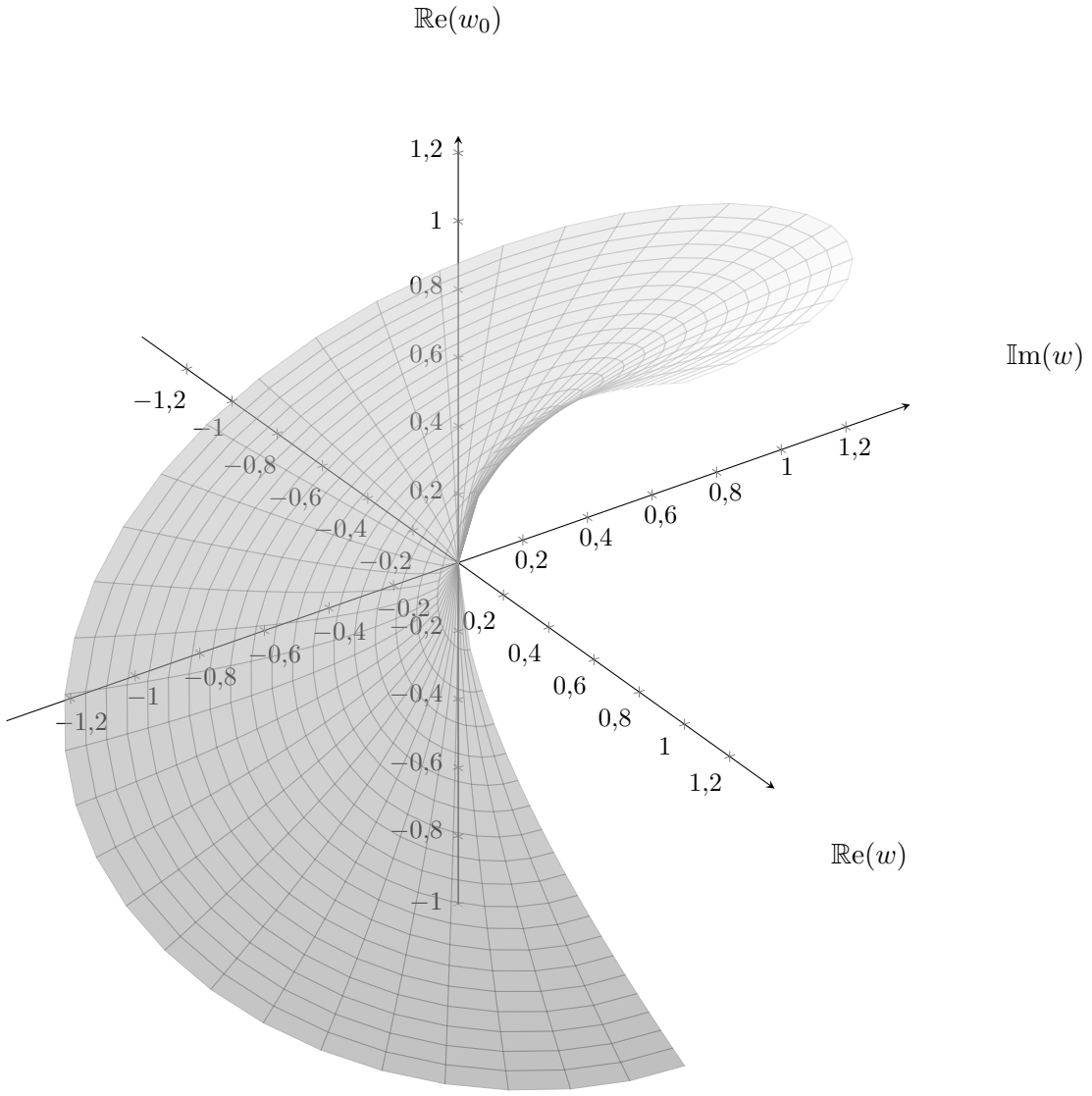


Figura 25: Partes real de la función que a w le asocia $\sqrt{|w|}e^{i\arg(w)/2}$.

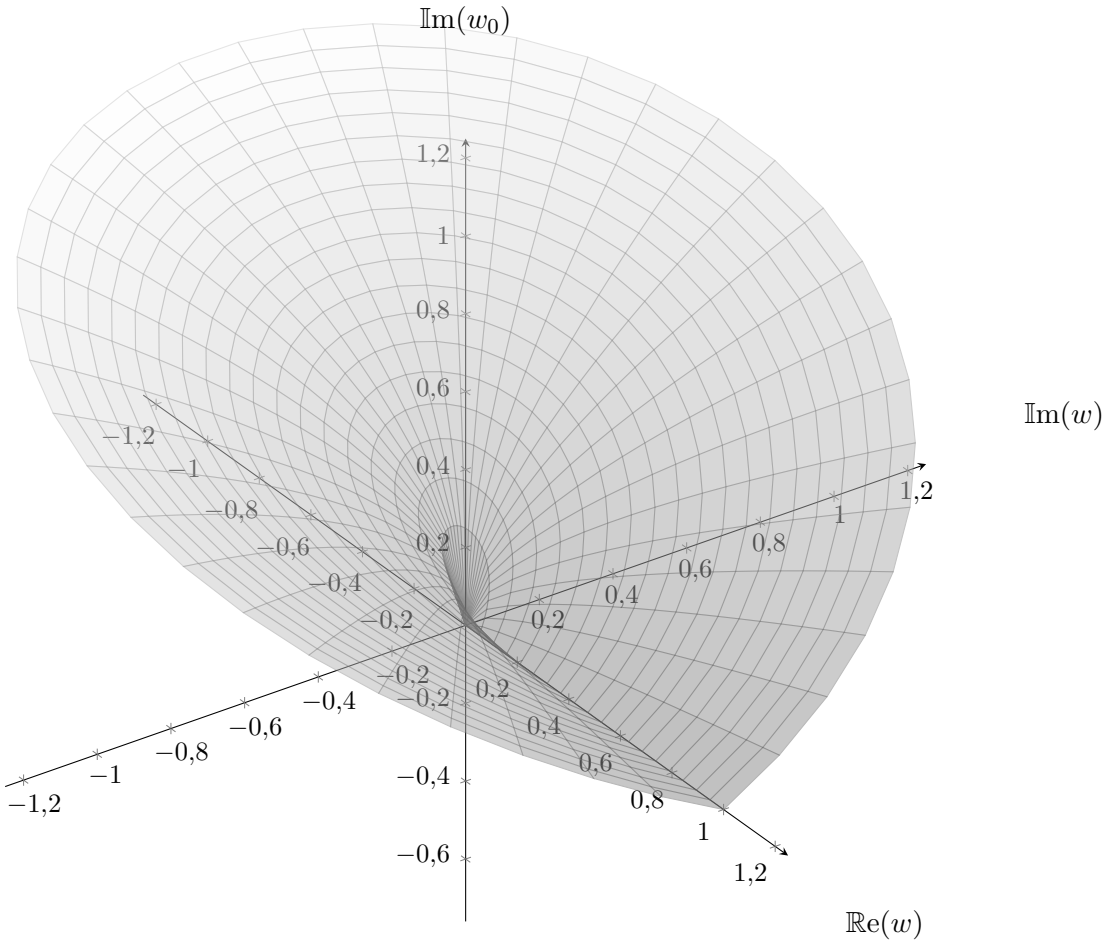


Figura 26: Partes imaginaria de la función que a w le asocia $\sqrt{|w|}e^{i\arg(w)/2}$.

Guía Básica

Determinar la veracidad de las siguientes afirmaciones:

1. En $\mathbb{R}$ la ecuación $x^2 = a$ siempre tiene solución.
2. En $\mathbb{C}$ la ecuación $x^2 = a$ siempre tiene solución.
3. $(\mathbb{C}, +, \cdot)$ es un cuerpo.
4. $(\mathbb{C}, +, \cdot)$ es un anillo sin divisores del cero.
5. $\mathbb{R}$ es isomorfo a un conjunto R, $R \subseteq \mathbb{C}$.
6. $\mathbb{I}\mathrm{m}(z)$ es un número imaginario.
7. $\mathbb{R}\mathrm{e}(z) + \mathbb{I}\mathrm{m}(z) \in \mathbb{R}$.
8. $\mathbb{R}\mathrm{e}(z_1 + z_2) = \mathbb{R}\mathrm{e}(z_1) + \mathbb{R}\mathrm{e}(z_2)$.
9. $\mathbb{I}\mathrm{m}(z_1 + z_2) = \mathbb{I}\mathrm{m}(z_1) + \mathbb{I}\mathrm{m}(z_2)$.
10. Para todo complejo z se cumple que $\overline{z} + z \in \mathbb{R}$.
11. Para todo complejo z se cumple que $\overline{z} - z$ es imaginario puro.
12. Siempre se cumple que $\mathbb{R}\mathrm{e}(z) \leq |z|$ y que $\mathbb{I}\mathrm{m}(z) \leq |z|$.
13. Para todo complejo z se cumple que $z^{-1} = \overline{z}$.
14. Para todo par de complejos z_1, z_2 se cumple que $|z_1 + z_2| \leq |z_1| + |z_2|$.
15. Para todo complejo z, existen $a, b \in \mathbb{R}, a, b > 0$ tales que $z = a + ib$.
16. Para todo complejo z, existen $a, b \in \mathbb{R}$ tales que $z = a + ib$.
17. El complejo $z = 4 + 2i$ tiene módulo cero.
18. El complejo $e^{i\theta}$ está definido como $\cos\theta + i \operatorname{sen}\theta$.
19. El complejo $e^{i\theta}$ está definido como $\operatorname{sen}\theta - i\cos\theta$.
20. El complejo $e^{i\theta}$ está definido como $\operatorname{sen}\theta + \cos\theta$.
21. $e^{i0} = 0$.
22. $e^{i0} = 1$.
23. $e^{i0} = -1$.
24. Para cualquier $\theta \in \mathbb{R}$, $|e^{i\theta}| < 1$.
25. Para cualquier $\theta \in \mathbb{R}$, $|e^{i\theta}| > 1$.
26. Existe $\theta \in \mathbb{R}$ tal que $|e^{i\theta}| = 0$.
27. Para cualquier $\theta \in \mathbb{R}$, $|e^{i\theta}| = 1$.
28. Para cualquier $\theta \in \mathbb{R}$, $\overline{e^{i\theta}} = e^{i\theta}$.
29. Para cualquier $\theta \in \mathbb{R}$, $\overline{e^{i\theta}} = e^{i(-\theta)}$.
30. El inverso multiplicativo de $e^{i\theta}$ es su conjugado.
31. Para todo $\theta, \varphi \in \mathbb{R}$, $e^{i\theta}e^{i\varphi} = e^{i\theta\varphi}$.
32. Para todo $\theta, \varphi \in \mathbb{R}$, $e^{i\theta}e^{i\varphi} = e^{i(\theta+\varphi)}$.
33. Para todo $\theta, \varphi \in \mathbb{R}$, $e^{i\theta} + e^{i\varphi} = e^{i\theta\varphi}$.

34. Para todo $n \in \mathbb{Z}$ y $\theta \in \mathbb{R}$, $(e^{i\theta})^n = e^{i(\theta+n)}$.
35. Para todo $n \in \mathbb{Z}$ y $\theta \in \mathbb{R}$, $(e^{i\theta})^n = e^{i(n\theta)}$.
36. Para todo $n \in \mathbb{Z}$ y $\theta \in \mathbb{R}$, $(e^{i\theta})^n = ne^{i\theta}$.
37. Todo número complejo $z \in \mathbb{C}$, puede escribirse como $z = re^{i\theta}$, para ciertos $r \in [0, +\infty[$ y $\theta \in \mathbb{R}$.
38. Todo número complejo $z \in \mathbb{C}$, puede escribirse como $z = e^{i\theta}$, para cierto $\theta \in \mathbb{R}$.
39. Si $z = re^{i\theta}$, entonces $\arg(z) = i\theta$.
40. Si $z = re^{i\theta}$, entonces $\arg(z) = r$.
41. Si $z = re^{i\theta}$, entonces $\arg(z) = \theta$.
42. La ecuación $|z| = r$, con $z = re^{i\theta}$ no tiene solución en $\mathbb{C}$.
43. Todo $z = re^{i\theta} \in \mathbb{C}$, satisface $|z| = r$.
44. $z, w \in \mathbb{C} \setminus \{0\}$ son iguales si y sólo si $|z| = |w| \ \wedge \ (\exists k \in \mathbb{Z}, \ \arg(z) = \arg(w) + 2k\pi)$.
45. $z, w \in \mathbb{C} \setminus \{0\}$ son iguales si y sólo si $(\exists k \in \mathbb{Z}, \ |z| = |w| + 2k\pi) \ \wedge \ \arg(z) = \arg(w)$.
46. $2e^{i\frac{\pi}{2}} = 2e^{-i\frac{3\pi}{2}}$.
47. $2e^{i\frac{\pi}{2}} = 2e^{-i\frac{\pi}{2}}$.
48. $\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}$.
49. $|\overline{z_1 + z_2}| \geq |\overline{z_1}| + |\overline{z_2}|$.
50. $|\overline{z_1 + z_2}| \leq |\overline{z_1}| + |\overline{z_2}|$.
51. $\overline{z} + z = 2i \cdot \mathbb{I}\mathrm{m}(z)$.
52. $\overline{z} + z = 2\mathbb{R}\mathrm{e}(z)$.
53. $\overline{z} + z = -2\mathbb{R}\mathrm{e}(z)$.
54. $\overline{z} + z = -2\mathbb{I}\mathrm{m}(z)$.
55. $\overline{z} - z = -2\mathbb{R}\mathrm{e}(z)$.
56. $\overline{z} - z = -2i \cdot \mathbb{I}\mathrm{m}(z)$.
57. $\overline{z} - z = -2\mathbb{I}\mathrm{m}(z)$.
58. $\overline{z} - z = 2\mathbb{R}\mathrm{e}(z)$.
59. $\overline{z_1 z_2} = \overline{z_1 z_2}$.
60. $|\overline{z_1 z_2}| = |z_1 \overline{z_2}|$.
61. $|\overline{z_1 z_2}| > |\overline{z_1}||\overline{z_2}|$.
62. $z \in \mathbb{R} \iff z = \overline{z}$.
63. $|z|^2 > z\overline{z}$.
64. $|z| = z\overline{z}$.
65. $|z|^2 = z\overline{z}$.
66. $z \neq 0 \implies z^{-1} = \frac{\overline{z}}{|z|^2}$.
67. $i^{-1} = i$.
68. $i^{-1} = -i$.

69. Dados $z \in \mathbb{C}, n \geq 2$ tales que $z^n = 1$, decimos que 1 es raíz n-ésima de z.
70. Dados $z \in \mathbb{C}, n \geq 2$ tales que $z^n = 1$, decimos que z es raíz n-ésima de la unidad.
71. Existen infinitas raíces n-ésimas de la unidad distintas en $\mathbb{C}$.
72. Hay exactamente $n + 1$ raíces n-ésimas de la unidad en $\mathbb{C}$.
73. Hay exactamente n raíces n-ésimas de la unidad en $\mathbb{C}$.
74. El complejo $\sqrt{5}e^{i\frac{6\pi}{5}}$ es raíz quinta de la unidad.
75. El complejo $e^{i\frac{6\pi}{5}}$ es raíz quinta de la unidad.
76. El complejo $e^{i\frac{6\pi}{5}}$ es raíz sexta de la unidad.
77. Las raíces n-ésimas de un complejo $\rho e^{i\varphi} \neq 0$ son $e^{i\frac{\varphi+2r\pi}{n}}$, para $r \in [0..n-1]$.
78. Las raíces n-ésimas de un complejo $\rho e^{i\varphi} \neq 0$ son $\sqrt[n]{\rho}e^{i\frac{\varphi+2r\pi}{n}}$, para $r \in [0..n-1]$.
79. Las raíces n-ésimas de un complejo $\rho e^{i\varphi} \neq 0$ son $\rho e^{i\frac{\varphi+2r\pi}{n}}$, para $r \in [0..n-1]$.
80. Hay exactamente 2 raíces n-ésimas de un complejo cualquiera $w \neq 0$.
81. Hay exactamente $n + 1$ raíces n-ésimas de un complejo cualquiera $w \neq 0$.
82. Hay exactamente n raíces n-ésimas de un complejo cualquiera $w \neq 0$.
83. Dado $n \geq 2$, la suma de las n raíces n-ésimas de la unidad vale i.
84. Dado $n \geq 2$, la suma de las n raíces n-ésimas de la unidad vale 0.
85. Dado $n \geq 2$, la suma de las n raíces n-ésimas de la unidad vale 1.

Guía de Ejercicios

1. Demuestre, dados $z_1, z_2 \in \mathbb{C}$ y $\alpha \in \mathbb{R}$, las siguientes propiedades:

   a) $\mathbb{R}\text{e}(z_1 + z_2) = \mathbb{R}\text{e}(z_1) + \mathbb{R}\text{e}(z_2)$.
   b) $\mathbb{I}\text{m}(z_1 + z_2) = \mathbb{I}\text{m}(z_1) + \mathbb{I}\text{m}(z_2)$.
   c) $\mathbb{R}\text{e}(\alpha z) = \alpha\mathbb{R}\text{e}(z)$.
   d) $\mathbb{I}\text{m}(\alpha z) = \alpha\mathbb{I}\text{m}(z)$.
   e) $z_1 = z_2 \iff \mathbb{R}\text{e}(z_1) = \mathbb{R}\text{e}(z_2) \wedge \mathbb{I}\text{m}(z_1) = \mathbb{I}\text{m}(z_2)$.

2. Grafique en el plano complejo, escribiendo de forma cartesiana los siguientes números complejos:

   a) $1 + 2i$.
   b) $(1 + 2i)^2$.
   c) $(1 + 2i)(3 - 2i)$.
   d) $\dfrac{1+i}{2-i}$.
   e) $\overline{\left(\dfrac{\sqrt{3}}{2} + \dfrac{1}{2}i\right)\left(\dfrac{\sqrt{3}}{2} + \dfrac{1}{2}i\right)}$.

3. Encuentre la intersección de las siguientes regiones del plano complejo

$$R_1 = \{z \in \mathbb{C} \mid |z-1| \leq 1\} \qquad \text{y} \qquad R_2 = \{z \in \mathbb{C} \mid |z-2| \leq 1\}.$$

Indicación: Grafique.

4. Demuestre las siguientes propiedades:

a) $e^{i0} = 1$.
b) $\forall \theta \in \mathbb{R},\ |e^{i\theta}| = 1$.
c) $\forall \theta \in \mathbb{R},\ \overline{e^{i\theta}} = (e^{i\theta})^{-1} = e^{i(-\theta)}$.

5. Exprese en forma polar los siguientes complejos:

a) $1 + i\sqrt{2}$
b) $2 - i\sqrt{3}$
c) $2 - 2i$
d) $(1 - i\sqrt{5})(4 - i\sqrt{2})$
e) $(3 + i3)(-3 + i\sqrt{2})$
f) $(2 + i)(2 - i)$
g) $\dfrac{(1 - i\sqrt{5})}{(4 - i\sqrt{2})}$
h) $\dfrac{(3 + i3)}{(-3 + i\sqrt{2})}$
i) $\dfrac{(2 + i)}{(2 - i)}$

6. Exprese en forma $a + bi$ los siguientes complejos:

a) $e^{i\frac{\pi}{6}}$
b) $3e^{i\frac{\pi}{3}}$
c) $5e^{i\frac{\pi}{2}}$
d) $(-e^{i\frac{\pi}{4}})(2e^{i\frac{\pi}{6}})$
e) $(-5e^{i\frac{\pi}{2}})(-5e^{i\frac{\pi}{2}})$
f) $\dfrac{(-5e^{i\frac{\pi}{6}})}{(3e^{i\frac{\pi}{3}})}$
g) $\dfrac{(3e^{i\frac{\pi}{8}})}{(-4e^{i\frac{\pi}{4}})}$

7. Encuentre el conjunto solución de las siguientes ecuaciones en $\mathbb{C}$. Para ello, escriba $z = x + iy$ y resuelva. ¿A qué lugar geométrico en $\mathbb{R}^2$ corresponde cada conjunto?

a) $|\frac{i-z}{z+2}| = 1$
b) $|\frac{2-z}{z-1}| = 4$
c) $|\frac{z+3i}{z-3}| = 2$
d) $|\frac{1+z}{z+2-4i}| = 1$
e) $|\frac{2+z}{z-3-2i}| = 2$
f) $|\frac{4i-z}{z-1+i}| = 1$

8. Calcule las raíces de $z^2 = -i$ y expréselas de la forma $a + bi$.
9. Exprese en forma $a + bi$ las raíces cuartas de $z_0 = \frac{1+i\sqrt{3}}{1-i\sqrt{3}}$.
10. Resuelva las siguientes ecuaciones en z:

a) $z^3 = 1 + 2i$
b) $z^4 = 2 - i\sqrt{3}$
c) $z^5 = -3 + 3i$
d) $z^6 = 4 + i\sqrt{5}$
e) $z^{10} = -5 - i\sqrt{2}$
f) $z^4 = 16e^{i\frac{\pi}{2}}$
g) $z^3 = 8e^{i\frac{\pi}{3}}$
h) $z^6 = 5e^{i\frac{\pi}{6}}$
i) $z^7 = 5e^{i\frac{\pi}{8}}$

Guía de Problemas

1. a) (10 min.) Sea $z \in \mathbb{C}$ tal que $|z| = |z + 1| = 1$. Deduzca que z es una raíz cúbica de la unidad.

b) (20 min.) Sean $z_1, z_2 \in \mathbb{C}$. Probar que $|1-z_2\overline{z}_1|^2-|z_1-z_2|^2 = (1-|z_1|^2)(1-|z_2|^2)$.

c) (20 min.) Deduzca usando lo anterior que si $|z_1| < 1$ y $|z_2| < 1$, entonces se tiene $\left|\frac{z_1-z_2}{1-z_2\overline{z}_1}\right| < 1$.

2. (10 min.) Sea $z \in \mathbb{C}$ tal que $|z| \neq 1$ y considere $n \geq 1$. Probar que $\frac{1}{1+z^n} + \frac{1}{1+\overline{z}^n} \in \mathbb{R}$.

3. a) (20 min.) Demuestre que $\forall z_1, z_2 \in \mathbb{C}\ z_1 \cdot \overline{z_2} + \overline{z_1} \cdot z_2 = 2|z_1 \cdot z_2| \cos\phi$. donde ϕ es el ángulo entre los complejos z_1 y z_2

b) (20 min.) Sean s, u, v complejos que satisfacen la relación $s = u - v$. Sea ϕ el ángulo entre los complejos u y v. Demuestre que $|s|^2 = |u|^2 + |v|^2 - 2|u||v|\cos\phi$.

4. (20 min.) Se define la relación $\mathcal{R} \subseteq \mathbb{C} \times \mathbb{C}$ por $z_1 \mathcal{R} z_2 \iff |z_1| = |z_2|$. Demuestre que $\mathcal{R}$ es relación de equivalencia y determine y grafique la clase de equivalencia del complejo $z_0 = 2 + i\sqrt{5}$.

5. (15 min.) Sea $z \in \mathbb{C}$, entonces pruebe que $|z + i| = |z - i| \iff z \in \mathbb{R}$.

6. (15 min.) Expresar de la forma $a + bi$ los siguientes complejos $(1 - i)^4(1 + i)^4$ y $1 + i + (i - 1)/(|1 - i|^2 + i)$.

7. Considere los números reales $S = \sum_{k=0}^{n} \binom{n}{k} \cos(k \cdot \alpha)$ y $S' = \sum_{k=0}^{n} \binom{n}{k} \operatorname{sen}(k \cdot \alpha)$, donde $\alpha \in \mathbb{R}$.

a) (30 min.) Probar la igualdad de números complejos

$$S + iS' = (1 + \cos(\alpha) + i\operatorname{sen}(\alpha))^n.$$

b) (30 min.) Escriba el número complejo $1 + \cos(\alpha) + i\operatorname{sen}(\alpha)$ en forma polar y deduzca que

$$S = 2^n(\cos(\alpha/2))^n \cdot \cos(n \cdot \alpha/2) \text{ y } S' = 2^n(\cos(\alpha/2))^n \cdot \operatorname{sen}(n \cdot \alpha/2).$$

Indicación: Recuerde que $\operatorname{sen}(2\alpha) = 2\operatorname{sen}(\alpha)\cos(\alpha)$ y $\cos(2\alpha) = cos^2(\alpha) - \operatorname{sen}^2(\alpha)$.

8. (20 min.) Demostrar utilizando las propiedades de las raíces de la unidad que $\forall n \geq 2$

$$\cos\frac{2\pi}{n} + \cos\frac{4\pi}{n} + \cos\frac{6\pi}{n} + ... + \cos\frac{2(n-1)\pi}{n} = -1,$$
$$sen\frac{2\pi}{n} + \operatorname{sen}\frac{4\pi}{n} + \operatorname{sen}\frac{6\pi}{n} + ... + \operatorname{sen}\frac{2(n-1)\pi}{n} = 0.$$

9. Se define el grupo abeliano $S \subseteq \mathbb{C}$ por $S = \{z \in \mathbb{C} \mid |z| = 1\}$.

a) (10 min.) Demuestre que si z es raíz n-ésima de la unidad ($n \geq 2$) y n es divisor de m, entonces z es raíz m-ésima de la unidad.

b) (30 min.) Sea $U = \{z \in \mathbb{C} \mid \exists n \in \mathbb{N}, n \geq 2, z$ es raíz n-ésima de la unidad$\}$. Mostrar que $(U, \cdot)$ es subgrupo del grupo $(S, \cdot)$.

SEMANA 13:

Ingeniería Matemática
FACULTAD DE CIENCIAS
FÍSICAS Y MATEMÁTICAS
UNIVERSIDAD DE CHILE

Polinomios

11.1 Introducción

Un polinomio es una expresión que consiste en variables (también llamadas indeterminadas) y constantes (llamadas coeficientes), y que involucra operaciones de adición, multiplicación, y exponenciación a exponentes enteros. Por ejemplo un polinomio en la indeterminada x y a coeficientes enteros es $2x^3 - 4x + 6$.

Los polinomios aparecen de forma natural en muchas áreas. Por ejemplo, en ecuaciones polinomiales usadas para modelar una amplia gama de situaciones y para caracterizar soluciones estable u óptimas. También son usadas para modelar procesos y aproximar otras funciones.

Nosotros nos abocaremos al estudio de un caso especial de los polinomios. Específicamente aquellos cuyos coeficientes pertenecen a $\mathbb{R}$ ó $\mathbb{C}$, y que definimos a continuación.

Definición 11.1 (Polinomio) *Sea $(\mathbb{K}, +, \cdot)$ un cuerpo, $\mathbb{R}$ ó $\mathbb{C}$. Un **polinomio** es un tipo particular de función de $\mathbb{K}$ en $\mathbb{K}$, dado por*

$$\begin{aligned} P : \mathbb{K} &\to \mathbb{K} \\ x &\to P(x) = p_0 + p_1 x + p_2 x^2 + \ldots + p_n x^n = \sum_{k=0}^{n} p_k x^k. \end{aligned}$$

*donde $n \in \mathbb{N}$ y $p_0, p_1, p_2, \ldots, p_n$ son constantes en $\mathbb{K}$ y se denominan **coeficientes** del polinomio P. Al conjunto de todos los polinomios con coeficientes en $\mathbb{K}$ se le denota $\mathbb{K}[x]$.*

Denotaremos los polinomios por letras mayúsculas, usualmente $P, Q, R, S, T, ...$ y esporádicamente letras como $A, B, C, ...$

Si nos referimos a un polinomio por una letra, entonces denotaremos sus coeficientes por la misma letra pero en minúscula. Por ejemplo, si denotamos un polinomio por P, sus coeficientes serían $p_0, p_1, p_2, ...$

Como los polinomios en $\mathbb{K}[x]$ son funciones de $\mathbb{K}$ en $\mathbb{K}$, la noción natural de igualdad de polinomios es la de igualdad de funciones. Como los dominios y codominios de $P, Q \in \mathbb{K}[x]$

coinciden, sigue

$$P = Q \iff P(x) = Q(x) \text{ para todo } x \in K. \qquad \text{(Igualdad de polinomios)}$$

El siguiente resultado da una caracterización alternativa, en términos de coeficientes, de la igualdad de polinomios.

Proposición 11.2 *Sean* $P, Q \in \mathbb{K}[x]$ *tales que* $P(x) = \sum_{k=0}^{n} p_k x^k$ *y* $Q(x) = \sum_{k=0}^{m} q_k x^k$. *Se tiene que*

$$P = Q \iff (n = m \text{ y } \forall k \in [0..n],\ p_k = q_k).$$

Dem. Por Equivalencia dividida.

$\Leftarrow$) Ésta es directa, y queda de ejercicio para el lector.

$\Rightarrow$) Notemos que podemos suponer que $m = n$. En efecto, si $m < n$, entonces podemos escribir $Q(x) = q_0 + q_1 x + q_2 x^2 + \ldots + q_n x^n$ tomando $q_{m+1} = 0, q_{m+2} = 0, \ldots, q_n = 0$. Se procede de modo similar si $m > n$.

Debemos demostrar que para todo $k \in [0..n]$, $p_k = q_k$. Lo haremos siguiendo un argumento de tipo inductivo:

Caso base $k = 0$: Sabemos que los polinomios P y Q son iguales (como funciones), por lo que $P(0) = Q(0)$. Pero $P(0) = p_0$ y $Q(0) = q_0$, con lo que concluimos que $p_0 = q_0$.

Paso inductivo: Sea $k \in [1..n]$, y supongamos que $p_0 = q_0, p_1 = q_1, \ldots, p_{k-1} = q_{k-1}$. Debemos demostrar que $p_k = q_k$.

Como P y Q son iguales, entonces para cualquier $x \in \mathbb{K}$:

$$p_0 + p_1 x + p_2 x^2 + \ldots + p_n x^n = q_0 + q_1 x + q_2 x^2 + \ldots + q_n x^n.$$

Usando la hipótesis inductiva, podemos cancelar los primeros k términos a cada lado, y obtener

$$p_k x^k + \ldots + p_n x^n = q_k x^k + \ldots + q_n x^n.$$

Factorizando por x^k a ambos lados, obtenemos que

$$x^k(p_k + \ldots + p_n x^{n-k}) = x^k(q_k + \ldots + q_n x^{n-k}).$$

Así, para todo $x \in \mathbb{K} \setminus \{0\}$ podemos dividir por x^k y obtener

$$p_k + \ldots + p_n x^{n-k} = q_k + \ldots + q_n x^{n-k}.$$

Afirmamos que $p_k = q_k$. En efecto, supongamos que $p_k \neq q_k$ y que $x \in \mathbb{C}$, $x \neq 0$, es arbitrario pero tal que su módulo es muy pequeño, específicamente,

$$|x| < \text{mín}\left\{\frac{|p_k - q_k|}{2C}, \frac{1}{2}\right\}, \quad \text{donde } C = \max_{i \in [k+1..n]} |p_i - q_i|.$$

Tenemos entonces, por desigualdad triangular, definición de C, la fórmula para la suma de una progresión geométrica y porque $|x| \leq 1/2$, que

$$\big|p_k - q_k\big| = \big|(p_{k+1} - q_{k+1})x + ... + (p_n - q_n)x^{n-k}\big| \leq \sum_{i=k+1}^{n} \big|p_i - q_i\big||x|^{i-k}$$

$$\leq C \sum_{i=k+1}^{n} |x|^{i-k} = C|x| \sum_{j=0}^{n-k-1} |x|^j = C|x|\frac{1-|x|^{n-k}}{1-|x|} \leq 2C|x|.$$

Como $|x| < |p_k - q_k|/(2C)$, sigue que $|p_k - q_k| < |p_k - q_k|$, lo que es una contradicción evidente. Luego, se debe tener que $p_k = q_k$ y. Esto concluye la inducción y la demostración. □

A continuación introducimos un importante parámetro asociado a un polinomio.

Definición 11.3 (Grado de un polinomio) *Sea $P(x) = p_0 + p_1 x + \ldots + p_n x^n$ un polinomio. Diremos que es de **grado** n si $p_n \neq 0$, en cuyo caso notaremos $gr(P) = n$.*

*Si $P(x) = 0$ (el llamado **polinomio nulo**), diremos que es de grado $-\infty$, y lo notaremos por $gr(P) = -\infty$.*

Es decir, $gr(P)$ es el k más grande posible tal que p_k es no nulo.

Convención: Si P es un polinomio de grado n y nos referimos a p_m con $m > n$, siempre se entenderá que $p_m = 0$.

Observación: De la Proposición 11.2 y la definición de grado, sigue que si $P = Q$, entonces $\mathrm{gr}(P) = \mathrm{gr}(Q)$. □

Con respecto a $-\infty$ adoptamos las siguientes convenciones. Para todo $n \in \mathbb{N}$,

$$\begin{aligned} n &> -\infty, \\ n + (-\infty) &= -\infty, \\ (-\infty) + (-\infty) &= -\infty. \end{aligned}$$

Ejemplo:

- $\mathrm{gr}(1 + 5x + 18x^4) = 4$.
- $\mathrm{gr}(x + 3) = 1$.
- $\mathrm{gr}(37) = 0$.
- $\mathrm{gr}(0) = -\infty$.

♢

Observación: Los polinomios de grado 0 en $\mathbb{K}[x]$ son exactamente los polinomios constantes no nulos (que no dependen de x). Es decir, $\mathrm{gr}(P) = 0$ si y solo si $\exists p_0 \in \mathbb{K} \setminus \{0\}$ tal que $P(x) = p_0$ para todo $x \in \mathbb{K}$. □

Definición 11.4 (Polinomio mónico) *Sea $P \in \mathbb{K}[x]$, $P \neq 0$. Diremos que P es **mónico** si para $n = gr(P)$ se tiene que $p_n = 1$. Es decir, si el coeficiente asociado a la potencia de x más grande vale 1.*

Ejemplo: Son polinomios mónicos:

- $25 + 32x + x^3$
- $5 + x^2$
- $x^5 + 5x^2 - 25$

♢

11.2 Anillos de polinomios

Sean $P, Q \in \mathbb{K}[x]$ dos polinomios:

$$P(x) = \sum_{k=0}^{n} p_k x^k, \qquad Q(x) = \sum_{k=0}^{n} q_k x^k$$

(recordar que eventualmente hay que "rellenar" con ceros para que ambos polinomios tengan la misma cantidad de coeficientes)

Por lo visto sobre estructuras en conjuntos de funciones, las estructuras $(\mathbb{K}, +)$ y $(\mathbb{K}, \cdot)$ inducen operaciones en $\mathbb{K}^{\mathbb{K}}$, dando lugar a estructuras $(\mathbb{K}^{\mathbb{K}}, +)$ y $(\mathbb{K}^{\mathbb{K}}, \cdot)$. Específicamente, dados $f, g \in \mathbb{K}^{\mathbb{K}}$, se definen $f + g, f \cdot g \in \mathbb{K}$ de forma que para todo $x \in \mathbb{K}$ se cumpla que:

$$(f + g)(x) = f(x) + g(x),$$
$$(f \cdot g)(x) = f(x) \cdot g(x).$$

Se verifica fácilmente lo siguiente.

Proposición 11.5 *Si $(\mathbb{K}, +, \cdot)$ es cuerpo, entonces $(\mathbb{K}^{\mathbb{K}}, +)$ es grupo abeliano (donde el neutro es la función constante igual a 0), $(\mathbb{K}^{\mathbb{K}}, \cdot)$ es una estructura algebraica donde $\cdot$ es asociativa y conmutativa, admite neutro (la función constante igual a 1) y distribuye con respecto a $+$ en $\mathbb{K}^{\mathbb{K}}$.*

Como los polinomios en $\mathbb{K}[x]$ son funciones de $\mathbb{K}$ en $\mathbb{K}$, es natural definir su suma y multiplicación como la suma y multiplicación de las funciones en $\mathbb{K}^{\mathbb{K}}$ que dichos polinomios determinan. Los siguientes resultados proveen caracterizaciones alternativas de la suma y producto de polinomios pero en términos de los coeficientes de los mismos.

Proposición 11.6 *Si $P, Q \in \mathbb{K}[x]$ son tales que $gr(P) = n$ y $gr(Q) = m$, entonces (recordando que $p_k = 0$ si $k > gr(P)$, y $q_k = 0$ si $k > gr(Q)$)*

$$(P+Q)(x) = \sum_{k=0}^{\text{máx}\{n,m\}} (p_k + q_k)x^k.$$

En particular, $P + Q$ es un polinomio en $\mathbb{K}[x]$ tal que

$$gr(P+Q) \leq \text{máx}\{gr(P), gr(Q)\}.$$

Dem. La primera parte es consecuencia directa del hecho que por definición de $+$ en $\mathbb{K}[x]$, las convenciones adoptadas y propiedades de las sumatarias, se tiene que

$$(P+Q)(x) = \Big(\sum_{k=0}^{n} p_k x^k\Big) + \Big(\sum_{k=0}^{m} q_k x^k\Big) = \sum_{k=0}^{\text{máx}\{n,m\}} (p_k + q_k)x^k.$$

De la Proposición 11.2 sigue que el k-ésimo coeficiente del polinomio $P + Q$ es $p_k + q_k$.

La segunda parte es consecuencia de que para $k > \text{máx}\{n, m\}$, o $p_k = 0$ o $q_k = 0$. □

Es importante recalcar que en el caso de la adición de polinomios, sólo tenemos una desigualdad, y no una igualdad, en la fórmula que relaciona el grado de la suma y el grado de los sumandos. Un posible ejemplo es considerar $P(x) = 1 + 5x + 7x^2$ y $Q(x) = 2 + 8x - 7x^2$. Se tiene que $\text{gr}(P) = \text{gr}(Q) = 2$, pero $\text{gr}(P + Q) = \text{gr}(3 + 13x) = 1$.

Proposición 11.7 *Si $P, Q \in \mathbb{K}[x]$ son tales que $gr(P) = n$ y $gr(Q) = m$, entonces (recordando que $p_k = 0$ si $k > gr(P)$ y $q_k = 0$ si $k > gr(Q)$)*

$$(P \cdot Q)(x) = \sum_{k=0}^{n+m} \big(\sum_{i=0}^{k} p_i q_{k-i}\big)x^k = \sum_{k=0}^{n+m} \big(\sum_{j=0}^{k} p_{k-j} q_j\big)x^k = \sum_{k=0}^{n+m} \big(\sum_{\substack{0 \leq i \leq n, 0 \leq j \leq m \\ i+j=k}} p_i q_j\big)x^k.$$

En particular, $P \cdot Q$ es un polinomio en $\mathbb{K}[x]$ tal que

$$gr(P \cdot Q) = gr(P) + gr(Q).$$

Dem. Es análoga a la demostración de la Proposición 11.6 y queda como ejercicio. □

Aunque quizás no sea del todo evidente, la Proposición 11.7, nos sugiere una forma de multiplicar polinomios, a saber, considerar los polinomios $P(x)$ y $Q(x)$ como suma de polinomios de la forma $P_i(x) = p_i x^i$ y $Q_j(x) = q_j x^j$, expandir el producto usando distributividad y agrupar para cada exponenete k que aparezca aquellos términos $P_i(x)Q_j(x) = p_i q_j x^{i+j}$ para los que $i + j = k$. Proceder de esta manera resulta más cómodo que usar la fórmula de la Proposición 11.7.

Ejemplo: Si $P(x) = 1 - x + 3x^2$ y $Q(x) = x^2 - x^4$, entonces

$$\begin{aligned}(P \cdot Q)(x) &= 1(x^2 - x^4) - x(x^2 - x^4) + 3x^2(x^2 - x^4) \\ &= x^2 - x^4 - x^3 + x^5 + 3x^4 - 3x^6 \\ &= x^2 - x^3 + 2x^4 + x^5 - 3x^6.\end{aligned}$$

$\diamondsuit$

Observemos que las fórmula para calcular el grado de una suma y producto de polinomios también son válidas cuando alguno de los polinomios involucrados es el polinomio nulo. En efecto, si $P(x) = 0$, entonces $(P + Q)(x) = Q(x)$ y $(P \cdot Q)(x) = 0$, por lo que $\mathrm{gr}(P + Q) = \mathrm{gr}(Q)$ y $\mathrm{gr}(P \cdot Q) = -\infty$. Se observa entonces que las referidas fórmulas se satisfacen porque

$$\begin{aligned} \text{máx}\{\mathrm{gr}(P), \mathrm{gr}(Q)\} &= \text{máx}\{-\infty, \mathrm{gr}(Q)\} = \mathrm{gr}(Q), \\ \mathrm{gr}(P \cdot Q) &= \mathrm{gr}(P) + \mathrm{gr}(Q) = (-\infty) + \mathrm{gr}(Q) = -\infty. \end{aligned}$$

Proposición 11.8 $(\mathbb{K}[x], +, \cdot)$ *es un dominio de integridad.*

Dem. Verificaremos sólo algunas partes, las otras quedan como ejercicio.

La unidad de $(\mathbb{K}[x], +, \cdot)$ es el polinomio constante $P(x) = 1$. Observemos que los coeficientes de este polinomio son

$$p_k = \begin{cases} 1, & \text{si } k = 0, \\ 0, & \text{si } k \neq 0. \end{cases}$$

Así, si $Q(x) = q_0 + q_1 x + \ldots + q_n x^n \in \mathbb{K}[x]$ es de grado n,

$$(P \cdot Q)(x) = \Big(\sum_{k=0}^{n} q_k x^k\Big)\Big(\sum_{k=0}^{n} p_k x^k\Big) = \Big(\sum_{k=0}^{n} q_k x^k\Big) \cdot 1. = \sum_{k=0}^{n} q_k x^k.$$

Verfiquemos ahora que $(\mathbb{K}[x], +, \cdot)$ no posee divisores de cero. En efecto, si $P, Q \in \mathbb{K}[x]$ son tales que $P \cdot Q = 0$, entonces

$$\mathrm{gr}(P) + \mathrm{gr}(Q) = \mathrm{gr}(P \cdot Q) = \mathrm{gr}(0) = -\infty.$$

Dadas convenciones aritméticas concernientes a $-\infty$ que definimos, al menos uno de los dos grados que aparecen en la fórmula debe valer $-\infty$. Es decir, al menos uno de los dos polinomios debe ser igual a cero. $\square$

Veremos que $(\mathbb{K}[x], +, \cdot)$ es un ejemplo de dominio de integridad, sin embargo, **no es cuerpo**.

Proposición 11.9 *En* $(\mathbb{K}[x], +, \cdot)$*, los únicos polinomios que poseen inverso son los constantes no nulos, es decir los polinomios de grado* 0*.*

Dem. Sea $P \in \mathbb{K}[x]$ de grado 0. Entonces $P(x) = p_0$ con $p_0 \neq 0$. Es fácil ver que P posee inverso, el cual es el polinomio $Q(x) = p_0^{-1}$ (notar que también es de grado 0).

Sea ahora $P \in \mathbb{K}[x]$ tal que posee un inverso $Q \in \mathbb{K}[x]$. Entonces $P \cdot Q = 1$, con lo que

$$\mathrm{gr}(P) + \mathrm{gr}(Q) = \mathrm{gr}(P \cdot Q) = \mathrm{gr}(1) = 0.$$

Como el grado de un polinomio es siempre positivo (con la excepción de que valga $-\infty$), debe tenerse en particular que $\mathrm{gr}(P) = 0$. $\square$

Guía Básica

Observación: En esta guía, $\mathbb{K}$ representa al cuerpo $\mathbb{R}$ ó $\mathbb{C}$.

Determinar la veracidad de las siguientes afirmaciones:

1. Dos polinomios son iguales si y sólo si sus coeficientes son iguales.
2. Dos polinomios son iguales si y sólo si tienen al menos un coeficiente en común.
3. Si dos polinomios tienen un coeficiente distinto, entonces no son iguales.
4. El grado de un polinomio P, es el k más grande tal que el coeficiente p_k de P es no nulo.
5. El grado de un polinomio P, es el k más pequeño tal que el coeficiente p_k de P es nulo.
6. Si dos polinomios tienen grados distintos pueden ser iguales.
7. Si dos polinomios son iguales, entonces tienen el mismo grado.
8. El grado de cualquier polinomio constante es 0.
9. El grado de cualquier polinomio constante y no nulo es 0.
10. El grado del polinomio nulo es $-\infty$.
11. El polinomio $P(x) = 1 + x + x^2 + x^6$ es mónico.
12. El polinomio $P(x) = 1 + x + 2x^2 + x^6$ no es mónico.
13. El polinomio $P(x) = 1 + x + 2x^2 + x^6$ es mónico.
14. Si $P(x) = \sum_{k=0}^{n} p_k x^k$ y $Q(x) = \sum_{k=0}^{n} q_k x^k$, entonces $(P+Q)(x) = \sum_{k=0}^{n} p_k q_k x^k$.
15. Si $P(x) = \sum_{k=0}^{n} p_k x^k$ y $Q(x) = \sum_{k=0}^{n} q_k x^k$, entonces $(P+Q)(x) = \sum_{k=0}^{n} (p_k + q_k) x^k$.
16. Si $P(x) = \sum_{k=0}^{n} p_k x^k$ y $Q(x) = \sum_{k=0}^{n} q_k x^k$, entonces $(P \cdot Q)(x) = \sum_{k=0}^{n} p_k q_k x^k$.
17. Si $P(x) = \sum_{k=0}^{n} p_k x^k$ y $Q(x) = \sum_{k=0}^{n} q_k x^k$, entonces el k-ésimo coeficiente de $(P \cdot Q)(x)$ es $\sum_{i=0}^{k} p_i q_i$.
18. Si $P(x) = \sum_{k=0}^{n} p_k x^k$ y $Q(x) = \sum_{k=0}^{n} q_k x^k$, entonces el k-ésimo coeficiente de $(P \cdot Q)(x)$ es $\sum_{i=0}^{k} p_i q_{k-i}$.
19. Al sumar dos polinomios, el grado del polinomio resultante es menor o igual al grado de alguno de los polinomios originales.
20. Al sumar dos polinomios, el grado del polinomio resultante es siempre menor al grado de ambos polinomios originales.
21. Al sumar dos polinomios, el grado del polinomio resultante es siempre igual al grado de alguno de los polinomios originales.
22. Existen pares de polinomios que al ser multiplicados generan un polinomio de grado estrictamente menor que los suyos.
23. Dado un polinomio no nulo $P(x)$, el grado del polinomio $(P(x))^2$ es siempre par.
24. Dado un polinomio no nulo $P(x)$, el grado del polinomio $(P(x))^2$ es siempre impar.

25. $(\mathbb{K}[x], +, \cdot)$ es un anillo conmutativo con unidad.
26. La unidad en $(\mathbb{K}[x], +, \cdot)$ es el polinomio nulo.
27. La unidad en $(\mathbb{K}[x], +, \cdot)$ tiene grado 0.
28. $(\mathbb{K}[x], +, \cdot)$ no es cuerpo.
29. $(\mathbb{K}[x], +, \cdot)$ no es cuerpo, pues posee divisores de cero.
30. En $(\mathbb{K}[x], +, \cdot)$, todo elemento tiene inverso (para $\cdot$).
31. En $(\mathbb{K}[x], +, \cdot)$, todo elemento con grado menor o igual a 0 tiene inverso (para $\cdot$).
32. En $(\mathbb{K}[x], +, \cdot)$, todo elemento con grado igual a 0 tiene inverso (para $\cdot$).

Guía de Ejercicios

1. Estudie si se tiene o no la igualdad entre los siguientes polinomios:

   a) $P(x) = x^4+2x^3+3x^2+4x+5$ y $Q(x) = -4(x^4-1)-2(x^3-x)-(x^2-x)+4x+5$.
   b) $P(x) = x^4 - x^3 + x^2 - x + 1$ y $Q(x) = (x^4 - 1) - (x^3 - x) + (x^2 - x) - x + 1$.
   c) $P(x) = 4x^4-2x^3+2x^2-2x+1$ y $Q(x) = 3(x^4-1)+0\cdot(x^3-x)+4(x^2-x)-2x+1$.
   d) $P(x) = x^4 + x^3 + x^2 + x + 1$ y $Q(x) = (x^4 - 1) + (x^3 - x) + (x^2 - x) + x + 2$.
   e) $P(x) = 2x^4 - x^3 + 5x^2 + 4x + 3$ y $Q(x) = 2(x^4 - 1) - (x^3 - x) + 3(x^2 - x) + 4x + 3$.

2. Determine un caso en el que, dados dos polinomios $P, Q \in \mathbb{K}[x]$, se tenga que $\text{gr}(P + Q) < \text{máx}\{\text{gr}(P), \text{gr}(Q)\}$. ¿Por qué nunca sucede que $\text{gr}(P \cdot Q) < \text{gr}(P) + \text{gr}(Q)$?
3. Determine la relación entre el grado del polinomio $P \triangle Q$ y los grados de P y Q, en los siguientes casos:

   a) $\triangle = +$.
   b) $\triangle = -$.
   c) $\triangle = \cdot$.
   d) En cada caso anterior, pero considerando que los grados de P y Q son iguales.

Guía de Problemas

1. (30 min.) Dado un polinomio $P(x) = \sum_{k=0}^{n} p_k x^k$ se define $L(P)(x) = \displaystyle\sum_{k=1}^{n} k p_k x^{k-1}$.

   a) Determine el grado de $L(P)(x)$.
   b) Demuestre que si $P(x)$, $Q(x)$ son polinomios de grado n y m respectivamente, entonces $L(P \cdot Q) = L(P) \cdot Q + P \cdot L(Q)$.
   c) Pruebe por inducción sobre n, que si $P(x) = (x - d)^n$, entonces $L(P)(x) = n \cdot (x - d)^{n-1}$.

SEMANA 14:

Polinomios

Ingeniería Matemática
FACULTAD DE CIENCIAS
FÍSICAS Y MATEMÁTICAS
UNIVERSIDAD DE CHILE

11.3 Raíces y factorización

Al ser $(\mathbb{K}[x], +, \cdot)$ un anillo, ocurre un fenómeno similar al de $\mathbb{Z}$: Las divisiones deben considerar un posible resto.

Teorema 11.10 (Teorema de la División) *Sean $P, D \in \mathbb{K}[x]$ con $D \neq 0$. Entonces existe un único par $Q, R \in \mathbb{K}[x]$ tal que*

(I) $P = Q \cdot D + R$.

(II) $gr(R) < gr(D)$.

Observación:

- La ecuación (I), se llama **división con resto de P por D**.
- El polinomio Q se llama **cuociente**.
- El polinomio R se llama **resto**.
- Cuando $R = 0$, diremos que D **divide a** P, lo cual notaremos $D \mid P$, al igual que en $\mathbb{N} \setminus \{0\}$. Es decir,

$$D \mid P \iff (\exists Q \in \mathbb{K}[x],\ P = Q \cdot D).$$

□

Para probar el Teorema de la División, usaremos un método de división similar al que conocemos en $\mathbb{Z}$ y que ejemplificaremos a continuación:

Ejemplo: Calculemos la división de $P(x) = 3x^3 + 2x - 2$ por $Q(x) = x - 4$.

$$3x^3{+}2x{-}2 : x{-}4 =$$

Para obtener el cuociente, debemos preguntarnos por qué multiplicar el término de mayor exponente de $x - 4$ para obtener el término de mayor exponente de $3x^3 + 2x - 2$. Es decir, por qué multiplicar x para obtener $3x^3$. La respuesta es $3x^2$. Entonces

$$\begin{array}{l} 3x^3 \quad +2x \quad -2 \ : \ x \ -4 = 3x^2 \\ -(3x^3{-}12x^2) \\ \qquad\quad 12x^2 \ +2x \quad -2 \end{array}$$

El término $3x^3 - 12x^2$ corresponde a la multiplicación de $3x^2$ por el divisor $x-4$, y aparece restándose para calcular el resto parcial correspondiente. El polinomio $12x^2 + 2x - 2$ es el resultado de calcular la resta entre el polinomio original y el término recién obtenido.

El proceso continúa iterativamente: x debe ser multiplicado por $12x$ para obtener $12x^2$, así que sumamos $12x$ al cuociente parcial $3x^2$ que llevábamos.

$$\begin{array}{rl} 3x^3 \quad +2x \quad -2 & : \; x-4 = 3x^2+12x \\ -(3x^3-12x^2) & \\ \quad 12x^2 \quad +2x \; -2 & \\ \quad -(12x^2-48x) & \\ \quad\quad 50x \; -2 & \end{array}$$

En cada etapa vamos calculando un nuevo resto parcial, y detenemos el proceso cuando este resto tiene grado menor que el de $x - 4$:

$$\begin{array}{rl} 3x^3 \quad +2x \quad -2 & : \quad x-4 = 3x^2+12x+50 \\ -(3x^3-12x^2) & \\ \quad 12x^2 \quad +2x \quad -2 & \\ \quad -(12x^2-48x) & \\ \quad\quad 50x \quad -2 & \\ \quad\quad -(50x-200) & \\ \quad\quad\quad 198 & \end{array}$$

Obtenemos así que el cuociente de esta división es $Q(x) = 3x^2 + 12x + 50$, y el resto es $R(x) = 198$. En términos del Teorema de la División, podemos entonces escribir

$$3x^3 + 2x - 2 = (x - 4)(3x^2 + 12x + 50) + 198.$$

$\diamondsuit$

Dem. (Teorema de la División): Primero probaremos la **existencia** de Q y R aplicando inducción en $\text{gr}(P) \geq \text{gr}(D) - 1$.

El caso base $\text{gr}(P) = 0$ es inmediato cuando $\text{gr}(D) \geq 1$, pues basta tomar $R = P$ y $Q = 0$.

Cuando $\text{gr}(D) = 0$ tenemos que $d_0 \neq 0$ y podemos definir Q con $q_0 = p_0/d_0$, $R = 0$ y con esto escribir $P = QD + R$ con $\text{gr}(R) < \text{gr}(D)$.

Para verificar el paso inductivo supongamos que el resultado es cierto para polinomios con grado menor que n y consideremos que $\text{gr}(P) = n$.

Si $n \leq \text{gr}(D) - 1$, entonces basta notar que $P = 0 \cdot D + P$. De donde $Q = 0$ y $R = P$, satisfacen las condiciones del enunciado.

Cuando $n \geq \text{gr}(D)$, del procedimiento de división ejemplificado anteriormente, si $m = \text{gr}(D)$, entonces $P'(x) = P(x) - \frac{p_n}{d_m} D(x) x^{n-m}$ es tal que su n-ésimo coeficiente es $p_n -$

$\frac{p_n}{d_m} d_m = 0$. Luego, P' es de grado menor que n. Por hipótesis inductiva aplicada a P', obtenemos que existen $Q', R' \in \mathbb{K}[x]$, $\text{gr}(R') < \text{gr}(D)$ tales que $P' = Q' \cdot D + R'$. Reemplazando por la definición de P' y despejando,

$$P(x) = P'(x) + \frac{p_n}{d_m} D(x) x^{n-m} = \underbrace{\left(Q'(x) + \frac{p_n}{d_m} x^{n-m} \right)}_{Q(x)} \cdot D(x) + \underbrace{R'(x)}_{R(x)} = (Q \cdot D + R)(x).$$

Los polinomios Q y R satisfacen las condiciones del enunciado.

Resta ahora probar la unicidad de dichos polinomios. Supongamos que tenemos dos descomposiciones (y probemos que son la misma):

$$P = Q_1 \cdot D + R_1 = Q_2 \cdot D + R_2.$$

En donde $\text{gr}(R_1) < \text{gr}(D)$ y $\text{gr}(R_2) < \text{gr}(D)$. Reagrupando, obtenemos $(Q_1 - Q_2) \cdot D = R_2 - R_1$. Pero, como $\text{gr}(R_2 - R_1) \leq \text{máx}(\text{gr}(R_2), \text{gr}(R_1)) < \text{gr}(D)$, entonces

$$\text{gr}(D) > \text{gr}(R_2 - R_1) = \text{gr}((Q_1 - Q_2) \cdot D) = \text{gr}(Q_1 - Q_2) + \text{gr}(D),$$

lo cual sólo puede ocurrir si $\text{gr}(Q_1 - Q_2) = -\infty$, o sea, $Q_1 - Q_2 = 0$. Como consecuencia, $R_2 - R_1 = 0 \cdot D = 0$. Concluimos entonces que $Q_1 = Q_2$ y $R_1 = R_2$. □

Teorema 11.11 (Teorema del Resto) *Sean $P \in \mathbb{K}[x]$ y $c \in \mathbb{K}$. El resto de dividir P por el polinomio $(x - c)$ es exactamente $P(c)$.*

Dem. Por el Teorema de la División, existen únicos $Q, R \in \mathbb{K}[x]$ con $\text{gr}(R) < 1$ tales que

$$P(x) = Q(x)(x - c) + R(x).$$

Como $\text{gr}(R) < 1$, existe $r_0 \in \mathbb{K}$ tal que $R(x) = r_0$. Evaluando la relación de división antes obtenida en $x = c$, obtenemos

$$P(c) = Q(c) \cdot 0 + r_0$$

por lo que el resto vale $r_0 = P(c)$. □

Definición 11.12 (Raíz) *Diremos que $c \in \mathbb{K}$ es una **raíz** del polinomio $P \in \mathbb{K}[x]$ si $P(c) = 0$.*

Proposición 11.13 *$c \in \mathbb{K}$ es raíz de $P \iff (x - c) \mid P(x)$.*

Dem.

$\Rightarrow$) Sabemos que $P(c)$ es el resto de dividir P por $(x - c)$, es decir existe $Q \in \mathbb{K}[x]$ tal que

$$P(x) = Q(x)(x - c) + P(c).$$

Como c es raíz de P, se tiene que $P(c) = 0$, y así $P(x) = Q(x)(x-c)$ con lo que $(x-c) \mid P(x)$.

$\Leftarrow$) Si $(x - c) \mid P(x)$, entonces existe $Q \in \mathbb{K}[x]$ tal que $P(x) = Q(x)(x - c)$. Luego, $P(c) = Q(c) \cdot 0 = 0$ y por lo tanto c es raíz de P. □

Se tienen las siguientes propiedades:

Proposición 11.14

(I) *Si $c_1, c_2, \ldots, c_k$ son raíces distintas de P, entonces $(x-c_1)(x-c_2)\cdots(x-c_k) \mid P(x)$.*

(II) *Si $P \in \mathbb{K}[x]$ es tal que $gr(P) = n \geq 1$, entonces P posee a lo más n raíces distintas.*

(III) *Sean $n \geq 0$, y $P, Q \in \mathbb{K}[x]$ tales que $gr(P) \leq n$ y $gr(Q) \leq n$. Si P y Q coinciden en $n+1$ puntos distintos, entonces son iguales (como polinomios).*

Dem. Demostraremos (I) y (II). La parte (III) se obtiene como consecuencia de (II), aplicándola al polinomio $(P - Q)$.

Para (I): Por inducción en k. El caso $k = 1$ corresponde a la Proposición 11.13.

Supongamos que $k > 1$. Sean $c_1, c_2, \ldots, c_k$ raíces distintas de P. Por hipótesis inductiva,

$$(x-c_1)(x-c_2)\ldots(x-c_{k-1}) \mid P(x)$$

o, equivalentemente, existe $Q \in \mathbb{K}[x]$ tal que $P(x) = Q(x)(x-c_1)(x-c_2)\cdots(x-c_{k-1})$.

Como c_k también es raíz de P, obtenemos que $0 = P(c_k) = Q(c_k)(c_k-c_1)(c_k-c_2)\cdots(c_k - c_{k-1})$. Gracias a que los valores c_i son todos distintos, y que estamos trabajando en un cuerpo por lo que todos los elementos no nulos son cancelables, sigue que $Q(c_k) = 0$, y concluimos que c_k es raíz del polinomio Q. Así, $(x - c_k) \mid Q(x)$, y existe $Q' \in \mathbb{K}[x]$ tal que $Q(x) = Q'(x)(x - c_k)$. Reemplazando esto en la descomposición de P, nos queda

$$P(x) = Q'(x)(x-c_1)(x-c_2)\cdots(x-c_k).$$

Es decir, $(x-c_1)(x-c_2)\cdots(x-c_k) \mid P(x)$.

Para (II): Sea k el número de raíces distintas que posee P, y sean $c_1, \ldots, c_k$ estas raíces. Aplicando Teorema de la División, tenemos que existe $Q \in \mathbb{K}[x]$ tal que $P(x) = Q(x)(x - c_1)\cdots(x - c_k)$. Luego,

$$n = \mathrm{gr}(P) = \mathrm{gr}(Q) + \mathrm{gr}(x-c_1) + \ldots + \mathrm{gr}(x-c_k)$$

de donde obtenemos que $n = \mathrm{gr}(Q) + k$ pues $\mathrm{gr}(x - c_i) = 1$ para $i \in [1..k]$.

Como $\mathrm{gr}(P) = n \geq 1$, entonces P no puede ser el polinomio nulo. Así, Q tampoco puede ser el polinomio nulo (razonar por contradicción), y por lo tanto $\mathrm{gr}(Q) \geq 0$. Luego, $k = n - \mathrm{gr}(Q) \leq n - 0 = n$. Es decir, P posee a lo más n raíces distintas. □

Teorema Fundamental del Álgebra

En la sección anterior vimos un resultado que dice que un polinomio de grado n posee a lo más n raíces distintas, pero deja la posibilidad abierta de que pudiera no tener raíces.

Cuando consideramos raíces en $\mathbb{R}$, el caso puede darse. Tan sólo consideremos $P(x) = 1+x^2$. Las raíces de este polinomio son i y $-i$, sin embargo éstas no son reales, sino complejas. El polinomio P no posee raíces en $\mathbb{R}$.

El Teorema Fundamental del Álgebra da una versión general de este caso, generalizando además el resultado de la sección anterior.

Teorema 11.15 (Teorema Fundamental del Álgebra (TFA)) *Si $P \in \mathbb{C}[x]$ es tal que $gr(P) = n \geq 1$, entonces P posee al menos una raíz en $\mathbb{C}$.*

No demostraremos rigurosamente este teorema, ya que para eso requerimos herramientas más avanzadas. Sin embargo, al final de este apunte esbozaremos un argumento que en parte explica porque debiese ser cierto el TFA. Antes, estudiaremos algunas aplicaciones y consecuencias del citado teorema.

Factorización en $\mathbb{C}$

Proposición 11.16 *Si $P \in \mathbb{C}[x]$ es tal que $gr(P) = n \geq 1$, entonces existen valores $\alpha, c_1, \ldots, c_m \in \mathbb{C}$ y naturales $l_1, \ldots, l_m \geq 1$ tales que $gr(P) = l_1 + \ldots + l_m$ y*

$$P(x) = \alpha(x - c_1)^{l_1} \ldots (x - c_m)^{l_m}$$

donde $\alpha = p_n$.

Dem. Como $\mathrm{gr}(P) \geq 1$, utilizamos el TFA para encontrar $r_1 \in \mathbb{C}$ que es raíz de P. Entonces, para algún $Q_1 \in \mathbb{C}[x]$, se tiene que

$$P(x) = Q_1(x)(x - r_1).$$

El grado de Q_1 es $\mathrm{gr}(Q_1) = \mathrm{gr}(P) - \mathrm{gr}(x - r_1) = n - 1$. Si $n - 1 \geq 1$, entonces podemos seguir aplicando el TFA, esta vez a Q_1. Así, existe una raíz $r_2 \in \mathbb{C}$ de Q_1, por lo que debe existir un $Q_2 \in \mathbb{C}[x]$ tal que

$$P(x) = Q_2(x)(x - r_1)(x - r_2).$$

Si continuamos iterando este proceso mientras $\mathrm{gr}(Q_i) \geq 1$, llegamos a una descomposición

$$P(x) = Q_n(x)(x - r_1)(x - r_2) \ldots (x - r_n)$$

donde $r_1, \ldots, r_n \in \mathbb{C}$ y $Q_n \in \mathbb{C}[x]$ es de grado 0. Por lo tanto, $Q_n(x) = \alpha$ donde α es un valor fijo en $\mathbb{C}$.

Para terminar de escribir la descomposición deseada, notamos que los valores r_i no necesariamente son distintos, así que los agrupamos de modo que el valor $c_i \in \mathbb{C}$ aparece l_i veces. Así $P(x) = \alpha(x - c_1)^{l_1} \cdots (x - c_m)^{l_m}$.

Queda como ejercicio para el lector demostrar que el complejo α que aparece en la descomposición de P es exactamente su coeficiente p_n. □

A continuación, veremos propiedades de las raíces complejas de polinomios a coeficientes reales.

Proposición 11.17 *Sea $P \in \mathbb{C}[x]$ tal que todos sus coeficientes estan en $\mathbb{R}$. Si $z \in \mathbb{C}$ es una raíz de P, entonces el conjugado $\overline{z}$ también es raíz de P.*

Dem. Sea $P(x) = \sum_{k=0}^{n} p_k x^k$ donde $p_k \in \mathbb{R}$ para $k = 0, \ldots, n$. Luego, $P(\overline{z}) = \sum_{k=0}^{n} p_k (\overline{z})^k$.

Observemos que, como $p_k \in \mathbb{R}$, entonces $p_k = \overline{p_k}$, y así, para todo $k \in [0..n]$, se tiene que $p_k(\overline{z})^k = \overline{p_k z^k}$. Luego,

$$P(\overline{z}) = \sum_{k=0}^{n} \overline{p_k z^k} = \overline{\sum_{k=0}^{n} p_k z^k} = \overline{P(z)}.$$

Como z es raíz de P, entonces $P(z) = 0$, y así $P(\overline{z}) = \overline{0} = 0$, con lo que $\overline{z}$ también es raíz de P. □

Factorización en $\mathbb{R}$

Proposición 11.18 *Si $P \in \mathbb{R}[x]$ es tal que $gr(P) = n \geq 1$, entonces existen valores $\alpha, c_1, \ldots, c_m, p_1, q_1, p_2, q_2 \ldots p_s, q_s \in \mathbb{R}$ tales que*

$$P(x) = \alpha(x - c_1)(x - c_2)\cdots(x - c_m)(x^2 + p_1 x + q_1)(x^2 + p_2 x + q_2)\cdots(x^2 + p_s x + q_s).$$

En donde $c_1, \ldots, c_m$ son las raíces reales de P, los polinomios $x^2 + p_1 x + q_1, \ldots, x^2 + p_s x + q_s$ (con posible repetición) no tienen raíces reales y α es el coeficiente p_n de P.

Dem. La demostración se basa en la existencia de la descomposición garantizada por la Proposición 11.16, salvo que consideramos primero todas las raíces reales de P (posiblemente repetidas), obteniendo:

$$P(x) = (x - c_1)(x - c_2)\ldots(x - c_m)Q(x).$$

Luego, por cada raíz compleja $z \in \mathbb{C}\setminus\mathbb{R}$ de P, por la Proposición 11.17 y dado que $P \in \mathbb{R}[x]$, sabemos que $\overline{z}$ es también raíz de P. (Notar que $z \neq \overline{z}$ porque z no es real.)

Así, $(x - z)$ y $(x - \overline{z})$ dividen a P. Luego, de la parte (I) de la Proposición 11.14, se tiene que $(x - z)(x - \overline{z})|P$. Pero, como $z + \overline{z} = 2\mathbb{R}\mathrm{e}(z) \in \mathbb{R}$ y $z \cdot \overline{z} = |z|^2 \in \mathbb{R}$,

$$(x - z)(x - \overline{z}) = x^2 - (z + \overline{z})x + z\overline{z} = x^2 - 2\mathbb{R}\mathrm{e}(z) \cdot x + |z|^2 \in \mathbb{R}[x].$$

Repitiendo el argumento para las otras raíces en $\mathbb{C} \setminus \mathbb{R}$ de Q obtenemos la descomposición buscada. □

Polinomios a coeficientes enteros

Proposición 11.19 *Sea $P \in \mathbb{R}[x]$. Si $\frac{r}{s} \in \mathbb{Q}$ (r y s primos relativos) es una raíz de P y $p_0, \ldots, p_n \in \mathbb{Z}$, entonces $r|p_0$ y $s|p_n$.*

Dem. Como $\frac{r}{s}$ es raíz de P,

$$\begin{aligned} P\left(\tfrac{r}{s}\right) &= p_n\left(\tfrac{r}{s}\right)^n + p_{n-1}\left(\tfrac{r}{s}\right)^{n-1} + \cdots + p_1\left(\tfrac{r}{s}\right) + p_0 = 0, \\ &\iff r\left(p_n r^{n-1} + p_{n-1} s r^{n-2} + \cdots + s^{n-1} p_1\right) = -p_0 s^n. \end{aligned}$$

De aquí, r divide a $-p_0 s^n$. Sin embargo, como r y s son primos relativos, r y s^n también lo son. Luego, necesariamente $r|p_0$. Queda propuesto como ejercicio probar que $s|p_n$. □

El siguiente corolario es útil para explorar cuáles son las raíces enteras de un polinomio mónico con coeficientes enteros.

Corolario 11.20 *Si $P \in \mathbb{R}[x]$ es mónico, con coeficientes $p_0, \ldots, p_{n-1} \in \mathbb{Z}$, entonces toda raíz racional de P es entera y divide a p_0.*

Ejemplo: Consideremos el polinomio (mónico y con coeficientes enteros) $P(x) = x^3 + 6x^2 - 3x - 4$. Gracias al resultado anterior, sabemos que toda raíz $x \in \mathbb{Q}$ de P, debe ser un entero y ser divisor de $p_0 = 4$. Luego, si $x \in \mathbb{Q}$ es raíz de P, entonces $x \in \{\pm 1, \pm 2, \pm 4\}$. Podríamos evaluar P en $x = 1{,}534$ para ver si es raíz. ¿Pero para qué? Lo anterior nos dice que eso sería tiempo perdido. ♢

11.4 Esbozo de demostración del TFA

De acuerdo a lo comprometido, en esta sección daremos una justificación informal, pero ojalá convincente, de porqué se cumple el Teorema Fundamental del Álgebra. El teorema nos dice que si P es un polinomio a coeficientes complejos, es decir $P \in \mathbb{C}[x]$, cuyo grado es positivo, entonces P admite al menos una raíz en $\mathbb{C}$.

El argumento que discutiremos es de tipo geométrico. Específicamente, se basa en el estudio de ciertas curvas (en el plano complejo) asociadas al polinomio P, y que definimos a continuación. Sea $\rho \in \mathbb{R}$, $\rho > 0$ y $\mathcal{P}_\rho : [0, 2\pi] \to \mathbb{C}$ la función definida por $\mathcal{P}_\rho(\theta) = P(\rho e^{i\theta})$. Observar que $\mathcal{P}_\rho(\theta)$, a medida que θ toma valores entre 0 y 2π, describe una curva en el plano complejo. De hecho, la curva es cerrada, puesto que $\mathcal{P}_\rho(0) = P(\rho) = \mathcal{P}_\rho(2\pi)$. El conjunto de puntos de la curva los denotaremos, abusando notación, por $\mathcal{P}_\rho = \{\mathcal{P}_\rho(\theta) \mid \theta \in [0, 2\pi]\} \subseteq \mathbb{C}$. Claramente, las siguientes afirmaciones son equivalentes:

(I) El polinomio P admite una raíz en $\mathbb{C}$.

(II) Existen $\rho_* \geq 0$ y $\theta_* \in [0, 2\pi]$ tales que $\mathcal{P}_{\rho_*}(\theta_*) = 0$.

(III) Existe $\rho_* \geq 0$ tal que el origen O del plano complejo pertenece a $\mathcal{P}_{\rho_*}$.

Concretamente, consideremos un polinomio particular, específicamente

$$P(z) = z^3 + \tfrac{1}{2}z^2 + iz + 3e^{i\pi/4}.$$

Observemos que si z es tal que $|z|$ es "muy pequeño", digamos "casi" igual a 0, entonces es de esperar que los términos z^3, $\frac{1}{2}z^2$ e iz de $P(z)$ sean en módulo "mucho menores"

que $3e^{i\pi/4}$, o sea, es de esperar que $P(z)$ sea "casi" igual a $3e^{i\pi/4}$. De hecho, notar que si $|z| \leq 1$, por desigualdad triangular y dado que $|i| = 1$,

$$\left|P(z) - 3e^{i\pi/4}\right| = |z^3 + \tfrac{1}{2}z^2 + iz| \leq |z^3| + \tfrac{1}{2}|z|^2 + |i||z| = |z|^3 + \tfrac{1}{2}|z|^2 + |z| \leq \tfrac{5}{2}.$$

En palabras, si $|z| \leq 1$, entonces $P(z)$ está dentro de un disco $\mathcal{D}_{5/2}$ de radio $\frac{5}{2}$ y centrado en $3e^{i\pi/4}$ (ver Figura 27). En particular, la curva $\mathcal{P}_1$ está completamente contenida en $\mathcal{D}_{5/2}$.

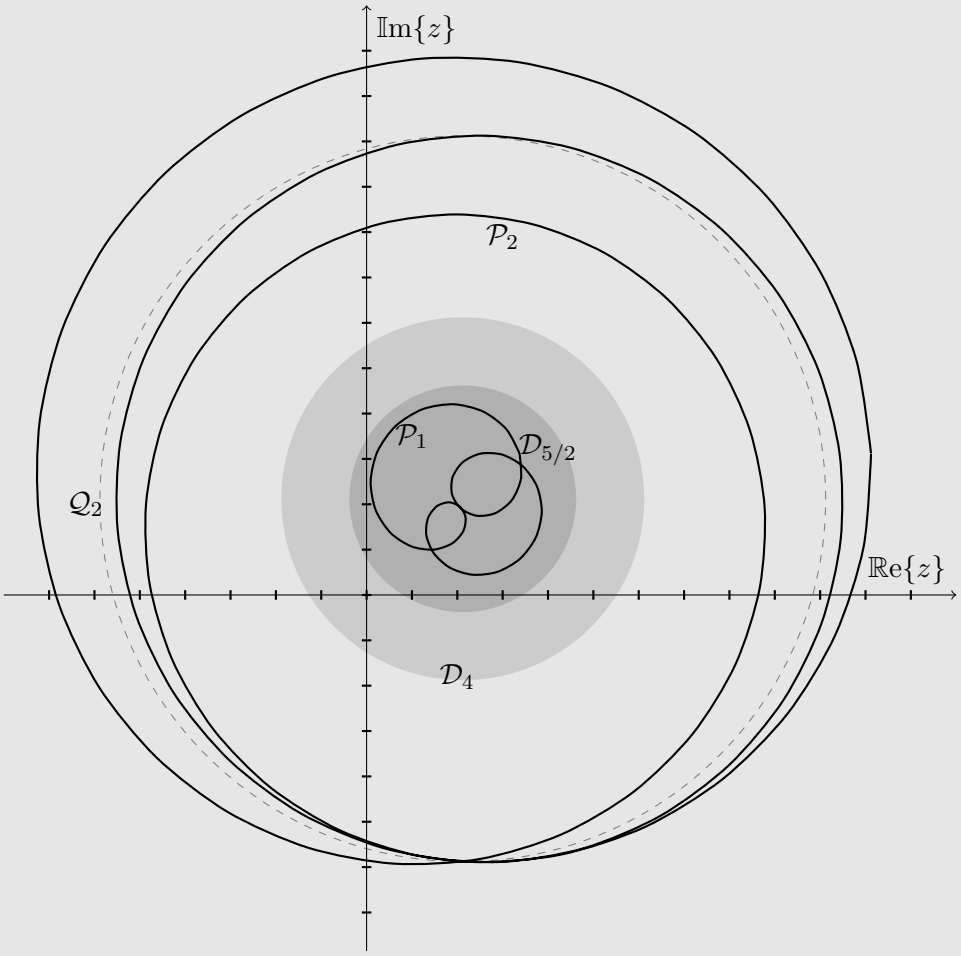


Figura 27: Ilustración de las curvas $\mathcal{P}_1$ y $\mathcal{P}_2$ (líneas continuas) asociadas a $P(z) = z^3 + \frac{1}{2}z^2 + iz + 3e^{i\pi/4}$, de la curva $\mathcal{Q}_2$ (línea segmentada) asociada a $Q(z) = z^3 + 3e^{i\pi/4}$ y de los discos $\mathcal{D}_{5/2}$ (gris oscuro) y $\mathcal{D}_2$ (gris claro).

Por otro lado, observemos que si z es tal que $|z|$ es "muy grande", ahora uno espera que los términos $\frac{1}{2}z^2$, iz y $3e^{i\pi/4}$ sean en módulo "muy pequeños" en comparación con z^3 y por lo tanto también en comparación con $z^3 + 3e^{i\pi/4}$. De hecho, si $|z| = 2$,

$$\left|P(z) - z^3 - 3e^{i\pi/4}\right| = \left|\tfrac{1}{2}z^2 + iz\right| \leq \tfrac{1}{2}|z^2| + |i||z| = 4. \tag{3}$$

Denotemos el polinomio $z^3 + 3e^{i\pi/4}$ por $Q(z)$. Definimos, asociado a Q la función $\mathcal{Q}_\rho : [0, 2\pi] \to \mathbb{C}$ y la curva $\mathcal{Q}_\rho \subseteq \mathbb{C}$ análogas a como lo hicimos para P. De (3), sigue que si $\theta \in [0, 2\pi]$,

$$\big|\mathcal{Q}_2(\theta) - \mathcal{P}_2(\theta)\big| \leq 4.$$

Más aún, notar que $\mathcal{Q}_2(\theta) = 8e^{i3\theta} + 3e^{i\pi/4}$ por lo que $\mathcal{Q}_2$ geométricamente corresponde a una circunferencia de radio 8 centrada en $3e^{i\pi/4}$ (ver Figura 27). Luego, (3) nos dice que todo punto en la curva $\mathcal{P}_2$ esta a distancia a lo más 4 de algún punto de la circunferencia $\mathcal{Q}_2$. Esto implica que todo punto de $\mathcal{P}_2$ se encuentra fuera del disco $\mathcal{D}_4$ de radio 4 y centrado en $3e^{i\pi/4}$ (ver nuevamente Figura 27).
Un punto importante a destacar es que si bien observamos que $\mathcal{Q}_2$ es una circunferencia, el estudio de la función $\mathcal{Q}_2(\theta) = 8e^{i3\theta} + 3e^{i\pi/4}$ nos permite inferir que a cuando θ va de 0 a 2π la expresión $\mathcal{Q}_2(\theta) = 8e^{i3\theta} + 3e^{i\pi/4}$ da 3 vueltas en torno a $3e^{i\pi/4}$ y a una distancia 8 de dicho punto. Como $3e^{i\pi/4}$ esta a distancia 3 del origen O del plano complejo, necesariamente debe tenerse que cada una de las 3 vueltas es también en torno al origen (ver Figura 27).
En resumen, el origen O queda en el exterior de la curva $\mathcal{P}_1$ pero al interior de la curva $\mathcal{P}_2$. Es razonable suponer que si uno hace variar ρ de 1 a 2 la curva $\mathcal{P}_\rho$ se deforma de manera "continua y suave" de $\mathcal{P}_1$ a $\mathcal{P}_2$. En particular, la deformación es tal que una curva no puede "saltar" sobre el origen O, sino que alguna debe pasar "sobre" el origen O. Es decir, debe existir un $\rho_* \in [1, 2]$ tal que el origen O pertenece a $\mathcal{P}_{\rho_*}$. Esto es equivalente a decir que para algún $\rho_* \in [1, 2]$ y $\theta_* \in [0, 2\pi]$ se tiene que $P(\rho_* e^{i\theta_*}) = 0$. Es decir, ¡el polinomio P tiene como raíz a $z = \rho_* e^{i\theta_*}$!

Caso general

Para el caso general de un polinomio $P \in \mathbb{C}[z]$ de grado $n > 0$, uno siempre puede suponer que P es mónico, pues de lo contrario basta dividir por p_n y obtener un polinomio mónico con el mismo conjunto de raíces que el original. Si el término constante $p_0 = 0$, entonces no hay nada que hacer, puesto que $P(0) = p_0 = 0$ y 0 es raíz de P. En lo que sigue asumimos que $p_0 \neq 0$.
La única dificultad para generalizar el argumento de la parte anterior es como escoger adecuadamente el intervalo de valores en que variar el parámetro ρ de la sección previa. Es claro que dicho intervalo esta de alguna manera relacionado al módulo de los coeficientes de P. Veamos como.
Primero observamos que por desigualdad triangular y por la fórmula de la suma de una progresión geométrica, si $|z| \leq 1/2$,

$$\begin{aligned}\big|P(z) - p_0\big| = \big|\sum_{k=1}^{n} p_k z^k\big| &\leq \sum_{k=1}^{n} \big|p_k z^k\big| \leq \big(\max_{k\in[1..n]} |p_k|\big) \sum_{k=1}^{n} |z|^k \\ &\leq \big(\max_{k\in[1..n]} |p_k|\big)|z|\frac{1-|z|^n}{1-|z|} \leq 2|z| \max_{k\in[1..n]} |p_k|.\end{aligned}$$

Luego, si $\rho \leq \rho_0 = |p_0|/\big(4\,\text{máx}_{k\in[1..n]}\,|p_k|\big)$, entonces para todo $\theta \in [0, 2pi]$,

$$\big|\mathcal{P}_{\rho_0}(\theta) - p_0\big| \leq \tfrac{1}{2}|p_0|,$$

o sea, la curva $\mathcal{P}_{\rho_0}$ esta completamente contenida en el disco $\mathcal{D}_{\rho_0}$ centrado en p_0 y de radio $|p_0|/2$. Como el origen no pertenece a $\mathcal{D}_{\rho_0}$, sigue que el origen O del plano complejo esta en el exterior de la curva $\mathcal{P}_{\rho_0}$.
Por otro lado, si definimos $Q(z) = z^n + p_0$, recordando que P es mónico con coeficiente constante p_0, por desigualdad triangular y la fórmula para la suma de una progresión geométrica, sigue que cuando $|z| > 1$,

$$\begin{aligned}\big|P(z) - Q(z)\big| \leq \sum_{k=1}^{n-1}\big|p_k z^k\big| = |z|^n \sum_{k=1}^{n-1}|p_k||z|^{-(n-k)} \leq |z|^n\big(\max_{k\in[1..n-1]}|p_k|\big)\sum_{j=1}^{n-1}\frac{1}{|z|^j}\\ = |z|^n\big(\max_{k\in[1..n-1]}|p_k|\big)\frac{1}{|z|}\cdot\frac{1-|z|^{-(n-1)}}{1-|z|^{-1}} \leq |z|^n\big(\max_{k\in[1..n-1]}|p_k|\big)\frac{1}{|z|-1}.\end{aligned}$$

Luego, si $\rho \geq \rho_1 = 1 + (3/|p_0|)\,\text{máx}_{k\in[1..n]}\,|p_k|$, entonces para todo $\theta \in [0, 2\pi]$,

$$\big|\mathcal{P}_{\rho_1}(\theta) - \mathcal{Q}_{\rho_1}(\theta)\big| \leq \rho_1^n\tfrac{1}{3}|p_0|,$$

Observando que $\mathcal{Q}_{\rho_1}$ es un circunferencia de radio ρ_1^n centrada en p_0, y argumentando como el el caso particular visto en la sección anterior, se concluye que al variar θ entre 0 y 2π el punto $\mathcal{Q}_{\rho_1}(\theta)$ gira n veces en torno a p_0 "arrastrando" consigo a $\mathcal{P}_{\rho_1}(\theta)$ y encerrando el origen O del plano complejo en el interior de la curva $\mathcal{P}_{\rho_1}$.
Para concluir, se argumenta como antes, es decir, hacemos variar ρ entre ρ_1 y ρ_2 y bajo los supuestos de "continuidad y suavidad" concluimos que debe existir $\rho_* \in [\rho_1, \rho_2]$ tal que $O \in \mathcal{P}_{\rho_*}$. Luego, existen $\rho_* > 0$ y $\theta_* \in [0, 2\pi]$ tales que $z_* = \rho_* e^{i\theta_*}$ es raíz de P.

Guía Básica

Observación: En esta guía, $\mathbb{K}$ representa al cuerpo $\mathbb{R}$ ó $\mathbb{C}$.

Determinar la veracidad de las siguientes afirmaciones:

1. Si $P, D \in \mathbb{K}[x]$ y $D \neq 0$, entonces existen $Q, R \in \mathbb{K}[x]$ tales que $P = Q \cdot D + R$.
2. Si $P, D \in \mathbb{K}[x]$ y $D \neq 0$, entonces existe $Q \in \mathbb{K}[x]$ tales que $P = Q \cdot D$.
3. Si $P, D \in \mathbb{K}[x]$ y $D \neq 0$, entonces existen $Q, R \in \mathbb{K}[x]$ tales que $P = Q \cdot D + R$, con $\text{gr}(D) > \text{gr}(R)$.
4. Para cualquier $P \in \mathbb{K}[x]$ y $c \in \mathbb{K}$, el resto de dividir P por $(x - c)$ es siempre cero.
5. Para cualquier $P \in \mathbb{K}[x]$ y $c \in \mathbb{K}$, el resto de dividir P por $(x - c)$ es $P(c) - c$.
6. Para cualquier $P \in \mathbb{K}[x]$ y $c \in \mathbb{K}$, el resto de dividir P por $(x - c)$ es $P(c)$.
7. $c \in \mathbb{K}$ es raíz de $P \in \mathbb{K}[x]$ si y sólo si $P(c) = c$.
8. $c \in \mathbb{K}$ es raíz de $P \in \mathbb{K}[x]$ si y sólo si $P(c) = 0$.
9. $c \in \mathbb{K}$ es raíz de $P \in \mathbb{K}[x]$ si y sólo si el resto de dividir P por $(x + c)$ es cero.
10. $c \in \mathbb{K}$ es raíz de $P \in \mathbb{K}[x]$ si y sólo si el resto de dividir P por $(x - c)$ es cero.
11. Si $c_1, c_2, \ldots, c_k$ son raíces distintas del polinomio P, entonces $(x - c_1)(x - c_2) \ldots (x - c_k) \mid P(x)$.
12. Si $c_1, c_2, \ldots, c_k$ son raíces distintas del polinomio P, entonces $(x + c_1)(x + c_2) \ldots (x + c_k) \mid P(x)$.
13. Si $c_1, c_2, \ldots, c_k$ son raíces distintas del polinomio P, entonces $(x - c_1)(x - c_2) \ldots (x - c_k) - P(x)$ es siempre el polinomio nulo.
14. Un polinomio $P \in \mathbb{K}[X]$ de grado $n \geq 1$, posee a lo más n raíces distintas.
15. Un polinomio $P \in \mathbb{K}[X]$ de grado $n \geq 1$, posee al menos $n + 1$ raíces distintas.
16. Existen polinomios no nulos de grado $n \geq 1$, con $n + 1$ raíces distintas.
17. Si dos polinomios de grado $n \geq 1$ tienen el mismo valor en $n + 1$ puntos, entonces son iguales.
18. Si dos polinomios de grado $n \geq 1$ tienen el mismo valor en n puntos, entonces son iguales.
19. Si un polinomio que tiene grado a lo más $n \geq 1$, toma el mismo valor en n puntos, entonces es un polinomio constante.
20. Si un polinomio que tiene grado a lo más $n \geq 1$, toma el mismo valor en $n + 1$ puntos, entonces es un polinomio constante.
21. El Teorema Fundamental del Álgebra señala que todo polinomio en $\mathbb{C}[X]$, de grado $n \geq 1$, tiene al menos una raíz en $\mathbb{R}$.
22. El Teorema Fundamental del Álgebra señala que todo polinomio en $\mathbb{C}[X]$, de grado $n \geq 1$, tiene al menos una raíz en $\mathbb{C}$.
23. El Teorema Fundamental del Álgebra señala que todo polinomio en $\mathbb{R}[X]$, de grado $n \geq 1$, tiene al menos una raíz en $\mathbb{R}$.

24. Sea $P \in \mathbb{C}[X]$ con grado $n \geq 1$, entonces existen $c_1, \ldots, c_m \in \mathbb{C}$ y $l_1, \ldots, l_m \geq 1$, tales que $P(x) = (x - c_1)^{l_1}(x - c_2)^{l_2} \ldots (x - c_m)^{l_m}$.
25. Sea $P \in \mathbb{C}[X]$ con grado $n \geq 1$, entonces existen $\alpha, c_1, \ldots, c_m \in \mathbb{C}$ y $l_1, \ldots, l_m \geq 1$, tales que $P(x) = \alpha(x - c_1)^{l_1}(x - c_2)^{l_2} \ldots (x - c_m)^{l_m}$.
26. Sea $P \in \mathbb{C}[X]$ con grado $n \geq 1$, entonces existen $\alpha, c_1, \ldots, c_m \in \mathbb{C}$ y $l_1, \ldots, l_m \geq 1$, tales que $P(x) = \alpha(x + c_1)^{l_1}(x + c_2)^{l_2} \ldots (x + c_m)^{l_m}$.
27. Sea $P \in \mathbb{C}[X]$ con grado $n \geq 1$, entonces existen $\alpha, c_1, \ldots, c_m \in \mathbb{R}$ y $l_1, \ldots, l_m \geq 1$, tales que $P(x) = \alpha(x - c_1)^{l_1}(x - c_2)^{l_2} \ldots (x - c_m)^{l_m}$.
28. Dado $P \in \mathbb{C}[X]$, si $z \in \mathbb{C}$ es raíz de P, entonces $\overline{z}$ también lo es.
29. Dado $P \in \mathbb{R}[X]$, si $z \in \mathbb{C}$ es raíz de P, entonces $\overline{z}$ también lo es.
30. Dado $P \in \mathbb{R}[X]$, si $z \in \mathbb{C}$ es raíz de P, entonces $-z$ también lo es.
31. Dado $P \in \mathbb{C}[X]$, si $z \in \mathbb{C}$ es raíz de P, entonces $-z$ también lo es.
32. Existe $P \in \mathbb{R}[X]$ de grado 3, con 3 raíces en $\mathbb{C} \setminus \mathbb{R}$.
33. No existe $P \in \mathbb{C}[X]$ de grado 3, con 3 raíces en $\mathbb{C} \setminus \mathbb{R}$.
34. Existe $P \in \mathbb{R}[X]$ de grado 4, con 4 raíces en $\mathbb{C} \setminus \mathbb{R}$.
35. Existe $P \in \mathbb{R}[X]$ de grado $n \geq 1$, con exactamente una raíz en $\mathbb{C} \setminus \mathbb{R}$.
36. Todo $P \in \mathbb{R}[X]$ de grado $n \geq 1$, tiene un número par de raíces en $\mathbb{C} \setminus \mathbb{R}$.
37. Todo $P \in \mathbb{R}[X]$ de grado $n \geq 1$, tiene un número impar de raíces en $\mathbb{C} \setminus \mathbb{R}$.
38. Todo $P \in \mathbb{R}[X]$ tiene al menos una raíz real.
39. Todo $P \in \mathbb{C}[X]$ tiene al menos una raíz compleja.
40. Si $p_0, \ldots, p_n \in \mathbb{Z}$ son los coeficientes de $P \in \mathbb{R}[X]$, entonces el numerador en la escritura $\frac{r}{s}$ de toda raíz $\mathbb{Q}$ de P, divide a p_0.
41. Si $p_0, \ldots, p_n \in \mathbb{Z}$ son los coeficientes de $P \in \mathbb{R}[X]$, entonces el denominador en la escritura $\frac{r}{s}$ de toda raíz $\mathbb{Q}$ de P, divide a p_0.
42. Si $p_0, \ldots, p_n \in \mathbb{Z}$ son los coeficientes de $P \in \mathbb{R}[X]$, entonces el denominador en la escritura $\frac{r}{s}$ de toda raíz $\mathbb{Q}$ de P, divide a p_n.
43. Existe un polinomio mónico con coeficientes enteros que tiene a $\frac{1}{3}$ como raíz.
44. Las únicas raíces racionales posibles de un polinomio mónico con coeficientes enteros son números enteros.
45. El polinomio $P(x) = 17x^{19} + 5x^{11} - 3x^5 + x - 1$ tiene como raíz a $1/2$.
46. El polinomio $P(x) = x^{16} + 5x^8 - 3x^2 + x - 3$ tiene como raíz a 2.

Guía de Ejercicios

1. Dado el polinomio $P(x) = x^5 - 2x^2 + 1$, divídalo por los siguientes polinomios D, para obtener $P = Q \cdot D + R$. En cada caso, explicite los polinomios Q y R.

   a) $D(x) = x^5$.

b) $D(x) = x^2 - 2$.
c) $D(x) = x^3$.
d) $D(x) = x^2 - 3x + 1$.
e) $D(x) = x - 1$.

2. Considere $P(x) = \sum_{k=0}^{n} p_k x^k \in \mathbb{R}[x]$, pruebe que si $\sum_{k=0}^{n} p_k = 0$ entonces $x = 1$ es raíz de P.
3. Encuentre las raíces de $P(x) = x^4 - x^3 + 2x^2 - 2x$.
Indicación: Trate de encontrar una raíz por tanteo y luego use división.
4. Considere el polinomio $P(x) = x^5 - 3x^3 + x^2 + 2x - 4$.

a) Encuentre un conjunto $A \subseteq \mathbb{Z}$, tal que toda raíz $x \in \mathbb{Q}$ de P pertenezca a A.
Indicación: Use los resultados para polinomios con coeficientes enteros.
b) Encontrar todas las raíces de P en $\mathbb{Q}$.
Indicación: Le basta buscar en el conjunto A, encontrado en la parte (a).

5. Para cada polinomio P, determine el cuociente y resto de dividir P por $(x - 2)$. ¿Es $x = 2$ raíz de estos polinomios?

a) $P(x) = 2x^3 - x^2 - x + 1$.
b) $P(x) = 5x^4 + x^3 - 3x^2 - x + 1$.
c) $P(x) = x^5 - 4x^3 + x^2 - 3x + 2$.
d) $P(x) = 3x^3 - 5x^2 - x - 2$.

Guía de Problemas

1. (30 min.) Sea $P(z) = z^3 + az^2 + bz + c$ un polinomio con raíces α, β, $\gamma \in \mathbb{C}$. Pruebe que:
$$\alpha\beta\gamma = -c, \quad \alpha\beta + \alpha\gamma + \beta\gamma = b, \quad \alpha + \beta + \gamma = -a$$
y use esto para encontrar las raíces del polinomio $Q(z) = z^3 - 11z^2 + 44z - 112$ sabiendo que tiene una raíz compleja (i.e en $\mathbb{C} \setminus \mathbb{R}$) de módulo 4.
2. (30 min.) Sabiendo que la ecuación $z^3 - 9z^2 + 33z = 65$ admite una solución $\mathbb{C} \setminus \mathbb{R}$ de módulo $\sqrt{13}$, determinar todas las soluciones (en $\mathbb{C}$) de la ecuación.
3. (30 min.) Si $n = 3k \pm 1$ para algún $k \in \mathbb{N}$, probar, sin usar inducción, que $x^{2n} + 1 + (x + 1)^{2n}$ es divisible por $x^2 + x + 1$.
4. (30 min.) Sea $P(x) = p_0 + p_1 x + \ldots + p_{n-1}x^{n-1} + x^n$, con $p_0, \ldots, p_{n-1} \in \mathbb{C}$, tal que $P(x)$ tiene n raíces distintas en $\mathbb{C}$ y si $z \in \mathbb{C}$ es raíz de $P(x)$, entonces su conjugado $\overline{z}$ también lo es. Demuestre que $p_0, \ldots, p_{n-1} \in \mathbb{R}$.
Indicación: Estudie el producto de polinomios $(x - z)(x + \overline{z})$ donde $z \in \mathbb{C}$.
5. (30 min.) Sean $P(x) \in \mathbb{C}[X]$, $\text{gr}(P(x)) \geq 4$, $a, b, c \in \mathbb{R}$, con $b \neq 0$. Se sabe que:

- El resto de dividir $P(x)$ por $(x^2 - b^2)$ es cx.

- El resto $R(x)$, de dividir $P(x)$ por $(x^2 - b^2)(x - a)$ es un polinomio mónico, es decir, el coeficiente asociado a x^n, donde $n = \text{gr}(R(x))$, es igual a 1.

a) Determine los valores $P(b)$ y $P(-b)$.
b) Justifique que $\text{gr}(R(x)) \leq 2$.
c) Determine $R(x)$.

6. (15 min.) Sean $F, G, H, R, R' \in \mathbb{K}[x]$ polinomios tales que $G, H \neq 0$. Si el resto de dividir F por $G \cdot H$ es R y el resto de dividir R por G es R', determine el resto de dividir F por G.
7. (30 min.) Sea $P(x) = x^3 + ax^2 + bx + c$ un polinomio con coeficientes en $\mathbb{R}$. Sea $R(x)$ el resto de la división de $P(x)$ por $(x-1)$. Si $R(4) = 0$ y $x = i$ es raíz de $P(x)$, calcule a, b y c.
8. El objetivo de este problema es probar el **Teorema de Interpolación**. Sea $\mathbb{K}$ cuerpo, $n \in \mathbb{N} \setminus \{0\}$, $x_1, \ldots, x_n, y_1, \ldots, y_n \in \mathbb{K}$, con $x_j \neq x_k$ si $j \neq k$. Entonces existe un único polinomio P de grado menor o igual a $(n-1)$ en $\mathbb{K}[x]$ tal que $\forall j \in [1..n]$, $P(x_j) = y_j$. Llamemos a este polinomio, polinomio de interpolación de la familia $(\{x_j\}_{j=1}^n, \{y_j\}_{j=1}^n)$.

a) (20 min.) Suponiendo la existencia de $P(x)$, demuestre la unicidad.
b) (40 min.) Para cada $j \in [1..n]$ definimos:

$$l_j(x) = \frac{\Pi_{k \in [1..n]: k \neq j}(x - x_k)}{\Pi_{k \in [1..n]: k \neq j}^n (x_j - x_k)} \in \mathbb{K}[x].$$

1) Determine el grado de $l_j(x)$ y pruebe que para todo j y $r \in [1..n]$,

$$l_j(x_r) = \delta_{j,r} = \begin{cases} 1, & \text{si } j = r, \\ 0, & \text{si } j \neq r. \end{cases}$$

2) Demuestre que $P(x) = \sum_{j=1}^n y_j l_j(x) \in \mathbb{K}[x]$ es el polinomio de interpolación para la familia $(\{x_j\}_{j=1}^n, \{y_j\}_{j=1}^n)$.

9. Sea $J_2 = \{P(x) \in \mathbb{R}[X] \mid \text{gr}(p) \leq 2, p_0 = 0, p_1 \neq 0\}$. En J_2 se define la l.c.i. $\triangle$ a través de $P(x) \triangle Q(x) = c_1 x + c_2 x^2$ en que $\sum_{i=0}^n c_i x^i = P(Q(x))$.

a) (20 min.) Probar que $(J_2, \triangle)$ es grupo no abeliano.
b) (20 min.) Sea $f : J_2 \to \mathbb{R} \setminus \{0\}$ tal que $f(p_1 x + p_2 x^2) = p_1$. Probar que f es un epimorfismo de $(J_2, \triangle)$ en $(\mathbb{R} \setminus \{0\}, \cdot)$.
c) (20 min.) Sea $H = \{P(x) \in J_2 \mid p_2 = 1\}$. Probar que $(H, \triangle)$ es subgrupo abeliano de $(J_2, \triangle)$.